Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Χρήση του εργαλείου sysmon για τον εντοπισμό επιθέσεων εσωτερικής μετακίνησης ενός επιτιθέμενου.** **Windows Sysmon tool for lateral movement alerts.**
Ονοματεπώνυμο Φοιτητή	**Παπαδόπουλος Νικόλαος**
Πατρώνυμο	**Βασίλειος**
Αριθμός Μητρώου	**ΜΠΣΠ 16022**
Επιβλέποντες	**Κωνσταντίνος Πατσάκης Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Σεπτέμβριος 2019**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
ΚΑΘΗΓΗΤΗΣ Κ. ΠΑΤΣΑΚΗΣ	ΚΑΘΗΓΗΤΗΣ Π. ΚΟΤΖΑΝΙΚΟΛΑΟΥ	ΚΑΘΗΓΗΤΗΣ Α. ΑΛΕΠΗΣ
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα

Περίληψη

Σε αυτή την διπλωματική εργασία παρουσιάζεται ένας τρόπος εγκατάστασης, παραμετροποίησης και λειτουργίας του Sysmon, το οποίο είναι ένα σύστημα παρακολούθησης συστήματος των windows. Το Sysmon παρέχει λεπτομερείς πληροφορίες σχετικά με τις δημιουργίες διαδικασιών, τις συνδέσεις δικτύου και τις αλλαγές στο χρόνο δημιουργίας των αρχείων. Συλλέγοντας τα συμβάντα που παράγει χρησιμοποιώντας τη συλλογή συμβάντων των Windows ή τους πράκτορες της SIEM και στη συνέχεια την ανάλυση τους, είναι ικανό να εντοπίσει κακόβουλη ή ανώμαλη δραστηριότητα και να καταλάβει πώς λειτουργούν οι εισβολείς και το κακόβουλο λογισμικό στο δίκτυό του συστήματος. Με τη βοήθεια του sysmon θα παρουσιαστούν διάφορα καταγεγραμμένα συμβάντα που εντοπίστηκαν κατά τη διαδικασία εσωτερικής μετακίνησης (Lateral movement) ανάμεσα σε 2 windows 10 συστήματα από τα οποία το ένα έχει το ρόλο του επιτιθέμενου και το άλλο το ρόλο του θύματος. Για να επιτευχθεί το παραπάνω θα παρουσιαστούν τεχνικές προτεινόμενης παραμετροποίησης του sysmon ώστε να κάνει σωστή καταγραφή, τεχνικές προτεινόμενης παραμετροποίησης των αρχείων καταγραφής των windows καθώς κα τα διάφορα εργαλεία που θα χρησιμοποιήσουμε ώστε να επιτύχουμε, να καταγράψουμε και να εντοπίσουμε την εσωτερική μετακίνηση μέσα σε ένα σύστημα.

ABSTRACT

This thesis presents a way of installing, configuring and operating Sysmon, which is a windows system monitoring system. Sysmon provides detailed information on process creations, network connections, and changes in file generation time. By collecting the events it produces using Windows Event Collection or the SIEM agents and then analyzing them, it is able to detect malicious or abnormal activity and understand how intruders and malware work on the system network. With the help of sysmon, there will be several recorded events identified during the lateral movement between 2 windows 10 systems, one of which has the role of the attacker and the other the role of the victim. To achieve the above, sysmon preferred configuration techniques will be introduced to perform proper logging, preferred event log configuration for windows as well as various tools that we will use to successfully achieve, log and detect lateral movement to the victim's system.

ΠΕΡΙΕΧΟΜΕΝΑ

Περιεχόμενο Πινάκων

Κεφάλαιο 1 Εισαγωγή

1.1 Κίνητρο - Περιγραφή

Πριν από λίγα χρόνια, μια περίπλοκη παραβίαση δεδομένων ήταν σπάνια, όχι μόνο εξαιτίας της ζημιάς που σημείωνε, αλλά και λόγω του πόσο δύσκολη ήταν να συμβεί μια τέτοια τεχνικά ειδικευμένη παραβίαση. Όχι όμως πια. Οι προηγμένες απειλές στον κυβερνοχώρο έχουν μεγαλώσει.

Το modus operandi, ή η «αλυσίδα θανάτωσης» του σύγχρονου επιτιθέμενου έχει ωριμάσει. Μια γρήγορη είσοδος μέσω ηλεκτρονικού "ψαρέματος" (phishing) σε συνδυασμό με τις αδυναμίες εφαρμογών ιστού ή εσφαλμένων ρυθμίσεων, ακολουθούμενη από συστηματικό έλεγχο πολλαπλών προσωπικών στοιχείων επιτυγχάνει τον στόχο της αποστολής.

Η ικανότητα ενός εξειδικευμένου επιτιθέμενου να παρακάμψει τους παραδοσιακούς μηχανισμούς προστασίας σημαίνει ότι η ασφάλεια στον κυβερνοχώρο έχει τώρα περισσότερο την ικανότητα να ανιχνεύει και να αντιδρά γρήγορα, παρά να προσπαθήσει να κλείσει κάθε πιθανή οπή.

Σε αντίθεση με όσα πιστεύουν οι περισσότεροι, η πιο κρίσιμη φάση μιας επίθεσης δεν είναι η αρχική εκμετάλλευση ή η τελική διήθηση δεδομένων. Είναι η μεσαία φάση, όπου ο επιτιθέμενος αναζητεί περιουσιακά στοιχεία, αποκτά πρόσθετα προνόμια και κινείται σιωπηλά από σύστημα σε σύστημα, από υποδίκτυο σε υποδίκτυο και τέλος στον τελικό του στόχο. Αυτή η φάση ονομάζεται εσωτερική μετακίνηση και είναι ο τόπος όπου ο επιτιθέμενος ξοδεύει τον περισσότερο χρόνο αλλά ταυτόχρονα είναι και η πιο ευάλωτη φάση ώστε να εντοπιστεί.

Η συμβατική σοφία δηλώνει ότι «η πρόληψη είναι καλύτερη από τη θεραπεία». Δυστυχώς, η επιφάνεια επίθεσης των σύγχρονων τερματικών είναι τόσο μεγάλη, όπου η προστασία είναι παρόμοια με την κατασκευή ενός φράχτη γύρω από ένα εθνικό σύνορο. Δηλαδή δεν πρόκειται ο επιτιθέμενος να μείνει απέξω. Η έρευνά μας δείχνει ότι το 80% μιας επίθεσης δαπανάται κατά τη διάρκεια της εσωτερικής μετακίνησης. Η πραγματική παραβίαση συμβαίνει αρκετά γρήγορα και ο τελικός στόχος επιτυγχάνεται γρήγορα. Η μετακίνηση από την αρχική παραβίαση στον τελικό στόχο κοστίζει στον επιτιθέμενο τόσο χρόνο όσο και πόρους. Ακόμα και ο πιο έμπειρος επιτιθέμενος λειτουργεί «τυφλά» τουλάχιστον μία φορά στο δίκτυο του θύματος. Μπορεί να ξέρει πού είναι τα προσωπικά στοιχεία, αλλά πρέπει να μετακινηθεί αργά και μυστικά για να φτάσει εκεί. Εάν ο επιτιθέμενος ανιχνευτεί κατά τη διάρκεια της παραπάνω διαδικασίας τότε αυτό σημαίνει ότι το θύμα έχει νικήσει.

Δυστυχώς, η παρακολούθηση των εσωτερικών δικτύων είναι δύσκολη. Έχει δοκιμαστεί η ανάλυση των αρχείων καταγραφής, η ανίχνευση και η μηχανική μάθηση της SIEM, όμως, ο όγκος των δεδομένων είναι σε petabytes, και ακόμη και οι καλύτερες λύσεις αναλυτικής ανάλυσης δημιουργούν έναν τεράστιο αριθμό ψευδών ειδοποιήσεων. Το πρόβλημα είναι τόσο μεγάλο ώστε, λιγότερο από το 4% των ειδοποιήσεων είναι αυτές που διερευνώνται! Αυτό οφείλεται στο γεγονός ότι ο όγκος και η σημασία των ειδοποιήσεων οδηγούν τις ομάδες ασφάλειας να απενεργοποιήσουν ή να αγνοήσουν αυτές τις λύσεις παρακολούθησης.

Η ανίχνευση της εσωτερικής μετακίνησης είναι εφικτή. Οι επιτιθέμενοι πρέπει να ανακαλύψουν στοιχεία μέσω της σάρωσης, της υπηρεσίας καταλόγου Active Directory ή των αποτυπωμάτων. Η χρήση νόμιμων διαχειριστικών εργαλείων ή εργαλεία κλοπής πιστοποιήσεων καθιστά την παραδοσιακή ανίχνευση πολύ δύσκολη, καθώς η παρακολούθηση αυτών θα δημιουργήσει χιλιάδες ψευδείς θετικές ενδείξεις. Οι συνήθης τεχνικές συνεχίζουν να εξελίσσονται (για παράδειγμα, να περάσουν το hash σε κλοπές συνθηματικών, υποκλοπή στην πλαστογράφηση ARP κ.α.), αλλά η βασική στρατηγική είναι η ίδια. Εύρεση περιουσιακών στοιχείων μεγαλύτερης αξίας από το τρέχον περιουσιακό στοιχείο και χειραγώγηση αυτών. Άρα η ιδανική λύση πρέπει να είναι:

- Αναγνώριση των τακτικών του επιτιθέμενου
- Αποτροπή δημιουργίας ψευδών ειδοποιήσεων
- Ικανός μηχανισμός ώστε να ανιχνεύει την εσωτερική κίνηση μεταξύ των προσωπικών δεδομένων.

1.2 Ανάλυση της χρήσης προστασίας κατά της εσωτερικής μετακίνησης

Οι έλεγχοι ασφαλείας που συμβουλεύονται στην καθοδήγηση έτοιμων τεχνικών για τον μετριασμό των κακόβουλων προγραμμάτων μπορούν να μειώσουν τον κίνδυνο επιτυχίας μιας αρχικής επίθεσης. Ωστόσο, πρέπει να υπολογιστεί ότι μία επίθεση με επαρκή χρόνο και πηγές θα είναι τελικά επιτυχής. Είναι επομένως σημαντικό: να εντοπίζονται παραβιάσεις όσο το δυνατόν συντομότερα, να εφαρμόζονται εσωτερικοί έλεγχοι ασφαλείας για τη μείωση των ζημιών που προκαλούνται από έναν επιτιθέμενο μετά την παραβίαση. Δίκτυα με ισχυρή προστασία των συνόρων, αλλά καμία εσωτερική ασφάλεια δίνει στους επιτιθέμενους τη δυνατότητα να διασχίσουν το δίκτυο μόλις αποκτήσουν πρόσβαση. Οι πιθανότητες επίτευξης των στόχων τους θα αυξηθούν τόσο πολύ ώστε να είναι σε θέση να διατηρήσουν μια μόνιμη θέση στο δίκτυο. Εφαρμόζοντας τις ακόλουθες τεχνικές, θα κερδίσετε χρόνο και θα διευκολύνετε την ανίχνευση απόπειρας εσωτερικής μετακίνησης.

- Προστασία κωδικών εισόδου.

Όλα τα διαπιστευτήρια σε ένα δίκτυο, ειδικά εκείνα των λογαριασμών διαχειριστή, θα πρέπει να προστατεύονται επαρκώς ώστε να αποτρέπουν τους επιτιθέμενους που τα χρησιμοποιούν στο να αποκτήσουν πρόσβαση σε συσκευές και συστήματα. Ένας κοινός τύπος επίθεσης συνεπάγεται με την κλοπή ενός διακριτικού ασφαλείας για την απόκτηση πρόσβασης σε άλλη συσκευή ή διακομιστή. Το "Pass the hash" είναι ένα παράδειγμα αυτού, όπου χρησιμοποιείται ένας κλεμμένος hash κωδικός για την πιστοποίηση του επιτιθέμενου. Οι κωδικοί πρόσβασης δεν πρέπει να αποθηκεύονται σε απλό κείμενο από τους χρήστες ή τα συστήματα και οι κωδικοί πρόσβασης hash πρέπει να προστατεύονται ώστε να εμποδίζουν τους επιτιθέμενους να έχουν εύκολη πρόσβαση σε αυτούς. Τα διαπιστευτήρια που χρησιμοποιούνται για την επαλήθευση ταυτότητας σε μια συσκευή (καθώς και τα διαπιστευτήρια που χρησιμοποιούνται για τον έλεγχο ταυτότητας σε υπηρεσίες) θα πρέπει να προστατεύονται από τη συσκευή. Οι συσκευές που υποστηρίζουν αποθήκευση διαπιστευτηρίων από υλικό θα προστατεύσουν καλύτερα αυτά τα διαπιστευτήρια. Τα διαπιστευτήρια δεν πρέπει να εισάγονται σε οποιαδήποτε άλλη συσκευή εκτός από εκείνες που έχουν εγκριθεί για προσωπική χρήση, καθώς αυτές οι συσκευές ενδέχεται να μην προστατεύουν επαρκώς τα διαπιστευτήρια.

Συνοψίζοντας:

Δεν πρέπει να γίνεται αποθήκευση κωδικών πρόσβασης σε απλό κείμενο και διασφάλιση ότι τα hashes των κωδικών πρόσβασης αποθηκεύονται σε προστατευμένες περιοχές.

Χρήση συσκευών με αποθηκευμένο χώρο αποθήκευσης διαπιστευτηρίων υλικού, όπου είναι δυνατόν. Χρησιμοποιήστε τα διαπιστευτήρια εργασίας μόνο σε συσκευές και υπηρεσίες που έχουν εγκριθεί για χρήση από την εργασία.

- Ανάπτυξη καλών πρακτικών επαλήθευσης ταυτότητας

Ο έλεγχος ταυτότητας πρέπει να είναι εύκολος για τον χρήστη, αλλά ταυτόχρονα αν δυσκολεύει τον επιτιθέμενο να αποκτήσει πρόσβαση. Για παράδειγμα, δεν πρέπει να γίνεται χρήση των κωδικών πρόσβασης σε διαφορετικά συστήματα και εξέταση της χρήσης των διαχειριστών κωδικών πρόσβασης στο δίκτυο. Αυτό θα περιορίσει τον αριθμό των χρηστών που αποθηκεύουν διαπιστευτήρια σε απλό κείμενο. Οι περιορισμοί σύνδεσης (όπως αποκλεισμός κωδικού πρόσβασης και περιορισμός) μειώνουν τις πιθανότητες ενός εισβολέα που τακτοποιείται σε έναν κεντρικό υπολογιστή και τα διαπιστευτήρια δεν έχουν ήδη αποκτηθεί. Διασφαλίστε ότι ένας μόνο λογαριασμός δεν μπορεί να επιτρέψει την πρόσβαση σε όλες τις συσκευές και τα στοιχεία σε ένα δίκτυο, ιδίως εάν οι λογαριασμοί αυτοί είναι προνομιακοί. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) θα πρέπει να χρησιμοποιείται για τις υπηρεσίες που απευθύνονται στο διαδίκτυο για την καταπολέμηση των επιθέσεων εξαναγκασμού και εικασίας για τον κωδικό πρόσβασης. Η δυνατότητα ενιαίας σύνδεσης (SSO) μπορεί να χρησιμοποιηθεί για να περιοριστεί ο αριθμός των χρησιμοποιούμενων κωδικών πρόσβασης και να μειωθεί η πιθανότητα κλοπής τους. Επίσης, πρέπει να γίνεται η χρήση εναλλακτικών τεχνικών μεθόδων ελέγχου ταυτότητας, όπως βιομετρικά στοιχεία, συνδέσεις εισόδου μιας χρήσης (μαγικές συνδέσεις), έξυπνες κάρτες και PIN που υποστηρίζονται από φυσικό υλικό.

Συνοψίζοντας:

Ακολουθήστε τις οδηγίες του κωδικού πρόσβασης και μην επαναχρησιμοποιήσετε κωδικούς πρόσβασης για διαφορετικά συστήματα.

Εξετάστε τη χρήση των διαχειριστών κωδικών πρόσβασης στο δίκτυο.

Ενεργοποιήστε τους περιορισμούς σύνδεσης.

Χρησιμοποιήστε έλεγχο ταυτότητας πολλαπλών παραγόντων για υπηρεσίες που χρησιμοποιούν το διαδίκτυο και λογαριασμούς υψηλού κινδύνου.

Όπου είναι δυνατόν, χρησιμοποιήστε εναλλακτικές μεθόδους ελέγχου ταυτότητας με κωδικούς πρόσβασης.

- Προστασία των λογαριασμών υψηλών προνομίων

Οι λογαριασμοί διαχείρισης τοπικού λογαριασμού και τομέα - με πρόσβαση στα περισσότερα συστήματα και δεδομένα - είναι ισχυρά εργαλεία σε ένα δίκτυο. Η χρήση τους θα πρέπει να ελέγχεται αυστηρά και να κλειδώνεται. Οι διαχειριστές πρέπει να χρησιμοποιούν ξεχωριστούς λογαριασμούς. ένα για την καθημερινή επιχειρησιακή χρήση (όπως περιήγηση στο διαδίκτυο και στο ηλεκτρονικό ταχυδρομείο) και ένα προνομιακό λογαριασμό διαχειριστή που θα πρέπει να χρησιμοποιείται μόνο σε ξεχωριστές διαχειριστικές συσκευές. Αυτό μειώνει τον κίνδυνο μίας μολυσμένης συσκευής που χρησιμοποιείται για σκοπούς διαχείρισης. Οι λογαριασμοί διαχειριστή θα πρέπει να αποτρέπονται από την περιήγηση στον ιστό και την πρόσβαση σε μηνύματα ηλεκτρονικού ταχυδρομείου και να χρησιμοποιούνται μόνο όταν μια εργασία απαιτεί αυξημένα δικαιώματα.

Συνοψίζοντας:

Οι διαχειριστές πρέπει να χρησιμοποιούν έναν κανονικό λογαριασμό για κανονικές δραστηριότητες χρήστη και έναν ξεχωριστό λογαριασμό διαχειριστή μόνο για δραστηριότητες διαχειριστή.

Χρήση ξεχωριστών συσκευών για κανονικούς λογαριασμούς και λογαριασμούς διαχειριστών, αν είναι δυνατόν.

Κλείσιμο των λογαριασμών διαχειριστή για την αποτροπή ενεργειών υψηλού κινδύνου, όπως περιήγηση στον ιστό και πρόσβαση σε μηνύματα ηλεκτρονικού ταχυδρομείου.

- Εφαρμογή της αρχής του λιγότερου προνομίου

Η αρχή του «λιγότερου προνομίου» (όπου οι λογαριασμοί και οι χρήστες έχουν την ελάχιστη απαιτούμενη πρόσβαση για την εκτέλεση του ρόλου τους) θα πρέπει να εφαρμόζεται όπου είναι δυνατόν. Ένα βαθμιδωτό μοντέλο για τους λογαριασμούς διαχείρισης διασφαλίζει ότι έχουν πρόσβαση μόνο στις συγκεκριμένες διοικητικές δυνατότητες που απαιτούνται, και όχι σε όλες. Η χρήση διαφόρων βαθμών διαχειριστικών λογαριασμών περιορίζει τον αριθμό των πολύ υψηλών προνομιούχων λογαριασμών που χρησιμοποιούνται και μειώνει την πρόσβαση που ένας εισβολέας κερδίζει εάν διακυβεύεται ένας λογαριασμός διαχειριστή χαμηλότερου προνομίου Λογαριασμοί με πλήρη δικαιώματα σε ένα δίκτυο (όπως ένας διαχειριστής τομέα, κεντρικός διαχειριστής ή λογαριασμός διαχειριστή σύννεφου) δεν πρέπει κανονικά να χρησιμοποιούνται. Ενώ απαιτούνται για ορισμένα καθήκοντα (όπως η αρχική δημιουργία ενός δικτύου, η εκτέλεση αναβαθμίσεων, η δημιουργία νέων προνομιούχων λογαριασμών ή η αποκατάσταση καταστροφών), οι λογαριασμοί διαχείρισης χαμηλότερου επιπέδου θα πρέπει να χρησιμοποιούνται για τις περισσότερες εργασίες.

Η χρήση προνομιακής πρόσβασης με βάση το χρόνο μπορεί να συμβάλει στη μείωση του αντίκτυπου διαρροής στοιχείων διαχειριστή, ειδικά καθώς θα ελέγχεται κάθε φορά που ο χρήστης το ζητά ή το λαμβάνει. Ο εντοπισμός των συσκευών, των υπηρεσιών και των χρηστών υψηλού κινδύνου μπορεί να βοηθήσει στον προγραμματισμό των χορηγημένων προνομίων, εξασφαλίζοντας ότι τα άτομα με τον υψηλότερο κίνδυνο έχουν τα χαμηλότερα προνόμια.

Συνοψίζοντας:

Χρήση ενός μοντέλου κλιμάκωσης για διαχειριστικούς λογαριασμούς, ώστε να μην έχουν καμία περιττή πρόσβαση ή προνόμια.

Χρήση λογαριασμών με πλήρη δικαιώματα σε μια επιχείρηση όταν είναι απολύτως απαραίτητο. Εξέταση της χρήσης των δικαιωμάτων που βασίζονται στο χρόνο για να περιοριστεί περαιτέρω τη χρήση τους.

Αξιολόγηση συσκευών, υπηρεσιών και χρηστών υψηλού κινδύνου για να ελαχιστοποιήσετε τις προσβάσεις τους.

- Κλείδωμα συσκευών

Οποιαδήποτε συσκευή ή σύστημα που είναι μέρος του δικτύου (ακόμα και εκείνες που δεν συνδέονται άμεσα με το διαδίκτυο) μπορεί να γίνει στόχος σε μια επίθεση εσωτερικής μετακίνησης. Όλες οι συσκευές θα πρέπει να ενημερώνονται, με τις τελευταίες ενημερώσεις λογισμικού το συντομότερο δυνατό. Οι αυτοματοποιημένες ενημερώσεις μπορούν επίσης να χρησιμοποιηθούν για την απλοποίηση αυτής της διαδικασίας, παρόλο που είναι σημαντικό να εξασφαλιστεί ότι τα περιττή ζεύγη συσκευών θα ενημερώνονται σε διαφορετικές χρονικές στιγμές για να διατηρηθεί ο πλεονασμός .Τα τερματικά πρέπει να ρυθμιστούν με ασφάλεια. Εάν είναι δυνατόν, οι εφαρμογές θα πρέπει να κατατεθούν σε μία επιτρεπτή λίστα (whitelist), ώστε να μπορούν να εκτελούνται μόνο εγκεκριμένες εφαρμογές. Αυτό μπορεί επίσης να γίνει χρησιμοποιώντας μια αρχιτεκτονική που επιτρέπει μόνο την εγκατάσταση και εκτέλεση εφαρμογών οι οποίες προέρχονται από μια αξιόπιστη πηγή. Εκτός από τα τείχη προστασίας στο όριο του δικτύου, τα τοπικά τείχη προστασίας στους κεντρικούς υπολογιστές πρέπει να έχουν τη δυνατότητα να περιορίζουν την περιττή εισερχόμενη και εξερχόμενη κίνηση. Από προεπιλογή, τα τείχη προστασίας θα πρέπει να αποκλείουν όλες τις εισερχόμενες συνδέσεις και να επιτρέπουν μόνο αυτές που επιτρέπονται ρητά. Ο κατάλογος των εγκεκριμένων συνδέσεων θα πρέπει να αναθεωρείται τακτικά για να καταργηθούν όσες δεν χρειάζονται πλέον.Πρέπει να ενεργοποιούνται οι ασφαλείς μηχανισμοί εκκίνησης όπου είναι δυνατόν, για να διασφαλιστεί η ακεραιότητα της διαδικασίας εκκίνησης σε συσκευές και να αυξηθεί η δυσκολία για έναν εισβολέα να κερδίσει παραμονή σε μια συσκευή.

Συνοψίζοντας:

Εφαρμογή των ενημερώσεων λογισμικού σε όλες τις συσκευές μόλις κυκλοφορήσουν και χρήση αυτοματοποιημένων ενημερώσεων όπου είναι δυνατόν.

Χρήση της λίστα κατάτμησης για να τον έλεγχο και τον περιορισμό της χρήσης των εφαρμογών. Ενεργοποίηση των τοπικών τειχών προστασίας στους κεντρικούς υπολογιστές.

Χρήση ασφαλούς μηχανισμού εκκίνησης, αν είναι διαθέσιμος.

- Διαχωρισμός των δίκτυών ως σύνολα

Ο κατακερματισμός του δικτύου (ή ο διαχωρισμός) περιλαμβάνει τη διάσπαση ενός δικτύου σε διάφορα τμήματα δικτύου. Αυτό αυξάνει σημαντικά τη δυσκολία ενός εισβολέα να επιτύχει το στόχο του μία φορά στο δίκτυο, καθώς το σημείο εισόδου του ενδέχεται να μην έχει κανένα μέσο για την επίτευξη της απόκτησης δεδομένων ή του συστήματος του στόχου.

Τα συστήματα και τα δεδομένα που δεν χρειάζεται να επικοινωνούν ή να αλληλοεπιδρούν μεταξύ τους θα πρέπει να διαχωρίζονται σε διαφορετικά τμήματα δικτύου και να επιτρέπουν στους χρήστες να έχουν πρόσβαση σε ένα τμήμα που χρειάζονται.

Αυτοί οι έλεγχοι ασφαλείας θα πρέπει να διασφαλίζουν ότι όλα τα δεδομένα και οι συνδέσεις που προέρχονται από το όριο του δικτύου δεν είναι αξιόπιστα. Τα πρότυπα ISO 27001 και 27002 παρέχουν κάποια εικόνα για την κατάτμηση του δικτύου και τις βέλτιστες πρακτικές για την υλοποίησή του σε ένα δίκτυο.

Συνοψίζοντας

Διαχωρισμός δικτύων ως συνόλων: προσδιορισμός, ομαδοποίηση και απομόνωση κρίσιμων δικτυακών συστημάτων και εφαρμογή κατάλληλων ελέγχων ασφαλείας δικτύου σε αυτά.

- Παρακολούθηση δικτύων

Είναι ζωτικής σημασίας να γίνετε παρακολούθηση του δικτύου για τυχόν γεγονότα ασφαλείας που μπορεί να έχουν ενδιαφέρον. Καθώς ανακαλύπτονται συνεχώς νέες ευπάθειες, ορισμένοι

επιτιθέμενοι θα αποκτήσουν τελικά πρόσβαση, ανεξάρτητα από το πόσο καλά προστατεύεται το δίκτυό. Μόλις συμβεί αυτό, η παρακολούθηση του δικτύου είναι ο μόνος τρόπος για να εντοπιστεί μια παραβίαση και, στη συνέχεια, να γίνει κάποιο αντίμετρο. Η βάση της παρακολούθησης είναι η καταγραφή και η αποθήκευση των ημερολογίων για ενδεχομένως ενδιαφέροντα συμβάντα ασφαλείας. Τα συστήματα μπορούν στη συνέχεια να αναλύσουν αυτά τα αρχεία καταγραφής και να αναζητήσουν ύποπτη συμπεριφορά που μπορεί να σηματοδοτεί ότι ένας επιτιθέμενος έχει υπονομεύσει το δίκτυό και να προειδοποιήσει τους υπεύθυνους. Πρέπει να γίνει ενεργοποίηση όλων των λειτουργιών καταγραφής και ασφάλειας στον τομέα των συστημάτων και των τεχνολογιών που χρησιμοποιεί το δίκτυό (όπως για παράδειγμα στα firewalls και την άλλη αρχιτεκτονική δικτύου) και επίσης να γίνει καταγραφή στα λειτουργικά συστήματα.

Η γνώση της θέσης των στοιχείων υψηλής αξίας σε ένα δίκτυο επιτρέπει την παροχή λεπτομερέστατης ειδοποίησης. Τα στοιχεία υψηλής αξίας μπορούν να περιλαμβάνουν σημαντικές υπηρεσίες και σημαντικούς διακομιστές (όπως τον ελεγκτή τομέα) στο δίκτυο, πέραν των διαφόρων χρηστών και λογαριασμών. Μερικοί αξιοσημείωτοι χρήστες περιλαμβάνουν:

προνομιακοί χρήστες (λόγω της πρόσβασης που διαθέτουν)

λογαριασμούς της διεύθυνσης (λόγω των πληροφοριών που ενδέχεται να περιέχουν)

λογαριασμούς κοινωνικών μέσων ενημέρωσης (λόγω της πιθανότητας βλάβης της φήμης σε περίπτωση χειραγώγησης)

Θα πρέπει να υπάρχει γνώση του δικτύου στο σύνολό του, συμπεριλαμβανομένης της δομής του και του τρόπου χρήσης του. Η διατήρηση του ελέγχου όλων των συσκευών που μπορούν να συνδεθούν στο δίκτυο και η ενημέρωση τους τακτικά βοηθάνε στην αναγνώριση της παράνομης χρήσης. Μπορεί να υπάρχει ασυνήθιστη δραστηριότητα στο στρώμα πρωτοκόλλου δικτύου, αλλά και σε ειδικές συνθήκες εφαρμογής, όπως η χρήση των διαπιστευτηρίων και τα συμβάντα ελέγχου ταυτότητας. Οι επιτιθέμενοι θα προσπαθήσουν να συνδυαστούν με τη συνήθη κυκλοφορία δικτύου χρησιμοποιώντας νόμιμα εργαλεία και συστήματα για να μετακινούνται εσωτερικά, κάτι που σημαίνει ότι συχνά παραβλέπετε από το τυπικό αντιικό λογισμικό και είναι πολύ πιο δύσκολο να εντοπιστεί. Η επίγνωση των κοινών εργαλείων και διαδικασιών που θα μπορούσε να χρησιμοποιήσει ένας επιτιθέμενος θα αυξήσει σημαντικά τις πιθανότητες ταυτοποίησης του. Η μεγαλύτερη πρόκληση στην παρακολούθηση του δικτύου είναι ο εντοπισμός γνήσιων περιστατικών ασφάλειας παρά οι ψευδείς θετικές ενέργειες που είναι κοινές στον μεγάλο όγκο του «θορύβου» που υπάρχει σε ένα δίκτυο. Η κατανόηση του δικτύου και η τυπική συμπεριφορά των χρηστών του μπορούν να βοηθήσουν στην άμβλυνση του προβλήματος των ψευδών θετικών ειδοποιήσεων, καθώς ο χρήστης γίνεται πιο έμπειρος στο να εντοπίζει ασυνήθιστη δραστηριότητα. Με την κατάτμηση ενός δικτύου υπάρχει η ευκαιρία να εστιαστεί στην παρακολούθηση των σημείων εστίασης της κυκλοφορίας που δημιουργούνται μεταξύ των τμημάτων.

Συνοψίζοντας:

Ενεργοποίηση των λειτουργιών καταγραφής και ελέγχου στα συστήματά και χρήση αυτών για να ανιχνεύσει ασυνήθιστης δραστηριότητας.

Διατήρηση του ελέγχου ή της καταγραφής όλων των συσκευών που μπορούν να συνδεθούν στο δίκτυό και κατανόηση των στοιχείων υψηλής αξίας.

Κατανόηση και εξοικείωση με το δίκτυό για το πώς χρησιμοποιείται συνήθως.

- Εξετάστε τη χρήση των honeypots

Τα honeypots είναι συστήματα που δημιουργούνται με μοναδικό σκοπό να απορροφούν την επίθεση. Η υλοποίηση honeypots, που έχουν εγκατασταθεί εσωτερικά σε ένα δίκτυο ως στόχος για πραγματικά συστήματα, μπορούν να αποτελέσουν πολύτιμα εργαλεία για την ανίχνευση μιας εισβολής στο δίκτυό. Δεδομένου ότι τα honeypots δεν είναι νόμιμα συστήματα στο δίκτυο (και δεν περιέχουν πραγματικά δεδομένα ή υπηρεσίες), οι απρόσμενες συνδέσεις μπορούν να θεωρηθούν ως εχθρικές δραστηριότητες (επειδή οι γνήσιοι χρήστες δεν χρειάζονται πρόσβαση στο honeypot). Εάν εντοπιστεί αλληλεπίδραση με το honeypot θα πρέπει να διερευνηθεί αμέσως. Η υλοποίηση των

honeypots πρέπει να χρησιμοποιείται για τη συμπλήρωση της παρακολούθησης του δικτύου και άλλων τεχνικών ανίχνευσης εισβολής. Τα honeypots δεν ωφελούν το δίκτυο άμεσα, αλλά δημιουργούνται για να συλλέξουν πληροφορίες σχετικά με τις τελευταίες τεχνικές που χρησιμοποιούν οι εισβολείς. Η χρήση ερευνητικών honeypots εισάγει ορισμένους κινδύνους. Τα ερευνητικά honeypots είναι εγγενώς επικίνδυνα, καθώς ενθαρρύνουν τους επιτιθέμενους να αλληλοεπιδρούν μαζί τους. Η υλοποίηση honeypots είναι λιγότερο επικίνδυνη, αλλά εξακολουθούν να εισάγουν κάποιο κίνδυνο για έναν οργανισμό, ανάλογα με το επίπεδο πολυπλοκότητάς τους. Για παράδειγμα, θα μπορούσαν να αξιοποιηθούν και να χρησιμοποιηθούν ως πλατφόρμα για την απορρόφηση επιθέσεων σε νόμιμα συστήματα στο δίκτυο κατά την εσωτερική μετακίνηση. Για τους λόγους αυτούς, τα honeypots θα πρέπει να χρησιμοποιούνται μόνο αν έχει γίνει αξιολόγηση στον αντίκτυπο της λανθασμένης εφαρμογής.

Συνοψίζοντας:

Η χρήση ενός honeypot στο δίκτυο, προϋποθέτει ότι υπάρχει η εξειδίκευση για να επιτευχθεί και η κατανόηση των κινδύνων που συνεπάγεται.

1.3 Γιατί η εσωτερική μετακίνηση υπερισχύει έναντι άλλων τεχνικών

Ο όρος "Εσωτερική Μετακίνηση" υπάρχει εδώ και τέσσερα χρόνια και ήταν στα νέα όταν τα ransomware όπως το WannaCry και τα APT όπως το APT28 και το APT29 χρησιμοποίησαν τεχνικές εσωτερικής μετακίνησης. Τις περισσότερες φορές ένας εισβολέας μπορεί να μην έχει άμεση πρόσβαση σε ένα μηχάνημα ή πόρο στο εσωτερικό δίκτυο, το οποίο ο επιτιθέμενος θεωρεί ένα πολύτιμο τρόπαιο. Το πολύτιμο αυτό τρόπαιο μπορεί να είναι ο ελεγκτής τομέα, ένα μηχάνημα που φιλοξενεί εμπιστευτικές πληροφορίες ή ο επιτιθέμενος μπορεί να έχει προγραμματίσει να έχει πρόσβαση σε όλα τα εσωτερικά μηχανήματα για να τα έχει προσθέσει σε ένα botnet. Σε μια τέτοια κατάσταση, ο επιτιθέμενος θα επιδιώξει έναν αδύναμο κρίκο στο δίκτυο-στόχο, τον οποίο μπορεί να διεισδύσει. Αυτός ο αδύναμος σύνδεσμος μπορεί να είναι ένας ανυποψίαστος χρήστης, ένας μη συνδεδεμένος υπολογιστής, ένα εκτεθειμένο Wi-Fi κ.λπ. Μόλις ο επιτιθέμενος ελέγξει τον αδύναμο αυτό σύνδεσμο, θα χρησιμοποιήσει την πρόσβαση αυτή για τον εντοπισμό άλλων πόρων στο εσωτερικό δίκτυο και θα προσπαθήσει να τα διεισδύσει έως ότου επιτευχθεί ο στόχος της επίθεσης στο δίκτυο. Οι μέθοδοι που χρησιμοποιεί ο επιτιθέμενος για τον εντοπισμό πόρων στο εσωτερικό δίκτυο, τη συγκέντρωση πληροφοριών ή διαπιστευτηρίων από το θύμα και τη χρήση των πληροφοριών που συγκεντρώνονται για να αποκτήσουν τον έλεγχο άλλων πόρων στο εσωτερικό δίκτυο, ονομάζονται "τεχνικές εσωτερική μετακίνησης". Στα δείγματα κακόβουλου λογισμικού που μελετήθηκαν πρόσφατα, ειδικά τα APT28 και APT29, χρησιμοποιήθηκαν μερικές από τις τεχνικές που περιγράφονται παρακάτω για να μετακινηθούν μέσα στο εσωτερικό δίκτυο. Τα βήματα δεν χρειάζεται να είναι με την ακριβή σειρά όπως φαίνεται παρακάτω και ο επιτιθέμενος ή το κακόβουλο λογισμικό μπορεί να χρησιμοποιήσει μόνο μερικά.

Διήθηση - Σε αυτό το στάδιο, ο εισβολέας αποκτά πρόσβαση σε ένα ή περισσότερα μηχανήματα στο εσωτερικό δίκτυο. Αυτό θα μπορούσε να γίνει μέσω:

Spear phishing, όπου ο εισβολέας προσελκύει χρήστες μέσω ηλεκτρονικού ταχυδρομείου για να επισκεφτεί κακόβουλους ιστότοπους ή να ανοίξει μολυσμένα έγγραφα. Αυτό παρατηρήθηκε στην περίπτωση του ATP28 όπου οι χρήστες έλαβαν ένα κακόβουλο έγγραφο της Microsoft το οποίο ήταν φορέας για ένα ενσωματωμένο dropper κακόβουλου λογισμικού. Καθοδήγηση με λήψη, όπου ένας εσωτερικός χρήστης επισκέπτεται άθελά έναν κακόβουλο ιστότοπο. Ένας κακόβουλος ιστότοπος στον οποίο επισκέπτεται ο χρήστης μπορεί να έχει κρυφό κάποιο κακόβουλο HTML αρχείο (ένα κρυφό iframe) που θα επέτρεπε στο πρόγραμμα περιήγησης να στείλει ένα αίτημα σε μια σελίδα, σε ένα διακομιστή όπου φιλοξενείται ένα εργαλείο εκμετάλλευσης. Το εργαλείο εκμετάλλευσης θα επιτηρούσε κρυφά το πρόγραμμα περιήγησης για ευπάθειες ή ευπρόσβλητα πρόσθετα και θα εκτελούσε εκμετάλλευση που θα το έθετε σε στάδιο για περαιτέρω λήψη κακόβουλου λογισμικού.

Άμεση επίθεση εναντίον μιας ευάλωτης υπηρεσίας. Αυτό παρατηρήθηκε με το ransomware της WannaCry. Μόλις μολύνει μια μηχανή, φορτώνει ένα δεύτερο κακόβουλο πρόγραμμα που ανιχνεύει

το εσωτερικό δίκτυο για μηχανές Windows ευάλωτες στο CVE-2017-0147 το οποίο εκμεταλλεύθηκε ο κώδικας EternalBlue ο οποίος ελευθερώθηκε από την ομάδα επιτιθέμενων "Shadow Brokers".

Αναγνώριση - Μόλις ολοκληρωθεί το στάδιο διείσδυσης, μπορεί να αναγνωριστεί ότι το χειραγωγημένο μηχάνημα δεν ήταν ο τελικός στόχος της επίθεσης. Σε αυτό το στάδιο, ο εισβολέας μπορεί να χρησιμοποιήσει εργαλεία που υπάρχουν ήδη στο σύστημα όπως η εντολή "net.exe" ή upload εργαλεία όπως "NetSess.exe", "smbat", σαρωτές κλπ. Nmap και Metasploit τα οποία έρχονται με ενσωματωμένα σενάρια που βοηθούν στη συλλογή χρήσιμων πληροφορίων από εσωτερικούς υπολογιστές. Ο επιτιθέμενος συνήθως προσπαθεί να βρει απαντήσεις στις επόμενες ερωτήσεις :

Τι άλλες μηχανές υπάρχουν στο δίκτυο;

Τι ενεργές συνεδρίες SMB εκτελούνται;

Ποιοι είναι τα μέλη όλων των ομάδων στον τομέα;

Ποιος κεντρικός υπολογιστής / χρήστης ή συνεδρία θα μπορούσε να είναι πολύτιμος για τον επόμενο γύρο επίθεσης;

Η επιτυχής έκβαση αυτού του σταδίου είναι ότι ο εισβολέας έχει εντοπίσει άλλες μηχανές, περιόδους λειτουργίας, λογαριασμούς χρηστών κ.λπ. στο εσωτερικό δίκτυο.

Συλλογή πιστώσεων - Όταν ένας χρήστης συνδέεται σε ένα μηχάνημα των Windows, ο κωδικός πρόσβασης χρήστη είναι σε hash και αποθηκεύεται στη μνήμη της διαδικασίας LSASS. Χρησιμοποιώντας εργαλεία όπως το Mimikatz, ένας επιτιθέμενος μπορεί να εξαγάγει αυτά τα αποθηκευμένα διαπιστευτήρια από τη μνήμη LSASS. Εάν ήταν ένα μηχάνημα στο οποίο είχε συνδεθεί ένας διαχειριστής τομέα, ο επιτιθέμενος θα είχε τώρα πρόσβαση στα προσωρινά διαπιστευτήρια. Ακόμη και αν η εξαγόμενη πιστοποίηση είναι ο κωδικός πρόσβασης με hash, ο επιτιθέμενος θα μπορούσε ακόμα να χρησιμοποιήσει αυτόν τον κωδικό πρόσβασης με hash σε μια τεχνική που ονομάζεται "Pass the hash" για να εκτελέσει εντολές σε άλλο μηχάνημα στο οποίο παρουσιάζεται ως διαχειριστής τομέα. Αυτό παρέχεται από μια εγγενή αδυναμία στον έλεγχο ταυτότητας NTLM που χρησιμοποιείται από το πρωτόκολλο SMB, το οποίο είναι η γλώσσα που χρησιμοποιούν τα μηχανήματα των Windows για να μιλήσουν μεταξύ τους. Ένα πιο σοβαρό σενάριο είναι όταν ο επιτιθέμενος θα κατάφερνε να συλλέξει το hash κωδικού NTLM για τον λογαριασμό "krbtgt" ενός ελεγκτή τομέα, δίνοντας στον επιτιθέμενο τη δυνατότητα να δημιουργήσει Kerberos TGT κατά βούληση. Αυτό είναι επίσης γνωστό ως "Golden Ticket Attack". Το εργαλείο Mimikatz διαθέτει επίσης μια ενότητα που καλύπτει τη διαδικασία LSASS, οπότε ο επιτιθέμενος μπορεί να εξακριβωθεί ως οποιοσδήποτε χρήστης, ενώ οι χρήστες που επηρεάζονται συνεχίζουν κανονικά χρησιμοποιώντας τα συνήθη διαπιστευτήρια τους. Αυτή η τεχνική είναι γνωστή ως "Skeleton Key Attack".

Εκτέλεση κώδικα - Ένας εισβολέας στο εσωτερικό δίκτυο μπορεί να επηρεάσει άλλες μηχανές στο δίκτυο με τους ακόλουθους τρόπους Χρησιμοποιώντας εντολές συλλογής με εργαλεία όπως το "PsExec" για απομακρυσμένη εκτέλεση κώδικα, η την εντολή "at.exe" για τον προγραμματισμό απομακρυσμένων εργασιών ή την πρόσβαση ανάγνωσης / εγγραφής σε προστατευμένα κοινόχρηστα αρχεία. Άμεση επίθεση στις υπηρεσίες που εκτελούνται σε εσωτερικές μηχανές. Αυτή ήταν η προσέγγιση που χρησιμοποιήθηκε από το κακόβουλο λογισμικό WannaCry το οποίο χρησιμοποίησε το EternalBlue exploit για να διεισδύσει σε εσωτερικά τερματικά. Το ATP28 χρησιμοποίησε μια ενδιαφέρουσα προσέγγιση όπου μαζί με τη χρήση της εκμετάλλευσης της Eternalblue χρησιμοποίησε επίσης το εργαλείο "Responder" για να φιλοξενήσει ψεύτικες υπηρεσίες SMB ώστε να αποκομίσει τα διαπιστευτήρια χρήστη από μηχανές που προσπαθούσαν να έχουν πρόσβαση στην ψεύτικη υπηρεσία. Στις περισσότερες επιθέσεις, όταν αυτό το στάδιο είναι επιτυχές, το μηχάνημα που έχει χειραγωγηθεί θα έχει ρύθμιση καναλιών "Command and Control" με ένα μηχάνημα ελεγχόμενο από επιτιθέμενο στο διαδίκτυο μέσω του οποίου θα ληφθούν πρόσθετα κακόβουλα προγράμματα και θα ληφθούν εντολές για περαιτέρω ενέργειες. Αυτά τα κανάλια μπορούν επίσης να λειτουργήσουν ως μέσο για την εκσκαφή δεδομένων.

Ανθεκτικότητα - Οι επιτιθέμενοι και το κακόβουλο λογισμικό προτιμούν να παραμένουν κρυμμένοι, για να επιβιώσουν σε μια επανεκκίνηση και να είναι ενεργοί. Ορισμένα ενδιαφέροντα δείγματα κακόβουλου λογισμικού που χρησιμοποίησαν ανθεκτικότητα με νέους τρόπους αναφέρονται παρακάτω:

Το Poweliks χρησιμοποίησε κόλπα μητρώου για να κρύψει τον κώδικα του στο μητρώο και να επιτύχει ανθεκτικότητα.

Το Kovter χρησιμοποίησε κόλπα μητρώου παρόμοια με τα Poweliks

Το APT29 χρησιμοποίησε το χώρο αποθήκευσης WMI για να αποθηκεύσει τον κώδικα του και να συνεχίσει.

Όλα τα παραπάνω δημιουργούν μία ισχυρή αλυσίδα αντιδράσεων σε ένα σύστημα και για αυτό το λόγο η τεχνική της εσωτερικής μετακίνησης έχει υπερισχύσει έναντι άλλων τεχνικών χειραγώγησης.

1.4 Κυνήγι απειλών από εργαλεία εσωτερικής μετακίνησης

Οι επιτιθέμενοι στα συστήματα μετά τη χειραγώγηση ασφάλειας είναι σαν τους αγοραστές σε ένα μπακάλικο. Είναι σπάνιο να κατευθύνονται κατευθείαν σε ένα μόνο μέρος για να πάρουν αυτό που χρειάζονται. Αντί αυτού, εισέρχονται στο κτίριο και κινούνται γύρω από τους διαδρόμους, μαζεύοντας κομμάτια κατά μήκος του δρόμου πριν από το check out. Με τον ίδιο τρόπο, οι επιτιθέμενοι δεν θα χτυπήσουν μόνο ένα σημείο στο δίκτυό το οποίο θα περιέχει όλα τα δεδομένα που προσπαθούν να κλέψουν. Πρέπει να μετακινούνται εσωτερικά από σύστημα σε σύστημα (ή από διάδρομο σε διάδρομο) για να συγκεντρώσουν τις πληροφορίες για τις οποίες ήρθαν. Για να μετακινούνται ελεύθερα χωρίς να προσελκύουν μεγάλη προσοχή, οι επιτιθέμενοι συχνά χρησιμοποιούν αξιόπιστο λογισμικό που φαίνεται φυσιολογικό σε ένα περιβάλλον. Ένα από τα αγαπημένα μεταξύ των επιτιθέμενων είναι ένας παλιός φίλος πολλών διαχειριστών πληροφορικής: SysInternals PsExec.

Σε αυτή την ενότητα, θα συζητήσουμε ορισμένες τακτικές που μπορούν να χρησιμοποιήσουν οι κυνηγοί απειλών για να εντοπίσουν περιπτώσεις όπου οι επιτιθέμενοι χρησιμοποιούν το PsExec (ακόμα και όταν μετονομαστεί ή κλωνοποιηθεί) και παρόμοια εργαλεία για να μετακινηθούν εσωτερικά μεταξύ των τερματικών στο δίκτυό.

PsExec

Η SysInternals κυκλοφόρησε για πρώτη φορά το PsExec πριν από μια δεκαετία και παρέχει στους διαχειριστές μια αξιόπιστη μέθοδο απομακρυσμένης πρόσβασης στα συστήματα μέσω του πρωτοκόλλου SMB (Server Message Block). Η θεμελιώδης συμπεριφορά του PsExec ακολουθεί ένα απλό πρότυπο:

Δημιουργεί μια σύνδεση δικτύου SMB σε ένα σύστημα προορισμού χρησιμοποιώντας τα διαπιστευτήρια διαχειριστή.

Μεταφέρει ένα αντίγραφο μιας διαδικασίας λήψης που ονομάζεται PSEXESVC.EXE στο κοινόχρηστο στοιχείο ADMIN $ του συστήματος του στόχου

Εκκινεί το PSEXESVC.EXE, το οποίο στέλνει είσοδο και έξοδο σε έναν ορισμένο σωλήνα (pipe)

Γενικά, ένας ονομασμένος σωλήνας είναι μια μέθοδος επικοινωνίας μεταξύ διαδικασιών και διάφοροι ειδικοί σωλήνες είναι συνήθεις στους τομείς Active Directory των Windows. Οι σωλήνες μπορούν να ονομάζονται για συγκεκριμένες χρήσεις και, στην περίπτωση αυτή, ένας σωλήνας για την επικοινωνία PsExec συνήθως μοιάζει έτσι: \\. \ Pipe \ psexesvc. Αυτή η λεπτομέρεια καθίσταται εξαιρετικά σημαντική όταν ψάχνετε για κακόβουλες χρήσεις του PsExec στο περιβάλλον σας, διότι ακόμη και μια αόριστη, μετονομαζόμενη έκδοση του PsExec θα χρησιμοποιεί ονομαστικούς σωλήνες για επικοινωνία. Στην πραγματικότητα, αυτή η συμπεριφορά είναι τόσο προβλέψιμη που τη βλέπουμε ακόμη και σε ένα άλλο λογισμικό που απλώς κλωνοποιεί τη λειτουργικότητα του PsExec. Τα δυαδικά μεταδεδομένα συμβάλλουν επίσης στην αναγνώριση των μετονομασμένων περιπτώσεων του PsExec. Για τη διαδικασία προέλευσης που δημιουργεί μια σύνδεση, η εσωτερική τιμή του PsExec

είναι απλά το PsExec, ενώ για τη διαδικασία λήψης του στόχου, το PsExeSvc.exe, έχει ένα εσωτερικό όνομα το PsExec Service Host. Δεδομένου ότι το PsExec είναι κατά κύριο λόγο διαθέσιμο ως προκατασκευασμένο δυαδικό αρχείο, αυτά τα μεταδεδομένα δεν αλλάζουν εύκολα και μπορεί να είναι χρήσιμα για να προσδιορισμό την εκτέλεσης.

Εκτός από τα μεταδεδομένα, το μητρώο των Windows (όπως το HKEY_CURRENT_USER \ software \ sysinternals \ psexec \ eulaaccepted) μπορεί να υποδεικνύει πότε έχει χρησιμοποιηθεί το PsExec. Επιπλέον, ένας διαχειριστής πρέπει να αποδεχθεί μια Άδεια Χρήσης Τελικού Χρήστη εάν θέλει να χρησιμοποιήσει το βοηθητικό πρόγραμμα και η αποδοχή εγγράφεται σε αυτό το κλειδί. Όπως συμβαίνει με τα δυαδικά αρχεία μεταδεδομένων και την ονομαστική χρήση των σωλήνων, αυτό δεν θα αλλάξει αν μετονομαστεί το PsExec, αλλά μπορεί να αφαιρεθεί εύκολα από έναν ενημερωμένο επιτιθέμενο. Δεδομένου ότι το PsExec είναι εύκολο στη χρήση και αξιόπιστο, αποτελεί πλέον μια φυσική επιλογή τόσο για το νόμιμο λογισμικό όσο και για τους επιτιθέμενους, καθώς ο καθένας χρειάζεται έναν τρόπο έκδοσης εντολών σε απομακρυσμένα συστήματα. Ωστόσο, οι όροι χορήγησης άδειας χρήσης του PsExec δεν επιτρέπουν την ανακατανομή με άλλα πακέτα λογισμικού, τα οποία παρουσίασαν πρόβλημα για τους προγραμματιστές λογισμικού, οπότε τώρα υπάρχει μια ποικιλία εργαλείων ανοικτού κώδικα που κλωνοποιούν τις δυνατότητες του PsExec.\

RemCom

Το RemCom είναι ένα βοηθητικό πρόγραμμα αναδιανομής ανοικτού κώδικα που παρέχει τις ίδιες λειτουργίες απομακρυσμένης διαχείρισης. Έχει επιτύχει ένα επίπεδο φήμης αφού οι αντίπαλοι το χρησιμοποίησαν για να προχωρήσουν εσωτερικά στην επίθεσή τους στην Δημοκρατική Εθνική Επιτροπή το 2016. Εντούτοις, περιλαμβάνεται επίσης σε αρκετά νόμιμα πακέτα λογισμικού. Από προεπιλογή, το RemCom στέλνει το RemComSvc.exe σε έναν απομακρυσμένο υπολογιστή, ο οποίος στη συνέχεια χρησιμοποιεί το όνομα pipe \\. Pipe \ remcom_comunication στη θέση του ονομαστικού σωλήνα του PsExec. Επιπλέον, το εσωτερικό όνομα της διαδικασίας έχει τιμή από το remcom.

PAExec

Το PAExec διαθέτει όλες τις ίδιες λειτουργίες των RemCom και PsExec και προορίζεται κυρίως για χρήση με τη λύση διαχείρισης διακομιστή PowerAdmin. Από προεπιλογή, ο PAExec χρησιμοποιεί έναν ονομασμένο σωλήνα που περιέχει το string PAExec σε συνδυασμό με ένα μοναδικό αναγνωριστικό διεργασίας και τιμές ονόματος υπολογιστή. Η διαδικασία λήψης ονομάζεται και συνήθως έχει μια εσωτερική τιμή ονόματος του paexec.

CSExec

Το CSExec είναι μια εξαιρετικά διαμορφώσιμη εφαρμογή C # της λειτουργικότητας του PsExec. Από προεπιλογή, το CSExec στέλνει το csexecsvc.exe στον απομακρυσμένο υπολογιστή και χρησιμοποιεί έναν ονομασμένο σωλήνα που ονομάζεται \\. \ Pipe \ csexecsvc. Η εσωτερική τιμή ονόματος μπορεί εύκολα να μεταβληθεί - αν και αυτό εξαρτάται από τις οδηγίες σύνταξης – αλλά μπορεί να περιέχει και το string csexec από προεπιλογή. Συγκρίνοντας και αντιπαραβάλλοντας όλους αυτούς τους κλώνους, πρέπει να γίνουν εμφανή μερικά πράγματα:

Όλοι οι κλώνοι είναι ανοικτού κώδικα, με τον πηγαίο κώδικα τους διαθέσιμο στο κοινό.

Οι επιτιθέμενοι μπορούν να κατεβάσουν τον κώδικα και να τον παραμετροποιήσουν με διαφορετικές τιμές για ονόματα ονομαστικών σωλήνων και δυαδικά εσωτερικά ονόματα.

Παρ 'όλα αυτά, η υποκείμενη λειτουργικότητα για την επικοινωνία θα παραμείνει η ίδια.

Τώρα που έχει δημιουργηθεί μια αξιόπιστη συμπεριφορά για μια ολόκληρη κατηγορία εσωτερικών εργαλείων κίνησης, μπορεί να σχεδιαστεί μια στρατηγική ανίχνευσης. Η ανίχνευση με βάση ονομασμένους σωλήνες μπορεί να πάρει λίγο περίπλοκη γιατί οι σωλήνες είναι κοινοί στα τελικά σημεία των Windows, αλλά ένα ξεκίνημα με την εξαίρεση των σωλήνων που γνωρίζουμε ότι είναι καλοήθεις. Μέσα στα περιβάλλοντα της υπηρεσίας καταλόγου Active Directory, θα βρεθούν ονομασμένοι σωλήνες όπως:

\\. \ pipe \ netlogon

\\. \ pipe \ samr

\\. \ pipe \ lsarpc

Μπορούν επίσης να βρεθούν και άλλοι καλοήθεις σε εξειδικευμένα περιβάλλοντα για διαδικασίες όπως ερωτήματα βάσης δεδομένων SQL και σε συστήματα mainframe. Σε ένα περιβάλλον μπορεί να δημιουργηθεί μια γραμμή βάσης ονομασμένων σωλήνων χρησιμοποιώντας Sysinternals PipeList ή το Sysmon παράλληλα με την καταγραφή συμβάντων των Windows. Αν γίνεται χρήση εργαλείων ανίχνευσης και απόκρισης τελικού σημείου (EDR) στο περιβάλλον, τότε μπορεί να γίνει επίσης εξέταση των τροποποιήσεων των αρχείων διαδικασίας για να βρεθούν επίσης ονομασμένοι σωλήνες.

Μόλις βρεθεί τη γραμμή βάσης, μπορεί να ξεκινήσει η διαδικασία της αναζήτησης για μη φυσιολογικούς σωλήνες. Οι καλοήθεις σωλήνες πρέπει να είναι άφθονοι, ενώ οι κακόβουλοι πρέπει να είναι οι ασυνήθιστοι. Αφού συγκεντρωθεί ένα σύνολο δεδομένων με ονομασμένους σωλήνες από τα τελικά σημεία, πιθανότατα θα υπάρχουν πολλές διαδικασίες που χρησιμοποιούν πολλούς σωλήνες. Ένας τρόπος για τη μείωση αυτού του θορύβου είναι να περιοριστεί η χρήση συγκεκριμένων διαδικασιών, έτσι ώστε να μπορούν να ξεχωρίζουν περισσότερο τα ευρήματα. Για παράδειγμα, για να αυξηθεί η αξιοπιστία των κυνηγών για το PsExec, τότε θα έπρεπε να απαγορευτεί η χρήση του από τους διαχειριστές και να γίνετε χρήση του PowerShell Remoting. Το PowerShell Remoting μπορεί να εκτελέσει τις ίδιες ενέργειες με το PsExec - και το κάνει με πιο ασφαλές μεθόδους. Με μερικές παραμετροποιήσεις όπως αυτή μπορεί να βελτιωθεί σιγά-σιγά το αποτελέσματα του κυνηγιού και παράλληλα να γίνεται καλύτερη εκμάθηση του περιβάλλοντος. Παρά τον πλούτο των εργαλείων εσωτερική μετακίνησης παρόμοιας με το PsExec, μια αειθαλής τακτική για την ανίχνευση αυτών των εργαλείων είναι να κυνηγηθούν οι απομακρυσμένοι ονομασμένοι σωλήνες που χρησιμοποιούνται από τις διαδικασίες στα τερματικά των Windows. Το κυνήγι με αυτό τον τρόπο θα βοηθήσει να αποκαλυφθεί η δραστηριότητα από μη εξουσιοδοτημένα εργαλεία απομακρυσμένης διαχείρισης σε πολλαπλές μορφές, ακόμα και όταν τα εργαλεία έχουν τροποποιηθεί από τους επιτιθέμενους. Η συλλογή και η ανάλυση δεδομένων με ονομασίες σωλήνων θα έχει επίσης οφέλη εκτός του τομέα των κλώνων PsExec, επιτρέποντάς να βρεθούν εργαλεία επιτιθέμενων για συγκεκαλυμμένη κίνηση και για αναγνώριση τα οποία διαφορετικά θα ήταν δύσκολο να βρεθούν.

Κεφάλαιο 2 Σχετικές εργασίες

2.1 Σχετικές εργασίες

Έχουν υλοποιηθεί αρκετές εργασίες με Sysmon για την ανίχνευση της εσωτερικής μετακίνησης Συγκρίναμε την εργασία με παρόμοια έργα και καταλήξαμε ότι είναι ελάχιστα αυτά που έχουν δημιουργηθεί με Sysmon και συνδυασμό του αρχείου καταγραφής των Windows. Από το έργο της JPCERT/CC (Detecting Lateral Movement through Tracking Event Logs) μπορούμε να μελετήσουμε το πως μπορούμε να παραμετροποιήσουμε τα αρχεία καταγραφής ώστε με τα κατάλληλα εργαλεία να πραγματοποιείται ειδοποίηση ασφαλείας για την πρόληψη της εσωτερικής μετακίνησης σε ένα σύστημα. Σε αυτή την εργασία θα μελετήσουμε παρόμοια εργαλεία και επιπλέον τρόπους παρακολούθησης των γεγονότων τα οποία προσδιορίζουν παράνομη είσοδο σε ένα σύστημα με σκοπό την εσωτερική μετακίνηση στο χειραγωγημένο σύστημα και την απόκτηση ζωτικών πληροφοριών. Επιπλέον το Sysmon με την κατάλληλη ρύθμιση του μέσω του ανοιχτού κώδικα sysmonconfig-export.xml αρχείου που περιέχει θα αποτελέσει ένα δεύτερο εργαλείο ικανό να πραγματοποιήσει συσχετισμό γεγονότων που παράγονται μεταξύ άλλων χαρακτηριστικών.

Σε αυτή την εργασία πραγματοποιήθηκε μία τροποποίηση στο αρχείο sysmonconfig-export.xml προκειμένου να καταγράφονται ειδοποιήσεις σχετικά με τα διάφορα γεγονότα που πιάνουν τα αρχεία καταγραφής των Windows σχετικά με το σύστημα μας. Η δυνατότητα συσχέτισης μπορεί να ελέγξει εάν ένα συμβάν μπορεί να συσχετιστεί με μια βάση δεδομένων ευπάθειας ή με τρωτά σημεία στα περιουσιακά στοιχεία του χρήστη. Όλα αυτά τα δεδομένα μπορούν να επεξεργαστούν για

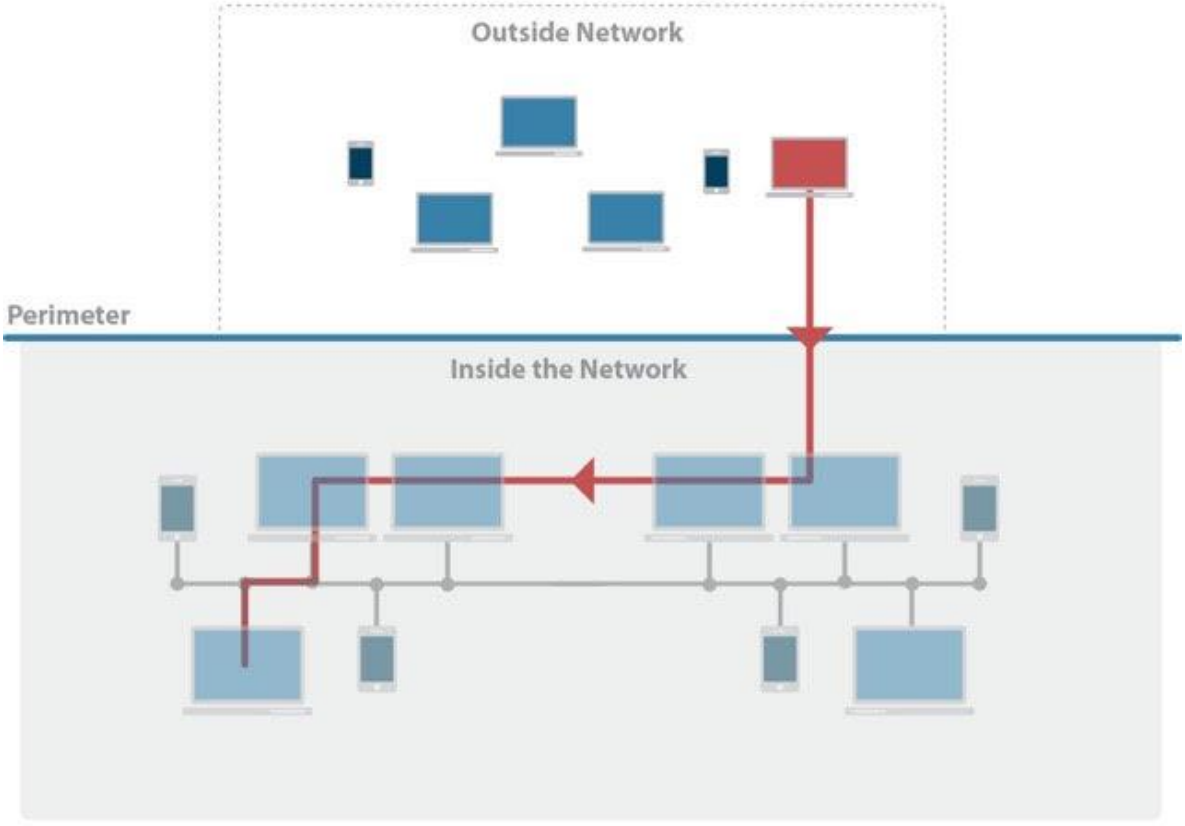
να εξάγουν τα πρότυπα ασφάλειας και να εκπαιδεύσουν τους χρήστες αλλά και το σύστημα κατάλληλα για τον εντοπισμό και την αντιμετώπιση της εσωτερικής μετακίνησης..

Κεφάλαιο 3 Εσωτερική μετακίνηση

3.1 Ανάλυση της εσωτερικής μετακίνησης

Η εσωτερική μετακίνηση αποτελείται από τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να εισάγουν και να ελέγχουν τα απομακρυσμένα συστήματα σε ένα δίκτυο. Ακολουθώντας τον πρωταρχικό στόχο τους, απαιτείται συχνά η εξερεύνηση του δικτύου για να βρεθεί ο στόχος και στη συνέχεια να αποκτήσει πρόσβαση σε αυτό. Η επίτευξη του στόχου τους συχνά περιλαμβάνει περιστροφή μέσω πολλαπλών συστημάτων και λογαριασμών για να επιτύχουν το σκοπό τους. Οι επιτιθέμενοι μπορούν να εγκαταστήσουν τα δικά τους εργαλεία απομακρυσμένης πρόσβασης για να επιτύχουν την εσωτερική μετακίνηση ή να χρησιμοποιήσουν τα νόμιμα διαπιστευτήρια με εγγενή εργαλεία δικτύου και λειτουργικού συστήματος, τα οποία μπορεί να είναι πιο κρυφά.

Με πιο απλά λόγια εσωτερική μετακίνηση είναι όταν ένας εισβολέας παίρνει την κατοχή ενός περιουσιακού στοιχείου μέσα σε ένα δίκτυο και στη συνέχεια επεκτείνει την προσέγγισή του από τη συγκεκριμένη συσκευή σε άλλους μέσα στο ίδιο δίκτυο.



Σχήμα 1 Εσωτερική μετακίνηση

Σε οποιοδήποτε δίκτυο, μπορούμε να απεικονίσουμε την περίμετρο με μια οριζόντια γραμμή. Το άνω μισό αντιπροσωπεύει αυτό που βρίσκεται έξω από το δίκτυο, ενώ αυτό που βρίσκεται κάτω από τη γραμμή αντιπροσωπεύει αυτό που είναι μέσα. Για να εισέλθει ένας εισβολέας μέσα στο δίκτυο,

πρέπει να κινηθεί κάθετα, δηλαδή από έξω προς τα μέσα (μερικές φορές αποκαλείται κυκλοφορία Βορρά-Νότου). Αλλά μόλις καθιερωθεί ένα σημείο στήριξης, μπορεί στη συνέχεια να κινηθεί εσωτερικά (ή οριζόντια) μέσα στο δίκτυο για να φτάσει στο στόχο του (μερικές φορές ονομάζεται κυκλοφορία Ανατολής-Δύσης). Συνολικά, υπάρχουν δύο συνήθεις τρόποι με τους οποίους μία απειλή κινείται εσωτερικά. Στην πρώτη προσέγγιση, ο εισβολέας χρησιμοποιεί αυτό που είναι γνωστό ως εσωτερική σάρωση για να μάθει τι άλλα μηχανήματα είναι μέσα στο δίκτυο. Συγκεκριμένα, ανιχνεύει ανοιχτές θύρες δικτύου και μηχανισμούς, οι οποίοι είναι γνωστοί για τις ευπάθειες τους. Σε αυτό το σημείο, ο επιτιθέμενος μπορεί να καταχραστεί αυτές τις αδυναμίες για να μετακινηθεί εσωτερικά σε ένα άλλο σύστημα.

Το δεύτερο μέσο εσωτερικής μετακίνησης εκμεταλλεύεται κλεμμένα διαπιστευτήρια και είναι πιο συνηθισμένο. Σε αυτόν τον τύπο επίθεσης, ο επιτιθέμενος μπορεί να χρησιμοποιήσει ένα ηλεκτρονικό ταχυδρομείο τύπου ηλεκτρονικού "ψαρέματος" για να μολύνει μια μηχανή που διασυνδέεται με έναν συγκεκριμένο διακομιστή.

Ο επιτιθέμενος μπορεί να χρησιμοποιήσει την πρόσβασή του για να εμφανίσει τους κωδικούς πρόσβασης μέσω εργαλείων keylogger και κλοπής κωδικών πρόσβασης όπως το Mimikaz. Στη συνέχεια, μπορεί να χρησιμοποιήσει οποιαδήποτε διαπιστευτήρια ήταν σε θέση να αποκτήσει για να υποδυθεί το θύμα και να συνδεθεί σε άλλο μηχάνημα. Μόλις καθιερώσει την πρόσβαση του σε αυτόν τον υπολογιστή, μπορεί στη συνέχεια να επαναλάβει την τακτική του αναζητώντας πρόσθετα κοινόχρηστα στοιχεία, διαπιστευτήρια ή / και προνόμια που μπορεί να εκμεταλλευτεί και με τη σειρά τους να χρησιμοποιήσει στην προσπάθεια της εγκατάστασης μιας απομακρυσμένης σύνδεσης με τη συσκευή που έχει στοχεύσει.

Σχήμα 2 Κίνηση επιτιθέμενου

Σε αυτό το σημείο αξίζει να αναφέρουμε ότι η εσωτερική μετακίνηση συχνά εκδηλώνεται ως μία ανώμαλη δραστηριότητα του δικτύου. Δηλαδή, είναι ύποπτο όταν ένα μηχάνημα που μιλά συχνά μόνο με συγκεκριμένα τερματικά να ξεκινά μια διεργασία σάρωσης ολόκληρου του δικτύου. Το ίδιο ισχύει και αν τι τερματικό προσπαθήσει να συνδεθεί με ανοιχτές θύρες, να αλληλεπιδράσει με υπηρεσίες διαπιστευτηρίων που συνήθως δεν αλληλεπιδρά ή να χρησιμοποιήσει ένα όνομα χρήστη που δεν έχει χρησιμοποιήσει πριν. Με γενικά λόγια όταν το τερματικό πραγματοποιεί μία ασυνήθιστη διεργασία χωρίς την άδεια του εκάστοτε χρήστη.

3.2 Είδη εσωτερικής μετακίνησης σε ένα Windows σύστημα

Η εσωτερική μετακίνηση αποτελεί μία από τις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να εισάγουν και να ελέγχουν τα απομακρυσμένα συστήματα σε ένα δίκτυο. Ακολουθώντας τον πρωταρχικό στόχο τους, απαιτείται συχνά η εξερεύνηση του δικτύου για να βρεθεί ο στόχος και στη συνέχεια να αποκτήσουν πρόσβαση σε αυτό. Η επίτευξη του στόχου τους συχνά περιλαμβάνει περιστροφή μέσω πολλαπλών συστημάτων και λογαριασμών. Οι επιτιθέμενοι μπορούν να εγκαταστήσουν τα δικά τους εργαλεία απομακρυσμένης πρόσβασης για να επιτύχουν την εσωτερική μετακίνηση ή να χρησιμοποιήσουν νόμιμα διαπιστευτήρια με εγγενή εργαλεία δικτύου και λειτουργικού συστήματος, τα οποία μπορεί να είναι πιο κρυφά.

Παρακάτω θα δούμε αναλυτικότερα τις τεχνικές αυτές για ένα σύστημα με λειτουργικό Windows:

- Λογισμικό ανάπτυξης εφαρμογών (Application deployment software)

Οι επιτιθέμενοι μπορούν να αναπτύξουν κακόβουλο λογισμικό σε συστήματα εντός ενός δικτύου χρησιμοποιώντας συστήματα ανάπτυξης εφαρμογών που χρησιμοποιούνται από τους διαχειριστές. Τα δικαιώματα που απαιτούνται για αυτήν τη δράση ποικίλλουν ανάλογα με τη διαμόρφωση του συστήματος. τα τοπικά διαπιστευτήρια μπορεί να επαρκούν για άμεση πρόσβαση στον εξυπηρετητή ή ενδέχεται να απαιτούνται διαπιστευτήρια συγκεκριμένου τομέα. Ωστόσο, το σύστημα μπορεί να απαιτεί έναν λογαριασμό διαχειριστή για να συνδεθεί ή να εκτελέσει την ανάπτυξη λογισμικού. Η πρόσβαση σε ένα σύστημα ανάπτυξης λογισμικού σε ολόκληρο το δίκτυο επιτρέπει στον επιτιθέμενο να έχει απομακρυσμένη εκτέλεση κώδικα σε όλα τα συστήματα που είναι συνδεδεμένα με αυτό. Η πρόσβαση μπορεί να χρησιμοποιηθεί για την εσωτερική μετάβαση σε συστήματα, τη συγκέντρωση πληροφοριών ή την πρόκληση συγκεκριμένου αποτελέσματος, όπως τη διαγραφή των σκληρών δίσκων σε όλους τους τελικούς προορισμούς.

- Κατανεμημένο μοντέλο αντικειμένων (Distributed Component Object Model)

Το μοντέλο αντικειμένων κατανεμημένων συνιστωσών των Windows (DCOM) είναι ένα μεσαίο λογισμικό που επεκτείνει τη λειτουργικότητα του μοντέλου αντικειμένων Component Object Model (COM) πέρα από έναν τοπικό υπολογιστή που χρησιμοποιεί την τεχνολογία κλήσης εξ αποστάσεως (RPC). Το COM είναι ένα στοιχείο της διεπαφής προγραμματισμού εφαρμογών των Windows (API) που επιτρέπει την αλληλεπίδραση μεταξύ αντικειμένων λογισμικού. Μέσω του COM, ένα αντικείμενο πελάτη μπορεί να καλέσει μεθόδους αντικειμένων διακομιστή, τα οποία είναι συνήθως είτε βιβλιοθήκες δυναμικής σύνδεσης (DLL) είτε εκτελέσιμα αρχεία (EXE).

Τα δικαιώματα αλληλεπίδρασης με τοπικά και απομακρυσμένα αντικείμενα COM του διακομιστή καθορίζονται από τις λίστες ελέγχου πρόσβασης (ACL) στο μητρώο. Από προεπιλογή, μόνο οι διαχειριστές μπορούν να ενεργοποιήσουν από απόσταση και να εκκινήσουν λειτουργίες COM μέσω DCOM. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει το DCOM για εσωτερική μετακίνηση. Μέσω του DCOM, ο επιτιθέμενος που λειτουργεί στο πλαίσιο ενός κατάλληλα προνομιούχου χρήστη μπορεί να αποκτήσει εξ αποστάσεως πρόσβαση και να πραγματοποιήσει άμεση εκτέλεση shellcode μέσω εφαρμογών του Office καθώς και άλλων αντικειμένων των Windows που περιέχουν μη-ασφαλής μεθόδους. Το DCOM μπορεί επίσης να εκτελεί μακροεντολές σε υπάρχοντα έγγραφα και μπορεί επίσης να ζητήσει την λειτουργία εκτέλεσης δυναμικής ανταλλαγής δεδομένων (DDE) απευθείας μέσω ενός στιγμιότυπου COM που δημιουργήθηκε από μια εφαρμογή του Microsoft Office παρακάμπτοντας την ανάγκη ενός κακόβουλου εγγράφου . Το DCOM μπορεί επίσης να εκθέσει λειτουργίες που μπορούν να χρησιμοποιηθούν σε άλλες περιοχές της αλυσίδας των αντιπάλων όπως η προσαύξηση δικαιωμάτων και η διατήρηση αυτών.

- Αξιοποίηση Απομακρυσμένων Υπηρεσιών (Exploitation of remote access)

Η αξιοποίηση ενός ευπαθούς λογισμικού συμβαίνει όταν ο επιτιθέμενος εκμεταλλεύεται ένα σφάλμα προγραμματισμού σε ένα πρόγραμμα, υπηρεσία ή εντός του λογισμικού του λειτουργικού συστήματος ή του ίδιου του πυρήνα για να εκτελέσει κώδικα που ελέγχεται από αυτών. Ένας κοινός στόχος για την μετα-συμβιβαστική αξιοποίηση απομακρυσμένων υπηρεσιών είναι η εσωτερική μετακίνηση για την πρόσβαση σε ένα απομακρυσμένο σύστημα. Ένας επιτιθέμενος μπορεί να χρειαστεί να προσδιορίσει εάν το απομακρυσμένο σύστημα βρίσκεται σε ευάλωτη κατάσταση, το οποίο μπορεί να γίνει μέσω μιας υπηρεσίας σάρωσης δικτύου ή άλλων μεθόδων εξερεύνησης που αναζητούν κοινό ευάλωτο λογισμικό που μπορεί να αναπτυχθεί στο δίκτυο, η εάν υπάρχει έλλειψη ορισμένων επιδιορθώσεων ευπάθειας ή εάν υπάρχει λογισμικό ασφαλείας που μπορεί να χρησιμοποιηθεί για την ανίχνευση ή την απομακρυσμένη εκμετάλλευση.

Οι διακομιστές είναι πιθανώς στόχος υψηλής αξίας για την εκμετάλλευση της εσωτερικής κίνησης, αλλά τα συστήματα παραμέτρων ενδέχεται επίσης να διατρέχουν κίνδυνο εάν παρέχουν πλεονέκτημα ή πρόσβαση σε πρόσθετους πόρους. Υπάρχουν αρκετές γνωστές ευπάθειες που υπάρχουν σε κοινές υπηρεσίες όπως SMB και RDP καθώς και εφαρμογές που μπορούν να χρησιμοποιηθούν σε εσωτερικά δίκτυα όπως MySQL και υπηρεσίες διακομιστή web.

Ανάλογα με το επίπεδο αδειών της ευπρόσβλητης απομακρυσμένης υπηρεσίας, ένας αντίπαλος μπορεί να επιτύχει την επαύξηση των προνομίων ως αποτέλεσμα και της εκμετάλλευσης της εσωτερικής μετακίνησης.

- Είσοδος με σενάρια (Logon scripts)

Τα Windows επιτρέπουν τη δημιουργία σεναρίων σύνδεσης κάθε φορά που ένας συγκεκριμένος χρήστης ή ομάδα χρηστών συνδεθεί σε ένα σύστημα.

Τα σενάρια μπορούν να χρησιμοποιηθούν για την εκτέλεση διαχειριστικών λειτουργιών, οι οποίες μπορεί συχνά να εκτελούν άλλα προγράμματα ή να στέλνουν πληροφορίες σε έναν εσωτερικό διακομιστή καταγραφής. Αν οι αντίπαλοι μπορούν να έχουν πρόσβαση σε αυτά τα σενάρια, ενδέχεται να εισαγάγουν πρόσθετο κώδικα στη δέσμη ενεργειών σύνδεσης για να εκτελέσουν τα εργαλεία τους όταν συνδεθεί ένας χρήστης. Αυτός ο κώδικας μπορεί να τους επιτρέψει να διατηρήσουν σύνδεση σε ένα μόνο όμως σύστημα, αν είναι τοπικό σενάριο ή να μετακινηθούν εσωτερικά σε ένα δίκτυο, αν το σενάριο είναι αποθηκευμένο σε κεντρικό διακομιστή και έχει προωθηθεί σε πολλά συστήματα. Ανάλογα με τη διαμόρφωση πρόσβασης της δέσμης ενεργειών σύνδεσης, ενδέχεται να απαιτούνται είτε τοπικά διαπιστευτήρια είτε ένας λογαριασμός διαχειριστή.

- Παράκαμψη του Hash (Pass the hash)

Η μετάδοση του hash (PtH) είναι μια μέθοδος ελέγχου ταυτότητας του χρήστη χωρίς να έχει πρόσβαση στον κωδικό πρόσβασης του χρήστη σε μορφή κειμένου. Αυτή η μέθοδος παρακάμπτει τα τυπικά βήματα ελέγχου ταυτότητας που απαιτούν έναν κωδικό πρόσβασης σε μορφή κειμένου κειμένου, κινείται απευθείας στο τμήμα του ελέγχου ταυτότητας που χρησιμοποιεί το hash ως κωδικό πρόσβασης. Σε αυτήν την τεχνική, τα έγκυρα hashes των κωδικών πρόσβασης για τον ενεργό λογαριασμό συλλέγονται χρησιμοποιώντας μια τεχνική πρόσβασης εισαγωγής διαπιστευτηρίων (Credential Access). Τα hashes που έχουν συλλεχθεί χρησιμοποιούνται για την μέθοδο PtH για τον έλεγχο ταυτότητας του χρήστη. Μετά την επικύρωση του χρήστη, το PtH μπορεί να χρησιμοποιηθεί για την εκτέλεση ενεργειών σε τοπικά ή απομακρυσμένα συστήματα. Τα Windows 7 και νεότερα με ενημέρωση KB2871997 απαιτούν έγκυρα διαπιστευτήρια απλού χρήστη ή τύπου RID 500 hashes για τον διαχειριστή.

- Παράκαμψη του εισιτηρίου (Pass the ticket)

Η παράκαμψη εισιτηρίου (PtT) είναι μια μέθοδος ελέγχου ταυτότητας σε ένα σύστημα που χρησιμοποιεί εισιτήρια Kerberos χωρίς να έχει πρόσβαση στον κωδικό πρόσβασης ενός λογαριασμού. Ο έλεγχος ταυτότητας Kerberos μπορεί να χρησιμοποιηθεί ως το πρώτο βήμα για την εσωτερική μετακίνηση σε ένα απομακρυσμένο σύστημα. Σε αυτήν την τεχνική, τα έγκυρα εισιτήρια Kerberos για τους έγκυρους λογαριασμούς καταγράφονται από το Dumped Credential. Μπορούν να ληφθούν εισιτήρια υπηρεσίας χρήστη ή εισιτήριο για έκδοση εισιτηρίων (TGT), ανάλογα με το επίπεδο πρόσβασης. Ένα εισιτήριο υπηρεσίας επιτρέπει την πρόσβαση σε έναν συγκεκριμένο πόρο, ενώ ένα TGT μπορεί να χρησιμοποιηθεί για να ζητήσει εισιτήρια υπηρεσιών από την Υπηρεσία Εισιτηρίων (TGS) για πρόσβαση σε οποιονδήποτε πόρο ο χρήστης έχει δικαιώματα πρόσβασης. Ασημένια εισιτήρια μπορούν να ληφθούν για υπηρεσίες που χρησιμοποιούν το Kerberos ως μηχανισμό ελέγχου ταυτότητας και χρησιμοποιούνται για τη δημιουργία εισιτηρίων για την πρόσβαση σε αυτόν τον συγκεκριμένο πόρο και στο σύστημα που φιλοξενεί τον πόρο (π.χ. SharePoint).

Χρυσά εισιτήρια μπορούν να αποκτηθούν για τον τομέα χρησιμοποιώντας το λογαριασμό Κλειδί Διανομής KRBTGT λογαριασμού NTLM hash, το οποίο επιτρέπει την δημιουργία TGT για οποιοδήποτε λογαριασμό στην υπηρεσία καταλόγου Active Directory.

- Πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας (Remote desktop protocol)

Η απομακρυσμένη επιφάνεια εργασίας είναι μια κοινή λειτουργία στα λειτουργικά συστήματα. Επιτρέπει σε έναν χρήστη να συνδεθεί σε μια διαδραστική συνεδρία με ένα γραφικό περιβάλλον σε ένα απομακρυσμένο σύστημα. Η Microsoft αναφέρεται στην εφαρμογή του Remote Desktop Protocol (RDP) ως Remote Desktop Services (RDS). Υπάρχουν και άλλες εφαρμογές και εργαλεία τρίτων που παρέχουν γραφική πρόσβαση σε απομακρυσμένες υπηρεσίες παρόμοιες με το RDS. Ο επιτιθέμενος μπορεί να συνδεθεί σε ένα απομακρυσμένο σύστημα μέσω του RDP / RDS για να επεκτείνει την

πρόσβαση εάν η υπηρεσία είναι ενεργοποιημένη και επιτρέπει πρόσβαση σε λογαριασμούς με γνωστά διαπιστευτήρια. Ο επιτιθέμενος πιθανότατα θα χρησιμοποιήσει τεχνικές πρόσβασης πιστοποίησης για να αποκτήσει τα διαπιστευτήρια που θα χρησιμοποιήσει με το RDP. Μπορεί επίσης να χρησιμοποιήσει το RDP σε συνδυασμό με την τεχνική προσβασιμότητας για την παραμονή του στο σύστημα. Ο επιτιθέμενος μπορεί επίσης να εκτελέσει αεροπειρατεία της συνόδου RDP, η οποία συνεπάγεται με την κλοπή της απομακρυσμένης περιόδου λειτουργίας ενός νόμιμου χρήστη. Συνήθως, ένας χρήστης ειδοποιείται όταν κάποιος άλλος προσπαθεί να κλέψει την αίτησή του και να σας ζητήσει μια ερώτηση.

Με δικαιώματα συστήματος και με χρήση της κονσόλας Terminal Services Console, c: \ windows \ system32 \ tscon.exe [αριθμός συνεδρίασης που πρόκειται να κλαπεί], ένας αντίπαλος μπορεί να καταλάβει μια συνεδρία χωρίς να χρειαστεί πιστοποιήσεις ή υποδείξεις προς τον χρήστη.

Αυτό μπορεί να γίνει εξ αποστάσεως ή τοπικά και με ενεργές ή αποσυνδεδεμένες συνεδρίες. Μπορεί επίσης να οδηγήσει σε απομάκρυνση αποκλεισμένου συστήματος και σε εξέλιξη των προνομίων του, κλέβοντας έναν λογαριασμό διαχειριστή ή ακόμα υψηλότερο. Όλα αυτά μπορούν να γίνουν με τη χρήση εγγενών εντολών των Windows, καθώς επίσης και μέσω του εργαλείου RedSnarf στο οποίο έχει προστεθεί ως χαρακτηριστικό.

- Απομακρυσμένη αντιγραφή αρχείου (Remote file copy)

Τα αρχεία μπορούν να αντιγραφούν από το ένα σύστημα στο άλλο για να οργανώσουν τα εργαλεία του επιτιθέμενου ή άλλα αρχεία κατά τη διάρκεια μιας ενέργειας. Τα αρχεία μπορούν να αντιγραφούν από ένα εξωτερικό ελεγχόμενο από τον επιτιθέμενο σύστημα μέσω του καναλιού Command and Control για να φέρουν εργαλεία στο δίκτυο του θύματος ή μέσω εναλλακτικών πρωτοκόλλων με άλλα εργαλεία όπως το FTP.

Οι επιτιθέμενοι μπορούν επίσης να αντιγράψουν τα αρχεία εσωτερικά μεταξύ των εσωτερικών συστημάτων του θύματος για να υποστηρίξουν την εσωτερική μετακίνηση με απομακρυσμένη εκτέλεση χρησιμοποιώντας εγγενή πρωτόκολλα κοινής χρήσης αρχείων, όπως κοινή χρήση αρχείων μέσω SMB με συνδεδεμένα δίκτυα ή με επαληθευμένες συνδέσεις με τα Windows Admin Shares ή το Remote Desktop Protocol.

- Απομακρυσμένες υπηρεσίες (Remote services)

Ο επιτιθέμενος μπορεί να χρησιμοποιήσει τους έγκυρους λογαριασμούς για να συνδεθεί σε μια υπηρεσία ειδικά σχεδιασμένη για να δέχεται απομακρυσμένες συνδέσεις, όπως telnet, SSH και VNC. Ο αντίπαλος μπορεί στη συνέχεια να εκτελέσει ενέργειες ως συνδεδεμένος χρήστης.

- Αντιγραφή μέσω αφαιρούμενων μέσων (Replication through removable media)

Ο επιτιθέμενος μπορεί να μετακινηθεί σε συστήματα, πιθανώς σε δίκτυα που έχουν αποσυνδεθεί ή έχουν κενά αέρα, αντιγράφοντας κακόβουλα προγράμματα σε αφαιρούμενα μέσα και εκμεταλλευόμενος τις δυνατότητες του Authorun όταν τα μέσα εισάγονται σε ένα σύστημα και εκτελούνται.

Στην περίπτωση εσωτερικής μετακίνησης, αυτό μπορεί να συμβεί με τροποποίηση εκτελέσιμων αρχείων που είναι αποθηκευμένα σε αφαιρούμενα μέσα ή με αντιγραφή κακόβουλου λογισμικού και μετονομασία για να μοιάζει με ένα νόμιμο αρχείο για να εξαπατήσουν τους χρήστες να το εκτελέσουν σε ξεχωριστό σύστημα.

Στην αρχική πρόσβαση, αυτό μπορεί να συμβεί με το χειροκίνητο χειρισμό των μέσων, την τροποποίηση των συστημάτων που χρησιμοποιήθηκαν για την αρχική διαμόρφωση του μέσου ή την τροποποίηση του ίδιου του υλικολογισμικού των μέσων.

- Κοινόχρηστο webroot (Shared waebroot)

Ο επιτιθέμενος μπορεί να προσθέσει κακόβουλο περιεχόμενο σε έναν ιστότοπο που είναι προσβάσιμος από το διαδίκτυο μέσω ενός κοινόχρηστου αρχείου ανοιχτού δικτύου το οποίο περιέχει τον κατάλογο webroot του ιστότοπου ή τον ιστότοπο περιεχομένου ιστού και, στη συνέχεια, το θύμα περιηγείται σε αυτό το περιεχόμενο με ένα πρόγραμμα περιήγησης στο Web για να αναγκάσει τον διακομιστή να εκτελέσει το κακόβουλο περιεχόμενο. Το κακόβουλο περιεχόμενο συνήθως θα

εκτελείται υπό τα πλαίσια και τα δικαιώματα της διαδικασίας του διακομιστή Web, συχνά οδηγώντας σε τοπικά δικαιώματα συστήματος ή διαχειριστή, ανάλογα με τον τρόπο διαμόρφωσης του διακομιστή Web. Αυτός ο μηχανισμός κοινής πρόσβασης και απομακρυσμένης εκτέλεσης θα μπορούσε να χρησιμοποιηθεί για εσωτερική μετακίνηση στο σύστημα που εκτελεί το διακομιστή Web. Για παράδειγμα, ένας διακομιστής Web που εκτελεί PHP με ανοιχτό κοινόχρηστο δίκτυο θα μπορούσε να επιτρέψει σε έναν αντίπαλο να φορτώσει ένα εργαλείο απομακρυσμένης πρόσβασης και ένα script PHP για να εκτελέσει το RAT στο σύστημα που εκτελεί τον διακομιστή Web όταν επισκέπτεται μια συγκεκριμένη σελίδα.

- Ουσιαστικό κοινόχρηστο περιεχόμενο (Taint shared content)

Το περιεχόμενο που είναι αποθηκευμένο σε μονάδες δικτύου ή σε άλλες κοινόχρηστες τοποθεσίες ενδέχεται να παραβιαστεί προσθέτοντας κακόβουλα προγράμματα, δέσμες ενεργειών ή εκμεταλλευόμενο κώδικα σε έγκυρα αρχεία. Μόλις ένας χρήστης ανοίξει το κοινόχρηστο περιεχόμενό του, το κακόβουλο τμήμα μπορεί να εκτελεστεί για να εκτελέσει τον κώδικα του επιτιθέμενου σε ένα απομακρυσμένο σύστημα. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει το πλαστό κοινόχρηστο περιεχόμενο για να μετακινηθεί εσωτερικά. Ένας άξονας κοινής χρήσης καταλόγου είναι μια παραλλαγή αυτής της τεχνικής που χρησιμοποιεί αρκετές άλλες τεχνικές για τη διάδοση κακόβουλου λογισμικού όταν οι χρήστες έχουν πρόσβαση σε έναν κοινόχρηστο κατάλογο δικτύου. Χρησιμοποιεί την τροποποίηση συντομεύσεων των αρχείων .LNK του καταλόγου που χρησιμοποιούν την μεταμφίεση (Masquerading) για να μοιάζουν με τους πραγματικούς καταλόγους, οι οποίοι είναι κρυμμένοι μέσω στα κρυφά αρχεία και καταλόγους. Οι κακόβουλοι κατάλογοι .LNK έχουν μια ενσωματωμένη εντολή που εκτελεί το κρυφό αρχείο κακόβουλου λογισμικού στον κατάλογο και, στη συνέχεια, ανοίγει τον πραγματικό κατάλογο που το θύμα επιθυμεί, έτσι ώστε να εμφανίζεται η αναμενόμενη ενέργεια του χρήστη. Όταν η παραπάνω ενέργεια χρησιμοποιείται με τους καταλόγους δικτύου, το οποίο είναι αρκετά συχνό γεγονός, η τεχνική μπορεί να έχει ως αποτέλεσμα συχνές επαναλήψεις και ευρεία πρόσβαση σε συστήματα και ενδεχομένως σε νέους λογαριασμούς υψηλότερων προνομίων.

- Λογισμικό τρίτων (Third-party software)

Οι εφαρμογές τρίτων και τα συστήματα ανάπτυξης λογισμικού ενδέχεται να χρησιμοποιούνται στο περιβάλλον δικτύου για σκοπούς διαχείρισης (π.χ. SCCM, VNC, HBSS, Altiris κ.λπ.). Εάν ένας επιτιθέμενος αποκτήσει πρόσβαση σε αυτά τα συστήματα, τότε μπορεί να είναι σε θέση να εκτελέσει κώδικα. Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση και να χρησιμοποιήσει συστήματα ανάπτυξης εφαρμογών τρίτων κατασκευαστών εγκατεστημένα σε ένα δίκτυο. Η πρόσβαση σε ένα σύστημα ανάπτυξης λογισμικού σε ολόκληρο το δίκτυο επιτρέπει σε έναν επιτιθέμενο να έχει απομακρυσμένη εκτέλεση κώδικα σε όλα τα συστήματα που είναι συνδεδεμένα σε ένα τέτοιο σύστημα. Η πρόσβαση μπορεί να χρησιμοποιηθεί για την εσωτερική μετάβαση σε συστήματα, τη συγκέντρωση πληροφοριών ή την πρόκληση συγκεκριμένου αποτελέσματος, όπως τη διαμόρφωση των σκληρών δίσκων σε όλα τα τελικά τερματικά. Τα δικαιώματα που απαιτούνται για αυτήν τη δράση ποικίλλουν ανάλογα με τη διαμόρφωση του συστήματος. τα τοπικά διαπιστευτήρια μπορεί να επαρκούν με άμεση πρόσβαση στον εξυπηρετητή ανάπτυξης ή ενδέχεται να απαιτούνται διαπιστευτήρια συγκεκριμένου χρήστη. Ωστόσο, το σύστημα μπορεί να απαιτεί έναν λογαριασμό διαχειριστή για να συνδεθεί ή να εκτελέσει το λογισμικό.

- Μερίδια λογαριασμού διαχειριστή των Windows (Windows admin shares)

Τα συστήματα των Windows έχουν κρυφά κοινόχρηστα στοιχεία του δικτύου τα οποία είναι προσβάσιμα μόνο σε διαχειριστές και παρέχουν τη δυνατότητα απομακρυσμένης αντιγραφής αρχείων και άλλων διαχειριστικών λειτουργιών. Τα παραδείγματα μεριδίων δικτύου περιλαμβάνουν C $, ADMIN $ και IPC $. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει αυτήν την τεχνική σε συνδυασμό με τους έγκυρους λογαριασμούς σε επίπεδο διαχειριστή για να αποκτήσει απομακρυσμένη πρόσβαση σε ένα σύστημα δικτύου μέσω του διακομιστή SMB ώστε να αλληλοεπιδράσει με συστήματα που χρησιμοποιούν κλήσεις απομακρυσμένης διαδικασίας (RPC) και να εκτελέσει δυαδικά αρχεία μέσω απομακρυσμένης εκτέλεσης.

Οι τεχνικές εκτέλεσης παραδειγμάτων που βασίζονται σε επικυρωμένες περιόδους σύνδεσης μέσω SMB / RPC είναι η προγραμματισμένη εργασία, η εκτέλεση υπηρεσίας και τα εργαλεία διαχείρισης των Windows. Ο επιτιθέμενος μπορεί επίσης να χρησιμοποιήσει τα hashes του NTLM για να αποκτήσει πρόσβαση σε διαχειριστές κοινών μεριδίων σε συστήματα με την τεχνική Pass the Hash και σε ορισμένα επίπεδα διαμόρφωσης και επιδιορθώσεων. Το βοηθητικό πρόγραμμα Net μπορεί να χρησιμοποιηθεί για να συνδεθεί με τα Windows admin shares σε απομακρυσμένα συστήματα χρησιμοποιώντας εντολές net use με έγκυρα πιστοποιητικά.

- Απομακρυσμένη διαχείριση παραθύρων (Windows remote management)

Η απομακρυσμένη διαχείριση των Windows (WinRM) είναι το όνομα μιας υπηρεσίας των Windows και ενός πρωτοκόλλου που επιτρέπει σε ένα χρήστη να αλληλοεπιδρά με ένα απομακρυσμένο σύστημα (π.χ. να εκτελέσει ένα εκτελέσιμο αρχείο, να τροποποιήσει το μητρώο, να τροποποιήσει τις υπηρεσίες). Μπορεί να καλείται με την εντολή winrm ή με οποιοδήποτε αριθμό προγραμμάτων, όπως το PowerShell.

3.3 Ανίχνευση της εσωτερικής μετακίνησης

Σε αυτό το κεφάλαιο θα περιγράψουμε το πως μπορεί κάποιος να ανιχνεύσει τεχνικές εσωτερικής μετακίνησης στο σύστημα του. Για να γίνει αυτό θα πρέπει να μπούμε στο μυαλό του επιτιθέμενου και να κατανοήσουμε τον τρόπο σκέψης αλλά και το τι ψάχνει.

- Κατανόηση του δικτύου.

Η κατανόηση των χαρακτηριστικών που βασίζονται στο δίκτυο πριν από μια επίθεση εσωτερικής μετακίνησης μπορεί να βοηθήσει στην ταυτοποίηση μιας τέτοιας επίθεσης. Τα εργαλεία ανάλυσης πακέτων μπορούν να βοηθήσουν στην αναγνώριση των χαρακτηριστικών του δικτύου, τα οποία μπορούν στη συνέχεια να βοηθήσουν τους αναλυτές ασφαλείας να απαντήσουν σε ερωτήσεις σχετικά με ένα δίκτυο: ποιες συσκευές επικοινωνούν, πώς εντοπίζονται, πού βρίσκονται, όταν συμβαίνει πραγματική επικοινωνία με το σύστημα. Είναι επίσης σημαντικό να κατανοήσουμε τις τεχνικές που οι επιτιθέμενοι χρησιμοποιούν για να αποκρύψουν τις ενέργειες τους και να παρακάμψουν τις κοινές τεχνολογίες ασφάλειας του δικτύου, προκειμένου να εντοπίσουμε καλύτερα τις επιθέσεις εσωτερικής μετακίνησης.

- Κυνήγι απειλής

Το κυνήγι της απειλής είναι ένα σημαντικό μέρος της ανίχνευσης της εσωτερικής μετακίνησης, καθώς δίνει τη δυνατότητα στους αναλυτές ασφαλείας να διερευνήσουν δυναμικά τη δραστηριότητα του δικτύου για να εντοπίσουν τις ανωμαλίες που δεν ανιχνεύουν άλλες μέθοδοι ανίχνευσης. Όπως αναφέρθηκε παραπάνω, οι περισσότερες τεχνολογίες ανίχνευσης αποφεύγουν να ειδοποιούν για πιθανή εσωτερική μετακίνηση λόγω του θορύβου που μπορεί να δημιουργήσει. Ως εκ τούτου, το κυνήγι απειλών είναι ο μόνος αποτελεσματικός τρόπος για να διαφοροποιήσουμε την αληθινή εσωτερική μετακίνηση από την κανονική δικτυακή δραστηριότητα.

- Αναγνώριση

Πολλοί επιτιθέμενοι χρησιμοποιούν τα RAT (εργαλεία απομακρυσμένης πρόσβασης) για να συνδεθούν από απόσταση στους υπολογιστές, να αποκτήσουν πρόσβαση και να ξεκινήσουν μια επίθεση εσωτερικής μετακίνησης. Πολλά εργαλεία απομακρυσμένης πρόσβασης χρησιμοποιούνται νόμιμα και δεν θεωρούνται κακόβουλα προγράμματα. Ωστόσο, αυτά τα εργαλεία παρακάμπτουν ενεργά τους ελέγχους δικτύου, αποκρύπτοντας ποια μέρη επικοινωνούν, πότε και πώς.

Αυτή η ικανότητα λειτουργίας κάτω από το ραντάρ είναι ελκυστική για κακόβουλους και εσωτερικούς επιτιθέμενους. Το επόμενο βήμα στην εσωτερική μετακίνηση είναι η αναγνώριση: η παρατήρηση, η εξερεύνηση και η χαρτογράφηση του δικτύου, των χρηστών και των συσκευών του. Αυτός ο χάρτης επιτρέπει στους επιτιθέμενους να κάνουν ενημερωμένες κινήσεις, να κατανοούν τους κανόνες ονοματολογίας και την ιεραρχία δικτύων και να εντοπίζουν τα πιθανά ωφέλιμα φορτία.

- Διαπιστευτήρια και προνόμια

Για να μετακινηθούν μέσω ενός δικτύου, οι επιτιθέμενοι πρέπει να συγκεντρώσουν τα απαιτούμενα στοιχεία σύνδεσης. Τα στοιχεία αυτά, μπορούν να συγκεντρωθούν χρησιμοποιώντας μια ποικιλία εργαλείων, όπως keyloggers και αναλυτές πρωτοκόλλων. Οι τακτικές κοινωνικής μηχανικής όπως οι επιθέσεις τυπογραφίας και phishing μπορούν επίσης να χρησιμοποιηθούν για να εξαπατήσουν τους χρήστες και να μοιραστούν τα διαπιστευτήρια σύνδεσης. Μια άλλη μέθοδος είναι η βίαιη επίθεση (brute force), όπου ένας εγκληματίας ουσιαστικά μαντεύει έναν κωδικό πρόσβασης, χρησιμοποιώντας μια πισίνα από πιθανούς κωδικούς, και τον χρησιμοποιεί για την κλοπή των δεδομένων. Προκειμένου να μετριαστούν οι επιθέσεις εσωτερικής μετακίνησης, οι αναλυτές ασφαλείας πρέπει να δημιουργήσουν εσωτερική ευφυΐα δικτύων για να γνωρίζουν ποιοι χρήστες και συσκευές βρίσκονται εντός του δίκτυού και τυπικά μοτίβα εισόδου για να υποδείξουν πότε πραγματοποιείται η κατάχρηση των διαπιστευτηρίων.

- Απόκτηση πρόσβασης

Μόλις ένας επιτιθέμενος έχει χαρτογραφήσει ένα δίκτυο και έχει μια σειρά κωδικών πρόσβασης και προνομίων, μπορεί να διεισδύσει πλήρως και να κινηθεί μέσω του δικτύου. Σε αυτό το στάδιο απαιτείται εξελιγμένη λογική ανίχνευσης (βασισμένη στις συμπεριφορές που συνήθως παρατηρούνται στο περιβάλλον, καθώς και γενικότερη ανίχνευση συγκεκριμένων πρωτοκόλλων, για παράδειγμα, σφάλματα Kerberos) για να εντοπιστούν απειλές που μπορούν εύκολα να ενεργήσουν κάτω από το ραντάρ.

3.4 Αντιμετώπιση των τεχνικών εσωτερικής μετακίνησης σε ένα σύστημα Windows.

Στη συνέχεια θα αναλύσουμε κάποιες τεχνικές αντιμετώπισης των παραπάνω τεχνικών εσωτερικής μετακίνησης:

- **Λογισμικό ανάπτυξης εφαρμογών (Application deployment software)**

Παρακολουθούμε τις εφαρμογές ανάπτυξης από ένα δευτερεύον σύστημα. Εκτελούμε την ανάπτυξη εφαρμογών σε τακτά χρονικά διαστήματα, ώστε να ξεχωρίζει η δραστηριότητα παράνομης ανάπτυξης. Παρακολουθούμε τη δραστηριότητα της διαδικασίας που δεν συσχετίζεται με το γνωστό λογισμικό. Παρακολουθούμε τη δραστηριότητα του συνδεδεμένου λογαριασμού στο σύστημα.

Μετρίαση	Περιγραφή
Υπογραφή κώδικα : Προστασία της ακεραιότητας του δυαδικού συστήματος και των εφαρμογών με επαλήθευση ψηφιακής υπογραφής για να αποτρέψουμε την εκτέλεση του μη αξιόπιστου κώδικα.	Εάν το σύστημα ανάπτυξης εφαρμογών μπορεί να παραμετροποιήσεις ώστε να παράγει μόνο υπογεγραμμένα δυαδικά αρχεία, βεβαιωνόμαστε ότι τα αξιόπιστα πιστοποιητικά υπογραφής δεν βρίσκονται μαζί με το σύστημα ανάπτυξης εφαρμογών. Αντίθετα βρίσκονται σε ένα σύστημα στο οποίο δεν είναι δυνατή η πρόσβαση από απόσταση ή η απομακρυσμένη πρόσβαση είναι αυστηρά ελεγχόμενη.
Έλεγχος ταυτοποίησης πολλαπλών παραγόντων: Χρησιμοποιούμε δύο ή περισσότερα στοιχεία για να πιστοποιήσουμε την ταυτότητά μας σε ένα σύστημα. Όπως το όνομα χρήστη και ο κωδικός πρόσβασης τα οποία όμως παράγονται είτε από μία φυσική έξυπνη κάρτα είτε από μία γεννήτρια συμβόλων.	Χρησιμοποιούμε έλεγχο ταυτότητας πολλαπλών παραγόντων για λογαριασμούς που χρησιμοποιούνται με διάφορα λογισμικά εφαρμογών.

Τμηματοποίηση δικτύου: Αρχιτεκτονικά τμήματα του δικτύου για την απομόνωση κρίσιμων συστημάτων, λειτουργιών ή πόρων. Χρησιμοποιούμε φυσική και λογική κατάτμηση για να αποτρέψουμε την πρόσβαση σε δυνητικά ευαίσθητα συστήματα και πληροφορίες. Χρησιμοποιούμε ένα DMZ για να περιέχει οποιεσδήποτε υπηρεσίες στο διαδίκτυο που δεν πρέπει να εκτίθενται από το εσωτερικό δίκτυο.	Εξασφαλίζουμε τη σωστή απομόνωση συστημάτων και της πρόσβασης για κρίσιμα συστήματα δικτύου μέσω της χρήσης τείχους προστασίας, διαχωρισμό προνομίων λογαριασμού, πολιτική ομάδας και ελέγχου ταυτότητας πολλαπλών παραγόντων.
Διαχείριση προνομίων λογαριασμού: Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	Αποκτούμε πρόσβαση σε συστήματα εφαρμογών μόνο με περιορισμένο αριθμό εξουσιοδοτημένων διαχειριστών. Βεβαιωνόμαστε ότι τα διαπιστευτήρια λογαριασμού που μπορούν να χρησιμοποιηθούν για την πρόσβαση σε συστήματα ανάπτυξης είναι μοναδικά και δεν χρησιμοποιούνται σε όλο το δίκτυο.
Ενημέρωση λογισμικού: Εκτελούμε τακτικές ενημερώσεις λογισμικού για να μετριάσουμε τον κίνδυνο εκμετάλλευσης.	Εγκαθιστούμε τακτικά στα συστήματα ανάπτυξης τις ενημερώσεις των εκδόσεων για να αποτρέψουμε πιθανή απομακρυσμένη πρόσβαση μέσω της εκμετάλλευσης της εξέλιξης των προνομίων.

- **Κατανεμημένο μοντέλο αντικειμένων (Distributed Component Object Model)**

Παρακολουθούμε αντικείμενα COM που φορτώνουν αρχεία DLL και άλλα στοιχεία που συνήθως δεν σχετίζονται με την εφαρμογή.

Παρακολουθούμε την αναπαραγωγή των διαδικασιών που σχετίζονται με αντικείμενα COM, ειδικά αυτές που επικαλείται ένας χρήστης διαφορετικός από αυτόν που είναι συνδεδεμένος αυτήν τη στιγμή.

Παρακολουθούμε την εισροή επισκεψιμότητας του Distributed Computing Environment / Remote Call Call (DCE / RPC).

Μετρίαση	Περιγραφή
Απομόνωση εφαρμογών και Sandboxing : Περιορίζουμε την εκτέλεση κώδικα σε ένα εικονικό περιβάλλον στο τελικό τερματικό.	Βεβαιωνόμαστε ότι είναι ενεργοποιημένες όλες οι ειδοποιήσεις COM και η προστατευμένη προβολή.
Απενεργοποίηση ή κατάργηση των δυνατοτήτων ή του προγράμματος: Καταργούμε ή αποκλείουμε την πρόσβαση σε περιττά και δυνητικά ευάλωτα λογισμικά για να αποτρέψουμε την κατάχρηση τους από των επιτιθέμενο.	Εξετάζουμε την απενεργοποίηση του DCOM μέσω του Dcomcnfg.exe.
Τμηματοποίηση δικτύου: Αρχιτεκτονικά τμήματα του δικτύου για την απομόνωση κρίσιμων συστημάτων, λειτουργιών ή πόρων. Χρησιμοποιούμε	Ενεργοποιούμε το τείχος προστασίας των Windows, το οποίο αποτρέπει τη λειτουργία DCOM από προεπιλογή.

φυσική και λογική κατάτμηση για να αποτρέψουμε την πρόσβαση σε δυνητικά ευαίσθητα συστήματα και πληροφορίες. Χρησιμοποιούμε ένα DMZ για να περιέχει οποιεσδήποτε υπηρεσίες στο διαδίκτυο που δεν πρέπει να εκτίθενται από το εσωτερικό δίκτυο.	
Διαχείριση προνομίων λογαριασμού: Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	Τροποποιούμε τις ρυθμίσεις του μητρώου (απευθείας ή χρησιμοποιώντας το Dcomcnfg.exe) στο HKEY_LOCAL_MACHINE \ SOFTWARE \ Classes \ AppID \ {{AppID_GUID}}) που σχετίζεται με την ασφάλεια ολόκληρης της διαδικασίας των επιμέρους εφαρμογών COM. Τροποποιούμε τις ρυθμίσεις μητρώου (απευθείας ή χρησιμοποιώντας Dcomcnfg.exe) στο HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Ole) που σχετίζεται με τις προεπιλογές ασφαλείας ολόκληρου του συστήματος για όλες τις εφαρμογές COM που δεν εξασφαλίζουν τη δική τους ασφάλεια σε επίπεδο διαδικασίας.

- **Αξιοποίηση Απομακρυσμένων Υπηρεσιών (Exploitation of remote access)**

Η ανίχνευση της εκμετάλλευσης λογισμικού μπορεί να είναι δύσκολη, ανάλογα με τα διαθέσιμα εργαλεία. Τα προγράμματα εκμετάλλευσης λογισμικού ενδέχεται να μην είναι πάντοτε επιτυχημένα ή μπορεί να προκαλέσουν την ασταθή διεργασία ή τη συντριβή της εκμεταλλευόμενης διαδικασίας. Επίσης, αναζητήστε συμπεριφορά στο σύστημα του τελικού τερματικού που μπορεί να υποδηλώνει κίνδυνο, όπως είναι η μη φυσιολογική συμπεριφορά των διαδικασιών. Αυτό θα μπορούσε να περιλαμβάνει ύποπτα αρχεία που έχουν εγγραφεί στο δίσκο, αποδείξεις για παρεμβολές συστήματος για απόκρυψη της εκτέλεσης των αρχείων, αποδεικτικά για αναζήτηση ή άλλης ασυνήθιστης κυκλοφορίας δικτύου που μπορεί να υποδεικνύει πρόσθετα εργαλεία που μεταφέρονται μέσα στο σύστημα.

Μετρίαση	Περιγραφή
Απομόνωση εφαρμογών και Sandboxing : Περιορίζουμε την εκτέλεση κώδικα σε ένα εικονικό περιβάλλον στο τελικό τερματικό.	Καταστούμε δύσκολο για τον επιτιθέμενο να προωθήσει τη λειτουργία του μέσω της εκμετάλλευσης ανεξερεύνητων ή μη ενημερωμένων τρωτών σημείων χρησιμοποιώντας sandboxing. Άλλοι τύποι virtualization και microsegmentation εφαρμογών μπορεί επίσης να μετριάσουν την επίδραση ορισμένων τύπων εκμετάλλευσης. Οι κίνδυνοι πρόσθετων εκμεταλλεύσεων και αδυναμιών σε αυτά τα συστήματα ενδέχεται να εξακολουθούν να υπάρχουν.
Απενεργοποίηση ή κατάργηση των δυνατοτήτων ή του προγράμματος:	Ελαχιστοποιούμε τις διαθέσιμες υπηρεσίες μόνο σε εκείνες που είναι απαραίτητες.

Καταργούμε ή αποκλείουμε την πρόσβαση σε περιττά και δυνητικά ευάλωτα λογισμικά για να αποτρέψουμε την κατάχρηση τους από των επιτιθέμενο.	
Απόκτηση προστασίας: Χρησιμοποιούμε τις δυνατότητες για την ανίχνευση και την παρεμπόδιση των συνθηκών που μπορεί να οδηγήσουν ή να είναι ενδεικτικές για την εκμετάλλευση λογισμικού.	Οι εφαρμογές ασφαλείας που αναζητούν συμπεριφορά που χρησιμοποιείται κατά την εκμετάλλευση, όπως το Windows Defender Exploit Guard (WDEG) και το Εργαλείο βελτίωσης της εμπειρίας μετριασμού (EMET) μπορούν να χρησιμοποιηθούν για να μετριάσουν κάποια συμπεριφορά εκμετάλλευσης. Ο έλεγχος της ακεραιότητας ροής ελέγχου είναι ένας άλλος τρόπος για την πιθανή αναγνώριση και διακοπή της εκμετάλλευσης λογισμικού. Πολλές από αυτές τις προστασίες εξαρτώνται από την αρχιτεκτονική και στοχεύουν στο δυαδικό σύστημα των εφαρμογών για συμβατότητα και μπορεί να μην λειτουργεί για όλα τα λογισμικά ή για όλες τις στενευμένες υπηρεσίες.
Τμηματοποίηση δικτύου: Αρχιτεκτονικά τμήματα του δικτύου για την απομόνωση κρίσιμων συστημάτων, λειτουργιών ή πόρων. Χρησιμοποιούμε φυσική και λογική κατάτμηση για να αποτρέψουμε την πρόσβαση σε δυνητικά ευαίσθητα συστήματα και πληροφορίες. Χρησιμοποιούμε ένα DMZ για να περιέχει οποιεσδήποτε υπηρεσίες στο διαδίκτυο που δεν πρέπει να εκτίθενται από το εσωτερικό δίκτυο.	Τμηματοποιούμε τα δίκτυα και τα συστήματα κατάλληλα για να μειώσουμε την πρόσβαση σε κρίσιμα συστήματα και υπηρεσίες ώστε να έχουμε ελεγχόμενες μεθόδους.
Διαχείριση προνομίων λογαριασμού: Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	Ελαχιστοποιούμε τα δικαιώματα και την πρόσβαση για λογαριασμούς υπηρεσίας για να περιορίσουμε τις επιπτώσεις της εκμετάλλευσης.
Πρόγραμμα ακεραιότητας απειλών: Ένα πρόγραμμα πληροφοριών για απειλές βοηθά έναν οργανισμό να δημιουργήσει τις δικές του καταγραφές πληροφοριών απειλής και να παρακολουθήσει τις τάσεις και να ενημερώσει τις αμυντικές προτεραιότητες ώστε να μετριάσει τον κίνδυνο.	Δημιουργούμε μια ισχυρή καταγραφή πληροφοριών σχετικά με απειλές στον κυβερνοχώρο για να καθορίσουμε ποιοι τύποι και τα επίπεδα της απειλής τα οποία μπορούν να χρησιμοποιούν τα προγράμματα εκμετάλλευσης λογισμικού.
Ενημέρωση λογισμικού: Εκτελούμε τακτικές ενημερώσεις λογισμικού για να μετριάσουμε τον κίνδυνο εκμετάλλευσης.	Ενημερώνουμε τακτικά το λογισμικό χρησιμοποιώντας τη διαχείριση των ενημερώσεων κώδικα για εσωτερικά σημεία και διακομιστές.

Σαρώσεις για ευπάθειες: Η σάρωση ευπάθειας χρησιμοποιείται για την εύρεση πιθανών εκμεταλλεύσιμων ευπαθειών λογισμικού και την αποκατάστασή τους.	Ελέγχουμε τακτικά το εσωτερικό δίκτυο για διαθέσιμες υπηρεσίες και για τον εντοπισμό νέων ενδεχομένως ευάλωτων υπηρεσιών.

- **Είσοδος με σενάρια (Logon scripts)**

Παρακολουθούμε σενάρια σύνδεσης για ασυνήθιστη πρόσβαση από μη φυσιολογικούς χρήστες ή σε μη φυσιολογικές ώρες. Αναζητούμε αρχεία που έχουν προστεθεί ή τροποποιηθεί από ασυνήθιστους λογαριασμούς εκτός των συνηθισμένων διοικητικών καθηκόντων.

Μετρίαση	Περιγραφή
Περιορισμός στα δικαιώματα αρχείων και καταλόγου: Περιορίζουμε την πρόσβαση ρυθμίζοντας δικαιώματα καταλόγου και αρχείων που δεν αφορούν συγκεκριμένους χρήστες ή προνομιούχους λογαριασμούς.	Περιορίζουμε την πρόσβαση εγγραφής σε δέσμες ενεργειών σύνδεσης σε συγκεκριμένους διαχειριστές.

- **Παράκαμψη του Hash (Pass the hash)**

Ελέγχουμε όλα τα συμβάντα χρήσης συνδέσεων και διαπιστευτηρίων και εξετάζουμε εάν υπάρχουν αποκλίσεις. Οι ασυνήθιστες απομακρυσμένες συνδέσεις που σχετίζονται με άλλη ύποπτη δραστηριότητα (όπως η εγγραφή και εκτέλεση δυαδικών αρχείων) ενδέχεται να υποδηλώνουν κακόβουλη δραστηριότητα. Οι επαληθεύσεις NTLM LogonType 3 που δεν συσχετίζονται με σύνδεση τομέα και δεν είναι ανώνυμες συνδέσεις είναι ύποπτες.

Μετρίαση	Περιγραφή
Πολιτικές κωδικού πρόσβασης: Ορισμός και επιβολή πολιτικών ασφαλών κωδικών πρόσβασης για λογαριασμούς.	Διασφαλίζουμε ότι οι ενσωματωμένοι και δημιουργημένοι λογαριασμοί τοπικού διαχειριστή έχουν πολύπλοκους και μοναδικούς κωδικούς πρόσβασης.
Διαχείριση προνομίων λογαριασμού: Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	Περιορίζουμε την επικάλυψη διαπιστευτηρίων σε όλα τα συστήματα, για να αποτρέψουμε τη ζημιά από συμβιβασμούς διαπιστευτηρίων και να μειώσετε την ικανότητα του επιτιθέμενου να εκτελέσει εσωτερική μετακίνηση μεταξύ συστημάτων.
Ενημέρωση λογισμικού: Εκτελούμε τακτικές ενημερώσεις λογισμικού για να μετριάσουμε τον κίνδυνο εκμετάλλευσης.	Εφαρμόζουμε την ενημέρωση KB2871997 στα συστήματα των Windows 7 και ανώτερων, για να περιορίσουμε την προεπιλεγμένη πρόσβαση λογαριασμών στην ομάδα τοπικών διαχειριστών.
Έλεγχος λογαριασμού χρήστη: Ρυθμίζουμε τον έλεγχο λογαριασμού χρηστών των Windows για να μετριάσουμε τον κίνδυνο του επιτιθέμενου να	Ενεργοποιούμε τη μετάβαση στις μετρήσεις κατακερματισμού για να εφαρμόσουμε περιορισμούς UAC σε τοπικούς λογαριασμούς κατά την σύνδεση στο δίκτυο. Το σχετικό κλειδί μητρώου είναι εγκατεστημένο στη διαδρομή HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion

αποκτήσει προνομιακή πρόσβαση.	\Policies\System\LocalAccountTokenFilterPolicy, μέσω GPO: Διαμόρφωση υπολογιστή>[Πολιτικές]>Πρότυπα διαχείρισης>SCM: Pass the Hash Mitigations: Εφαρμόζουμε περιορισμούς UAC στους τοπικούς λογαριασμούς στις συνδέσεις δικτύου.
Διαχείριση λογαριασμού χρηστών: Διαχείριση της δημιουργίας, της τροποποίησης, της χρήσης και των αδειών που σχετίζονται με τους λογαριασμούς χρηστών.	Αποτροπή ενός χρήστη τομέα να είναι στην ομάδα τοπικών διαχειριστών σε πολλά συστήματα.

- **Παράκαμψη του εισιτηρίου (Pass the ticket)**

Ελέγχουμε όλα τα συμβάντα χρήσης ταυτότητας Kerberos και διαπιστευτηρίων ώστε να δούμε εάν υπάρχουν αποκλίσεις. Τα ασυνήθιστα απομακρυσμένα συμβάντα ελέγχου ταυτότητας που σχετίζονται με άλλη ύποπτη δραστηριότητα (όπως η εγγραφή και εκτέλεση δυαδικών αρχείων) μπορεί να υποδηλώνουν κακόβουλη δραστηριότητα. Το Αναγνωριστικό συμβάντος 4769 δημιουργείται στον ελεγκτή τομέα όταν χρησιμοποιείται ένα χρυσό εισιτήριο μετά την διπλή επαναφορά του κωδικού πρόσβασης KRBTGT. Ο κωδικός κατάστασης 0x1F υποδεικνύει ότι η ενέργεια απέτυχε λόγω του "Ο έλεγχος ακεραιότητας του αποκρυπτογραφημένου πεδίου απέτυχε" και υποδεικνύει κακή χρήση ενός ακυρωμένου χρυσού εισιτήριου.

Μετρίαση	Περιγραφή
Διαμόρφωση υπηρεσίας καταλόγου Active Directory: Ρυθμίζουμε την υπηρεσία καταλόγου Active Directory για να αποτρέψουμε τη χρήση ορισμένων τεχνικών, χρησιμοποιώντας φιλτράρισμα SID, κλπ.	Για να περιορίσουμε το αντίκτυπο ενός χρυσού εισιτηρίου που δημιουργήθηκε προηγουμένως, επαναφέρουμε δύο φορές τον ενσωματωμένο κωδικό πρόσβασης του λογαριασμού KRBTGT, γεγονός που θα ακυρώσει τυχόν υπάρχοντα χρυσά εισιτήρια που έχουν δημιουργηθεί με του hash KRBTGT και άλλων εισερχόμενων εισιτήριων Kerberos.
Πολιτικές κωδικού πρόσβασης: Ορισμός και επιβολή πολιτικών ασφαλών κωδικών πρόσβασης για λογαριασμούς.	Διασφαλίζουμε ότι οι λογαριασμοί τοπικών διαχειριστών έχουν σύνθετους και μοναδικούς κωδικούς πρόσβασης.
Διαχείριση προνομίων λογαριασμού: Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	Περιορίζουμε τις άδειες λογαριασμού διαχειριστή σε ελεγκτές τομέα και περιορισμένους διακομιστές. Ανάθεση διαφορετικών λειτουργιών διαχειριστή για να διαχωριστούν οι λογαριασμοί.
Διαχείριση λογαριασμού χρηστών: Διαχείριση της δημιουργίας, της τροποποίησης, της χρήσης και των αδειών που σχετίζονται με τους λογαριασμούς χρηστών.	Αποτροπή ενός χρήστη τομέα να είναι στην ομάδα τοπικών διαχειριστών σε πολλά συστήματα.

- **Πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας (Remote desktop protocol)**

Η χρήση του RDP μπορεί να είναι νόμιμη, ανάλογα με το περιβάλλον του δικτύου και τον τρόπο χρήσης του. Άλλοι παράγοντες, όπως τα πρότυπα πρόσβασης και η δραστηριότητα που συμβαίνει μετά από μια απομακρυσμένη σύνδεση, ενδέχεται να υποδηλώνουν ύποπτη ή κακόβουλη συμπεριφορά με το RDP. Παρακολουθούμε τους λογαριασμούς χρηστών που έχουν συνδεθεί σε συστήματα που κανονικά δεν θα είχαν πρόσβαση ή δεν έχουν προσπελάσει πολλά συστήματα σε

σχετικά σύντομο χρονικό διάστημα. Επίσης, ρυθμίζουμε την παρακολούθηση της διαδικασίας για τη χρήση του tscon.exe και παρακολουθούμε τη δημιουργία υπηρεσίας που χρησιμοποιεί τα cmd.exe / k ή cmd.exe / c στα επιχειρήματά της για την αποτροπή της κατάχρησης της λειτουργίας RDP.

Μετρίαση	Περιγραφή
Έλεγχος: Εκτελέστε ελέγχους ή σαρώσεις συστημάτων, άδειες, μη ασφαλές λογισμικό, μη ασφαλείς διαμορφώσεις κ.λπ. για να εντοπιστούν πιθανές αδυναμίες.	Ελέγχουμε τακτικά τα μέλη της ομάδας Remote Desktop Users. Καταργούμε τους άχρηστους λογαριασμούς από τις ομάδες χρηστών απομακρυσμένης επιφάνειας εργασίας
Απενεργοποίηση ή κατάργηση των δυνατοτήτων ή του προγράμματος: Αποτροπή της πρόσβασης σε κοινόχρηστα αρχεία, της απομακρυσμένης πρόσβασης σε συστήματα και περιττές υπηρεσίες. Οι μηχανισμοί περιορισμού της πρόσβασης μπορούν να περιλαμβάνουν τη χρήση συσκευών συγκέντρωσης δικτύου, πύλες RDP κ.λπ.	Απενεργοποίηση της υπηρεσίας RDP εάν δεν είναι απαραίτητη.
Περιορισμός στην πρόσβαση στους πόρους μέσω δικτύου: Αποτροπή της πρόσβασης σε κοινόχρηστα αρχεία, απομακρυσμένη πρόσβαση σε συστήματα και περιττές υπηρεσίες. Οι μηχανισμοί περιορισμού της πρόσβασης μπορούν να περιλαμβάνουν τη χρήση συσκευών συγκέντρωσης δικτύου, πύλες RDP κ.λπ.	Χρήση πυλών απομακρυσμένης επιφάνειας εργασίας.
Έλεγχος ταυτοποίησης πολλαπλών παραγόντων: Χρησιμοποιούμε δύο ή περισσότερα στοιχεία για να πιστοποιήσουμε την ταυτότητά μας σε ένα σύστημα. Όπως το όνομα χρήστη και ο κωδικός πρόσβασης τα οποία όμως παράγονται είτε από μία φυσική έξυπνη κάρτα είτε από μία γεννήτρια συμβόλων.	Χρήση ελέγχου ταυτότητας πολλαπλών διαπιστευτηρίων για απομακρυσμένες συνδέσεις.
Τμηματοποίηση δικτύου: Αρχιτεκτονικά τμήματα του δικτύου για την απομόνωση κρίσιμων συστημάτων, λειτουργιών ή πόρων. Χρησιμοποιούμε φυσική και λογική κατάτμηση για να αποτρέψουμε την πρόσβαση σε δυνητικά ευαίσθητα συστήματα και πληροφορίες. Χρησιμοποιούμε ένα DMZ για να περιέχει οποιεσδήποτε υπηρεσίες στο διαδίκτυο που δεν πρέπει να εκτίθενται από το εσωτερικό δίκτυο.	Αποτρέπουμε την πρόσβαση του RDP από το Διαδίκτυο. Ενεργοποιήστε τους κανόνες τείχους προστασίας για να την απόκλιση της επισκεψιμότητας RDP μεταξύ των ζωνών ασφαλείας δικτύου εντός ενός δικτύου.
Ρύθμιση λειτουργικού συστήματος: Αλλαγή της διαμόρφωσης που σχετίζετε με το λειτουργικό σύστημα ή ένα κοινό χαρακτηριστικό του λειτουργικού	Αλλαγή στα GPO για να οριστούν συντομότερες συνεδρίες χρονικού ορίου αλλά και το μέγιστο χρονικό διάστημα που μπορεί να είναι ενεργή οποιαδήποτε

συστήματος που έχει ως αποτέλεσμα την ασφάλεια του συστήματος έναντι των τεχνικών επίθεσης.	μεμονωμένη περίοδος λειτουργίας. Αλλάζουμε τα GPO για να καθορίσετε το μέγιστο χρονικό διάστημα που μία αποσυνδεδεμένη συνεδρία παραμένει ενεργή στον εξυπηρετητή κεντρικού υπολογιστή RD.
Διαχείριση προνομίων λογαριασμού: Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	Αφαίρεση από την τοπική ομάδα Administrators από τη λίστα των ομάδων που επιτρέπεται να συνδεθούν μέσω του RDP.
Διαχείριση λογαριασμού χρηστών: Διαχείριση της δημιουργίας, της τροποποίησης, της χρήσης και των αδειών που σχετίζονται με τους λογαριασμούς χρηστών.	Περιορισμός των δικαιωμάτων των απομακρυσμένων χρηστών εάν είναι απαραίτητη η απομακρυσμένη πρόσβαση.

- **Απομακρυσμένη αντιγραφή αρχείου (Remote file copy)**

Παρακολούθηση της δημιουργίας αρχείων και της μεταφοράς αρχείων μέσα σε ένα δίκτυο μέσω SMB. Οι ασυνήθιστες διαδικασίες με εξωτερικές συνδέσεις δικτύου που δημιουργούν αρχεία στο σύστημα ενδέχεται να είναι ύποπτες. Η ενεργοποίηση βοηθητικών προγραμμάτων, όπως το FTP, των οποίων δεν γίνεται συχνή χρήση μπορεί επίσης να είναι ύποπτη. Ανάλυση δεδομένων δικτύου για ασυνήθιστες ροές δεδομένων (π.χ. ένας πελάτης που στέλνει σημαντικά περισσότερα δεδομένα από αυτά που λαμβάνει από έναν διακομιστή). Οι διαδικασίες που χρησιμοποιούν το δίκτυο και δεν έχουν προηγούμενη συχνή επικοινωνία μέσω δικτύου ή δεν έχουν ενεργοποιηθεί ποτέ πριν είναι ύποπτες. Ανάλυση των περιεχόμενων των πακέτων για να ανιχνευτούν επικοινωνίες που δεν ακολουθούν την αναμενόμενη συμπεριφορά πρωτοκόλλου για τη θύρα που χρησιμοποιείται.

Μετρίαση	Περιγραφή
Αποτροπή παρεμβολών δικτύου: Χρήση υπογραφών ανίχνευσης εισβολής για να αποκλειστεί η κυκλοφορία στα όρια του δικτύου.	Τα συστήματα ανίχνευσης και πρόληψης εισβολής δικτύου που χρησιμοποιούν υπογραφές δικτύου για τον εντοπισμό επισκεψιμότητας για συγκεκριμένο κακόβουλο λογισμικό ή για ασυνήθιστη μεταφορά δεδομένων σε γνωστά εργαλεία και πρωτόκολλα, όπως το FTP, μπορούν να χρησιμοποιηθούν για να μετριάσουν τη δραστηριότητα σε επίπεδο δικτύου. Οι υπογραφές είναι συχνά για μοναδικούς δείκτες μέσα στα πρωτόκολλα και μπορεί να βασίζονται στην συγκεκριμένη τεχνική παρατήρησης που χρησιμοποιείται από έναν συγκεκριμένο επιτιθέμενο ή εργαλείο και πιθανότατα να είναι διαφορετικές σε διάφορες οικογένειες και εκδόσεις malware. Ο επιτιθέμενος πιθανόν να αλλάξει τις υπογραφές του εργαλείου C2 με την πάροδο του χρόνου ή να κατασκευάσει πρωτόκολλα με τέτοιο τρόπο ώστε να αποφευχθεί η ανίχνευση με κοινά αμυντικά εργαλεία

- **Απομακρυσμένες υπηρεσίες (Remote services)**

Διόρθωση της χρήσης της δραστηριότητας σύνδεσης που σχετίζεται με απομακρυσμένες υπηρεσίες με ασυνήθιστη συμπεριφορά, κακόβουλη ή ύποπτη δραστηριότητα. Ο επιτιθέμενος θα πρέπει πιθανόν να μάθει για το περιβάλλον και τις σχέσεις μεταξύ των συστημάτων μέσω των τεχνικών ανακάλυψης πριν επιχειρήσει την εσωτερική μετακίνηση.

Μετρίαση	Περιγραφή
Έλεγχος ταυτοποίησης πολλαπλών παραγόντων: Χρησιμοποιούμε δύο ή περισσότερα στοιχεία για να πιστοποιήσουμε την ταυτότητά μας σε ένα σύστημα. Όπως το όνομα χρήστη και ο κωδικός πρόσβασης τα οποία όμως παράγονται είτε από μία φυσική έξυπνη κάρτα είτε από μία γεννήτρια συμβόλων.	Χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων σε συνδέσεις απομακρυσμένης υπηρεσίας όπου είναι δυνατόν
Διαχείριση λογαριασμού χρηστών: Διαχείριση της δημιουργίας, της τροποποίησης, της χρήσης και των αδειών που σχετίζονται με τους λογαριασμούς χρηστών.	Περιορισμός των λογαριασμών που ενδέχεται να χρησιμοποιούν απομακρυσμένες υπηρεσίες. Περιορισμός των δικαιωμάτων για λογαριασμούς που διατρέχουν μεγαλύτερο κίνδυνο συμβιβασμού. για παράδειγμα, ρύθμιση του SSH, ώστε οι χρήστες να μπορούν να εκτελούν μόνο συγκεκριμένα προγράμματα.

- **Αντιγραφή μέσω αφαιρούμενων μέσων (Replication through removable media)**

Παρακολούθηση της πρόσβασης στα αρχεία που προέρχονται από αφαιρούμενα μέσα. Εντοπισμός διεργασιών που εκτελούνται από αφαιρούμενα μέσα μετά την τοποθέτησή τους ή όταν εκκινούνται από έναν χρήστη. Εάν χρήση ενός εργαλείου απομακρυσμένης πρόσβασης ώστε να μετακινηθεί εσωτερικά, τότε είναι πιθανό να προκύψουν πρόσθετες ενέργειες μετά την εκτέλεση, όπως το άνοιγμα συνδέσεων δικτύου για την εντολή Command and Control και την αναζήτηση πληροφοριών συστήματος και δικτύου.

Μετρίαση	Περιγραφή
Απενεργοποίηση ή κατάργηση των δυνατοτήτων ή του προγράμματος: Αποτροπή της πρόσβασης σε κοινόχρηστα αρχεία, της απομακρυσμένης πρόσβασης σε συστήματα και περιττές υπηρεσίες. Οι μηχανισμοί περιορισμού της πρόσβασης μπορούν να περιλαμβάνουν τη χρήση συσκευών συγκέντρωσης δικτύου, πύλες RDP κ.λπ.	Απενεργοποίηση του Autorun αν δεν είναι απαραίτητο. Αποκλεισμός ή περιορισμός των αφαιρούμενων μέσων, εάν δεν απαιτούνται από τις καθημερινές συνήθειες διεργασιών που εκτελούμε.
Περιορισμός της εγκατάσταση υλικού: Αποκλεισμός των χρηστών ή των ομάδων από την εγκατάσταση ή τη χρήση μη εγκεκριμένου υλικού σε συστήματα, συμπεριλαμβανομένων των συσκευών USB.	Περιορισμός της χρήσης συσκευών USB και αφαιρούμενων μέσων εντός ενός δικτύου.

- **Κοινόχρηστο webroot (Shared waebroot)**

Παρακολούθηση των αρχείων και των διαδικασιών για να εντοπιστεί πότε γράφονται αρχεία σε ένα διακομιστή Web με μια διαδικασία που δεν είναι η κανονική διαδικασία διακομιστή Web ή όταν τα αρχεία γράφονται εκτός των κανονικών περιόδων διαχείρισης.

Παρακολούθηση της διαδικασίας για τον εντοπισμό των κανονικών διαδικασιών που εκτελούνται στον διακομιστή Web και για την ανίχνευση διαδικασιών που συνήθως δεν εκτελούνται.

Μετρίαση	Περιγραφή
Περιορισμός της πρόσβαση στους πόρους μέσω δικτύου: Αποτροπή της πρόσβασης σε κοινόχρηστα αρχεία, σε απομακρυσμένες πρόσβασης συστημάτων και περιττές υπηρεσίες. Οι μηχανισμοί περιορισμού της πρόσβασης μπορούν να περιλαμβάνουν τη χρήση συσκευών συγκέντρωσης δικτύου, πύλες RDP κ.λπ.	Αποκλεισμός της απομακρυσμένης πρόσβασης στο webroot ή σε άλλους καταλόγους που χρησιμοποιούνται για την προβολή περιεχομένου ιστού.
Τμηματοποίηση δικτύου: Αρχιτεκτονικά τμήματα του δικτύου για την απομόνωση κρίσιμων συστημάτων, λειτουργιών ή πόρων. Χρησιμοποιούμε φυσική και λογική κατάτμηση για να αποτρέψουμε την πρόσβαση σε δυνητικά ευαίσθητα συστήματα και πληροφορίες. Χρησιμοποιούμε ένα DMZ για να περιέχει οποιεσδήποτε υπηρεσίες στο διαδίκτυο που δεν πρέπει να εκτίθενται από το εσωτερικό δίκτυο.	Δίκτυα που επιτρέπουν την ανοιχτή ανάπτυξη και δοκιμή περιεχομένου Web και επιτρέπουν στους χρήστες να δημιουργήσουν δικούς τους διακομιστές ιστού στο δίκτυο ενδέχεται να είναι ιδιαίτερα ευάλωτοι εάν τα συστήματα και οι διακομιστές ιστού δεν είναι σωστά ασφαλισμένοι για να περιορίσουν την μη εξουσιοδοτημένη πρόσβαση στο κοινόχρηστο δίκτυο.
Διαχείριση προνομίων λογαριασμού: Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	Τα δίκτυα που επιτρέπουν την ανοιχτή ανάπτυξη και δοκιμή περιεχομένου Web και επιτρέπουν στους χρήστες να δημιουργήσουν τους δικούς τους εξυπηρετητές ιστού στο δίκτυο ενδέχεται να είναι ιδιαίτερα ευάλωτοι εάν τα συστήματα και οι διακομιστές Web δεν είναι σωστά ασφαλισμένοι για να περιορίσουν την μη εξουσιοδοτημένη χρήση του λογαριασμού και την πρόσβαση στο κοινόχρηστο δίκτυο χωρίς έλεγχο ταυτότητας.
Περιορισμός στα δικαιώματα αρχείων και καταλόγου: Περιορίζουμε την πρόσβαση ρυθμίζοντας δικαιώματα καταλόγου και αρχείων που δεν αφορούν συγκεκριμένους χρήστες ή προνομιούχους λογαριασμούς.	Απενεργοποίηση της εκτέλεσης σε καταλόγους στο webroot. Διασφάλιση της ύπαρξης κατάλληλης άδειας σε καταλόγους που είναι προσβάσιμοι μέσω ενός διακομιστή Web.
Διαχείριση λογαριασμού χρηστών: Διαχείριση της δημιουργίας, της τροποποίησης, της χρήσης και των αδειών που σχετίζονται με τους λογαριασμούς χρηστών.	Διασφάλιση των δικαιωμάτων της διαδικασίας διακομιστή Web ότι είναι μόνο αυτά που απαιτούνται όταν δεν χρησιμοποιούνται ενσωματωμένοι λογαριασμό, αντί να δημιουργηθούν συγκεκριμένοι λογαριασμοί για να

	περιορίσουν την περιττή πρόσβαση ή τις επικαλύψεις δικαιωμάτων στα συστήματα.

- **Ουσιαστικό κοινόχρηστο περιεχόμενο (Taint shared content)**

Οι διαδικασίες που γράφουν ή αντικαθιστούν πολλά αρχεία σε έναν κοινόχρηστο κατάλογο δικτύου ενδέχεται να είναι ύποπτοι. Παρακολούθηση διαδικασιών που εκτελούνται από αφαιρούμενα μέσα για κακόβουλη ή μη φυσιολογική δραστηριότητα, όπως συνδέσεις δικτύου λόγω εντολών και ελέγχου και πιθανές τεχνικές ανίχνευσης δικτύου. Συχνή σάρωση καταλόγων κοινόχρηστου δικτύου για κακόβουλα αρχεία, κρυφά αρχεία, αρχεία .LNK και άλλους τύπους αρχείων που ενδέχεται να μην είναι τυπικοί και υπάρχουν σε καταλόγους που χρησιμοποιούνται για την κοινή χρήση συγκεκριμένων τύπων αρχείων.

Μετρίαση	Περιγραφή
Αποτροπή εκτελέσεων: Αποκλεισμός εκτέλεσης κώδικα σε ένα σύστημα μέσω της παραμετροποίησης της λίστας προσβάσεων των εφαρμογών (black and white lists) και τον αποκλεισμό της εκτέλεσης σεναρίων.	Προσδιορισμός του δυνητικά κακόβουλου λογισμικού που μπορεί να χρησιμοποιηθεί για να προσβάλει περιεχόμενο ή να προκύψει από αυτό και να ελέγξει ή και να αποκλείσει τα άγνωστα προγράμματα, κάνοντας χρήση εργαλείων με δυνατότητες κατάτμησης, όπως το AppLocker ή τις πολιτικές περιορισμού λογισμικού, όπου χρειάζεται.
Απόκτηση Προστασίας: Χρήση δυνατοτήτων για την ανίχνευση και την παρεμπόδιση των συνθηκών που μπορεί να οδηγήσουν ή να είναι ενδεικτικές για συμβάντα εκμετάλλευσης λογισμικού.	Χρήση βοηθητικών προγραμμάτων που ανιχνεύουν ή μετριάζουν τα κοινά χαρακτηριστικά που χρησιμοποιούνται στην εκμετάλλευση, όπως το εργαλείο Microsoft Enhanced Mitigation Experience (EMET).
Περιορισμός στα δικαιώματα αρχείων και καταλόγου: Περιορίζουμε την πρόσβαση ρυθμίζοντας δικαιώματα καταλόγου και αρχείων που δεν αφορούν συγκεκριμένους χρήστες ή προνομιούχους λογαριασμούς.	Προστασία των κοινόχρηστων φακέλων ελαχιστοποιώντας τους χρήστες που έχουν πρόσβαση εγγραφής.

- **Λογισμικό τρίτων (Third-party software)**

Οι μέθοδοι ανίχνευσης θα διαφέρουν ανάλογα με τον τύπο του λογισμικού ή του συστήματος και με τους τρόπους με τους οποίους γίνετε συνήθης χρήση αυτών. Η ίδια διαδικασία διερεύνησης μπορεί να εφαρμοστεί εδώ όπως και σε άλλες δυνητικές κακόβουλες δραστηριότητες όπου ο φορέας διανομής είναι αρχικά άγνωστος αλλά η προσκόπτουσα δραστηριότητα ακολουθεί ένα διακριτό πρότυπο. Ανάλυση των δέντρων εκτέλεσης διεργασιών, την προηγούμενη δραστηριότητα της εφαρμογής (όπως ποιες μορφές αρχείων συνήθως εξάγονται) και τις δραστηριότητες ή τα συμβάντα που προκύπτουν από το αρχείο / δυαδικό / σενάριο που εξάγετε στα συστήματα. Συχνά αυτές οι εφαρμογές τρίτων θα έχουν δικά τους αρχεία καταγραφών που μπορούν να συλλεχθούν και να συσχετιστούν με άλλα δεδομένα από το περιβάλλον. Διασφάλιση των αρχείων ανάπτυξης λογισμικού και αναζήτηση ύποπτης ή μη εξουσιοδοτημένης δραστηριότητας. Ένα σύστημα που δεν χρησιμοποιείται συνήθως για να εξάγει το λογισμικό στους χρήστες και ξαφνικά χρησιμοποιείται για μια τέτοια εργασία εκτός μιας γνωστής λειτουργίας διαχειριστή μπορεί να είναι ύποπτο. Εκτέλεση της ανάπτυξης εφαρμογών σε τακτά χρονικά διαστήματα, ώστε να ξεχωρίζει η δραστηριότητα παράνομης ανάπτυξης. Παρακολούθηση της δραστηριότητας της διαδικασίας που δεν συσχετίζεται με το γνωστό μη κακόβουλο λογισμικό. Παρακολούθηση της δραστηριότητας σύνδεσης λογαριασμού στο σύστημα ανάπτυξης.

Μετρίαση	Περιγραφή
Διαμόρφωση καταλόγου Active Directory: Ρύθμιση του καταλόγου Active Directory για την αποτροπή της χρήσης ορισμένων τεχνικών. Χρήση φιλτραρίσματος SID, κλπ.	Διασφάλιση της σωστής απομόνωσης των συστημάτων κα της πρόσβασης για κρίσιμα συστήματα δικτύου μέσω της χρήσης των ομάδων πολιτικής.
Έλεγχος ταυτοποίησης πολλαπλών παραγόντων: Χρησιμοποιούμε δύο ή περισσότερα στοιχεία για να πιστοποιήσουμε την ταυτότητά μας σε ένα σύστημα. Όπως το όνομα χρήστη και ο κωδικός πρόσβασης τα οποία όμως παράγονται είτε από μία φυσική έξυπνη κάρτα είτε από μία γεννήτρια συμβόλων.	Διασφάλιση της σωστής απομόνωσης των συστημάτων και της πρόσβασης για κρίσιμα συστήματα δικτύου μέσω της χρήσης ελέγχου ταυτότητας πολλαπλών παραγόντων.
Τμηματοποίηση δικτύου: Αρχιτεκτονικά τμήματα του δικτύου για την απομόνωση κρίσιμων συστημάτων, λειτουργιών ή πόρων. Χρησιμοποιούμε φυσική και λογική κατάτμηση για να αποτρέψουμε την πρόσβαση σε δυνητικά ευαίσθητα συστήματα και πληροφορίες. Χρησιμοποιούμε ένα DMZ για να περιέχει οποιεσδήποτε υπηρεσίες στο διαδίκτυο που δεν πρέπει να εκτίθενται από το εσωτερικό δίκτυο.	Διασφάλιση της σωστής απομόνωσης του συστήματος για κρίσιμα συστήματα δικτύου μέσω της χρήσης τείχους προστασίας.
Πολιτική κωδικών πρόσβασης: Ορισμός και επιβολή πολιτικών ασφαλών κωδικών πρόσβασης για όλους τους λογαριασμούς.	Διασφάλιση ότι τα διαπιστευτήρια λογαριασμού που μπορούν να χρησιμοποιηθούν για την πρόσβαση σε συστήματα ανάπτυξης είναι μοναδικά και δεν χρησιμοποιούνται σε όλο το δίκτυο.
Διαχείριση προνομίων λογαριασμού: Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	Δικαίωμα πρόσβασης σε συστήματα ανάπτυξης εφαρμογών μόνο σε περιορισμένο αριθμό εξουσιοδοτημένων διαχειριστών.
Απομακρυσμένη αποθήκευση δεδομένων: Χρήση του αρχείου απομακρυσμένης καταγραφής ενεργειών ασφάλειας και αποθήκευσης ευαίσθητων αρχείων, όπου η πρόσβαση μπορεί να ελεγχθεί καλύτερα για να αποφευχθεί η έκθεση των δεδομένων καταγραφής ανίχνευσης εισβολής ή ευαίσθητων πληροφοριών.	Εάν το σύστημα ανάπτυξης εφαρμογών μπορεί να ρυθμιστεί ώστε να αναπτύξει μόνο υπογεγραμμένα δυαδικά αρχεία, βεβαιωθείτε ότι τα αξιόπιστα πιστοποιητικά υπογραφής δεν βρίσκονται μαζί με το σύστημα ανάπτυξης εφαρμογών και αντίθετα βρίσκονται σε ένα σύστημα στο οποίο δεν είναι δυνατή η πρόσβαση από απόσταση ή η όποια επιτρεπόμενη απομακρυσμένη πρόσβαση ελέγχεται αυστηρά.
Ενημέρωση λογισμικού:	Εγκατάσταση τακτικών ενημερωμένων εκδόσεων στα συστήματα ανάπτυξης για

Εκτέλεση τακτικών ενημερώσεων λογισμικού για να μετριαστεί ο κίνδυνος εκμετάλλευσης.	την αποτροπή πιθανών απομακρυσμένων προσβάσεων μέσω της εκμετάλλευσης για την εξέλιξη προνομίων.
Διαχείριση λογαριασμού χρηστών: Διαχείριση της δημιουργίας, της τροποποίησης, της χρήσης και των αδειών που σχετίζονται με τους λογαριασμούς χρηστών.	Διασφάλιση ότι όλοι οι λογαριασμοί τρίτων που χρησιμοποιούνται για την πρόσβαση σε αυτά τα συστήματα μπορούν να ανιχνευθούν και δεν χρησιμοποιούνται σε όλο το δίκτυο ή χρησιμοποιούνται από άλλους παρόχους στο ίδιο περιβάλλον. Βεβαίωση ότι υπάρχουν τακτικές αναθεωρήσεις των λογαριασμών που παρέχονται σε αυτά τα συστήματα για να εξακριβωθεί η συνεχιζόμενη ανάγκη και να διασφαλιστεί ότι υπάρχει διακυβέρνηση για να εντοπιστεί η αποδέσμευση της πρόσβασης που δεν απαιτείται πλέον. Διασφάλιση της σωστής απομόνωσης συστήματος και πρόσβασης για κρίσιμα συστήματα δικτύου μέσω της χρήσης του διαχωρισμού προνομίων λογαριασμού.
Εκπαίδευση χρηστών: Εκπαίδευση των χρηστών ώστε να γνωρίζουν τις προσπάθειες πρόσβασης ή χειραγώγησης από έναν επιτιθέμενο ώστε να μειωθεί ο κίνδυνος επιτυχίας του spearphishing, της κοινωνικής μηχανικής και άλλων τεχνικών που αφορούν την αλληλεπίδραση των χρηστών.	Ύπαρξη μιας αυστηρής πολιτικής έγκρισης για τη χρήση συστημάτων ανάπτυξης.

- **Μερίδια λογαριασμού διαχειριστή των Windows (Windows admin shares)**

Βεβαιωθείτε ότι η σωστή καταγραφή των λογαριασμών που χρησιμοποιούνται για την είσοδο σε συστήματα ενεργοποιείται και συλλέγεται κεντρικά. Η καταγραφή των Windows είναι σε θέση να συλλέξει επιτυχής και αποτύχεις δραστηριότητες για λογαριασμούς που μπορούν να χρησιμοποιηθούν για να μετακινηθούν εσωτερικά και μπορούν να συλλεχθούν χρησιμοποιώντας εργαλεία όπως το Windows Event Forwarding. Παρακολούθηση συμβάντων απομακρυσμένης σύνδεσης και σχετικής δραστηριότητας SMB για μεταφορά αρχείων και εκτέλεση απομακρυσμένης διαδικασίας. Παρακολούθηση τις ενέργειες απομακρυσμένων χρηστών που συνδέονται με κοινόχρηστα στοιχεία διαχείρισης. Παρακολούθηση της χρήσης εργαλείων και εντολών για τη σύνδεση σε απομακρυσμένα κοινόχρηστα στοιχεία, όπως το Net, στη διεπαφή γραμμής εντολών και τεχνικές Discovery που θα μπορούσαν να χρησιμοποιηθούν για την εύρεση εξ αποστάσεως προσβάσιμων συστημάτων.

Μετρίαση	Περιγραφή
Πολιτική κωδικών πρόσβασης: Ορισμός και επιβολή πολιτικών ασφαλών κωδικών πρόσβασης για όλους τους λογαριασμούς.	Αποτροπή της χρήσης των ίδιων κωδικών πρόσβασης των λογαριασμών των τοπικών διαχειριστών σε όλα τα συστήματα. Διασφάλιση της πολυπλοκότητας και της μοναδικότητας του κωδικού πρόσβασης, ώστε οι κωδικοί πρόσβασης να μην μπορούν να σπαστούν ή να υπολογιστούν.
Διαχείριση προνομίων λογαριασμού:	Κατάργηση της απομακρυσμένης χρήσης τοπικών διαπιστευτηρίων διαχειριστή για

Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	την είσοδο σε συστήματα. Απαγόρευση στους λογαριασμούς χρηστών τομέα να είναι στην ομάδα τοπικών διαχειριστών για τα συστήματα.

- **Απομακρυσμένη διαχείριση παραθύρων (Windows remote management)**

Παρακολούθηση της χρήσης του WinRM μέσα σε ένα περιβάλλον παρακολουθώντας την εκτέλεση της υπηρεσίας. Αν δεν χρησιμοποιείται κανονικά ή είναι απενεργοποιημένη, τότε αυτό μπορεί να αποτελεί ένδειξη ύποπτης συμπεριφοράς. Παρακολούθηση των διαδικασιών που δημιουργήθηκαν και τις ενέργειες που έγιναν από τη χρήση της διαδικασίας WinRM ή από ένα σενάριο που επικαλείται το WinRM ώστε να γίνει η συσχέτιση με άλλα σχετικά γεγονότα.

Μετρίαση	Περιγραφή
Απενεργοποίηση ή κατάργηση των δυνατοτήτων ή του προγράμματος: Αποτροπή της πρόσβασης σε κοινόχρηστα αρχεία, της απομακρυσμένης πρόσβασης σε συστήματα και περιττές υπηρεσίες. Οι μηχανισμοί περιορισμού της πρόσβασης μπορούν να περιλαμβάνουν τη χρήση συσκευών συγκέντρωσης δικτύου, πύλες RDP κ.λπ.	Απενεργοποίηση της υπηρεσίας του WinRM.
Τμηματοποίηση δικτύου: Αρχιτεκτονικά τμήματα του δικτύου για την απομόνωση κρίσιμων συστημάτων, λειτουργιών ή πόρων. Χρησιμοποιούμε φυσική και λογική κατάτμηση για να αποτρέψουμε την πρόσβαση σε δυνητικά ευαίσθητα συστήματα και πληροφορίες. Χρησιμοποιούμε ένα DMZ για να περιέχει οποιεσδήποτε υπηρεσίες στο διαδίκτυο που δεν πρέπει να εκτίθενται από το εσωτερικό δίκτυο.	Εάν η υπηρεσία είναι απαραίτητη, κλειδώστε τους κρίσιμους θύλακες με χωριστή υποδομή WinRM και ακολουθήστε τις βέλτιστες πρακτικές WinRM σχετικά με τη χρήση firewalls υποδοχής για να περιορίσετε την πρόσβαση WinRM για να επιτρέψετε την επικοινωνία μόνο προς / από συγκεκριμένες συσκευές.
Διαχείριση προνομίων λογαριασμού: Διαχειριζόμαστε τη δημιουργία, την τροποποίηση, τη χρήση και τα δικαιώματα που σχετίζονται με προνομιακούς λογαριασμούς του συστήματος, συμπεριλαμβανομένου του SYSTEM και του root.	Εάν η υπηρεσία είναι απαραίτητη, κλειδώστε τους κρίσιμους θύλακες του WinRM με ξεχωριστούς λογαριασμούς και δικαιώματα.

3.5 Μεθοδολογία επιτιθέμενου

- Κλοπή διαπιστευτηρίων

Οι επιθέσεις μέσω ηλεκτρονικού "ψαρέματος" (phishing), απειλητικών σημείων πρόσβασης Wi-Fi, USB drops, ακόμα και φυσικές επιθέσεις σε συσκευές χωρίς παρακολούθηση έχουν γίνει ένας κοινός φορέας επίθεσης. Καθώς οι ομάδες πληροφοριακών συστημάτων βελτίωσαν την ικανότητα της ασφάλισης των περιμετρικών δικτύων, έχει αυξηθεί η χρήση εξωτερικών επιθέσεων για την εκμετάλλευση των τρωτών σημείων όλο και πιο δύσκολο για τους επιτιθέμενους. Ως

αποτέλεσμα, οι επιθέσεις συνήθως στοχεύουν τους πελάτες μέσω ηλεκτρονικών μηνυμάτων ηλεκτρονικού "ψαρέματος" (phishing) ή μηνύματα κοινωνικής δικτύωσης που έχουν σχεδιαστεί για να προσελκύουν έναν χρήστη να κάνει κλικ σε σύνδεσμο, σε εκτελέσιμο αρχείο ή σε κάποια μακροεντολή για την εκτέλεση κακόβουλου κώδικα. Εκτός από τις κοινές τεχνικές ηλεκτρονικού ψαρέματος, οι επιτιθέμενοι στοχεύουν στα Wi-Fi των υποδομών μιας επιχείρησης (όπως ξενοδοχεία και καφετέριες) για να εκτελέσουν επιθέσεις και να πραγματοποιήσουν την επίθεση διαμεσολάβησης κακόβουλου λογισμικού στα τηλέφωνα των ταξιδιωτών και τους φορητούς υπολογιστές, ή να κλέψουν τα διαπιστευτήρια τους καθώς τα εισάγουν από τα σημεία πρόσβασης Wi-Fi για να αποκτήσουν αργότερα πρόσβαση σε εταιρικούς πόρους του δικτύου.

BYOD (bring your own device) πολιτικές, οι οποίες επιτρέπουν στους χρήστες τη χρήση μιας προσωπικής τους συσκευής η οποία επιτρέπεται στη συνέχεια να συνδεθεί σε ένα ασφαλές εσωτερικό δίκτυο έχουν αυξήσει την αποτελεσματικότητα των επιθέσεων.

Μόλις ένα σύστημα χειραγωγηθεί, οι επιτιθέμενοι θα προσπαθήσουν να συλλέξουν τα διαπιστευτήρια από αυτό. Εργαλεία όπως Meterpreter της Metasploit, Mimikatz, Mimikittenz, Windows Credential, Editor, καταγραφείς κλειδιών, sniffers και άλλα, επιτρέπουν στους εισβολείς είναι σε θέση να καταγράψουν ευαίσθητα δεδομένα, όπως τα ονόματα χρηστών και τους κωδικούς πρόσβασης από συστήματα εντός δικτύου ή εκτός δικτύου όταν το θύμα θα έχει επιστρέψει στο εταιρικό δίκτυο. Λάβετε υπόψη ότι τα διαπιστευτήρια δεν χρειάζεται να είναι πλήρες ζεύγος κωδικών πρόσβασης με όνομα χρήστη και σαφή κείμενο.

Οι επιτιθέμενοι μπορούν να κλέψουν τις hash παραστάσεις των κωδικών πρόσβασης, να τις φορτώσουν στη μνήμη και να επιτρέψουν τα Windows να εκτελέσουν τη διαδικασία passthrough για έλεγχο ταυτότητας σε άλλα συστήματα ως αυθαίρετος χρήστης μέσω της τεχνικής pass-the-hash. Ακόμη και με τον έλεγχο ταυτότητας πολλών παραγόντων κατά τη χρήση, μετά την επαλήθευση ενός χρήστη ένας εισβολέας μπορεί να κλέψει τα πιστοποιημένα εισιτήρια υπηρεσίας Kerberos για να μιμηθεί τον χρήστη και την πρόσβαση σε απομακρυσμένα συστήματα. Αυτά τα εισιτήρια εξυπηρέτησης εκδίδονται με ισχύ 10 ωρών εξ ορισμού, δίνοντας έναν εισβολέα έναν επαρκή χρόνο για την αξιοποίηση του ολοκληρωμένου ελέγχου ταυτότητας για την πρόσβαση σε δικτυακούς πόρους. Οι επιτιθέμενοι που χειραγωγούν τον ελεγκτή τομέα μπορούν να είναι σε θέση να μιμηθούν την ίδια την υπηρεσία Kerberos, χορηγώντας

οι ίδιοι το αποκαλούμενο "Χρυσό Εισιτήριο" ικανό να εκδίδει διαπιστευτήρια για οποιονδήποτε πόρο στο περιβάλλον Kerberos. Ενώ πολλές από τις παραπάνω επιθέσεις επικεντρώνονται στα Windows, μην ξεχνάτε ότι και τα υπόλοιπα λειτουργικά συστήματα δεν έχουν ανοσία σε παρόμοιες επιθέσεις. Είτε γίνει χρήση RDP είτε ssh, ένας εισβολέας με έγκυρα διαπιστευτήρια μπορεί να προκαλέσει τον όλεθρο στο εσωτερικό σας δίκτυο.

- Πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας (RDP)

Μεγάλο στήριγμα της διαχειριστικής πρόσβασης σε απομακρυσμένα συστήματα, είναι το πρωτόκολλο RDP, το οποίο εξακολουθεί να χρησιμοποιείτε από μεγάλο αριθμό διαχειριστών, παρά τις προσπάθειες της Microsoft να ενθαρρύνει τη χρήση του PowerShell για διοικητικές εργασίες. Συνεπώς, η απομακρυσμένη επιφάνεια εργασίας και οι υπηρεσίες Terminal Services παρέχουν ένα ελκυστικό τρόπο επίθεσης για τους επιτιθέμενους οι οποίοι προσπαθούν να το παρομοιάσουν με μία συνήθης δραστηριότητα του δικτύου. Μόλις επιτευχθεί αυτό σε ένα σύστημα, ο επιτιθέμενος μπορεί απλώς να αξιοποιήσει τα ενσωματωμένα εργαλεία της Microsoft για να επιτρέψει την απομακρυσμένη πρόσβαση σε άλλα συστήματα που χρησιμοποιούν RDP και έγκυρα διαπιστευτήρια.

Ο επιτιθέμενος μπορεί απλά να χρησιμοποιήσει το εργαλείο Microsoft Remote Desktop Connection (mstsc.exe) για να απόκτηση πρόσβαση σε ένα σύστημα του θύματος. Ενώ το θύμα δεν κάνει έκθεση της προεπιλεγμένης θύρας 3389 στο Διαδίκτυο, η προώθηση των θυρών που έχει δημιουργηθεί ως σημείο αναφοράς για την πρόσβαση από το Διαδίκτυο στα συστήματα, καθιστά δυνατή την επίτευξη αυτού του στόχου είτε από εξωτερικούς είτε από εσωτερικούς κεντρικούς υπολογιστές.

Ανάλογα με το διαθέσιμο εύρος ζώνης, αυτή η προσέγγιση βασισμένη σε GUI μπορεί να είναι λιγότερο από την ιδανική για έναν επιτιθέμενο, αλλά αν αυτή είναι μια μέθοδος που χρησιμοποιείται συχνά στο περιβάλλον του θύματος, οι επιτιθέμενοι είναι πιθανό να τη χρησιμοποιήσουν ώστε να την συνδυάσουν με την κανονική, συνήθης κυκλοφορία του δικτύου.

- At/schtasks

Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τα ενσωματωμένα παράθυρα των Windows και τις εντολές schtasks ώστε να επεκτείνουν την επιρροή τους και να διατηρούν την παραμονή τους σε ένα περιβάλλον του θύματος. Η εντολή, ενώ έχει αποσυρθεί στις τελευταίες εκδόσεις των Windows, εξακολουθεί να χρησιμοποιείται σε παλαιότερες εκδόσεις των Windows.

Η εντολή επιτρέπει τη διεξαγωγή μιας διαδικασίας σε τακτά χρονικά διαστήματα στο μέλλον είτε σε τοπική είτε σε απομακρυσμένη μηχανή.

Η σύνταξη είναι:

[\ targetIP] [HH: MM] [A | P] [εντολή]

Όπου το targetIP ορίζει ένα απομακρυσμένο σύστημα που θα ονομάζεται, ο χρόνος καθορίζεται με ΜΜ ή ΠΜ, και η εντολή που θα εκτελεστεί λαμβάνοντας τα παραπάνω σαν επιλογές. Ομοίως, τα νεότερα συστήματα Windows υποστηρίζουν την εντολή schtasks, αλλά με την παρακάτω σύνταξη:

schtasks /create /tn [taskname] /s [targetIP] /u [user] /p [password] /sc [frequency] /st [starttime] /s d [startdate] /tr [command]

Για άλλη μια φορά, αυτή η εντολή επιτρέπει την εκτέλεση μιας διαδικασίας σε ένα τοπικό ή απομακρυσμένο σύστημα σε καθορισμένο χρόνο. Επιπλέον, εάν εκτελείται με τα διαπιστευτήρια διαχειριστή, η επιλογή / ru SYSTEM επιτρέπει στο συγκεκριμένο πρόγραμμα να εκτελεστεί με δικαιώματα συστήματος. Οι επιτιθέμενοι με έγκυρα διαπιστευτήρια είναι επομένως σε θέση να προγραμματίσουν τις εντολές που θα τρέξουν σε συστήματα ως μέσα εξόρυξης δεδομένων, διατήρησης της πρόσβασης, την επέκταση του ελέγχου ή άλλων εργασιών που κρίνουν κατάλληλες.

- SC

Η εντολή ελεγκτή υπηρεσίας, sc, είναι σε θέση να δημιουργήσει, να σταματήσει και να ξεκινήσει υπηρεσίες. Οι υπηρεσίες είναι διαδικασίες που τρέχουν έξω από το περιβάλλον ενός συνδεδεμένου χρήστη, επιτρέποντάς τους να ξεκινήσουν αυτόματα κατά την εκκίνηση του συστήματος. Εκτελώντας μια διαδικασία ως υπηρεσία, ο επιτιθέμενος μπορεί να εξασφαλίσει την παραμονή της υπηρεσίας στο σύστημα, συμπεριλαμβανομένης της δυνατότητας αυτοματοποίησης της επανεκκίνησης ή την εκτέλεση της διακοπής διαδικασίας σε άλλες ενέργειες. Για άλλη μια φορά, η εντολή sc επιτρέπει αυτές τις ενέργειες να εκτελούνται στο τοπικό σύστημα ή σε απομακρυσμένα συστήματα με τα κατάλληλα διαπιστευτήρια. Η σύνταξη για τη δημιουργία της αρχικοποίησης μιας επικυρωμένης σύνδεσης με ένα απομακρυσμένο σύστημα είναι:

net use \\[targetIP] [password] /u:[Admin_User

Όπου το targetIP προσδιορίζει το απομακρυσμένο σύστημα και το Admin_User είναι το όνομα του χρήστη ενός λογαριασμού με δικαιώματα διαχειριστή στο σύστημα προορισμού. Για τη δημιουργία μιας υπηρεσίας στο απομακρυσμένο σύστημα, η σύνταξη είναι:

sc \\[targetIP] create [svcname] binpath= [executable]

Σημειώστε ότι το εκτελέσιμο πρέπει να είναι ατμοποιημένο κατά τέτοιο τρόπο που να παρέχει την απαραίτητη υπηρεσία τις επιλογές ελέγχου, συμπεριλαμβανομένης της απόκρισης πίσω στο λειτουργικό σύστημα, όταν ξεκινήσει με επιτυχία. Χωρίς αυτήν την επιβεβαίωση, τα Windows θα σκοτώσουν την υπηρεσία μετά από περίπου 30 δευτερόλεπτα. Οποιοδήποτε αυθαίρετο εκτελέσιμο μπορεί να τροποποιηθεί ως υπηρεσία μέσω της χρήσης του δωρεάν εργαλείου ServifyThis, το οποίο είναι διαθέσιμο από το GitHub από τους InGuardians (https://github.com/inguardians/ServifyThis).

Η υπηρεσία μπορεί στη συνέχεια να ξεκινήσει με την εντολή:

sc \\[targetIP] start [svcname]

- Μέσα διαχείρισης της γραμμής εντολών των Windows (WMIC)

Το Windows Management Instrumentation είναι μια πλατφόρμα που παρέχει η Microsoft για την απλούστευση των διοικητικών εργασιών. Το WMIC είναι το εργαλείο γραμμής εντολών που μπορεί να εκτελέσει εντολές WMI σε τοπικά ή απομακρυσμένα συστήματα. Το WMI χρησιμοποιεί το DCOM για να συνδεθεί με συστήματα που εκτελούν εντολές, πράγμα που σημαίνει ότι σε περιβάλλοντα με απενεργοποιημένο WinRM ή / και απενεργοποιημένο PowerShell, το WMI παρέχει μια ελκυστική επιλογή για επιτιθέμενους.

Το πεδίο εφαρμογής του WMI είναι πραγματικά τεράστιο, που σημαίνει ότι οι επιτιθέμενοι είναι σε θέση να εκτελέσουν μια τεράστια ποικιλία διαφορετικών ενεργειών σε απομακρυσμένα συστήματα που χρησιμοποιούν wmic, συμπεριλαμβανομένων αρχείων καταχώρησης, ενεργοποίησης / ξεκλειδώματος λογαριασμών χρηστών, πληροφοριών συστήματος, υπηρεσιών εκκίνησης και διακοπής, δημιουργίας ή διακοπής , και πολλά άλλα καθήκοντα.

- WinRM

Η απομακρυσμένη διαχείριση των Windows επιτρέπει την αποστολή εντολών σε απομακρυσμένους υπολογιστές με Windows μέσω HTTP ή HTTPS με τη χρήση του πρωτοκόλλου Web Services for Management. Το WinRM εκτελείται ως υπηρεσία στο λογαριασμό υπηρεσίας δικτύου και ως εγγενή στοιχεία της Microsoft, χρησιμοποιώντας αυτά τα εργαλεία θα γίνει παράκαμψη πολλών επιτρεπόμενων λιστών, παρέχοντας μια ακόμη ελκυστική επιλογή για τους επιτιθέμενους.

Η χρήση της εντολής Απομακρυσμένες υπηρεσίες των Windows, winers, επιτρέπει την εκτέλεση αυθαίρετων εντολών στο απομακρυσμένο σύστημα. Μία shell εντολή μπορεί να επιστραφεί με την ακόλουθη σύνταξη:

winrs -r:http://target_host “cmd”

Όπου το target_host είναι το απομακρυσμένο σύστημα στο οποίο θα εκτελεστεί το cmd.exe. Ένα αλληλεπιδραστικό shell επιστρέφεται στον χρήστη που εκτελεί αυτήν την εντολή.

- PowerShell

Το PowerShell είναι ένα ακόμη παράδειγμα ενός εργαλείου που παρέχει πολλές δυνατότητες, αλλά αν η δυνατότητα αυτή χρησιμοποιείται για καλό ή κακό είναι εξ ολοκλήρου στη διακριτική ευχέρεια του χρήστη. Το χαρακτηριστικό εξομοίωσης του PowerShell το καθιστά ιδανικό για να μετακινηθεί κάνεις σε όλο το δίκτυο. Οποιαδήποτε ενέργεια μπορεί να γίνει σε ένα σύστημα Windows μπορεί να γίνει μέσω του PowerShell, χωρίς να χρειάζεται να εγκατασταθεί πρόσθετο κακόβουλο λογισμικό. Το PowerShell Empire εκμεταλλεύεται αυτό το γεγονός σαν ένα ολοκληρωμένο εργαλείο, το οποίο μετά την χρήση του, επιτρέπει σε έναν επιτιθέμενο να διατηρήσει σχεδόν ανεξέλεγκτο έλεγχο πάνω σε ένα δίκτυο, χρησιμοποιώντας όλα τα scripts του PowerShell. Το PowerShell έχει γίνει ένας αγαπημένος μηχανισμός επίθεσης για τους επιτιθέμενους όλων των ειδών.

Εκτός από την απομακρυσμένη χρήση του PowerShell, πολλά cmd PowerShell επιτρέπουν την υποστήριξη της παραμέτρου ComputerName ώστε να επιτρέπουν την εκτέλεση του cmd σε ένα απομακρυσμένο σύστημα. Αυτά τα cmd επιτρέπουν γενικά τη χρήση της κλήσης της απομακρυσμένης διαδικασίας (RPC) για να επιτευχθεί αυτό (αν και ο μηχανισμός μπορεί να ποικίλει) αντί να γίνεται χρήση της απομακρυσμένης χρήσης του PowerShell.

- Psexec

Το psexec δεν είναι μία ενσωματωμένη δυαδική λειτουργία των Windows, αλλά παρέχεται από το Sysinternals, το οποίο ανήκει στη Microsoft. Ως αποτέλεσμα, πολλοί διαχειριστές το χρησιμοποιούν στο περιβάλλον τους, οπότε δεν είναι κάτι το ασυνήθιστο αν το βρούμε να τρέχει σε ένα σύστημα. Η εντολή επιτρέπει την απομακρυσμένη εκτέλεση προγραμμάτων σε συστήματα όταν

παρέχονται τα απαραίτητα διαπιστευτήρια. Αν το εκτελέσιμο αρχείο που πρόκειται να εκτελεστεί δεν είναι ήδη στο στόχο μπορεί να αντιγραφεί με το psexec στο στόχο και στη συνέχεια να εκτελεστεί.

Η έκδοση Sysinternals των εργαλείων εκτελείται στη γραμμή εντολών με την ακόλουθη σύνταξη:

psexec \\[targetIP] [-d] [-u user] [–p password] [command].

Όπου το targetIP είναι το απομακρυσμένο σύστημα και η εντολή είναι οποιοδήποτε εκτελέσιμο αρχείο στο σύστημα.

Ο διακόπτης -c μπορεί να προστεθεί για να αντιγράψει πρώτα το εκτελέσιμο στο στόχο, αν το επιθυμητό εκτελέσιμο αρχείο δεν είναι ήδη στο στόχο. Η ομάδα του Metasploit πρόσθεσε επίσης μια έκδοση του psexec ως λειτουργική μονάδα εκμετάλλευσης στο πλαίσιο του Metasploit. Η υπομονάδα psexec απαιτεί την έγκυρη πιστοποίηση για την πρόσβαση στο απομακρυσμένο σύστημα, αλλά μπορεί να δεχθεί είτε έναν κωδικό πρόσβασης σαν σαφές κείμενο είτε μια αναπαράσταση hash του κωδικού πρόσβασης για να διευκολύνει τις επιθέσεις pass-the-hash. Εάν δεν υπάρχει έγκυρη πιστοποίηση, θα γίνει προσπάθεια σύνδεσης ως επισκέπτης.

3.6 Μεθοδολογία αμυνόμενου

- Κλοπή διαπιστευτηρίων

Οι επιθέσεις από την πλευρά του πελάτη είναι ασταθείς, οπότε η εστίαση στην υπεράσπιση εναντίον τους είναι ένα καλό μέρος για να ξεκινήσουμε. Παρόλο που καμία λύση δεν προσφέρει 100% αποτελεσματικότητα, θα πρέπει να προσπαθήσουμε να κάνουμε τους πελάτες μας να είναι όσο πιο σκληροί σε παραβιάσεις γίνεται και να ελαχιστοποιούν τις ζημίες σε περίπτωση χειραγώγησης. Η χρήση προϊόντων ασφαλείας για την ανίχνευση και την αποτροπή επιθέσεων είναι ένα καλό μέρος για να ξεκινήσουμε, αλλά δεν πρέπει να εναποθέτουμε την πίστη μας σε κάποια συγκεκριμένη λύση. Ανεξάρτητα από το πόσο προηγμένο μπορεί να είναι το προϊόν ασφαλείας που χρησιμοποιεί κάποιος, οι επιτιθέμενοι εργάζονται ήδη για την εύρεση τεχνικών παράκαμψης. Οι βέλτιστες πρακτικές για τις σωστότερες λύσεις εξακολουθούν να ισχύουν, επομένως η καλύτερη προσέγγιση είναι ο συνδυασμός των antivirus, της λίστας με τις επιτρεπόμενες καταχωρήσεις (whitelist) και της ανίχνευσης με ισχυρές πολιτικές ελέγχου. Επίσης, πρέπει να διασφαλιστεί ότι έχει πραγματοποιηθεί προσθήκη ρύθμισης ελέγχου διαχειριστή patch και ασφάλειας δικτύου στο περιβάλλον για να προστατευτούν τα τερματικά. Αν επιτρέπετε στα τερματικά να εγκαταλείψουν φυσικά το περιβάλλον σας, αναγνωρίστε τους κινδύνους από την επιστροφή τους με κακόβουλο λογισμικό. Τα προγράμματα BYOD θα πρέπει να αντιμετωπίζουν κάθε συσκευή που ανήκει σε εργαζόμενο ως πιθανό επιτιθέμενο και επιτρέπουν μόνο την πρόσβαση σε περιορισμένα τμήματα του δικτύου και τα τμήματα αυτά θα πρέπει να παρακολουθούνται σε μεγάλο βαθμό με τεχνολογίες κυνηγιού απειλών.

Δίνοντάς λογαριασμούς στους χρήστες με τα λιγότερα προνόμια που είναι απαραίτητα για την εκτέλεση εργασιών. Αυτό περιλαμβάνει όλους τους λογαριασμούς διαχειριστή που μπορείτε να χρησιμοποιήσετε στο περιβάλλον σας. Μην χρησιμοποιείτε το λογαριασμό γενικού διαχειριστή για κοινές λειτουργίες διαχείρισης. Πρέπει να γίνεται δημιουργία λογαριασμών διαχείρισης με συγκεκριμένες οργανωτικές μονάδες ή εργασίες και χρήση του λογαριασμού με το λιγότερο προνόμιο που απαιτείται για να ολοκληρώσετε την κάθε εργασία. Θυμηθείτε, εάν το πλαίσιο στο οποίο πρόκειται να συνδεθείτε έχει παραβιαστεί, ο εισβολέας μπορεί να ανακτήσει τα διαπιστευτήριά σας από τη μνήμη, δίνοντάς του πρόσβαση σε οτιδήποτε μπορεί να έχει πρόσβαση ο λογαριασμός σας. Χρήση ασφαλών διαχειριστικών σταθμών εργασίας για προνομιακή πρόσβαση στο λογαριασμό, αντί της χρήσης του σταθμού εργασίας καθημερινής χρήσης για εργασίες διαχείρισης. Οι επιτιθέμενοι θα στοχεύουν στους υπολογιστές των διαχειριστών, γνωρίζοντας ότι οι βασικοί καταχωρητές και τα εργαλεία ανάκτησης της RAM σε αυτά τα συστήματα ενδέχεται να οδηγήσουν σε διαπιστευτήρια για αυξημένους λογαριασμούς. Χρησιμοποιώντας ένα αυστηρό σύστημα περιορισμένης πρόσβασης με πρόσθετα στοιχεία ελέγχου εισερχόμενης σύνδεσης για την πραγματοποίηση συνδέσεων

διαχείρισης, γίνετε πολύ δύσκολο για έναν εισβολέα να αποκτήσει τα προνομιακά διαπιστευτήρια που αναζητά.

Εκτός από την προστασία των διαπιστευτηρίων, γίνεται διασφάλιση ότι έχουν αποθηκευτεί με ασφάλεια όλες οι παραστάσεις κωδικών πρόσβασης hash. Απαγόρευση στις εφαρμογές ιστού να χρησιμοποιούν αδύναμους αλγόριθμους κατακερματισμού κωδικού πρόσβασης, όπως μη αναρτημένο MD5 για την αποθήκευση διαπιστευτηρίων. Εάν τα διαπιστευτήρια χάνονται, πρέπει να γίνεται διασφάλιση ότι γίνετε παρακολούθηση του εσωτερικού του δικτύου για τον εντοπισμό και τη χρήση τους. Οι σταθμοί εργασίας συνήθως συνδέονται σε μια σειρά από διακομιστές σε ένα περιβάλλον. Όταν γίνετε αντιληπτό σε έναν σταθμό εργασίας ότι ξαφνικά επικοινωνεί με άλλους σταθμούς εργασίας ή με διακομιστές στους οποίους δεν είχε πρόσβαση ποτέ πριν, αυτό πρέπει να είναι μια ένδειξη. Πολλοί οργανισμοί απλά δεν παρακολουθούν τη δραστηριότητα των εσωτερικών χρηστών και οι επιτιθέμενοι αξιοποιούν σε μεγάλο βαθμό αυτό το τυφλό σημείο.

- Εξέταση του λογαριασμού σύνδεσης και των συμβάντων σύνδεσης

Η σύνδεση στο λογαριασμό είναι ο όρος της Microsoft για τον έλεγχο ταυτότητας. Η σύνδεση είναι ο όρος που χρησιμοποιείται για να αναφερθεί σε έναν λογαριασμό που αποκτά πρόσβαση σε έναν πόρο. Και τα δύο συμβάντα λογαριασμός σύνδεσης και συμβάν σύνδεσης θα καταγράφονται στο αρχείο καταγραφής συμβάντων ασφαλείας. Ο έλεγχος της ταυτότητας (λογαριασμός σύνδεσης) των λογαριασμών τομέα εκτελείται από έναν ελεγκτή τομέα εντός ενός δικτύου των Windows. Τοπικοί λογαριασμοί (εκείνοι που υπάρχουν σε ένα τοπικό αρχείο SAM και όχι ως μέρος της υπηρεσίας καταλόγου Active Directory) επικυρώνονται από το τοπικό σύστημα όπου υπάρχουν. Τα συμβάντα σύνδεσης στο λογαριασμό θα καταγράφονται από το σύστημα που εκτελεί τον έλεγχο ταυτότητας. Ο έλεγχος των συμβάντων συνδεδεμένων λογαριασμών και συμβάντων σύνδεσης πραγματοποιείται εύκολα από την πολιτική ομάδας. Παρόλο που η Microsoft συνεχίζει να ενεργοποιεί την καταγραφή περισσότερων στοιχείων στις νέες εκδόσεις των Windows, οι διαχειριστές θα πρέπει να επανεξετάζουν τις πολιτικές ελέγχου τους σε τακτική βάση, ώστε να εξασφαλίζουν ότι όλα τα συστήματα δημιουργούν επαρκή αρχεία καταγραφής. Η δυνατότητα αποθήκευσης αρχείων καταγραφής συμβάντων σε απομακρυσμένα συστήματα (είτε χρησιμοποιώντας τις εγγενείς λειτουργίες απομακρυσμένης καταγραφής από τη Microsoft είτε από τρίτους κατασκευαστές SIEM ή άλλα εργαλεία) βοηθά στην προστασία των αρχείων καταγραφής από αλλοίωση ή καταστροφή.

Επομένως, οι ελεγκτές τομέα σε ένα δίκτυό θα πρέπει να είναι σε θέση να παρέχουν μια αρκετά συγκεντρωτική καταγραφή για τους λογαριασμούς στους οποίους έχουν πιστοποιηθεί σε ολόκληρο τον τομέα. Για να υπάρξει μια πλήρη εικόνα, θα πρέπει να γίνετε ερώτηση σε κάθε DC από εκείνο που εκτελεί τον έλεγχο ταυτότητας και δημιουργεί το σχετικό αρχείο καταγραφής συμβάντων. Από την άλλη πλευρά, εάν διασφαλίσουμε ότι οι διακομιστές-μέλη ή οι σταθμοί εργασίας πραγματοποιούν τη δική τους πιστοποίηση ταυτότητας, είναι μια καλή ένδειξη ότι οι τοπικοί λογαριασμοί χρηστών χρησιμοποιούνται. Καθώς αυτό δεν γίνεται συνήθως στα περισσότερα περιβάλλοντα, τα συμβάντα σύνδεσης λογαριασμών σε ελεγκτές που δεν είναι στο δίκτυο μπορούν συχνά να είναι ένας δείκτης χειραγώγησης. Αντιθέτως, τα αρχεία καταγραφής συμβάντων σύνδεσης δημιουργούνται από το σύστημα στο οποίο γίνεται πρόσβαση, επομένως τα συμβάντα σύνδεσης θα δημιουργηθούν από τα συστήματα σε ολόκληρο το δίκτυο, παρέχοντας έναν ακόμη λόγο για τη συγκέντρωση των καταγραφών σε μια κεντρική τοποθεσία.

Τα αναγνωριστικά συμβάντων που παρουσιάζουν ιδιαίτερο ενδιαφέρον στους ελεγκτές τομέα σας περιλαμβάνουν τα εξής:

- 4768 - Η έκδοση ενός Ticket Granting Ticket (TGT) δείχνει ότι ένας συγκεκριμένος λογαριασμός χρήστη πιστοποιήθηκε από τον ελεγκτή τομέα.
- 4769 - Ένα δελτίο υπηρεσίας εκδόθηκε σε ένα συγκεκριμένο λογαριασμό χρήστη για έναν καθορισμένο πόρο. Αυτό το συμβάν θα δείξει την πηγή προέλευσης του συστήματος που έκανε την αίτηση, τον λογαριασμό χρήστη που χρησιμοποιήθηκε και την υπηρεσία για την πρόσβαση. Αυτά τα συμβάντα παρέχουν μια χρήσιμη πηγή στοιχείων καθώς παρακολουθούν την επαλήθευση της ταυτότητας των χρηστών σε όλο το δίκτυο.

- 4776 - Παρόλο που είναι λιγότερο συνηθισμένο σε ένα περιβάλλον τομέα, το NTLM (υπηρεσία της Microsoft για αυθεντικοποίηση χρηστών) ενδέχεται να εξακολουθεί να χρησιμοποιείται για τον έλεγχο της ταυτότητας. Επιπλέον, πολλά εργαλεία επίθεσης υποβαθμίζουν τις προσπάθειες ελέγχου ταυτότητας του NTLM κατά την επικύρωση. Ενώ αυτοί οι τύποι ταυτοποίησης ενεργοποιούνται συχνά σε νόμιμη κυκλοφορία, όπως ορισμένες αιτήσεις επαλήθευσης που προέρχονται από τη διεύθυνση IP και όχι από το όνομα του υπολογιστή, η παρουσία τους μπορεί επίσης να υποδεικνύει και ένα μη τυποποιημένο εργαλείο που χρησιμοποιείται για τον έλεγχο ταυτότητας

Σε διακομιστές μελών και σταθμούς εργασίας, τα αναγνωριστικά συμβάντων περιλαμβάνουν:

- 4624 - Έχει γίνει μια σύνδεση σε ένα σύστημα. Ο τύπος 2 υποδεικνύει μια αλληλεπιδραστική (τοπική) σύνδεση, ενώ ένας τύπος 3 δηλώνει απομακρυσμένη σύνδεση ή σύνδεση στο δίκτυο.
- 4672 - Αυτό το Αναγνωριστικό συμβάντος καταγράφεται όταν ορισμένα δικαιώματα που σχετίζονται με αυξημένη ή διαχειριστή πρόσβαση παραχωρούνται σε μια σύνδεση. Όπως συμβαίνει με όλα τα συμβάντα σύνδεσης, το αρχείο καταγραφής συμβάντων θα δημιουργηθεί από το σύστημα στο οποίο έγινε η πρόσβαση.
- 4776 - Έχει πραγματοποιηθεί έλεγχος ταυτότητας με βάση το NTLM. Όταν εντοπιστεί σε ελεγκτή εκτός τομέα, αυτό υποδεικνύει τη χρήση ενός τοπικού λογαριασμού χρήστη. Δεδομένου ότι οι περισσότεροι τομείς σχεδιάζονται για να χρησιμοποιούν τομείς αντί για τοπικούς λογαριασμούς χρηστών, η παρουσία αυτού του αναγνωριστικού συμβάντος σε διακομιστές-μέλη ή σταθμούς εργασίας-πελάτη είναι συχνά ύποπτος.

- Πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας (RDP)

Ξέροντας ότι το RDP αξιοποιεί τον τυπικό έλεγχο ταυτότητας της Microsoft για τον έλεγχο των πηγών πρόσβασης, τα αρχεία καταγραφής που σχετίζονται με τα συμβάντα σύνδεσης και τα συμβάντα σύνδεσης που περιγράφονται παραπάνω ισχύουν για συνδέσεις RDP. Εκτός από τα συμβάντα σύνδεσης λογαριασμού, άλλες καταχωρήσεις καταγραφής συμβάντων που μπορεί να είναι χρήσιμες για την ανίχνευση και παρακολούθηση κακόβουλης χρήσης του RDP στο περιβάλλον σας είναι τα παρακάτω:

- 4624 - Το συμβάν σύνδεσης θα εμφανίζει είτε με Τύπο 10 είτε με Τύπο 3 όταν χρησιμοποιείται το RDP, ανάλογα με τις εκδόσεις των Windows που χρησιμοποιούνται και τις συγκεκριμένες παραμέτρους τους.
- 4778 - Καταγράφει την επανασύνδεση μιας σύνδεσης.
- 4779 - Καταγράφει την αποσύνδεση μιας περιόδου σύνδεσης. Όπως συμβαίνει με πολλά συμβάντα απόκρισης, αυτό μπορεί να μην καταγραφεί ακόμη και κατά τη διάρκεια της κανονικής δραστηριότητας.

Επιπλέον, το %SystemRoot%/System32/winevt/Logs/Microsoft-WindowsTerminalServices-LocalSessionManager%4Operational ενδέχεται να παρέχει πρόσθετες λεπτομέρειες σχετικά με τις συνδέσεις RDP σε ένα περιβάλλον. Υπάρχουν επίσης λύσεις παρακολούθησης ασφάλειας δικτύου για να παρακολουθήσετε δραστηριότητα στη θύρα 3389, η οποία είναι η προεπιλεγμένη θύρα για RDP συνδέσεις.

- At/schtasks

Οι διαχειριστές πρέπει να χρησιμοποιούν συνεχώς την εντολή schtasks για να ελέγξουν τις διεργασίες που έχουν προγραμματιστεί προς εκτέλεση. Η εντολή schtasks θα εμφανίσει στοιχεία που έχουν προγραμματιστεί τόσο με schtasks όσο και με at ενώ η εντολή at δεν θα εμφανίσει στοιχεία που έχουν προγραμματιστεί με schtasks. Με την ακόλουθη εντολή γίνεται εξαγωγή της λίστας εργασιών σε ένα αρχείο τιμών οι οποίες είναι διαχωρισμένες με κόμματα:

Schtasks /query /fo csv > scheduled_tasks.csv

Προαιρετικά μπορεί κάποιος να συμπεριλάβει την τιμή /v για να ενεργοποιήσει τη λεπτομερή έξοδο εάν χρειάζεται επιπλέον λεπτομέρειες.

Το PowerShell μπορεί να αξιοποιηθεί για να διερευνήσει τα απομακρυσμένα συστήματα με αυτοματοποιημένο τρόπο. Το cmdlet PowerShell Get-ScheduledTask θα εμφανίσει τη διαδρομή, το όνομα και την κατάσταση των προγραμματισμένων εργασιών κατά την εκτέλεση. Οποιαδήποτε χρήση πιστοποιημένων διαπιστευτηρίων για προγραμματισμό εργασιών σε απομακρυσμένα συστήματα θα αφήσει βέβαια τη σχετική σύνδεση και τα συμβάντα σύνδεσης, όπως συζητήθηκε προηγουμένως.

- Sc

Όπως και με την εντολή schtasks, οι διαχειριστές θα πρέπει να καθορίσουν μια γραμμή αναφοράς για τις υπηρεσίες που εκτελούνται σε κάθε σύστημα. Αυτό μπορεί να επιτευχθεί χρησιμοποιώντας το WMIC ή το PowerShell είτε ως τοπικό σενάριο που εκτελείται σε καθορισμένα χρονικά διαστήματα, είτε ως κεντρικό σενάριο που ερωτά απομακρυσμένα συστήματα και αποθηκεύει αυτόν τον τύπο δεδομένων σε μια κεντρική τοποθεσία. Η ιστορική καταγραφή των θυρών, των διαδικασιών, των υπηρεσιών κ.λπ. που χρησιμοποιούνται σε κάθε σύστημα (ή τουλάχιστον σε κρίσιμα συστήματα) που συλλέγονται από τέτοιες δέσμες ενεργειών παρέχει μια μεγάλη αναφορά στην έρευνα όταν δηλώνεται ένα περιστατικό. Το αναγνωριστικό συμβάντος 7045 καταγράφει τη δημιουργία μιας νέας υπηρεσίας στο σύστημα, συμπεριλαμβανομένης της διαδρομής προς το όνομα του αρχείου υπηρεσίας εκτελέσιμης λειτουργίας. Αυτό το συμβάν, που καταγράφηκε στο αρχείο καταγραφής συμβάντων του συστήματος, μπορεί να είναι χρήσιμο για τον εντοπισμό της δημιουργίας κακόβουλων υπηρεσιών στα συστήματα των θυμάτων. Οποιαδήποτε χρήση διαπιστευμένων πιστοποιητικών για την τροποποίηση υπηρεσιών σε απομακρυσμένα συστήματα θα αφήσει επίσης τα συνδεδεμένα στοιχεία σύνδεσης και τα συμβάντα σύνδεσης

- Μέσα διαχείρισης της γραμμής εντολών των Windows (WMIC)

Για άλλη μια φορά, η χρήση του WMIC απαιτεί την πραγματοποίηση επικυρωμένης πρόσβασης στο σύστημα προορισμού, οπότε χρησιμοποιώντας συμβάντα ελέγχου και συμβάντα σύνδεσης για τον εντοπισμό ασυνήθιστης πρόσβασης στο σύστημα είναι ένας χρήσιμος δείκτης για τον εντοπισμό ύποπτης δραστηριότητας του WMI. Επιπλέον, η χρήση του WMIC δεν περιορίζεται σε κακόβουλους επιθέσεις. Οι αμυνόμενοι θα πρέπει να αξιοποιούν το WMIC για να βοηθήσουν στην αυτοματοποίηση της δημιουργίας βασικών γραμμών του συστήματος, στην ανίχνευση συγκεκριμένων δεικτών συμβιβασμού και άλλων καθηκόντων ασφαλείας, προκειμένου να εκμεταλλευτεί εξολοκλήρου τις δυνατότητες που παρέχει το WMI.

Για να ανιχνευθεί κακόβουλη χρήση του WMI σε ένα περιβάλλον, τα σενάρια PowerShell μπορούν να σας βοηθήσουν για να δημιουργηθούν ειδοποιήσεις δραστηριότητας που μπορούν να τροφοδοτηθούν σε ένα SIEM για βελτιωμένη ανίχνευση. Ο Matt Graeber έχει γράψει μερικά σενάρια που χρησιμεύουν ως καλό σημείο εκκίνησης για τέτοιες προσπάθειες και μπορούν να τροποποιηθούν για να προσαρμόσουν το περιβάλλον σας. Μπορείτε να βρείτε το έργο του Matt στο GitHub στη διεύθυνση https://github.com/mattifestation.

- WinRM

Το WinRM χρησιμοποιεί θύρα TCP 5985 για κυκλοφορία HTTP και θύρα TCP 5986 για HTTPS από προεπιλογή. Είναι επομένως σκόπιμο να ρυθμιστούν τα εργαλεία παρακολούθησης της ασφάλειας δικτύου για να γίνει αναζήτηση ασυνήθιστης δραστηριότητας σε αυτές τις θύρες. Επιπλέον, συγκεκριμένα αναγνωριστικά συμβάντων μπορεί να είναι χρήσιμα όταν γίνει προσπάθεια εντοπισμού κακόβουλης χρήσης του WinRM. Αυτά τα συμβάντα θα καταγραφούν στο αρχείο καταγραφής %SystemRoot%/System32/winevt/Logs/MicrosoftWindows-WinRM% 4Operational.

Όταν ξεκινάει μια σύνδεση χρησιμοποιώντας το WinRM, θα δημιουργηθεί Event ID 6. Αυτό το συμβάν θα περιλαμβάνει τον απομακρυσμένο προορισμό στον οποίο επιχειρήθηκε η σύνδεση. Επομένως, η εμφάνιση του αναγνωριστικού συμβάντος 6 σε τοπικούς σταθμούς εργασίας ή σε άλλους υπολογιστές όπου οι εργασίες διαχείρισης δεν εκτελούνται συχνά ενδέχεται να είναι ύποπτες.

Επιπλέον, το αναγνωριστικό συμβάντος 91 θα καταγραφεί στο σύστημα όπου λαμβάνεται η σύνδεση. Αυτό το αρχείο καταγραφής θα περιλαμβάνει το πεδίο χρήστη που εμφανίζει το λογαριασμό που χρησιμοποιείται για τον έλεγχο της σύνδεσης. Για άλλη μια φορά, τα τυποποιημένα συμβάντα

σύνδεσης και σύνδεσης μπορούν επίσης να χρησιμοποιηθούν για να συμπληρωθούν πρόσθετα κενά σχετικά με τα συστήματα, τους λογαριασμούς και τους χρόνους που σχετίζονται με τη δραστηριότητα αυτή.

- PowerShell

Η απομακρυσμένη λειτουργία του PowerShell είναι ενεργοποιημένη από προεπιλογή για τα μέλη της ομάδας διαχειριστών και της ομάδας απομακρυσμένης διαχείρισης χρηστών από τον Windows Server 2012 και μετέπειτα. Εάν η σύνδεση δικτύου έχει οριστεί σε ένα ιδιωτικό δίκτυο, το τείχος προστασίας των Windows θα επιτρέψει παρομοίως την απομακρυσμένη χρήση του PowerShell. Ενώ η απενεργοποίηση της απομακρυσμένης χρήσης του PowerShell μπορεί να αποτρέψει τη χρήση του από τους επιτιθέμενους, απενεργοποιεί επίσης ένα από τα πιο ισχυρά εργαλεία του οπλοστασίου του διαχειριστή για καθημερινές διοικητικές εργασίες, καθώς και για τη βασική λειτουργία και το χειρισμό συμβάντων. Ακριβώς όπως οι επιτιθέμενοι έχουν εργαλεία όπως το Empire για να τους βοηθήσουν να κάνουν τη δουλειά τους, έτσι ώστε οι αμυνόμενοι έχουν πακέτα όπως το Kansa για να τους βοηθήσουν να κάνουν τη δική τους δουλειά. Το Kansa επιτρέπει στους αμυνόμενους να συλλέγουν δεδομένα από συλλογές συστημάτων, να στοιβάζουν τα αποτελέσματα και να αναζητούν για αποκλίσεις από τον κανόνα. Αυτό μπορεί να είναι ένα ισχυρό εργαλείο τόσο για την προετοιμασία όσο και για την αντιμετώπιση περιστατικών.

Η Microsoft συνεχίζει να αυξάνει το ποσό των διαθέσιμων καταγραφών γύρω από το PowerShell για να βοηθήσει στην καταπολέμηση της κακομεταχείρισης. Για άλλη μια φορά, αυτές οι εγκαταστάσεις καταγραφής πρέπει να ενεργοποιούνται μέσω της Πολιτικής ομάδας, συγκεκριμένα στη ρύθμιση παραμέτρων υπολογιστή > Πολιτικές > Πρότυπα διαχείρισης > Στοιχεία των Windows > Windows PowerShell.

Υπάρχουν τρεις βασικές κατηγορίες καταγραφής που μπορεί να είναι διαθέσιμες, ανάλογα με την εκάστοτε έκδοση των Windows.

Εντοπισμός ενότητας

- Καταγραφή συμβάντων εκτέλεσης αγωγών.
- Καταγραφή των αρχείων καταγραφής συμβάντων.

Καταγραφή αποκλεισμού εκτέλεσης σεναρίων

- Καταγράφει τις απομακρυσμένες εντολές που έχουν σταλθεί στο PowerShell.
- Αποτυπώνει μόνο τις εντολές, όχι την έξοδο.
- Καταγράφει τα αρχεία καταγραφής συμβάντων.

Μεταγραφή

- Καταγράφει την είσοδο και την έξοδο του PowerShell.
- Δεν θα συλλάβει την έξοδο των εξωτερικών προγραμμάτων που εκτελούνται, παρά μόνο του PowerShell.
- Καταγράφει αρχεία κειμένου.

Αφού ενεργοποιηθεί, αυτά τα αρχεία καταγραφής μπορούν να παρέχουν πληθώρα πληροφοριών σχετικά με τη χρήση του PowerShell στα συστήματά. Αν τρέχουν συνήθως πολλά σενάρια PowerShell, αυτό μπορεί να παράγει ένα μεγάλο όγκο δεδομένων, οπότε πρέπει να έχουν ρυθμιστεί οι εγκαταστάσεις ελέγχου ώστε να επιτευχθεί ισορροπία μεταξύ ορατότητας και φορτίου πριν από την ανάπτυξη τέτοιων αλλαγών στην παραγωγή.

Οι καταχωρίσεις του αρχείου καταγραφής συμβάντων PowerShell εμφανίζονται σε διαφορετικά αρχεία καταγραφής συμβάντων. Μέσα στο %SystemRoot%/System32/winevt/Logs/Microsoft-Windows-PowerShell%4Operational

θα βρείτε δύο συμβάντα ιδιαίτερης σημασίας:

- 4103
  - Εμφανίζει την εκτέλεση του pipeline από τη μονάδα καταγραφής μονάδων.
  - Περιλαμβάνει το πλαίσιο χρήστη που χρησιμοποιείται για την εκτέλεση των εντολών.

- Το πεδίο Hostname θα εμφανίσει την "Κονσόλα" εάν έχει εκτελεστεί τοπικά ή θα εμφανιστεί αν έχει τρέξει από ένα απομακρυσμένο σύστημα.
- Μπορεί να συσχετίσει τη σύνδεση με το λογαριασμό και το αρχείο καταγραφής

- 4104
  - Εμφανίζει καταχωρήσεις καταγραφής εκτέλεσης σεναρίων που μπλοκαρίστηκαν.
  - Θα εμφανιστεί ως συμβάν σε επίπεδο "Προειδοποίησης" αν η Microsoft κρίνει ότι η δραστηριότητα είναι "ύποπτη.
- Event 400
  - Υποδεικνύει την έναρξη εκτέλεσης εντολών ή συνεδρίας
  - Το πεδίο Hostname εμφανίζει αν η (τοπική) κονσόλα ή η απομακρυσμένη περίοδος σύνδεσης προκάλεσε την εκτέλεση.
- Event 800
  - Δείχνει λεπτομέρειες εκτέλεσης αγωγού
  - Το αναγνωριστικό χρήστη εμφανίζει το λογαριασμό που χρησιμοποιήθηκε
  - Το πεδίο Hostname εμφανίζει αν η (τοπική) κονσόλα ή η απομακρυσμένη περίοδος σύνδεσης προκάλεσε την εκτέλεση
  - Επειδή πολλά κακόβουλα σενάρια κωδικοποιούν επιλογές με το Base64, ελέγξτε το πεδίο HostApplication για επιλογές που κωδικοποιούνται με το παράμετρο -enc.

Η απομακρυσμένη εκτέλεση του PowerShell χρησιμοποιεί το WinRM για τη δημιουργία συνδέσεων σε απομακρυσμένα μηχανήματα. Ως αποτέλεσμα, οι ίδιες μέθοδοι ανίχνευσης που χρησιμοποιούνται για το WinRM ισχύουν επίσης για την απομακρυσμένη εκτέλεση του PowerShell. Ανεξάρτητα από το αν χρησιμοποιείται HTTP ή HTTPS στη μεταφορά WinRM, το PowerShell κρυπτογραφεί όλες τις απομακρυσμένες εντολές με το AES-256 μετά τον αρχικό έλεγχο ταυτότητας.

Οι αμυνόμενοι του δικτύου μπορούν να βοηθήσουν στη διασφάλιση του PowerShell στο περιβάλλον τους, δημιουργώντας περιορισμένα τελικά σημεία με περιορισμένες διαμορφώσεις συνεδριών PowerShell, που επιτρέπουν πιο λεπτομερή έλεγχο των χρηστών που μπορούν να χρησιμοποιήσουν το PowerShell απομακρυσμένα και να ελέγχουν ποια cmdlets μπορούν να εκτελέσουν. Τα σενάρια μπορούν επίσης να περιοριστούν με βάση διάφορους παράγοντες, όπως εάν είναι τοπικοί ή απομακρυσμένοι και εάν έχουν υπογραφεί. Ωστόσο, υπάρχουν πολλές τεχνικές παράκαμψης της πολιτικής εκτέλεσης για τους επιτιθέμενους για να παρακάμψουν αυτούς τους ελέγχους δέσμης ενεργειών, οπότε δεν πρέπει ο αμυνόμενος να επαναπαύεται. Πρέπει να γίνεται ενεργή παρακολούθηση του δικτύου για ενδείξεις κακόβουλης δραστηριότητας PowerShell, παρά τους περιορισμούς αυτούς.

Κεφάλαιο 4 Επεξήγηση των προγραμμάτων για εσωτερική μετακίνηση

4.1 Εργαλείο επαύξησης δικαιωμάτων

Αποφυγή του ελέγχου για τον λογαριασμό του χρήστη

Ο έλεγχος λογαριασμού χρηστών των Windows (UAC) επιτρέπει σε ένα πρόγραμμα να αυξάνει τα προνόμιά του για να εκτελέσει μια εργασία κάτω από δικαιώματα διαχειριστή, προτρέποντας τον χρήστη να επιβεβαιώσει. Ο αντίκτυπος στον χρήστη κυμαίνεται από την άρνηση της λειτουργίας υπό υψηλή επιβολή ώστε να επιτρέπεται στο χρήστη να εκτελέσει τη δράση αν είναι στην ομάδα των τοπικών διαχειριστών και να κάνει κλικ στη γραμμή εντολών ή να τους επιτρέψει να εισαγάγουν έναν κωδικό πρόσβασης διαχειριστή για να ολοκληρώσουν τη δράση.

Εάν το επίπεδο προστασίας UAC ενός υπολογιστή είναι ρυθμισμένο σε οτιδήποτε άλλο εκτός από το υψηλότερο επίπεδο, ορισμένα προγράμματα των Windows επιτρέπεται να ανυψώνουν προνόμια ή να εκτελούν ορισμένα ανυψωμένα αντικείμενα COM χωρίς να ζητούν άδεια

από το χρήστη μέσω του πλαισίου ειδοποιήσεων UAC. Ένα παράδειγμα αυτού είναι η χρήση του rundll32.exe για τη φόρτωση ενός συγκεκριμένα επεξεργασμένου DLL το οποίο φορτώνει ένα αντικείμενο αυτόματης αύξησης COM και εκτελεί μια λειτουργία αρχείου σε έναν προστατευμένο κατάλογο ο οποίος συνήθως απαιτεί αυξημένη πρόσβαση. Το κακόβουλο λογισμικό μπορεί επίσης να εγχέεται σε μια αξιόπιστη διαδικασία για να αποκτήσει αυξημένα προνόμια χωρίς να ζητήσει άδεια από ένα χρήστη. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν αυτές τις τεχνικές για να αυξήσουν τα προνόμια στον διαχειριστή, εάν η διαδικασία προορισμού είναι απροστάτευτη.

4.2 Εργαλεία απομακρυσμένων εντολών

Psexec

Βοηθητικά προγράμματα όπως το Telnet και τα προγράμματα απομακρυσμένου ελέγχου, όπως το PC Anywhere της Symantec, επιτρέπουν να εκτελέσουμε προγράμματα σε απομακρυσμένα συστήματα, αλλά μπορεί να είναι περίπλοκα στην εγκατάσταση και να απαιτηθεί η εγκατάσταση λογισμικού πελάτη στα απομακρυσμένα συστήματα στα οποία επιθυμεί κάποιος να έχει πρόσβαση. Το PsExec είναι μια ελαφριά αντικατάσταση telnet που επιτρέπει την εκτέλεση διαδικασιών σε άλλα συστήματα, με πλήρη αλληλεπίδραση για εφαρμογές κονσόλας, χωρίς χρειάζεται η εγκατάσταση λογισμικού πελάτη. Οι πιο ισχυρές χρήσεις του PsExec περιλαμβάνουν την εκκίνηση διαδραστικών εντολών σε απομακρυσμένα συστήματα και την εκκίνηση εργαλείων απομακρυσμένης ενεργοποίησης όπως το IpConfig που διαφορετικά δεν θα είχαν τη δυνατότητα να εμφανίζουν πληροφορίες σχετικά με τα απομακρυσμένα συστήματα.

Σημείωση: ορισμένοι ανιχνευτές προστασίας από ιούς θα αναφέρουν ότι ένα ή περισσότερα από τα εργαλεία έχουν μολυνθεί από ιό απομακρυσμένης διαχείρισης. Κανένα από τα PsTools δεν περιέχει ιούς, αλλά έχουν χρησιμοποιηθεί από ιούς, γι 'αυτό και προκαλούν ειδοποιήσεις για ιούς.

Εγκατάσταση:

Απλά αντιγράφουμε το PsExec στην εκτελέσιμη διαδρομή. Πληκτρολογώντας "psexec" εμφανίζεται η σύνταξη χρήσης του.

Παραδείγματα

Η ακόλουθη εντολή εκκινεί μια διαδραστική εντολή για την εντολή \\ marklap:

psexec \\ marklap cmd

Αυτή η εντολή εκτελεί το IpConfig στο απομακρυσμένο σύστημα με την επιλογή / all και εμφανίζει την έξοδο τοπικά:

psexec \\ marklap ipconfig / all

Αυτή η εντολή αντιγράφει το πρόγραμμα test.exe στο απομακρυσμένο σύστημα και το εκτελεί διαδραστικά:

psexec \\ marklap -c test.exe

Καθορίζει την πλήρη διαδρομή προς ένα πρόγραμμα που είναι ήδη εγκατεστημένο σε ένα απομακρυσμένο σύστημα αν δεν είναι στη διαδρομή του συστήματος:

psexec \\ marklap c: \ bin \ test.exe

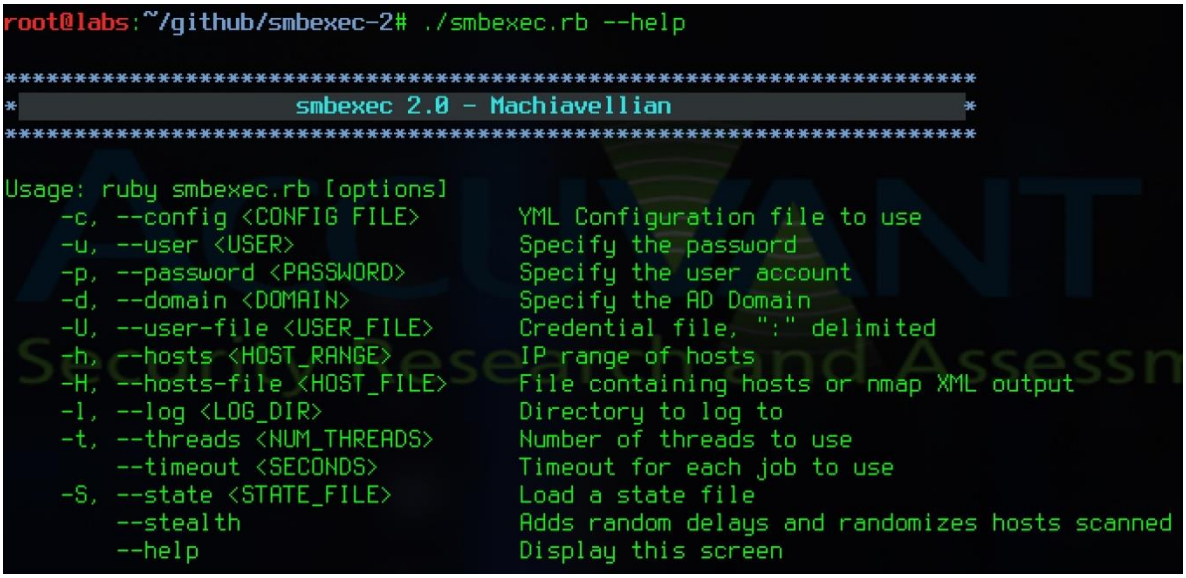
Εκτελεί το Regedit διαδραστικά στο λογαριασμό System για να γίνει προβολή των περιεχόμενων των κλειδιών SAM και SECURITY ::

psexec -i -d -s c: \ windows \ regedit.exe

Για να γίνει εκτέλεση του Internet Explorer όπως και για τα δικαιώματα περιορισμένων χρηστών, γίνεται χρήση της παρακάτω εντολής:

psexec -l -d "c: \ αρχεία προγράμματος \ internet explorer \ iexplore.exe"

SMBexec

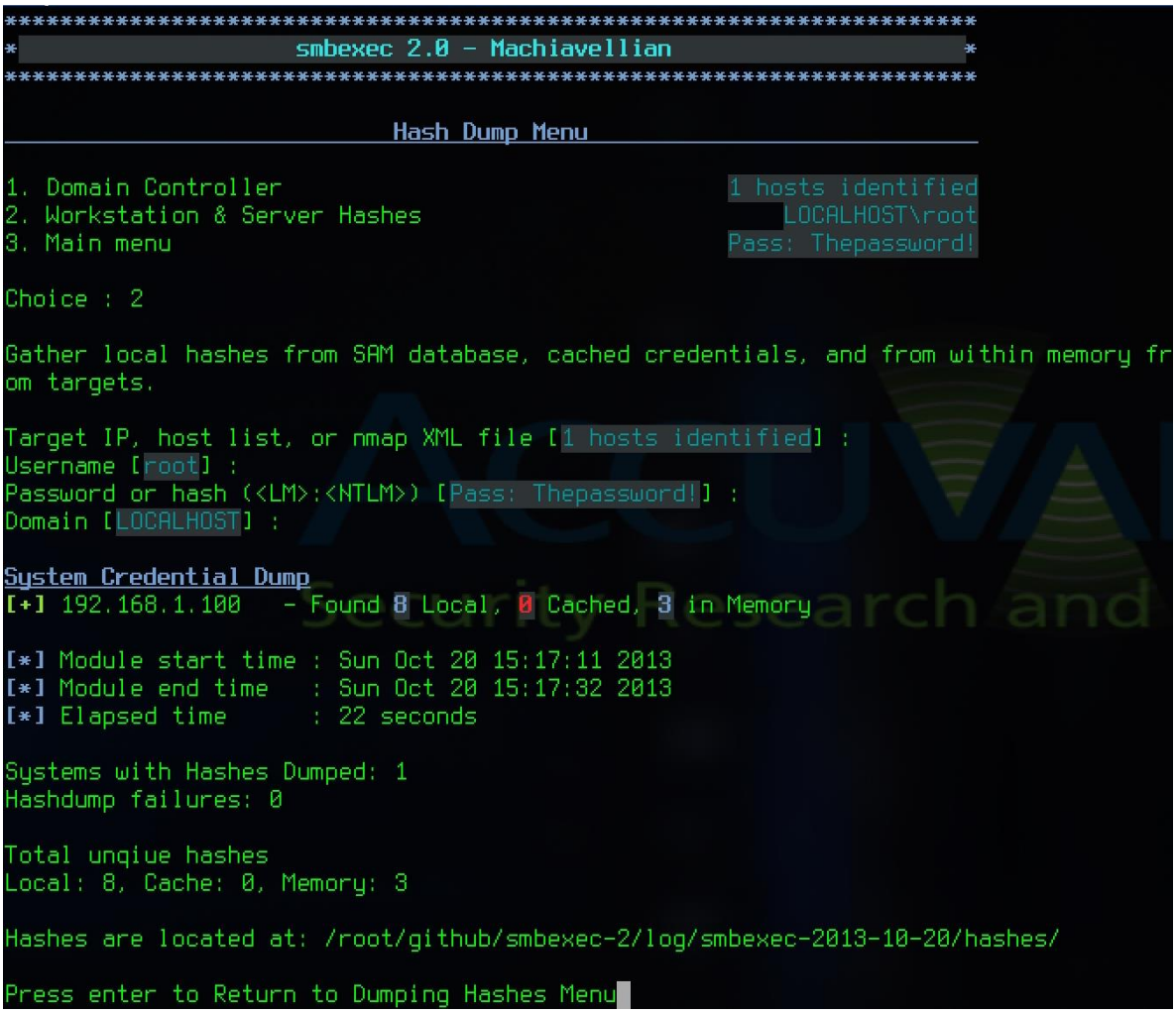


Σχήμα 3 smbexec

Το smbexec είναι ένα εργαλείο που εστιάζει στη χρήση των προγκατεστημένων λειτουργιών / παραμέτρων των Windows με σκοπό την εκμετάλλευση και στην επέκταση της πρόσβασης σε ένα δίκτυο μετά την απόκτηση ορισμένων διαπιστευτηρίων, είτε πρόκειται για hash κωδικούς είτε για κωδικούς πρόσβασης για έναν τοπικό λογαριασμό ή έναν λογαριασμό τομέα. Επιτρέπει στον επιτιθέμενο να εντοπίζει γρήγορα στόχους και να αποκτά πρόσβαση σε αυτούς σε μεγάλα δίκτυα χωρίς να χρειάζεται να ανησυχεί πολύ για το αντιικό και το ελέγχου λογαριασμού χρήστη (UAC).

Με τη μετάβαση στο Ruby από το κέλυφος υπάρχουν πολλά πλεονεκτήματα. Το μεγαλύτερο πλεονέκτημα είναι το multi-threading, το οποίο κάνει μια σημαντική διαφορά όταν ο επιτιθέμενος δοκιμάζει σε ένα μεγαλύτερο δίκτυο. Εκτός από τα κέρδη ταχύτητας υπάρχει επίσης μια σημαντική αύξηση στην καταγραφή, όταν τρέχει οποιαδήποτε λειτουργική μονάδα, δημιουργείται ένα αρχείο εντοπισμού σφαλμάτων που περιέχει πληροφορίες σχετικά με την ενότητα, και δείχνει το χρόνο εκτέλεσης της εντολής μαζί με το αποτέλεσμα.

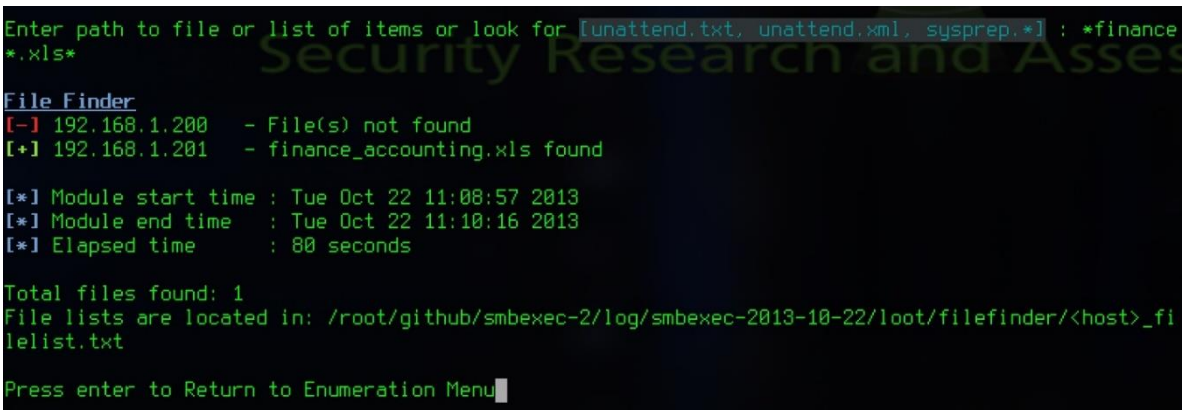
Ακολουθεί ένα παράδειγμα της εμφάνισης της έκδοσης 2.0 χρησιμοποιώντας τη λειτουργική μονάδα hashdump:



Σχήμα 4 smbexec με τη χρήση hashdump

Από προεπιλογή στις τεχνικές διείσδυσης γίνεται αναζητά αρχείων χωρίς επίκεντρο τα οποία, αν υπάρχουν, συνήθως έχουν προνομιακά διαπιστευτήρια που περιέχονται μέσα, αλλά μπορεί να γίνει αναζήτηση σε οτιδήποτε άλλο θελήσει ο επιτιθέμενος. Επιπλέον, ψάχνοντας για άλλα πράγματα όπως το passwords.xls, προσωπικά ψάχνω κάτι σαν * finance * .xls * για να ψάξω για δεδομένα που θα θεωρούσε κανείς κρίσιμα για το δίκτυο, μπορεί να καταστήσει πολύ πιο εύκολη την επίδειξη των επιπτώσεων μιας ευπάθειας, αν για παράδειγμα υπάρχει πρόσβαση σε ένα σωρό από σταθμούς εργασίας. Τα αποτελέσματα αυτής της ενότητας μπορούν να γίνουν πολύ μεγάλα, χιλιάδες ανά τερματικό, ακόμη και αν αποφασίσει κανείς να αναζητήσει κάτι πιο ασαφές όπως * .xls ή * .doc, έτσι ώστε τα αποτελέσματα να αποθηκεύονται σε αρχεία κειμένου μέσα στον κατάλογο αρχείων καταγραφής ώστε να μπορεί κάποιος να χρησιμοποιήσει κάποια γραμμή εντολών fu με σκοπό να αναλύσει τα δεδομένα και να αναζητήσει αυτό που θέλει.

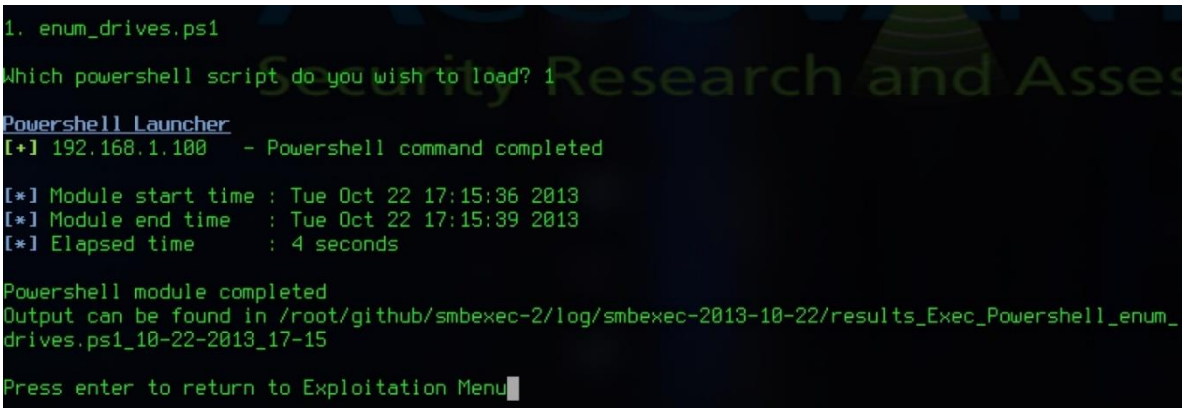
Μονάδα εύρεσης αρχείων:



Σχήμα 5 Χρήση του smbexec για εύρεση αρχείων

Η άλλη ενότητα μπορεί να παραδώσει και να εκτελέσει αυθαίρετες powershell εντολές έναντι των στόχων. Για να το επιτευχθεί αυτό, πρέπει μόνο να βάλουμε το μη διαδραστικό σενάριο powershell στο φάκελο powershell και θα είναι διαθέσιμο για χρήση. Τα αποτελέσματα της δέσμης ενεργειών powershell θα αποθηκευτούν και σε αρχεία κειμένου μέσα στον κατάλογο αρχείων καταγραφής.

Μονάδα Powershell:

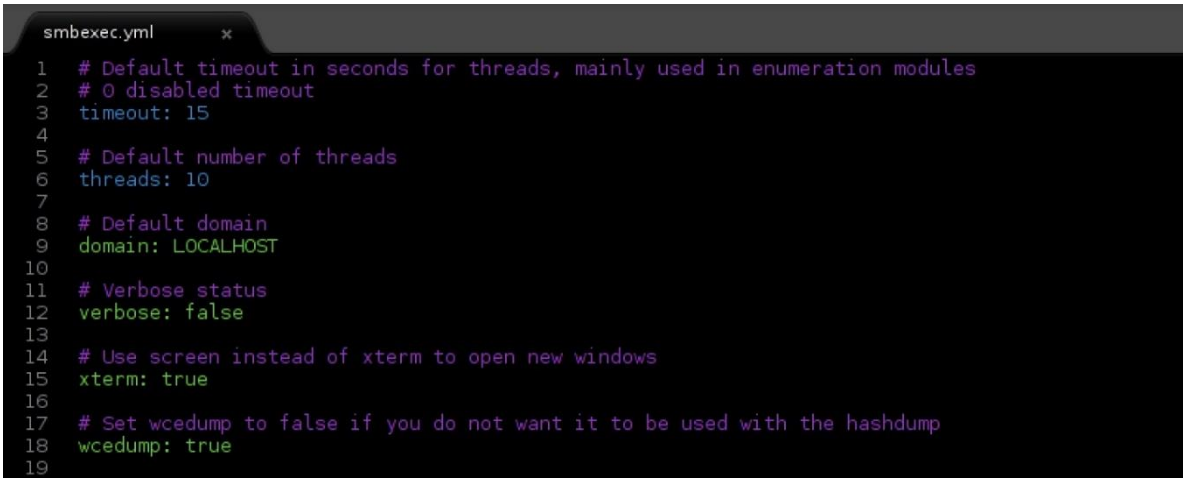


Εικόνα 6 Χρήση powershell μέσω του smbexec

Ένα διαμορφωμένο αρχείο διαμόρφωσης (smbexec.yml) όσο οι και επιλογές γραμμής εντολών που καλύπτουν τις περισσότερες περιπτώσεις χρήσης για το smbexec έχουν ήδη εφαρμοστεί για τη διευκόλυνση του χρήστη. Μπορεί να γίνει εισαγωγή διαπιστευτηρίων, ένα εύρος ip (υποστηριζόμενο σε κανόνες του nmap ή το ίδιο το nmap xml αρχείο) ή ο αριθμός των νημάτων πριν πραγματοποιηθεί εκκίνηση του smbexec τα οποία και θα τα θυμάται για όλα τα τερματικά.

Το αρχείο διαμόρφωσης έχει πιο λεπτομερή έλεγχο του τρόπου με τον οποίο λειτουργεί το εργαλείο, για παράδειγμα μπορεί να ρυθμιστεί η χρήση συνεδριών οθόνης σε παράθυρα xterm ή να χρησιμοποιηθεί το nmap και να γίνει χρήση ενός απλού ανιχνευτή θυρών TCP πλήρους σύνδεσης. Μπορούν επίσης να αλλαχθούν οι διαδρομές στις εξαρτήσεις, από προεπιλογή το αρχείο διαμόρφωσης είναι για μια εικόνα Kali.

Έτσι μοιάζει το αρχείο διαμόρφωσης smbexec.yml:



Σχήμα 7 Αρχείο διαμόρφωσης smbexec.yml

Wmiexec

Το Msiexec είναι το πρόγραμμα εγκατάστασης των Windows της Microsoft. Εμφανίζεται συχνά ως msiexec.exe στη Διαχείριση εργασιών των Windows. Χρησιμοποιείται για την εγκατάσταση προγραμμάτων που είναι ενσωματωμένα στη μορφή εγκατάστασης MSI. αυτά τα αρχεία έχουν την επέκταση .MSI ή .msi στο τέλος του ονόματος αρχείου. Όταν ένα από αυτά τα αρχεία ανοίγεται, το msiexec φορτώνεται αυτόματα και ξεκινάει τη διαδικασία εγκατάστασης.

Winrm

- Το Windows Remote Management ή το WinRM είναι ένα πρωτόκολλο απομακρυσμένης διαχείρισης ενσωματωμένο στα Windows στην απλούστερη μορφή του που χρησιμοποιεί το πρωτόκολλο Simple Access Protocol για τη διασύνδεση με απομακρυσμένους υπολογιστές και διακομιστές καθώς και λειτουργικά συστήματα και εφαρμογές.
- Το WinRM είναι ένα εργαλείο γραμμής εντολών που χρησιμοποιείται για τις ακόλουθες εργασίες: Απομακρυσμένη επικοινωνία και διασύνδεση με κεντρικούς υπολογιστές μέσω άμεσα διαθέσιμων καναλιών / θυρών εντός του δικτύου, συμπεριλαμβανομένων σταθμών εργασίας, διακομιστών και οποιουδήποτε λειτουργικού συστήματος το υποστηρίζει.
- Υποστηρίζει εκτέλεση εντολών από απόσταση σε συστήματα που δεν είναι τοπικά, αλλά είναι προσβάσιμα από το δίκτυο
- Παρακολουθεί, και δίνει τη δυνατότητα διαχείρισης και διαμόρφωσης των διακομιστών, των λειτουργικών συστημάτων και υπολογιστών-πελάτες από μια απομακρυσμένη τοποθεσία.

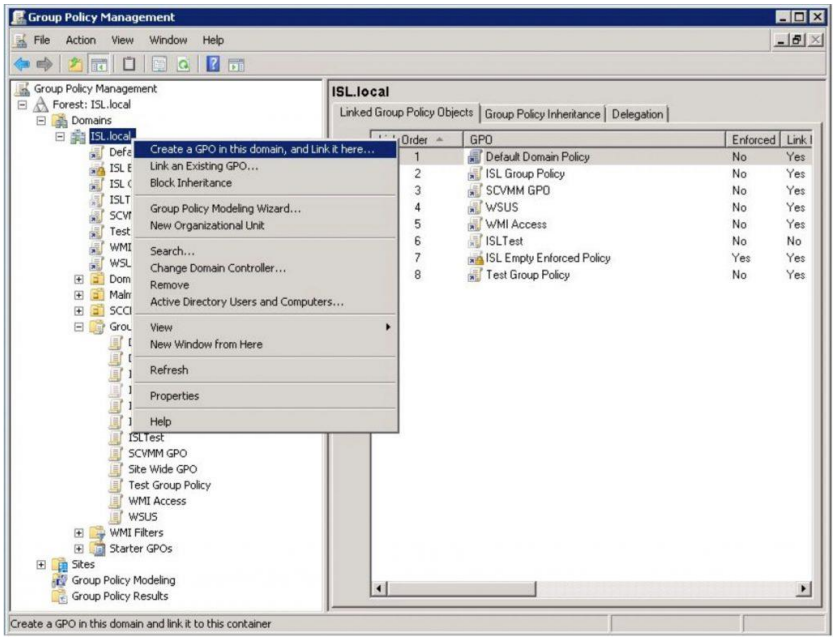
Το WinRM είναι ενεργοποιημένο από προεπιλογή στον Windows Server 2012 R2 αλλά είναι απενεργοποιημένο σε όλα τα λειτουργικά συστήματα πελάτη τα οποία είναι νεότερα από το Windows Server 2012. Για τα Windows XP και Windows Server 2003 (και τα δύο είναι EOL) πρέπει να γίνει εγκατάσταση του "Windows Management Framework Core Package (Windows PowerShell 2.0 και WinRM 2.0)" για να ενεργοποιηθεί η υποστήριξη του WinRM.

Το WinRM μπορεί να χρησιμοποιεί τόσο μέσω HTTP (θύρα 5985) όσο και μέσω HTTPS (θύρα 5986). Αυτός ο οδηγός θα επικεντρωθεί στο HTTP, καθώς δεν απαιτεί την εγκατάσταση πιστοποιητικών στις μηχανές προορισμού. Θα ενεργοποιήσουμε το WinRM μέσω ενός GPO, ο οποίος είναι ο ευκολότερος τρόπος για να επιτρέπουν σε όλες τις μηχανές στον τομέα να δέχονται συνδέσεις μέσω του WinRM. Υπάρχουν μερικά βήματα που πρέπει να ολοκληρωθούν για να λειτουργήσει το WinRM:

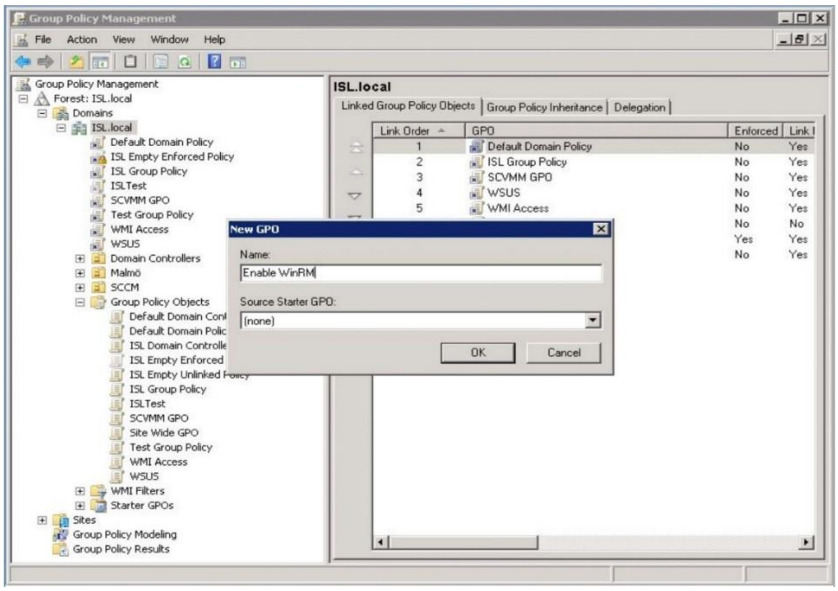
- Δημιουργήστε ένα GPO
- Διαμόρφωση του ακροατή WinRM

- Αυτόματη εκκίνηση της υπηρεσίας WinRM
- Άνοιγμα των θυρών του WinRM στο τείχος προστασίας

Στον διακομιστή AD σας, δημιουργήστε και συνδέστε ένα νέο GPO στον τομέα σας.

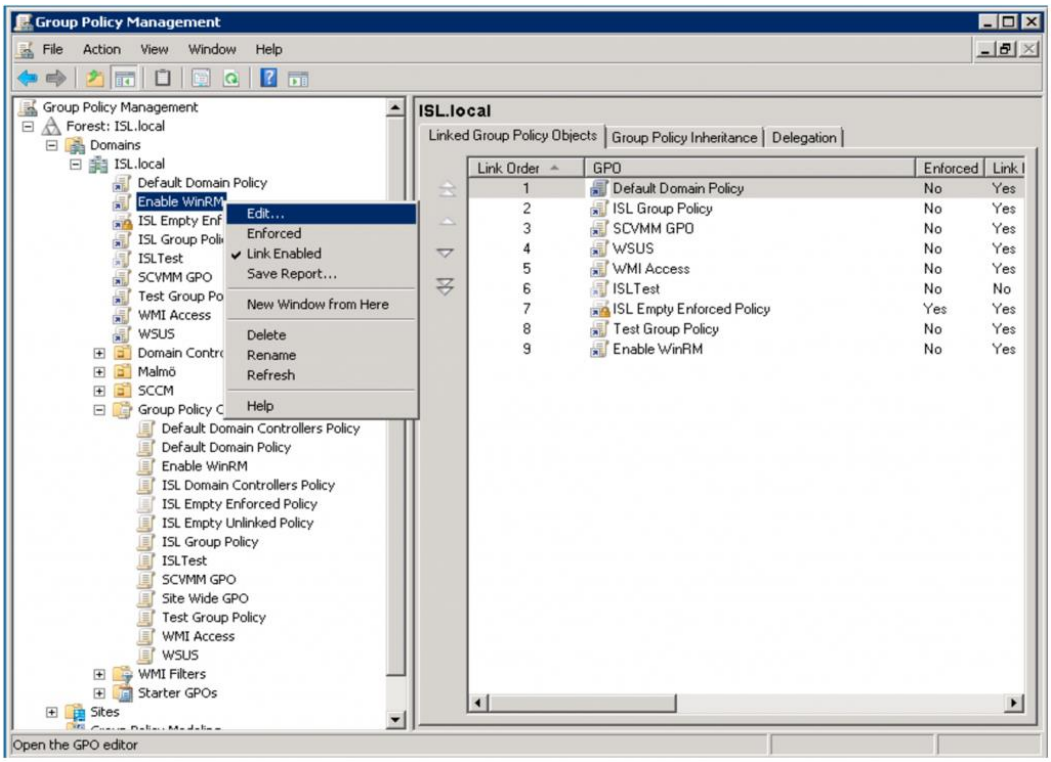


Σχήμα 8 Δημιουργία GPO 1



Σχήμα 9 Δημιουργία GPO 2

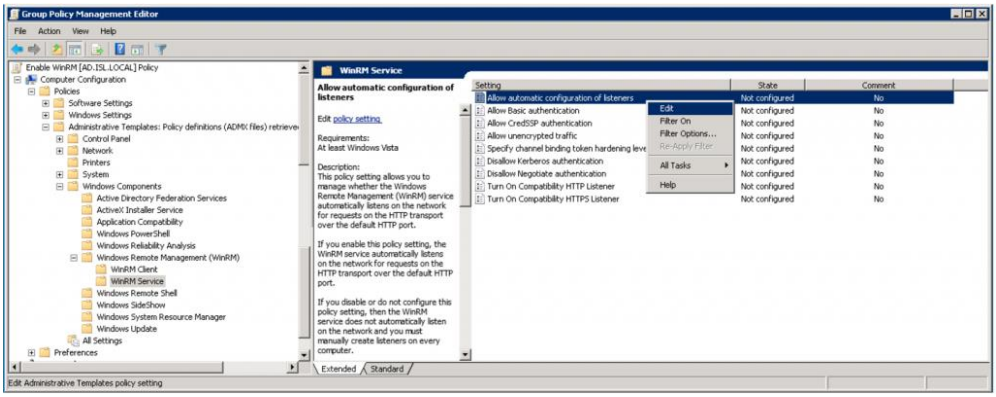
Αφού δημιουργηθεί το GPO, κάνουμε δεξί κλικ και επιλέγουμε στην "Επεξεργασία ...".



Σχήμα 10 Επεξεργασία GPO

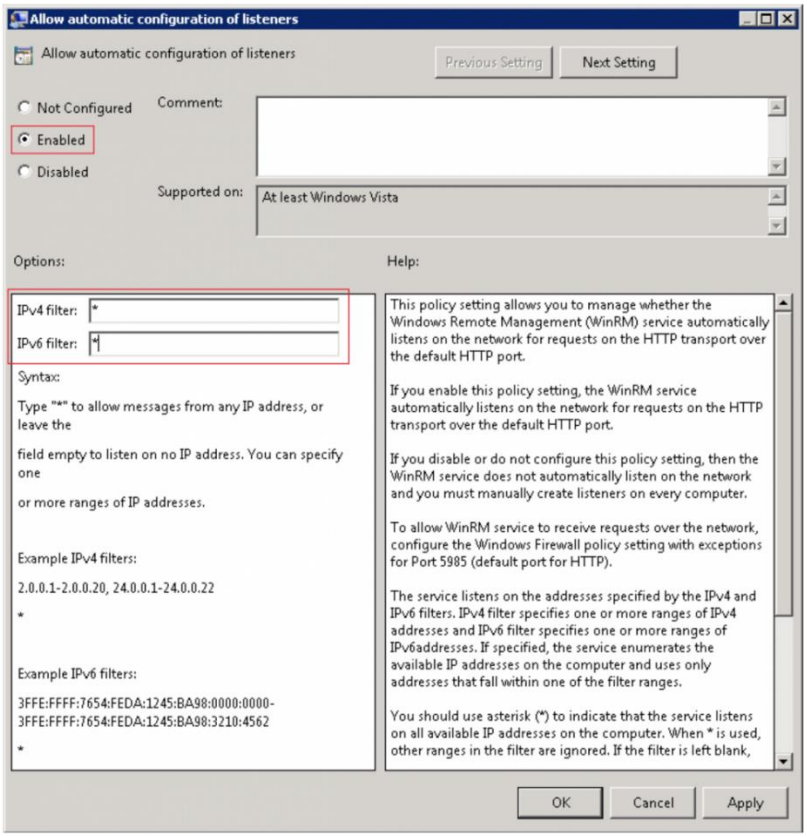
Διαμόρφωση του ακροατή WinRM

Στο πρόγραμμα επεξεργασίας πολιτικής ομάδας πολιτικής: κάνουμε ανάπτυξη της ρύθμισης Διαμόρφωση υπολογιστή> Πολιτικές> Πρότυπα διαχείρισης> Στοιχεία των Windows> Διαχείριση απομακρυσμένης διαχείρισης Windows (WinRM)> Υπηρεσία WinRM. Στη δεξιά πλευρά, επεξεργαζόμαστε τη ρύθμιση πολιτικής "Να επιτρέπεται η αυτόματη ρύθμιση των ακροατών". Η ίδια ρύθμιση μπορεί να ονομαστεί "Να επιτρέπεται η διαχείριση απομακρυσμένης διαχείρισης διακομιστή μέσω WinRM" σε ορισμένες διαμορφώσεις.



Σχήμα 11 Διαμόρφωση του ακροατή WinRM

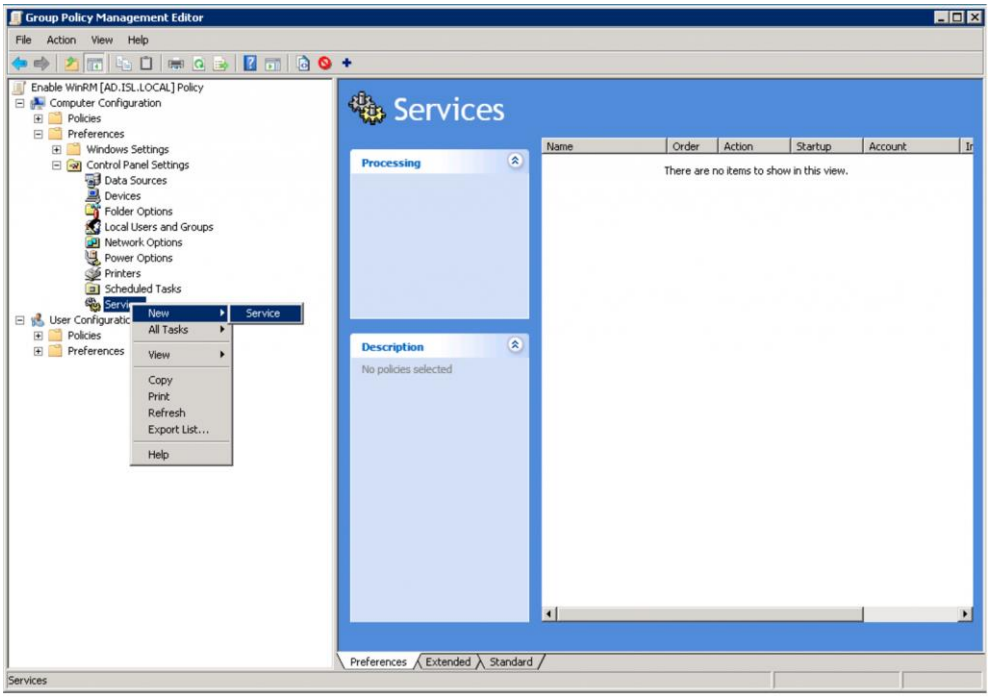
Εδώ καθορίζουμε ποιες διευθύνσεις IP θα ακούσει η υπηρεσία WinRM. Ο προσδιορισμός του "*" εδώ σημαίνει ότι η υπηρεσία θα ακούσει σε όλες τις διεπαφές που πρέπει να είναι έτοιμες.



Σχήμα 12 Καθορισμός IP που ακούει ο WinRM

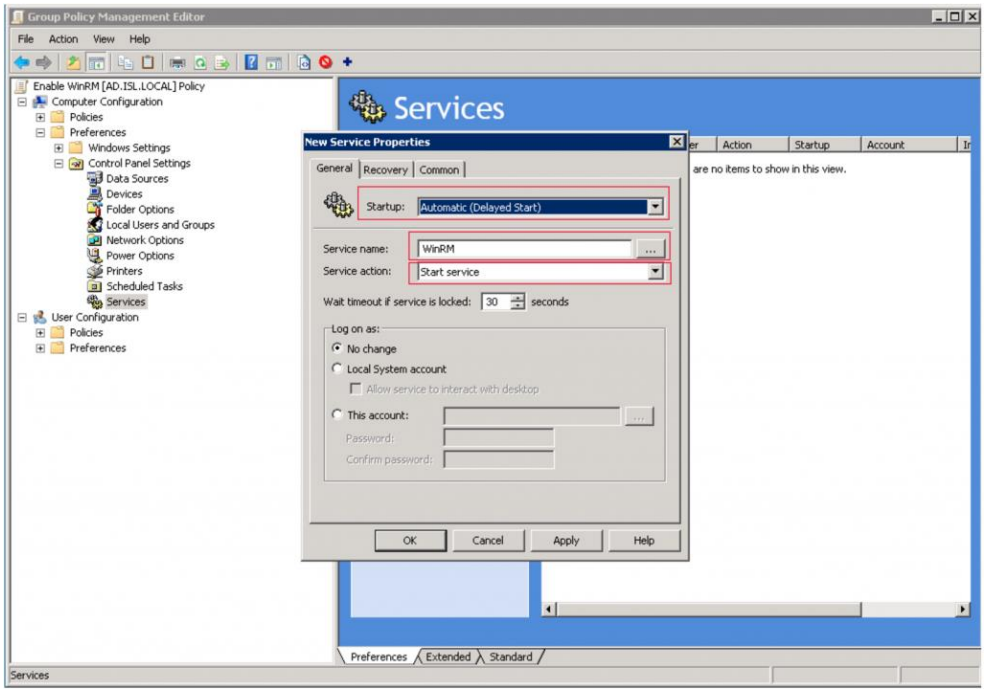
Αυτόματη εκκίνηση της υπηρεσίας WinRM

Στη συνέχεια πρέπει να βεβαιωθούμε ότι η υπηρεσία WinRM ξεκινά αυτόματα σε όλα τα μηχανήματα. Στο πρόγραμμα επεξεργασίας πολιτικής ομάδας πολιτικής: ανοίγουμε τη ρύθμιση παραμέτρων υπολογιστή> Προτιμήσεις> Ρυθμίσεις πίνακα ελέγχου> Υπηρεσίες. Κάνουμε δεξί κλικ στις Υπηρεσίες και επιλέγουμε Νέα> Υπηρεσία.



Σχήμα 13 Αυτόματη εκκίνηση του WinRM 1

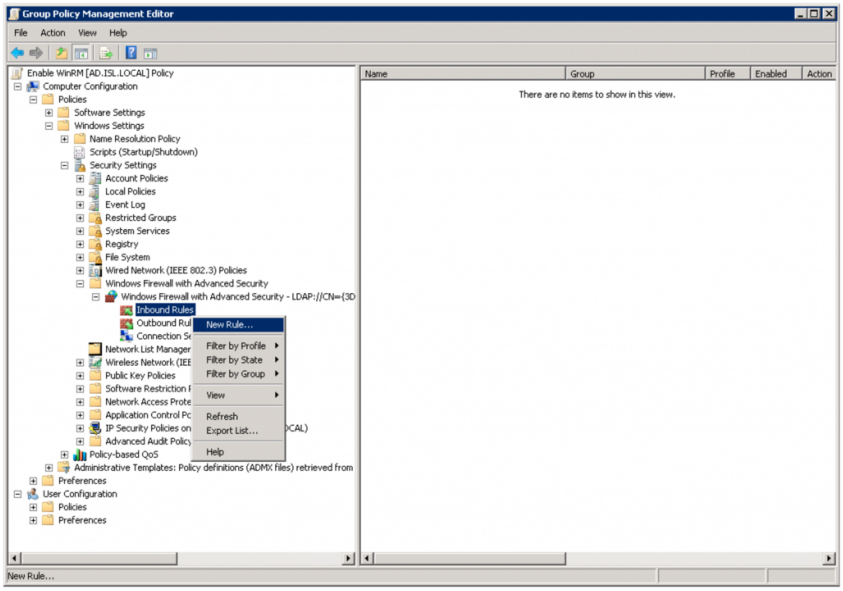
Ορίζουμε την εκκίνηση στην επιλογή "Αυτόματη (καθυστερημένη εκκίνηση)" και κάνουμε κλικ στο "..." δίπλα στην επιλογή Όνομα υπηρεσίας και αναζητούμε την Διαχείριση απομακρυσμένης διαχείρισης των Windows (WS-Management) και την επιλέγουμε. Τέλος, ορίζουμε την ενέργεια Υπηρεσία σε "Έναρξη υπηρεσίας". Κάνουμε κλικ στο OK για να αποθηκεύουμε τις ρυθμίσεις.



Σχήμα 14 Αυτόματη εκκίνηση του WinRM 2

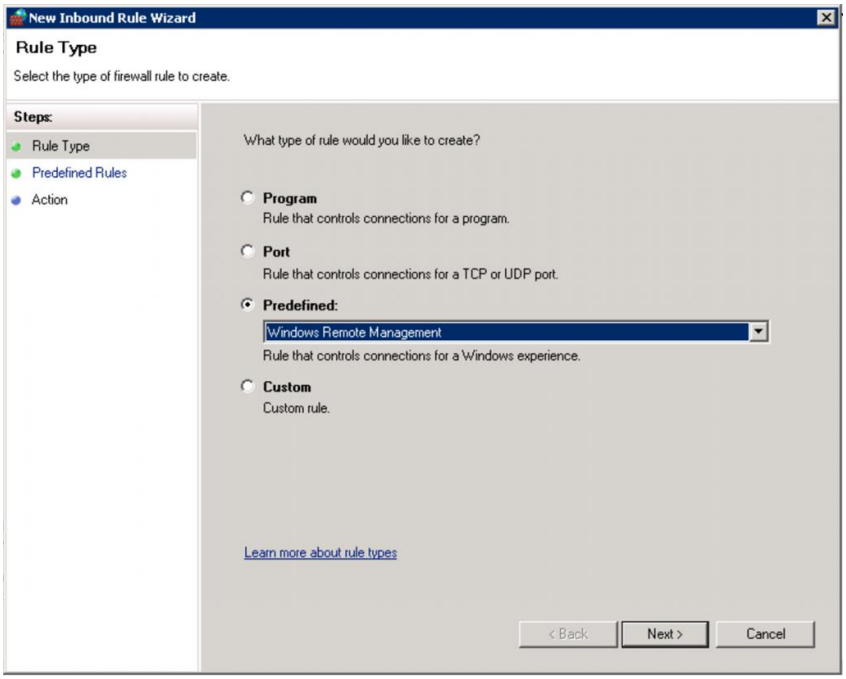
Ανοίγουμε τις θύρες WinRM στο τείχος προστασίας

Το WinRM χρησιμοποιεί θύρες 5985 (HTTP) και 5986 (HTTPS). Για να ανοίξουμε το τείχος προστασίας για τη θύρα 5985, κάνουμε ανάπτυξη του στοιχείου Διαμόρφωση υπολογιστή> Πολιτικές> Ρυθμίσεις Windows> Ρυθμίσεις ασφαλείας> Τείχος προστασίας των Windows με προηγμένη ασφάλεια> Τείχος προστασίας των Windows με προηγμένη ασφάλεια> Εισερχόμενους κανόνες. Κάνουμε δεξί κλικ στον κόμβο Εισερχόμενων κανόνων και επιλέγουμε Νέο κανόνα.



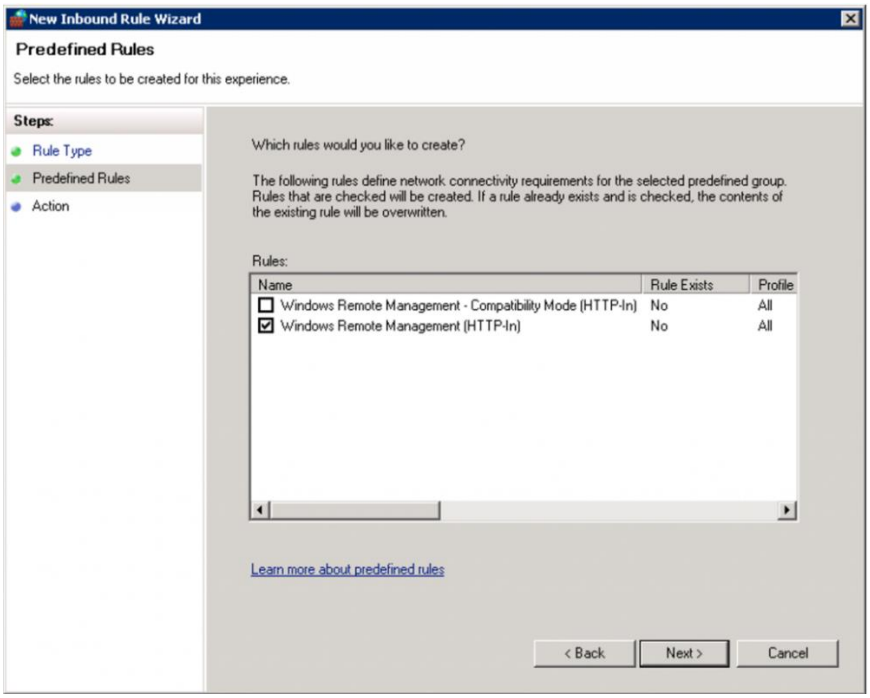
Σχήμα 15 Δημιουργία κανόνα για εξαίρεση των θυρών από το τείχος προστασίας

Θα χρησιμοποιήσουμε έναν προκαθορισμένο κανόνα, οπότε επιλέγουμε "Απομακρυσμένη διαχείριση των Windows" από το αναπτυσσόμενο μενού και κάνουμε κλικ στο κουμπί Επόμενο.



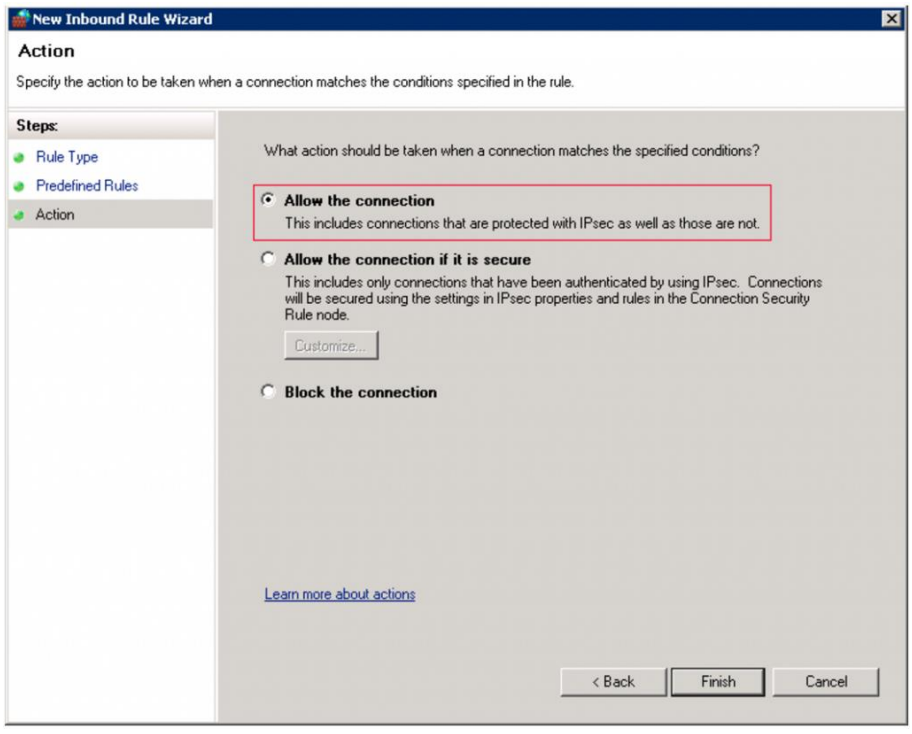
Σχήμα 16 Επιλογή κανόνων για εξαίρεση των θυρών από το τείχος προστασίας

Βεβαιωνόμαστε ότι έχουμε επιλέξει "Απομακρυσμένη διαχείριση των Windows (HTTP-In)". Δεν χρειαζόμαστε τη λειτουργία συμβατότητας. Κάντε κλικ στο κουμπί Επόμενο.



Σχήμα 17 Επιπλέον επιλογές για τη δημιουργία κανόνα

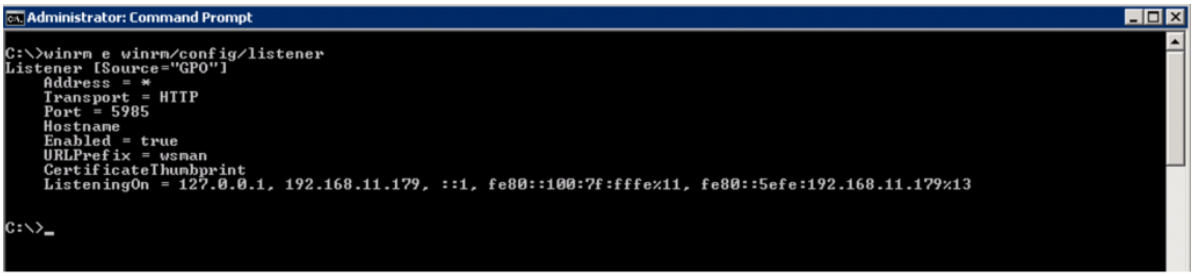
Επιλέγουμε "Να επιτρέπεται η σύνδεση" ως ενέργεια και κάνουμε κλικ στο κουμπί Τέλος.



Σχήμα 18 Ολοκλήρωση της δημιουργίας κανόνα

Επαληθεύουμε τις ρυθμίσεις WinRM

Τώρα το GPO διαμορφώνεται και συνδέεται με τον τομέα. Είτε περιμένουμε να μεταδοθεί το GPO στα μηχανήματά είτε να αναβαθμίσουμε. Για να ελέγξουμε τη διαμόρφωση σε ένα συγκεκριμένο μηχάνημα, συνδεόμαστε σε αυτό και εκτελούμε το "gpupdate / force" σε μια γραμμή εντολών για να αναγκάσουμε την ενημέρωση των ρυθμίσεων GPO. Στη συνέχεια, μπορούμε να πληκτρολογήσετε "winrm e winrm / config / listener" για να δούμε τις ρυθμίσεις του ακροατή. Θα πρέπει να φαίνονται κάπως έτσι:



Σχήμα 19 Προβολή ρυθμίσεων ακροατή

ΔΟΚΙΜΗ ΣΥΝΔΕΣΗΣ

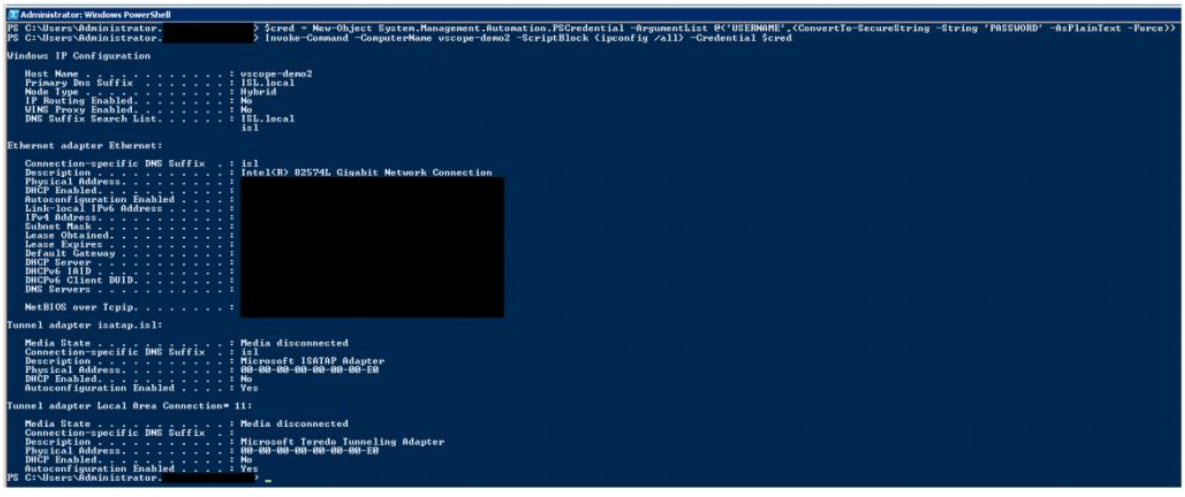
Ανοίγουμε ένα PowerShell για να δοκιμάσουμε μια σύνδεση WinRM. Αρχικά, δημιουργούμε διαπιστευτήρια που χρησιμοποιούνται για τη σύνδεση με το απομακρυσμένο μηχάνημα. Χρησιμοποιούμε έναν λογαριασμό τομέα με επαρκή δικαιώματα (κατά προτίμηση έναν λογαριασμό διαχειριστή):

PS> $cred = New-Object System.Management.Automation.PSCredential -ArgumentList @('USERNAME',(ConvertTo-SecureString -String 'PASSWORD' -AsPlainText -Force))

Αντικαταστούμε το "USERNAME" και το "PASSWORD" με τα στοιχεία σύνδεσής. Στη συνέχεια καλούμε μια απομακρυσμένη εντολή σε ένα απομακρυσμένο μηχάνημα. Σε αυτό το παράδειγμα τρέχουμε το "ipconfig / all" στο "vscope-demo2".

PS> Invoke-Command -ComputerName vscope-demo2 -ScriptBlock {ipconfig /all} -Credential $cred

Θα πρέπει να δούμε την έξοδο από το ipconfig ότι όλα είναι καλά.



Σχήμα 20 Δοκιμή σύνδεσης του WinRM

Για να ενεργοποιήσουμε το WinRM στο vScope, προσθέτουμε μια πιστοποίηση WMI μέσω του Discovery Manager και κάτω από την ενότητα "Advanced", βεβαιωνόμαστε ότι έχουμε επιλέξει το "Enable WinRM". Αυτό θα επιτρέψει το WinRM να συνδεθεί μέσω HTTP. Για να χρησιμοποιήσουμε

το HTTPS (βεβαιωνόμαστε ότι έχουμε διαμορφώσει τις μηχανές για αυτό) και επιλέγουμε "WinRM Use HTTPS".

Επαλήθευση διαπιστευτηρίων

Για να επαληθεύσουμε τα διαπιστευτήρια που χρησιμοποιούνται για την απομακρυσμένη πρόσβαση στο WMI, χρησιμοποιούμε την ακόλουθη δέσμη ενεργειών από το διακομιστή vScope (ή το διακομιστή μεσολάβησης, εάν χρησιμοποιείτε)

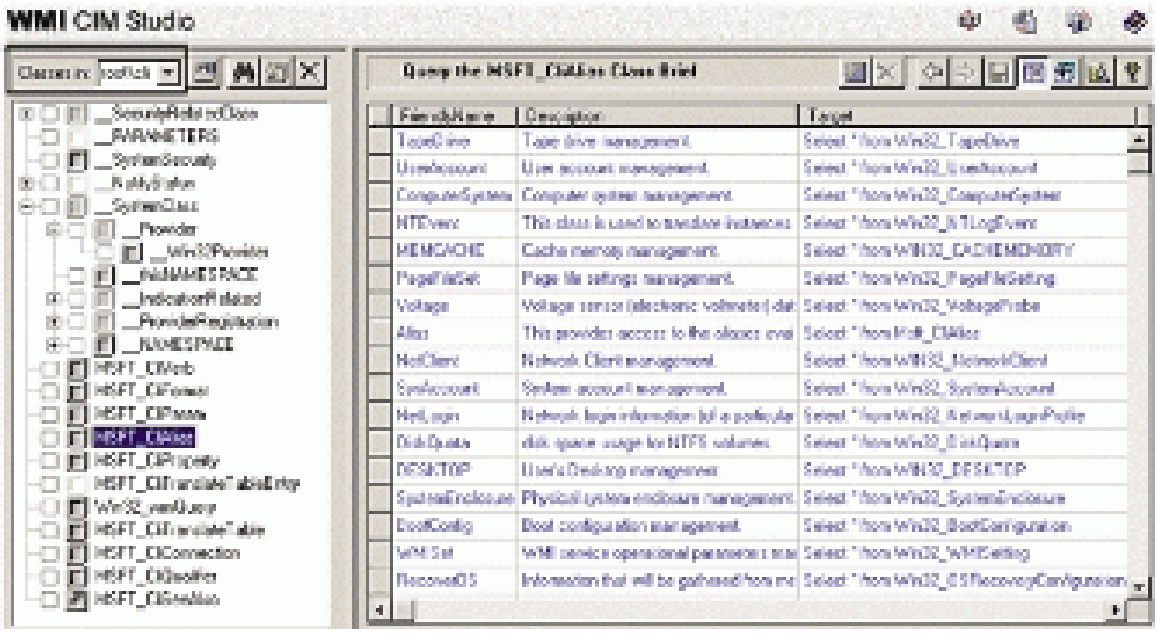
Get-WmiObject -Class Win32_ComputerSystem -ComputerName 192.168.100.100 -Credential domain\mywmiuser Αυτή η εντολή θα ανοίξει μια ερώτηση όπου θα εισάγουμε τον κωδικό πρόσβασης για την πιστοποίηση. Εάν όλα λειτουργούν θα πρέπει να δούμε πληροφορίες σχετικά με το μηχάνημα-στόχο, διαφορετικά θα εμφανιστεί ένα μήνυμα σφάλματος.

- Wmic

Το WMIC επεκτείνει το WMI για λειτουργία πολλών διεπαφών γραμμής εντολών και μέσω δεσμών ενεργειών. Πριν από το WMIC, χρησιμοποιούσαμε εφαρμογές που βασίζονται στο WMI (όπως SMS), API Scripting WMI ή εργαλεία όπως το CIM Studio για τη διαχείριση υπολογιστών με δυνατότητα WMI. Χωρίς μια σταθερή κατανόηση σε μια γλώσσα προγραμματισμού όπως η C ++ ή μια γλώσσα scripting όπως το VBScript και μια βασική κατανόηση του χώρου ονομάτων WMI, η διαχείριση συστημάτων με το WMI ήταν δύσκολη. Το WMIC αλλάζει αυτή την κατάσταση δίνοντάς μια ισχυρή, φιλική προς το χρήστη διεπαφή στο χώρο ονομάτων του WMI.

Το WMIC είναι πιο διαισθητικό από το WMI, σε μεγάλο βαθμό εξαιτίας των ψευδωνύμων. Τα ψευδώνυμα παίρνουν απλές εντολές που εισάγουμε στη γραμμή εντολών και στη συνέχεια ενεργούν με βάση τον χώρο ονομάτων WMI με έναν προκαθορισμένο τρόπο, όπως η κατασκευή μιας σύνθετης εντολής WQL Query Language (WQL) από μια απλή εντολή Get alias WMIC. Έτσι, τα ψευδώνυμα ενεργούν ως ενδιάμεσοι μεταξύ των χρηστών και του χώρου ονομάτων. Για παράδειγμα, όταν εκτελέσουμε μια απλή εντολή WMIC όπως **useraccount list brief** από τη γραμμή εντολών WMIC για να λάβουμε πληροφορίες λογαριασμού χρήστη, το alias Useraccount εκτελεί ένα ερώτημα WQL της κλάσης Win32_Useraccount και εμφανίζει συγκεκριμένα δεδομένα από αυτήν την κλάση σε μορφή κειμένου. Το WMIC εμφανίζει επίσης τις ιδιότητες της κλάσης Win32_Useraccount στην κονσόλα σε μορφή κειμένου. Το WMIC μπορεί να επιστρέψει τα αποτελέσματα μιας εντολής σε άλλες μορφές, όπως η XML, HTML και η τιμή διαχωριζόμενη με κόμματα (CSV).

Το WMIC αποθηκεύει ψευδώνυμα ως παρουσίες μιας κλάσης στο σχήμα WMI. Το προεπιλεγμένο ψευδώνυμο classMSFT_CliAlias και οι υπόλοιπες κλάσεις που υποστηρίζουν το WMIC αποθηκεύονται στον προεπιλεγμένο χώρο ονομάτων της πλατφόρμας ή στο role-root \ cli. Ένας ρόλος είναι απλώς ένα στοιχείο στο χώρο ονομάτων WMI που έχει σχεδιαστεί ειδικά για να υποστηρίζει το WMIC. Ο προεπιλεγμένος ρόλος, root \ cli, συνδέεται στο χώρο ονομάτων root \ cimv2 για να λειτουργήσει στις κλάσεις του root \ cimv2. Συνήθως δεν θα χρησιμοποιηθεί το CIM Studio όταν γίνεται εκτέλεση του WMIC, αλλά μπορεί κάποιος να χρησιμοποιήσει το CIM Studio για να βρει το χώρο ονομάτων root \ cli σε μια λίστα με χώρους ονομάτων WMI. Το σχήμα 20 δείχνει τον κόμβο root \ cli και ορισμένες από τις ιδιότητες στην κλάση MSFT_CliAlias.



Σχήμα 21 Κόμβος root\cli

Μπορούμε να προσθέσουμε νέα ψευδώνυμα στο χώρο ονομάτων root \ cli και σε άλλα namespaces. Μπορούμε επίσης να έχουμε πρόσβαση στο χώρο ονομάτων WMI απευθείας με τις εντολές Κλάση και Διαδρομή.

WMImplant

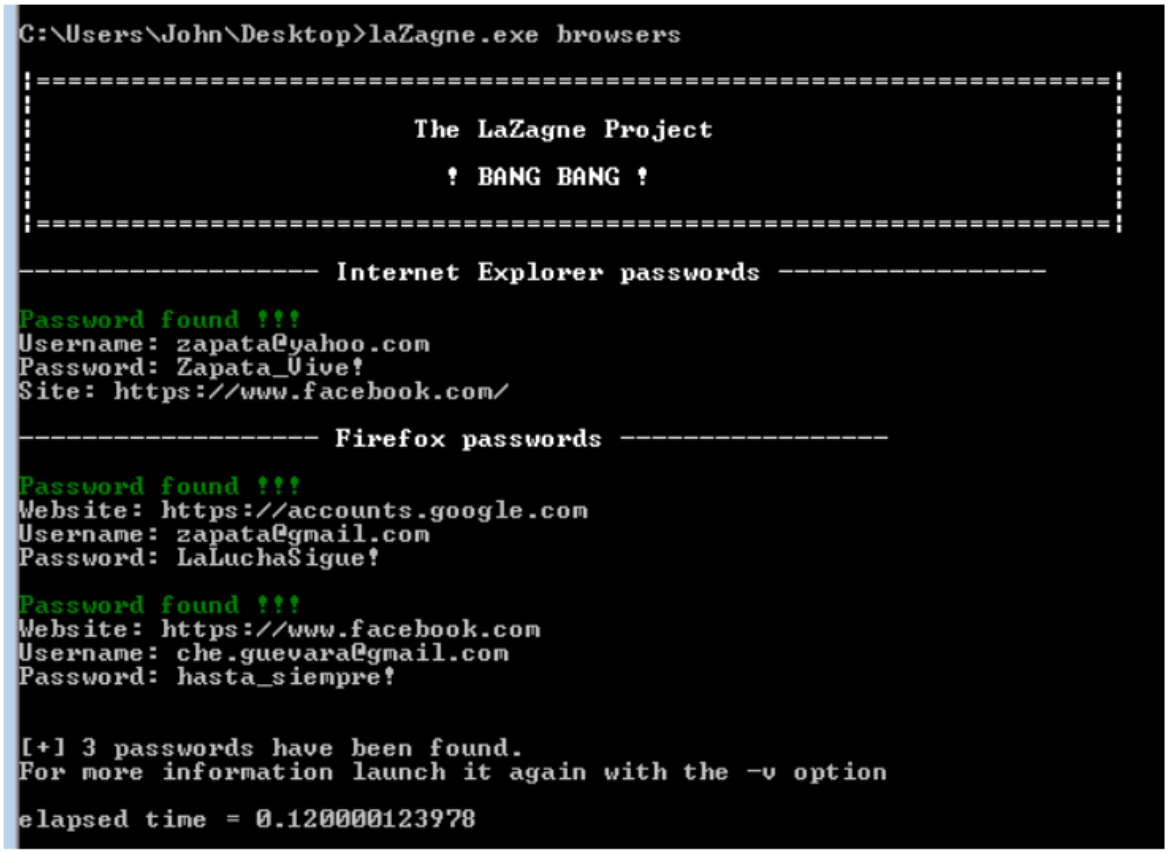
Το WMImplant είναι ένα εργαλείο βασισμένο στο PowerShell που αξιοποιεί το WMI και για να εκτελεί ενέργειες κατά των στοχοθετημένων μηχανών, αλλά και ως το κανάλι C2 για την έκδοση εντολών και τη λήψη αποτελεσμάτων. Το WMImplant πιθανόν να απαιτεί δικαιώματα τοπικού διαχειριστή στο συγκεκριμένο μηχάνημα.

Το WMImplant είναι ένα εργαλείο που έχει σχεδιαστεί για να χρησιμοποιεί πλήρως το WMI. Το WMI δεν είναι μόνο ο μηχανισμός για την ενεργοποίηση ενεργειών στο στοχευόμενο μηχάνημα, αλλά είναι και το ίδιο το κανάλι C2. Όπου απαιτείται, το WMImplant αποθηκεύει δεδομένα σε ιδιότητες του WMI, αλλά σε μια περίπτωση αποθηκεύει δεδομένα στο μητρώο του συστήματος. Όταν αλληλοεπιδρά με τις ιδιότητες του WMI, το WMImplant καταγράφει την αρχική τιμή ιδιότητας, αλλάζει την τιμή και στη συνέχεια επαναφέρει την αρχική τιμή όταν ολοκληρωθεί. Όταν αλληλοεπιδρά με το μητρώο, το WMImplant δημιουργεί ένα νέο κλειδί μητρώου, αποθηκεύει τα δεδομένα στην τιμή του μητρώου, ανακτά τα δεδομένα και κατόπιν καταργεί το κλειδί.

4.3 Εργαλεία συλλογής πληροφορίων

PROJECT LAZAGNE

Το project lazagne είναι ένα ανοικτού κώδικα λογισμικό που σκοπό έχει την ανάκτηση πολλών κωδικών πρόσβασης οι οποίοι είναι αποθηκευμένοι σε ένα τοπικό μηχάνημα. Κάθε λογισμικό αποθηκεύει τους κωδικούς τους χρησιμοποιώντας διαφορετικές τεχνικές (κείμενο, APIs, αλγορίθμους, βάσεις δεδομένων, κ.α.). Το εργαλείο αυτό δημιουργήθηκε για να βρίσκει κωδικούς για τα πιο γνωστά λογισμικά.



Σχήμα 22 Project LaZagne

Αυτό το project έχει προστεθεί στο pupy σαν ένα post – exploitation module. Ο κώδικας Python θα ερμηνευτεί στη μνήμη χωρίς να αγγίξει τον δίσκο και λειτουργεί για Windows και Linux . Η τελευταία έκδοση του linux δεν είναι ενημερωμένη γι αυτό το λόγο η καλύτερη λύση είναι να χρησιμοποιηθεί το pupy για αυτή τη χρήση.

	Windows	Linux	Apple
Browsers	Chrome Firefox IE Opera	Firefox Opera	Firefox Chrome
Chats	Jitsi Pidgin Skype	Jitsi Pidgin	
Databases	DBvisualizer Postgresql Robomongo Squirrel SQLdeveloper	DBvisualizer Squirrel SQLdeveloper	
Games	Galconfusion Kalypsomedia Rogue's Tale Turba		
Git	Git for Windows		
Mails	Outlook Thunderbird	ClawsMail Thunderbird	
Dump from memory	Keepass Wdigest (mimikatz method)	System password	
Svn	Tortoise		
Sysadmin	Apache Directory Studio CoreFTP Cyberduck FileZilla FTPNavigator OpenSSH PuttyCM RDPManager WinSCP	AWS Docker Environment Variables FileZilla History files SSH private keys	
Wifi	Wireless Network	Network Manager	* cf Keychains
Internal mechanism passwords storage	.NET Passport Generic network Hashdump (LM/NT) LSA Secrets	GNOME Keyring* KWallet* Hashdump	Keychains Hashdump

Σχήμα 23 Προγράμματα για την αποθήκευση κωδικών αναλόγως το λειτουργικό σύστημα. Χρησιμοποιείται από πολλά εργαλεία για να γίνει αποθήκευση των κωδικών: Chrome, Owncloud, Evolution, KMail κ.α.

PUPY

Το pupy είναι μία ανοιχτού λογισμικού πλατφόρμα (cross-platform) (Windows, Linux, OSX, Android) με πολλές χρήσεις RAT (Remote Administration Tool) και ένα εργαλείο post-exploitation γραμμένο κυρίως σε python. Οι λειτουργίες του τρέχουν όλες στην μνήμη και αφήνουν ελάχιστα αποτυπώματα. Το pupy μπορεί να επικοινωνήσει με διάφορες μεθόδου, περιορίζοντας τις διαδικασίες (reflactive

injection), φορτώνοντας απομακρυσμένα τον κώδικα python, πακέτα python και python C - επεκτάσεις από τη μνήμη.

Τα modules pupy μπορούν να έχουν κρυφή απομακρυσμένη πρόσβαση σε αντικείμενα της python χρησιμοποιώντας rpyc για να εκτελέσουν διάφορες διαδραστικές διαδικασίες.

Το pupy μπορεί να δημιουργήσει payloads σε διάφορες εκδόσεις όπως εκτελέσιμα PE, reflective DLLs, καθαρά αρχεία python, powershell, apk …

Όταν φορτώνεται ένα payload μπορεί κανείς να επιλέξει το πώς θα εκτελεστεί (connect, bind, …), τη μεταφορά (ssl, http, rsa, obfs3, scramblesuit, …) και έναν αριθμό ομάδων σεναρίων. Οι ομάδες σεναρίων είναι σενάρια της python τα οποία είναι ενσωματωμένα ώστε να εκτελούν ποικίλα έργα χωρίς να χρειάζεται σύνδεση (χωρίς να χρειάζεται συνεδρία (session)), όπως να ξεκινήσει κάποιο σενάριο στο παρασκήνιο, προσθέτοντας επιμονή, ξεκινάει ένα keylogger, ανιχνεύει κάποιο sandbox,

ΕΓΚΑΤΑΣΤΑΣΗ

- git clone https://github.com/n1nj4sec/pupy.git pupy
- cd pupy
- git submodule init
- git submodule update
- pip install -r pupy/requirements.txt
- wget https://github.com/n1nj4sec/pupy/releases/download/latest/payload_templates.txz
- tar xvf payload_templates.txz && mv payload_templates/*pupy/payload_templates/ && rm payload_templates.txz && rm -r payload_templates

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

- Υποστηρίζεται σε πολλές πλατφόρμες (σε windows xp, 7, 8, 10, kali linux, ubuntu, osx, android)
- Στα windows, το Pupy payload μπορεί να συνταχθεί σαν μία reflective DLL και ολόκληρος ο διερμηνέας της python να φορτωθεί από τη μνήμη. Το Pupy δεν επηρεάζει το δίσκο.
- Το pupy μπορεί επίσης να συμπεριληφθεί σε ένα αρχείο .py και να τρέξει χωρίς καθόλου εξαρτήσεις από την κανονική βιβλιοθήκη της python σε όλα τα λειτουργικά συστήματα.
    - Το pycrypto αντικαθίσταστε από καθαρή python aes && rsa υλοποιήσεις όταν δεν είναι διαθέσιμες
- Το Pupy μπορεί αντανακλαστικά να μεταναστεύσει σε άλλες διαδικασίες.
- Το Pupy μπορεί απομακρυσμένα να εισάγει, από τη μνήμη, καθαρά πακέτα python (.py, .pyc) και να μεταφράσει την python σε C επεκτάσεις (.pyd, .so). Τα εισαχθέντα module της python δεν επηρεάζουν τον δίσκο.
- Το Pupy είναι εύκολα επεκτάσιμο, τα modules είναι εύκολο να γραφούν και ταξινομούνται από το λειτουργικό σύστημα και την κατηγορία.
- Πολλά modules έχουν ήδη υλοποιηθεί!
- Το Pupy χρησιμοποιεί rpyc και ένα module μπορεί απευθείας να προσπελάσει αντικείμενα python objects σε έναν απομακρυσμένο client.
    - Μπορούμε να έχουμε απομακρυσμένη πρόσβαση σε διαδραστικά αντικείμενα στο pupy shell και μπορούμε να έχουμε αυτόματη ολοκλήρωση σε απομακρυσμένα χαρακτηριστικά!
- Η επικοινωνία μεταφοράς είναι modular και stackable. Μπορεί κάποιος να απομακρύνει δεδομένα χρησιμοποιώντας HTTP over HTTP over AES over XOR. Μπορεί κάποιος να κάνει και συνδυασμό των διαθέσιμων μεταφορών
- Το Pupy μπορεί να επικοινωνήσει χρησιμοποιώντας obfsproxy pluggable transports
- Όλα τα μη-διαδραστικά modules μπορούν να αποσταλούν σε πολλούς hosts με μία εντολή.
- Εντολές και σενάρια που τρέχουν σε απομακρυσμένους hosts μπορούν να διακοπούν.
- Αυτόματη ολοκλήρωση σε εντολές και arguments

- Προσαρμοσμένες ρυθμίσεις μπορούν να οριστούν σε: ψευδώνυμα εντολών (command aliases), τα modules τρέχουν αυτόματα κατά τις συνδέσεις, ...
- Διασραστικά python shells με αυτόματη ολοκλήρωση στη μνήμη του απομακρυσμένου διερμηνέα της python μπορούν να ανοίξουν.
- Διαδραστικά shells (cmd.exe, /bin/bash, ...) μπορούν να ανοίξουν απομακρυσμένα. Απομακρυσμένα shells on Unix & windows clients έχον ένα αληθινό tty με όλες τις λειτουργίες του πληκτρολογίου να λειτουργούνε άψογα όπως σε ένα ssh shell
- Το Pupy μπορεί να εκτελέσει PE exe απομακρυσμένα από τη μνήμη (cf. ex with mimikatz)
- Το Pupy μπορεί να δημιουργήσει payloads σε διάφορα formats : apk,lin_x86,lin_x64,so_x86,so_x64,exe_x86,exe_x64,dll_x86,dll_x64,py,pyinst,py_oneliner, ps1,ps1_oneliner,rubber_ducky
- Το Pupy μπορεί να αναπτυχθεί στη μνήμη, από μία απλή γραμμή κώδικα χρησιμοποιώντας pupygen.py's python ή powershell one-liners.
- Τα "scriptlets" μπορούν να ενσωματωθούν στα payloads που έχουν δημιουργηθεί ώστε να εκτελέσουν κάποιες διεργασίες "χωρίς σύνδεση" χωρίς να χρειάζεται σύνδεση δικτύου (ex: ενεργοποιώντας keylogger, προσθέτοντας persistence, εκτελώντας προσωπικά python script, ελέγχοντας κάποιο_vm ...)

ΕΦΑΡΜΟΣΜΕΝΕΣ ΜΕΤΑΦΟΡΕΣ

Όλες οι μεταφορές στο pupy είναι στοιβάσιμες. Αυτό σημαίνει ότι κατά την δημιουργία μίας προσωπικής σύνδεσης conf (pupy/network/transport/<transport_name>/conf.py), μπορεί κάποιος να κάνει το pupy session να μοιάζει σαν ¨τίποτα¨ Για παράδειγμα μπορεί κάποιος να στοιβάξει HTTP over HTTP over base64 over HTTP over AES over obfs3 :o)

- rsa
  - Ένα επίπεδο με έλεγχο ταυτότητας & κρυπτογράφηση χρησιμοποιώντας RSA και AES256 συχνά στοιβάζεται με άλλα επίπεδα.
- aes
  - Ένα επίπεδο που χρησιμοποιεί ένα στατικό AES256 κλειδί.
- ssl
  - TCP μεταφορά τυλιγμένη με SSL
- ssl_rsa
  - το ίδιο με το ssl αλλά στοιβαγμένο με ένα rsa επίπεδο
- http
  - Ένα επίπεδο που κάνει την κίνηση να φαίνεται σαν HTTP κίνηση. Το HTTP είναι είναι στοιβαγμένο σε ένα rsa επίπεδο.
- obfs3
  - Ένα πρωτόκολλο για να κρατήσει ένα τρίτο μέρος να λέει ποιο πρωτόκολλο χρησιμοποιείται, με βάση τα περιεχόμενα του μηνύματος
  - obfs3 είναι στοιβαγμένο με ένα rsa επίπεδο για καλύτερη ασφάλεια.
- scramblesuit
- Ένα πολύμορφο πρωτόκολλο δικτύου για την περιποίηση της λογοκρισίας
- scramblesuit είναι στοιβαγμένο σε ένα rsa επίπεδο για καλύτερη ασφάλεια.
- udp
- Το rsa επίπεδο αλλά πάνω από ένα πρωτόκολλο UDP (θα μπορούσε να είναι ένα buggy, δεν χειρίζεται ακόμα απώλεια πακέτων)
- other
- Τα υπόλοιπα επίπεδα δίνονται για παραδείγματα κώδικα : (dummy, base64, XOR, ...)

MIMIKATZ

Το Mimikatz είναι ένα εργαλείο post-exploitation γραμμένο από τον Benjamin Delpy. Μετά την αρχική φάση εκμετάλλευσης, οι επιτιθέμενοι μπορεί να θέλουν να αποκτήσουν πιο σταθερή θέση στον

υπολογιστή/δίκτυο. Κάτι τέτοιο συχνά απαιτεί μια σειρά συμπληρωματικών εργαλείων. ΤΟ Mimikatz είναι μια προσπάθεια να συγκεντρωθούν μαζί μερικά από τα πιο χρήσιμα σημεία που θέλουν οι επιτιθέμενοι να εκτελέσουν επιθέσεις.

Το Metasploit αποφάσισε να συμπεριλάβει το Mimikatz ως σενάριο μετρητή για να επιτρέψει την εύκολη πρόσβαση στο πλήρες σύνολο των δυνατοτήτων χωρίς να χρειάζεται να ανεβάσετε αρχεία στον ευπαθή δίσκο.

Μετά την απόκτηση ενός μετρητή shell, πρέπει να διασφαλίσουμε ότι η συνεδρία μας εκτελείται με προνόμια συστήματος SYSTEM για να λειτουργεί σωστά το Mimikatz.

```
meterpreter > getuid
Server username: WINXP-E95CE571A1\Administrator

meterpreter > getsystem
...got system (via technique 1).

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Σχήμα 24 Έλεγχος προνομίων για την ορθή λειτουργία του Mimikatz

Το Mimikatz υποστηρίζει αρχιτεκτονικές Windows 32bit και 64bit. Μετά την αναβάθμιση των προνομίων μας στο SYSTEM, πρέπει να επαληθεύσουμε, με την εντολή sysinfo, ποια είναι η αρχιτεκτονική του ευπαθές μηχανήματος. Αυτό θα είναι σχετικό με τα μηχανήματα 64bit, καθώς ενδέχεται να έχουμε διακυβεύσει μια διαδικασία 32bit σε μια αρχιτεκτονική 64bit. Εάν συμβαίνει αυτό, ο μετρητής θα επιχειρήσει να φορτώσει στη μνήμη μια 32-bit έκδοση του Mimikatz, πράγμα που θα έχει ως αποτέλεσμα να μην λειτουργούν τα περισσότερα χαρακτηριστικά. Αυτό μπορεί να αποφευχθεί εξετάζοντας τη λίστα τρέχουσας διαδικασίας και τη μετάβαση σε μια διαδικασία 64bit πριν φορτώσετε το Mimikatz.

```
meterpreter > sysinfo
Computer        : WINXP-E95CE571A1
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
```

Σχήμα 25 Προβολή αρχιτεκτονικής του συστήματος μέσω της εντολής sysinfo

Δεδομένου ότι πρόκειται για μια μηχανή 32 bit, μπορούμε να προχωρήσουμε στη φόρτωση της μονάδας Mimikatz στη μνήμη.

```
meterpreter > load mimikatz
Loading extension mimikatz...success.

meterpreter > help mimikatz

Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds
    livessp           Attempt to retrieve livessp creds
    mimikatz_command  Run a custom commannd
    msv               Attempt to retrieve msv creds (hashes)
    ssp               Attempt to retrieve ssp creds
    tspkg             Attempt to retrieve tspkg creds
    wdigest           Attempt to retrieve wdigest creds
```

Σχήμα 26 Φόρτωση του Mimikatz στη μνήμη

Το Metasploit μας παρέχει κάποιες ενσωματωμένες εντολές που προβάλλουν το πιο συνηθισμένο χαρακτηριστικό του Mimikatz, το dumping hashes και τα διαπιστευτήρια καθαρού κειμένου απευθείας από τη μνήμη. Ωστόσο, η επιλογή mimikatz_command μας δίνει πλήρη πρόσβαση σε όλες τις λειτουργίες του Mimikatz.

```
meterpreter > mimikatz_command -f version
mimikatz 1.0 x86 (RC) (Nov  7 2013 08:21:02)
```

Σχήμα 27 Εκτέλεση της εντολής mimikatz-comand

Παρόλο που είναι ελαφρώς ανορθόδοξος, μπορούμε να λάβουμε μια πλήρη λίστα των διαθέσιμων ενοτήτων, προσπαθώντας να φορτώσουμε ένα ανύπαρκτο χαρακτηριστικό.

4.4 Εργαλείο ελέγχου συστήματος

Empire

Το PowerShell Empire είναι ένα πλαίσιο για την εκμετάλλευση σε υπολογιστές και διακομιστές με λειτουργικά συστήματα Microsoft Windows, Windows Server ή και τα δύο. Ορισμένες από τις δραστηριότητες και τους στόχους που μπορεί να επιτευχθούν περιλαμβάνουν την κλιμάκωση προνομίων (άνοδος προνομίων από έναν τυπικό λογαριασμό χρήστη σε διαχειριστή), αναγνώριση δικτύων και ξενιστών (ανακαλύπτοντας ποιες υποδοχές και υπηρεσίες υπάρχουν), εσωτερική μετακίνηση μεταξύ κεντρικών υπολογιστών και συλλογή διαπιστευτηρίων. Όλα αυτά είναι βασικά συστατικά μιας σύγχρονης δοκιμής διείσδυσης. Το PowerShell Empire το επιτυγχάνει αυτό μέσω τριών βασικών στοιχείων: ακροατές, stagers και πράκτορες.

- Ένας ακροατής είναι μια διαδικασία που ακούει σε σύνδεση στο μηχάνημα που επιτίθεται. Αυτό βοηθά το Empire να στείλει τα ευρήματα πίσω στον υπολογιστή του επιτιθέμενου.
- Ένας stager είναι ένα απόσπασμα κώδικα που επιτρέπει στο κακόβουλο λογισμικό να εκτελείται μέσω του πράκτορα στον χειραγωγημένο κεντρικό υπολογιστή.
- Ένας πράκτορας είναι ένα πρόγραμμα που διατηρεί μια σύνδεση μεταξύ του υπολογιστή σας και της χειραγωγημένης υποδοχής.
- Οι ενότητες είναι αυτές που εκτελούν τις κακόβουλες εντολές μας, οι οποίες μπορούν να συγκεντρώσουν διαπιστευτήρια και να κλιμακώσουν τα προνόμιά μας όπως αναφέρθηκε παραπάνω.

Κεφάλαιο 5 Sysmon

5.1 Παρουσίαση του εργαλείου Sysmon

Το Sysmon είναι ένα σύστημα παρακολούθησης συστήματος των windows. Το Sysmon παρέχει λεπτομερείς πληροφορίες σχετικά με τις δημιουργίες διαδικασιών, τις συνδέσεις δικτύου και τις αλλαγές στο χρόνο δημιουργίας των αρχείων. Συλλέγοντας τα συμβάντα που παράγει χρησιμοποιώντας τη Συλλογή συμβάντων των Windows ή τους πράκτορες της SIEM και στη συνέχεια την ανάλυση τους, είναι ικανό να εντοπίσει κακόβουλη ή ανώμαλη δραστηριότητα και να καταλάβει πώς λειτουργούν οι εισβολείς και το κακόβουλο λογισμικό στο δίκτυό του συστήματος. (Mark Russinovich and Thomas Garnier, 2019)

Η συλλογή συμβάντων επιτρέπει στους διαχειριστές να λαμβάνουν συμβάντα από απομακρυσμένους υπολογιστές και να τις αποθηκεύουν σε ένα τοπικό αρχείο καταγραφής συμβάντων στον υπολογιστή συλλογής. Ο προορισμός του αρχείου καταγραφής για τα συμβάντα είναι ιδιοκτησία της συνδρομής. Όλα τα δεδομένα στο προωθούμενο γεγονός αποθηκεύονται στο αρχείο καταγραφής συμβάντων συλλέκτη (καμία από τις πληροφορίες δεν έχει χαθεί). Πρόσθετες πληροφορίες σχετικά με την προώθηση συμβάντων προστίθενται επίσης στο γεγονός.

Η ακόλουθη λίστα περιγράφει τα είδη των συμβάντων καταγραφής :

- Συνδρομές που ξεκινούν από την προέλευση: Επιτρέπει να οριστεί μια συνδρομή συμβάντος σε έναν υπολογιστή συλλογής γεγονότων χωρίς να οριστούν οι υπολογιστές προέλευσης συμβάντος. Στη συνέχεια, μπορούν να ρυθμιστούν πολλοί υπολογιστές πηγής απομακρυσμένου συμβάντος (χρησιμοποιώντας μια ρύθμιση πολιτικής ομάδας) για να προωθήσουν τα καταγεγραμμένα γεγονότα στον υπολογιστή συλλογής συμβάντων. Αυτός ο τύπος συνδρομής είναι χρήσιμος όταν είναι άγνωστο ή δεν θέλουμε να καθορίσουμε όλους τους υπολογιστές πηγών συμβάντων που θα προωθούν τα γεγονότα.
- Συνδρομές που ξεκινούν από τον συλλέκτη: Επιτρέπει τη δημιουργία μιας συνδρομής συμβάντος γνωρίζοντας όλους τους υπολογιστές πηγής εκδήλωσης που θα προωθούν τα γεγονότα. Όλες οι πηγές συμβάντων ορίζονται τη στιγμή που δημιουργείται η συνδρομή.

Οι πράκτορες SIEM (security information and event management) παρέχουν ανάλυση πραγματικού χρόνου για ειδοποιήσεις ασφαλείας, οι οποίες δημιουργούνται από εφαρμογές ή από εξαρτήματα του διαδικτύου.

Παραδείγματα ειδοποιήσεων ασφαλείας:

Κανόνας	Στόχος	Ενεργοποίηση	Γεγονός
Επαναλαμβανόμενη επίθεση-Πηγή Εισόδου	Πρόωρη προειδοποίηση για βίαιες επιθέσεις, εικασίες κωδικού πρόσβασης και λανθασμένες εφαρμογές.	Ειδοποίηση για 3 ή περισσότερες αποτυχημένες συνδέσεις σε 1 λεπτό από έναν κεντρικό υπολογιστή	Active Directory, Syslog (Unix Hosts, Switches, Routers, VPN), RADIUS, TACACS, Monitored Applications.

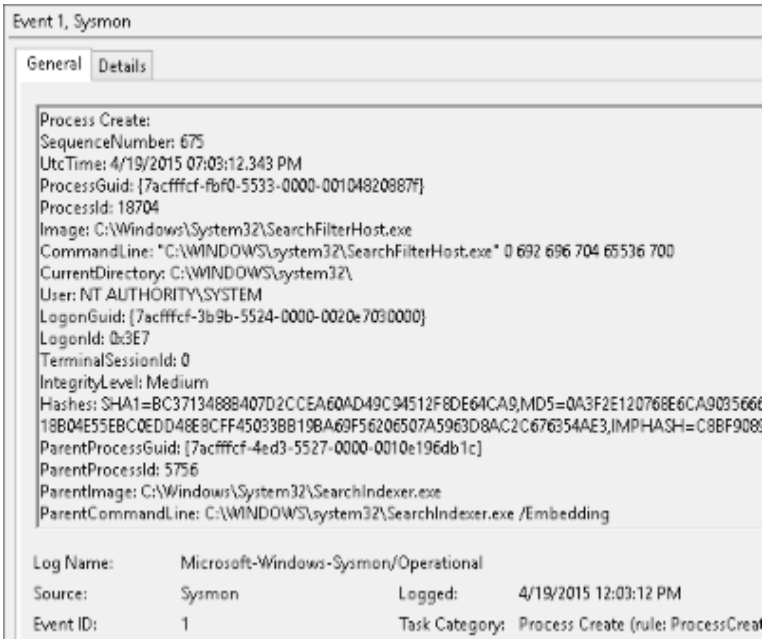
Επαναλαμβανόμενη επίθεση -Τοίχος Προστασίας	Πρόωρη προειδοποίηση για σαρώσεις, διαδόσεις σκουληκιών κλπ.	Ειδοποίηση σχετικά με 15 ή περισσότερα Firewall Drop / Reject / Deny γεγονότα από μια διεύθυνση IP σε ένα λεπτό.	Firewalls, Routers and Switches.
Επαναλαμβανόμενη επίθεση - Σύστημα πρόληψης εισβολής δικτύου	Πρόωρη προειδοποίηση για σαρώσεις, διαδόσεις σκουληκιών κλπ.	Ειδοποίηση για 7 ή περισσότερα γεγονότα IDS από μία μόνο διεύθυνση IP σε ένα λεπτό	Συσκευές ανίχνευσης και πρόληψης εισβολής δικτύου
Επαναλαμβανόμενη επίθεση – Σύστημα πρόληψης εισβολής του κεντρικού υπολογιστή	Βρίσκει συστήματα υποδοχής που ενδέχεται να έχουν μολυνθεί ή παραβιαστεί. (που παρουσιάζουν συμπεριφορές μόλυνσης)	Ειδοποίηση για 3 ή περισσότερα συμβάντα από μια διεύθυνση IP σε 10 λεπτά	Προειδοποιήσεις πρόληψης εισβολής του συστήματος του κεντρικού υπολογιστή
Ανίχνευση / αφαίρεση ιού	Ειδοποίηση όταν ανιχνεύεται ιός, spyware ή άλλο κακόβουλο λογισμικό σε έναν κεντρικό υπολογιστή	Προειδοποίηση όταν ένας μόνο κεντρικός υπολογιστής βλέπει ένα αναγνωρίσιμο κομμάτι κακόβουλου λογισμικού	Anti-Virus, HIPS, Network/System Behavioral Anomaly Detectors
Εντοπίστηκε ιός ή λογισμικό υποκλοπής, αλλά απέτυχε να καθαριστεί	Ειδοποίηση όταν έχει περάσει > 1 ώρα από την ανίχνευση κακόβουλου λογισμικού, σε μια πηγή, χωρίς να καταργηθεί με επιτυχία ο αντίστοιχος ιός	Ειδοποίηση όταν ένας μόνος κεντρικός υπολογιστής αποτύχει να καθαρίσει αυτόματα το κακόβουλο λογισμικό εντός 1 ώρας από την ανίχνευση	Event Sources: Firewall, NIPS, Anti-Virus, HIPS, Failed Login Events

5.2 Περιγραφή των δυνατοτήτων του Sysmon

Το Sysmon περιέχει τις ακόλουθες δυνατότητες :

1. Καταγράφει τη διαδικασία δημιουργίας με πλήρη γραμμή εντολών για τρέχουσες και γονικές διαδικασίες
2. Καταγράφει το hash των αρχείων εικόνας διαδικασίας χρησιμοποιώντας SHA1 (προεπιλογή), MD5, SHA256 ή IMPHASH.
3. Μπορεί να χρησιμοποιήσει ταυτόχρονα πολλά Hashes.
4. Περιλαμβάνει μια διεργασία GUID που δημιουργεί συμβάντα για να επιτρέψει τη συσχέτιση των συμβάντων ακόμη και όταν τα Windows επαναχρησιμοποιήσουν ίδια αναγνωριστικά διεργασίας.
5. Περιλαμβάνει έναν οδηγό GUID για κάθε γεγονός για να επιτρέψει τη συσχέτιση των συμβάντων στην ίδια σύνδεση.
6. Καταγράφει τη φόρτωση των προγραμμάτων οδήγησης ή των βιβλιοθηκών DLL με τις υπογραφές και τα hashes τους.
7. Καταγράφει προσβάσεις σε δίσκους και μονάδες εγγραφής
8. Προαιρετικά καταγράφει συνδέσεις δικτύου, συμπεριλαμβανομένης της διαδικασίας προέλευσης κάθε σύνδεσης, των διευθύνσεων IP, των αριθμών θυρών, των ονομάτων κεντρικών υπολογιστών και των ονομάτων των θυρών.

9. Εντοπίζει αλλαγές στο χρόνο δημιουργίας αρχείων για να καταλάβει πότε δημιουργήθηκε πραγματικά ένα αρχείο. Η τροποποίηση του αρχείου δημιουργίας timestamps είναι μια τεχνική που συνήθως χρησιμοποιείται από κακόβουλο λογισμικό για να καλύψει τα ίχνη του.
10. Πραγματοποιείτε αυτόματη επαναφόρτωση διαμόρφωσης αν αλλάξει στο μητρώο.
11. Πραγματοποιείτε φιλτράρισμα κανόνων ώστε να επιτρέψει ή να αποκλείσει δυναμικά ορισμένα συμβάντα.
12. Δημιουργεί συμβάντα από την αρχή της διαδικασίας εκκίνησης για τη λήψη δραστηριότητας από ακόμη και εξελιγμένο κακόβουλο λογισμικό πυρήνα.



Σχήμα 28 Γενικές πληροφορίες για το Event 1

Όλα τα παραπάνω χωρίζονται σε γεγονότα και αναγνωρίζονται με ένα αριθμητικό ID αντίστοιχα.

Από την έκδοση Vista και μετέπειτα, τα συμβάντα αποθηκεύονται στο "Αρχεία εφαρμογών και υπηρεσιών / Microsoft / Windows / Sysmon / Operational" και σε παλαιότερα συστήματα τα συμβάντα γράφονται στο αρχείο καταγραφής συμβάντων συστήματος. Τα χρονικά σήματα συμβάντων είναι σε κανονική ώρα UTC.

Τα παρακάτω είναι παραδείγματα κάθε τύπου συμβάντος που δημιουργεί το Sysmon :

Event ID 1: Δημιουργία Διαδικασιών (Process creation)

Το συμβάν δημιουργίας διεργασίας παρέχει εκτεταμένες πληροφορίες σχετικά με μια νεοσυσταθείσα διαδικασία. Η πλήρης γραμμή εντολών παρέχει ένα πλαίσιο για την εκτέλεση της διαδικασίας. Το πεδίο ProcessGUID είναι μια μοναδική τιμή για αυτή τη διαδικασία σε έναν τομέα, ώστε να διευκολυνθεί η συσχέτιση συμβάντων. Το hash είναι ένα πλήρες hash του αρχείου με τους αλγορίθμους στο πεδίο HashType.

Event ID 2: Αλλαγή χρόνου δημιουργίας αρχείου από μία διαδικασία (A process changed a file creation time)

Το συμβάν αλλαγής χρόνου δημιουργίας του αρχείου καταγράφεται όταν ο χρόνος δημιουργίας ενός αρχείου τροποποιείται ρητά από μια διαδικασία. Αυτό το συμβάν βοηθά στην παρακολούθηση του πραγματικού χρόνου δημιουργίας ενός αρχείου. Οι επιτιθέμενοι ενδέχεται να αλλάξουν τον χρόνο δημιουργίας ενός αρχείου ενός backdoor για να φανεί σαν να έχουν

εγκατασταθεί με το λειτουργικό σύστημα. Σημειώστε ότι πολλές διαδικασίες αλλάζουν νόμιμα το χρόνο δημιουργίας ενός αρχείου αυτό δεν δηλώνει απαραίτητα κακόβουλη δραστηριότητα.

Event ID 3: Σύνδεση στο δίκτυο (Network connection)

Το γεγονός σύνδεσης δικτύου καταγράφει συνδέσεις TCP / UDP στο μηχάνημα. Η συγκεκριμένη ρύθμιση είναι απενεργοποιημένη σαν προεπιλογή. Κάθε σύνδεση συνδέεται με μια διεργασία μέσω των πεδίων ProcessId και ProcessGUID. Το γεγονός περιέχει επίσης τις διευθύνσεις IP, τους αριθμούς θυρών και την κατάσταση IPv6.

Event ID 4: Αλλαγή της κατάστασης εξυπηρέτησης του Sysmon (Sysmon service state changed)

Η κατάσταση αλλαγής εξυπηρέτησης αναφέρει την κατάσταση της υπηρεσίας Sysmon (ξεκίνησε ή σταμάτησε).

Event ID 5: Η διαδικασία τερματίστηκε (Process terminated)

Η διαδικασία τερματίζει τις αναφορές συμβάντων όταν τερματίζεται μια διαδικασία. Παρέχει το UtcTime, ProcessGuid και ProcessId της διαδικασίας.

Event ID 6: Φόρτωση οδηγού (Driver loader)

Τα συμβάντα που φορτώνονται από τον οδηγό παρέχουν πληροφορίες σχετικά με ένα πρόγραμμα οδήγησης που φορτώνεται στο σύστημα. Τα διαμορφωμένα Hashes παρέχονται σαν πληροφορίες υπογραφής. Η υπογραφή δημιουργείται ασύγχρονα για λόγους απόδοσης και υποδεικνύει εάν το αρχείο αφαιρέθηκε μετά τη φόρτωση.

Event ID 7: Φόρτωση εικόνας

Το συμβάν φορτωμένης εικόνας καταγράφεται όταν μια ενότητα φορτώνεται σε μια συγκεκριμένη διαδικασία. Αυτή η ρύθμιση είναι απενεργοποιημένη σαν προεπιλογή και πρέπει να ρυθμιστεί με την επιλογή -l. Υποδεικνύει τη διαδικασία στην οποία φορτώνεται η μονάδα, τα hashes και οι πληροφορίες υπογραφής. Η υπογραφή δημιουργείται ασύγχρονα για λόγους απόδοσης και υποδεικνύει εάν το αρχείο αφαιρέθηκε μετά τη φόρτωση. Αυτό το συμβάν θα πρέπει να ρυθμιστεί προσεκτικά, καθώς η παρακολούθηση όλων των συμβάντων φόρτωσης εικόνας θα δημιουργήσει ένα μεγάλο αριθμό γεγονότων.

Event ID 8: Δημιουργία απομακρυσμένου νήματος (Create remote threat)

Το συμβάν δημιουργίας απομακρυσμένου νήματος εντοπίζει πότε μια διαδικασία δημιουργεί ένα νήμα σε μια άλλη διαδικασία. Αυτή η τεχνική χρησιμοποιείται από κάποιο κακόβουλο λογισμικό για την έγχυση κώδικα και την απόκρυψη του από άλλες διαδικασίες. Το συμβάν υποδεικνύει τη διαδικασία πηγής και στόχου. Παρέχει πληροφορίες σχετικά με τον κώδικα που θα εκτελεστεί στο νέο νήμα: StartAddress, StartModule και StartFunction. Σημειώστε ότι τα πεδία StartModule και StartFunction είναι συμπεράσματα και ενδέχεται να είναι κενά αν η διεύθυνση εκκίνησης βρίσκεται εκτός των φορτωμένων μονάδων ή των γνωστών εξαγόμενων λειτουργιών.

Event ID 9: Ακαθάριστη πρόσβαση ανάγνωσης (Raw access read)

Το συμβάν RawAccessRead ανιχνεύει πότε μια διαδικασία διεξάγει εργασίες ανάγνωσης από τη μονάδα δίσκου χρησιμοποιώντας την \\. \ δήλωση. Αυτή η τεχνική χρησιμοποιείται συχνά από κακόβουλο λογισμικό για την απομάκρυνση δεδομένων από αρχεία που είναι κλειδωμένα για ανάγνωση, καθώς και για την αποφυγή εργαλείων ελέγχου πρόσβασης αρχείων. Το συμβάν υποδεικνύει τη διαδικασία προέλευσης και τη συσκευή προορισμού.

Event ID 10: Διαδικασία πρόσβασης (Process Access)

Η διαδικασία προσεγγίζει αναφορές συμβάντων όταν μια διαδικασία ανοίγει μια άλλη διαδικασία, μια ενέργεια που ακολουθείται συχνά από ερωτήματα πληροφοριών ή την ανάγνωση και τη γραφή του χώρου διευθύνσεων της διεργασίας στόχου. Αυτό επιτρέπει την ανίχνευση εργαλείων hacking που διαβάζουν τα περιεχόμενα της μνήμης από διαδικασίες όπως το Local Security Authority (Lsass.exe) για να κλέψουν τα διαπιστευτήρια για χρήση στις επιθέσεις Pass-the-Hash. Η ενεργοποίησή της μπορεί να δημιουργήσει μεγάλο όγκο δεδομένων καταγραφής εάν υπάρχουν ενεργοποιημένα διαγνωστικά βοηθητικά προγράμματα που ανοίγουν επανειλημμένα

διεργασίες για να διερευνήσουν την κατάσταση τους, οπότε γενικά θα πρέπει να γίνεται μόνο με φίλτρα που καταργούν τις αναμενόμενες προσπελάσεις.

Event ID 11: Δημιουργία αρχείου (File create)

Οι εγγραφές δημιουργίας αρχείων καταγράφονται όταν ένα αρχείο δημιουργείται ή αντικαθίσταται. Αυτό το συμβάν είναι χρήσιμο για την παρακολούθηση τοποθεσιών αυτόματης έναρξης, όπως ο φάκελος εκκίνησης, καθώς και οι προσωρινές τοποθεσίες ή τοποθεσίες λήψεων, οι οποίες είναι κοινές θέσεις κακόβουλων προγραμμάτων που πέφτουν κατά την αρχική μόλυνση.

Event ID 12: Συμβάν μητρώου – Δημιουργία και διαγραφή αντικειμένων (Registry event – Object create and delete)

Το κλειδί μητρώου και η τιμή δημιουργούν και διαγράφουν συνδέσεις λειτουργιών σε αυτόν τον τύπο συμβάντος, οι οποίες μπορούν να είναι χρήσιμες για την παρακολούθηση των αλλαγών στις τοποθεσίες αυτόματης εκκίνησης του μητρώου ή για συγκεκριμένες τροποποιήσεις στο μητρώο μέσω κακόβουλου λογισμικού.

Το Sysmon χρησιμοποιεί συντομευμένες εκδόσεις των ονομάτων κλειδιών μητρώου, με τις ακόλουθες αντιστοιχίσεις:

Key name	**Abbreviation**
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_LOCAL_MACHINE\System\ControlSet00x	HKLM\System\CurrentControlSet
HKEY_LOCAL_MACHINE\Classes	HKCR

Event ID 13: Συμβάν μητρώου - Ρύθμιση τιμής (Registry event – Value set)

Αυτός ο τύπος συμβάντος μητρώου αναγνωρίζει τις τροποποιήσεις τιμής μητρώου. Το συμβάν καταγράφει την τιμή που έχει εγγραφεί για τις τιμές μητρώου τύπου DWORD και QWORD.

Event ID 14: Συμβάν μητρώου – Μετονομασία κλειδιού και τιμής (Registry Event - Key and Value Rename)

Μετονομάζοντας το κλειδί μητρώου και την τιμή ενεργοποιείται σύνδεση για αυτόν τον τύπο συμβάντος, καταγράφοντας το νέο όνομα του κλειδιού ή της τιμής που αλλάχθηκε.

Event ID 15: Δημιουργία αρχείου κατακερματισμού ροής (File create stream hash)

Αυτό το συμβάν καταγράφεται όταν δημιουργείται μια ονομαστική ροή αρχείου και παράγει συμβάντα που καταγράφουν το hash των περιεχομένων του αρχείου στο οποίο έχει εκχωρηθεί η ροή (πριν ονομαστεί), καθώς και τα περιεχόμενα της ροής με όνομα. Υπάρχουν παραλλαγές κακόβουλου λογισμικού που ρίχνουν τα εκτελέσιμα τους ή τις ρυθμίσεις διαμόρφωσης τους μέσω των λήψεων του προγράμματος περιήγησης και αυτό το συμβάν έχει ως στόχο να καταγράψει τα γεγονότα που βασίζονται στο πρόγραμμα περιήγησης μαρκάροντας τα σαν ροή Zone.Identifier "σημάδι του διαδικτύου".

Event ID 16: Η κατάσταση ρύθμισης του Sysmon έχει αλλάξει (Sysmon config state changed)

Αυτό το συμβάν μπορεί να περιλαμβάνει ή όχι ένα hash. Το hash θα εξαρτηθεί από το αν ο Sysmon κλήθηκε με ένα αρχείο XML διαμόρφωσης ή αν χρησιμοποιήθηκε μόνο μέσω ρυθμίσεων διαμόρφωσης στη γραμμή εντολών. Αν καθορίστηκε μια ρύθμιση παραμέτρων μέσω αρχείου XML, τότε θα έχει καταγραφεί το hash του αρχείου, έτσι ώστε να μπορέσουμε να ανιχνεύσουμε εάν κάποιος επιχειρεί να κάνει παραμετροποίηση του Sysmon με ένα μη εξουσιοδοτημένο αρχείο ρυθμίσεων το οποίο θα παράγει ένα διαφορετικό hash.

Event ID 17: Συμβάν δημιουργίας σωλήνα (Pipe created event)

Αυτό το συμβάν δημιουργείται όταν δημιουργηθεί ένας ονομασμένος σωλήνας. Το κακόβουλο λογισμικό χρησιμοποιεί συχνά ονομασμένους σωλήνες για επικοινωνία μεταξύ των διαδικασιών.

Event ID 18: Συμβάν σύνδεση σωλήνα (Pipe connected event)

Αυτό το συμβάν καταγράφεται όταν πραγματοποιείται μια ορισμένη σύνδεση σωλήνα μεταξύ ενός προγράμματος-πελάτη και ενός διακομιστή.

Event ID 19: Συμβάν Wmi φίλτρου (Wmi event filter activity detected)

Όταν καταγράφεται ένα φίλτρο συμβάντος WMI, το οποίο είναι μια μέθοδος που χρησιμοποιείται από το κακόβουλο λογισμικό για εκτέλεση, το συμβάν αυτό καταγράφει το χώρο ονομάτων WMI, το όνομα φίλτρου και την έκφραση φίλτρου.

Event ID 20: Συμβάν Wmi κατανάλωσης (Wmi event consumer activity detected)

Αυτό το συμβάν καταγράφει την καταχώριση των καταναλωτών WMI, καταγράφοντας το όνομα του καταναλωτή, το αρχείο καταγραφής και τον προορισμό.

Event ID 21: Συμβάν Wmi κατανάλωσης σε φίλτρο (Wmi Event Consumer To Filter activity detected)

Όταν ένας καταναλωτής συνδέεται με ένα φίλτρο, αυτό το συμβάν καταγράφει το όνομα του καταναλωτή και τη διαδρομή του φίλτρου.

Event ID 22: Συμβάν DNS (DNS query)

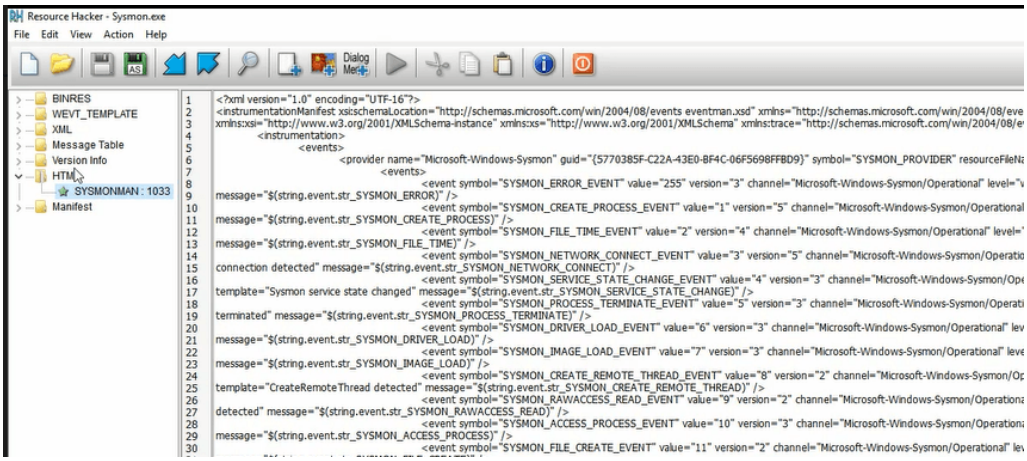
Αυτό το συμβάν δημιουργείται όταν μια διεργασία εκτελεί ένα ερώτημα DNS, είτε το αποτέλεσμα είναι επιτυχές είτε αποτυγχάνει, είτε είναι προσωρινά αποθηκευμένο ή όχι. Η τηλεμετρία για αυτό το συμβάν προστέθηκε για τα Windows 8.1, άρα δεν είναι διαθέσιμη στα Windows 7 και νωρίτερα.

Event ID 255: Σφάλμα (Error)

Αυτό το συμβάν δημιουργείται όταν παρουσιαστεί σφάλμα στο Sysmon. Σφάλματα μπορούν να συμβούν αν το σύστημα βρίσκεται σε μεγάλο φόρτο εργασίας και ορισμένες εντολές δεν μπορούν να εκτελεστούν ή εάν υπάρχει σφάλμα στην υπηρεσία Sysmon.

5.3 Ρυθμίσεις και χρήση του εργαλείου Sysmon

Για να μπορεί κάποιος να δημιουργήσει ένα αρχείο διαμόρφωσης Sysmon, θα πρέπει πρώτα να μάθει πώς μπορεί να ελέγξει τι προσφέρει το Sysmon. Για παράδειγμα, αν ανοιχθεί το εκτελέσιμο αρχείο Sysmon μπορεί να ελεγχθεί το πώς φαίνονται οι δηλώσεις και οι δυνατότητες του.



Σχήμα 29 Άνοιγμα του εκτελέσιμου αρχείου Sysmon και προβολή των περιεχομένων του.

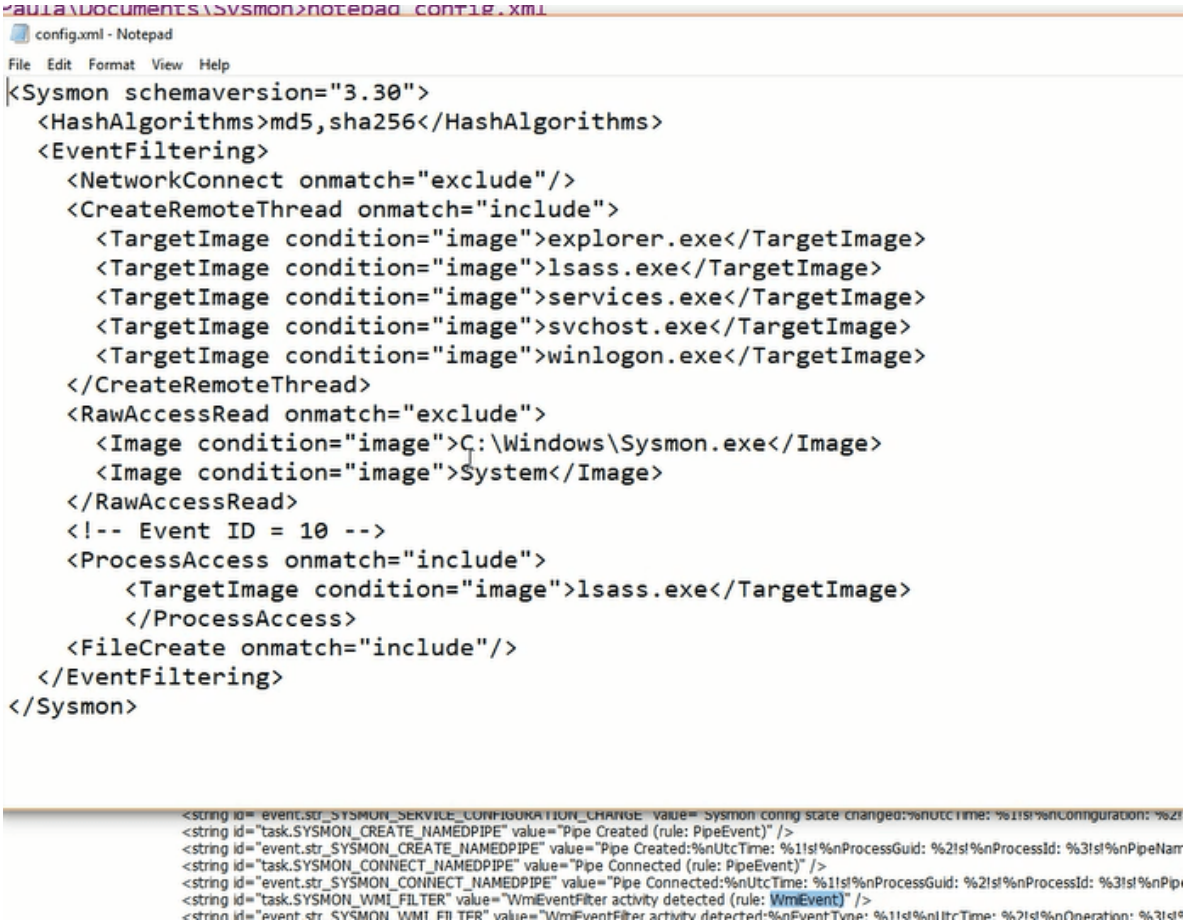
Εδώ μπορεί κανείς να δει τα πρότυπα που καθορίζουν διαφορετικούς τύπους προσέγγισης για την καταγραφή.

Αυτά είναι τα γεγονότα που θα καταγράφουν στο αρχείο καταγραφής συμβάντων: η αλλαγή χρόνου δημιουργίας αρχείου, η παρακολούθηση διεργασιών, η δημιουργία διεργασιών, ο τερματισμός διεργασιών, η ανίχνευση σύνδεσης δικτύου, το φορτωμένο πρόγραμμα οδήγησης και τα υπόλοιπα που αναφέρθηκαν παραπάνω.

```
</template>
<template tid="File creation time changed">
        <data name="UtcTime" inType="win:UnicodeString" outType="xs:string" />
        <data name="ProcessGuid" inType="win:GUID" />
        <data name="ProcessId" inType="win:UInt32" outType="win:PID" />
        <data name="Image" inType="win:UnicodeString" outType="xs:string" />
        <data name="TargetFilename" inType="win:UnicodeString" outType="xs:string" />
        <data name="CreationUtcTime" inType="win:UnicodeString" outType="xs:string" />
        <data name="PreviousCreationUtcTime" inType="win:UnicodeString" outType="xs:string" />
</template>
<template tid="Network connection detected">
```

Σχήμα 30 Συμβάντα που καταγράφονται στο αρχείο καταγραφής

Μέσα στο Sysmon, υπάρχει η δυνατότητα παρακολούθησης του φίλτρου συμβάντων WMI. Υπάρχει επίσης ο καταναλωτής γεγονότων, το φίλτρο συμβάντων, η δραστηριότητα του ConsumerToFilter και ούτω καθεξής. Δηλαδή, εάν υπάρχει κακόβουλο λογισμικό που χρησιμοποιεί το WMI ή εάν το WMI τροποποιηθεί, τότε το είδος πληροφοριών θα βρεθεί στο Sysmon. Κάθε φορά που γίνονται αλλαγές στη δημιουργία των κανόνων, επειδή έτσι λειτουργεί με το Sysmon, ίσως να αναρωτηθεί κανείς τι είδους ονόματα πρέπει να χρησιμοποιήσει στο αρχείο config για να το λειτουργήσει. Η απάντηση σε αυτή την ερώτηση είναι πολύ απλή. Πρέπει να υπάρχουν ονόματα κανόνων, όπως το "συμβάν σωληνώσεων κανόνα", το "συμβάν WMI κανόνας" και ούτω καθεξής. Στη συνέχεια, βάσει αυτού, δημιουργούνται οι κανόνες στο αρχείο ρυθμίσεων.



Σχήμα 31 Δημιουργία κανόνων στο αρχείο ρυθμίσεων

Δεν χρειάζεται να ρυθμίσει κανείς τα πάντα, μπορεί να διαμορφώσει μόνο μερικά πράγματα, περιλαμβάνοντας ορισμένα γεγονότα είτε εξαιρώντας τα.

Για την περίπτωση σύνδεσης στο δίκτυο, γίνεται παρακολούθηση όλων των τύπων συμβάντων.

Για τη δημιουργία ενός απομακρυσμένου νήματος, στη συγκεκριμένη περίπτωση, γίνεται παρακολούθηση μόνο του εξερευνητή, του LSASS, των υπηρεσιών, του svchost και του Winlogon.

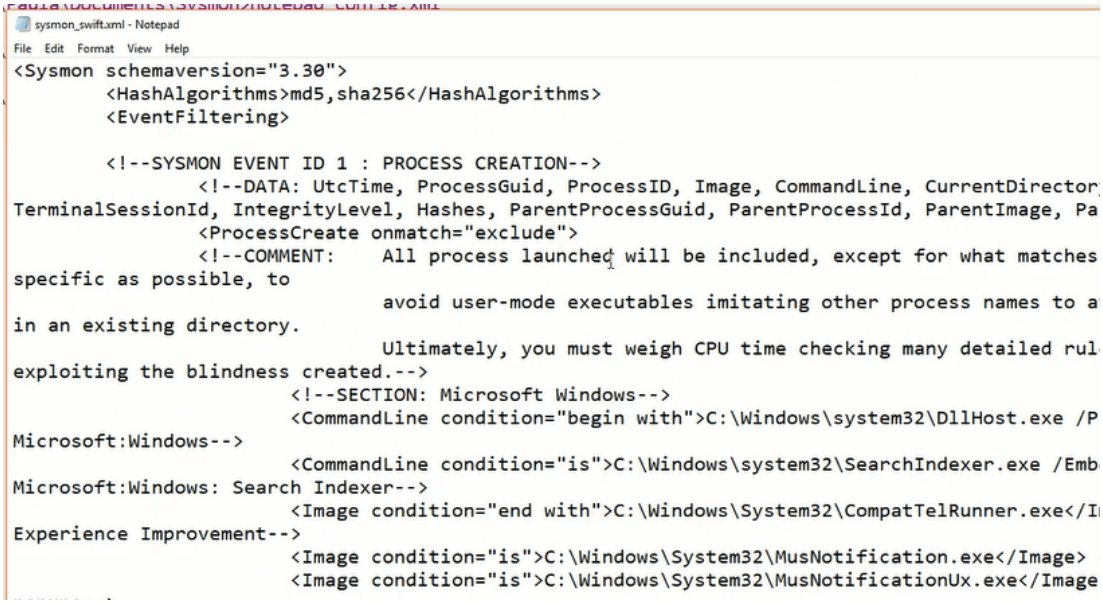
Δημιουργία γεγονότος ακατέργαστης πρόσβασης, γίνεται παρακολούθηση των διαδικασιών όπως η πρόσβαση στην διαδικασία, η οποία είναι καλή για pass-the-hash, περιλαμβάνοντας μόνο το LSASS.

Στην περίπτωση του FileCreate onmatch = "include" δεν καταγράφετε τίποτα επειδή δεν συμπεριλαμβάνουμε τίποτα στο αρχείο, πράγμα που σημαίνει, φυσικά, ότι δεν παρακολουθείται τίποτα.

Τώρα, η ερώτηση είναι, μπορεί κάποιος να το κάνει πιο περίπλοκο;

Μπορεί κανείς να παρακολουθήσει μόνο ορισμένες διαδικασίες που δεν είναι τόσο γνωστές;

Λοιπόν, το Sysmon σε αυτή τη περίπτωση δεν είναι τόσο ευέλικτο. Επομένως, πρέπει να γίνει εργασία στα αρχεία όπως φαίνεται στη παρακάτω εικόνα.



Σχήμα 32 Παραμετροποίηση των αρχείων του Sysmon

Τώρα, εδώ μπορούμε να δει κανείς ότι έχουν αναφερθεί διαφορετικούς τύπους διαδικασιών που δεν χρήζουν παρακολούθησης. Γίνεται λοιπόν απόκλιση όλων των ονομάτων των γνωστών διαδικασιών, πράγμα που θα μπορούσε ενδεχομένως να οδηγήσει σε ένα μικρό πρόβλημα, επειδή εδώ καθορίζεται μόνο από το όνομα .

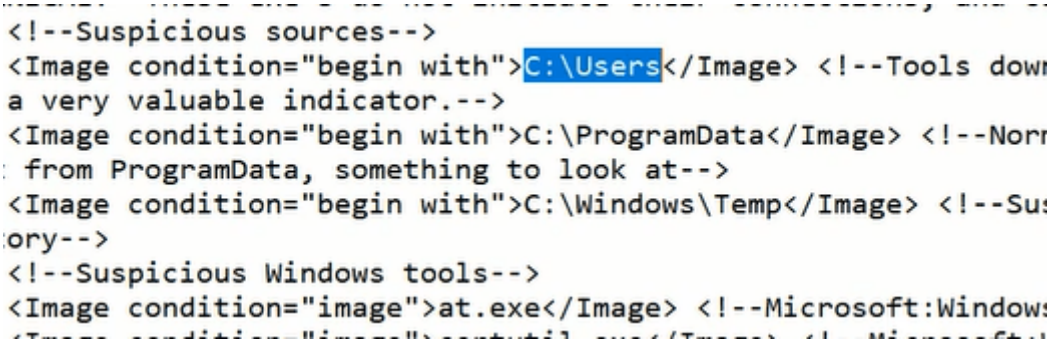
Για παράδειγμα, το Windows defender και ούτω καθεξής. Μπορεί όμως αυτό το κακόβουλο λογισμικό που ταιριάζει σε αυτούς τους κανόνες να ονομάζεται ως ένα από αυτά τα αρχεία;

Η απάντηση είναι ναι.

Για αυτό το λόγο πρέπει να δημιουργούνται λοιπόν διαφορετικές συνθήκες στο αρχείο για αυτές τις διαδικασίες οι οποίες όμως δημιουργούν ένα πραγματικά μεγάλο αρχείο.

Γίνετε εξαίρεση επίσης του OneDrive, των προγραμμάτων εγκατάστασης και ούτω καθεξής. Όλα τα γνωστά αρχεία λοιπόν που θα μπορούσαν να επηρεάσουν το χρόνο δημιουργίας των αρχείων.

Γίνετε εξαίρεση επίσης κάποιων πραγμάτων από το δίκτυο. Αυτή είναι πραγματικά μια πολύ ενδιαφέρουσα προσέγγιση, επειδή υπάρχουν διαφορετικοί τύποι επιλογών. Επομένως, γίνετε εξαίρεση όλων εκτός από αυτά που μας ενδιαφέρουν, για παράδειγμα, οτιδήποτε επεξεργάζεται μέσα στο C: \users και προσπαθεί να δημιουργήσει μια επικοινωνία δικτύου. Οτιδήποτε από το C: \ Windows \ Temp και ούτω καθεξής.



Σχήμα 33 Προβολή των γεγονότων στην διεύθυνση C:\Users

Αυτό είναι, γενικά, μία σύνδεση δικτύου που δημιουργείται από διαφορετικούς τύπους αρχείων που συνήθως δεν είναι αυτά που χρησιμοποιούνται για να δημιουργήσουν μια τέτοια εργασία, εντός της νομικής διαμόρφωσης του λειτουργικού συστήματος.

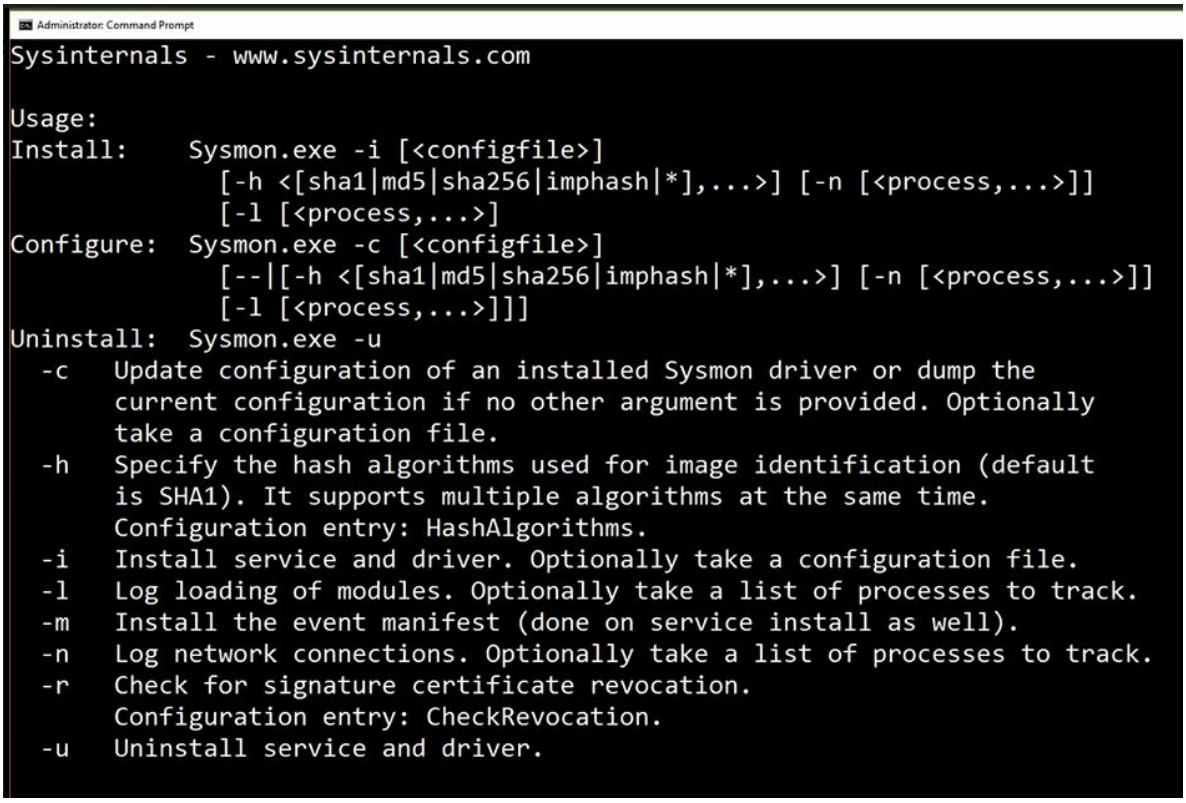
Φυσικά, όλες οι πόρτες προορισμού, επιπλέον συνδέσεις σε ορισμένες πόρτες. Υπάρχουν διαφορετικοί τύποι οδηγών φορτωμένοι στον πυρήνα.

Το ερώτημα είναι: πρέπει να γίνεται παρακολουθήσει ή όχι;

Από την εντολή DriverLoad onmatch = "exclude", δεν αποκλείονται πραγματικά πολλά. Εξαιρούμε διάφορους τύπους οδηγών εγκατάστασης από τα Windows και της Intel αλλά όλα τα υπόλοιπα θα είναι μέσα στην καταγραφή.

Εδώ υπάρχει η ακατέργαστη πρόσβαση στο δίσκο. Έτσι, δημιουργούνται πολλές επιλογές για το πώς μπορούμε να παρακολουθήσουμε το Sysmon.

Αρχικά θα γίνει η εγκατάσταση του Sysmon. Υπάρχει το αρχείο εγκατάστασης, Sysmon.exe και μπορεί κάποιος απλά να τρέξει μία εντολή εδώ για να μάθουμε τι είδους επιλογές έχουμε.



Σχήμα 34 Επιλογές του Sysmon.exe

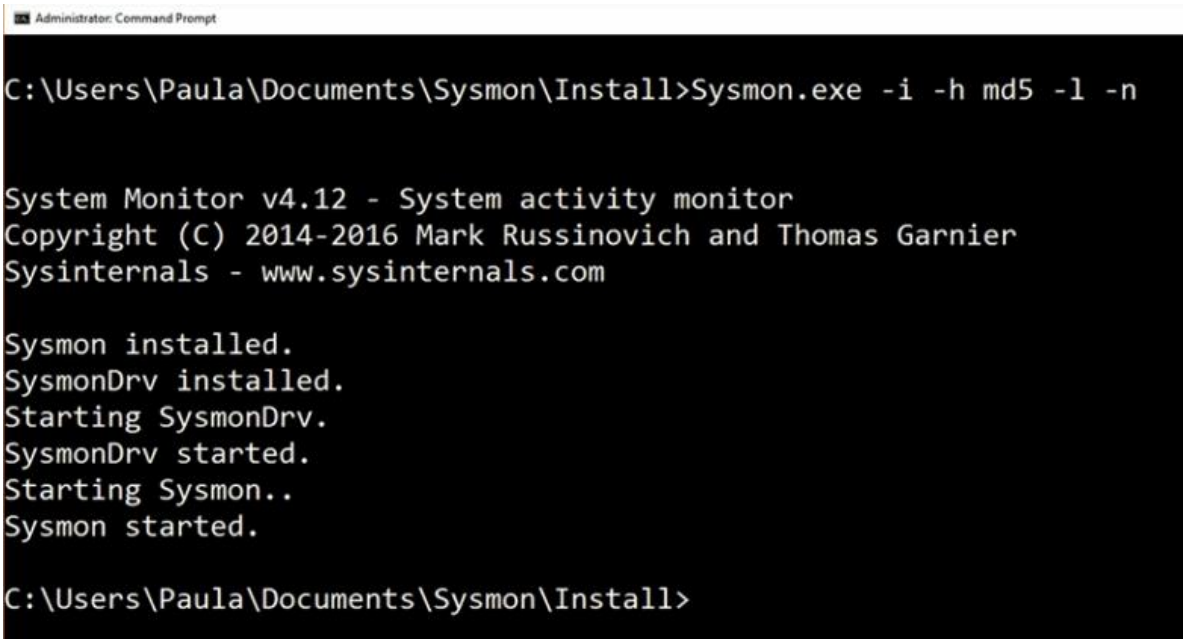
Ένα από τα ενδιαφέροντα πράγματα είναι ότι ακόμα και αν δεν έχουν καθοριστεί συγκεκριμένες ρυθμίσεις, το Sysmon θα εγκατασταθεί χωρίς προβλήματα και αυτό ακριβώς θα γίνει στην αρχή. Υπάρχει μια επιλογή -c και μπορεί να ενημερώσει τη διαμόρφωση κάθε φορά που το Sysmon είναι ήδη εγκατεστημένο. Μπορούν επίσης να καθοριστούν οι αλγόριθμοι κατακερματισμού.

Μπορεί να οριστεί ο SHA-1 αλλά υπάρχουν και πολλές άλλες επιλογές όπως είναι το imphash που είναι σαν ένα εισερχόμενο hash. Η λίστα εισαγωγών είναι ακόμη ένα μέσο στο οποίο μπορούμε να βασιζόμαστε αρχεία εικόνων. Αυτό είναι ιδιαίτερα ενδιαφέρον, ειδικά όταν οι προγραμματιστές αλλάζουν την έκδοση του αρχείου και άλλων αλλά ο κατάλογος των εισαγωγών παραμένει ο ίδιος.

Επίσης, έχουμε την επιλογή -l, για τη φόρτωση των ενοτήτων. Έχουμε επίσης, για παράδειγμα, μια ακόμη ενδιαφέρουσα επιλογή που είναι -n οποία χρησιμοποιείται για την καταγραφή

διαφορετικών τύπων συνδέσεων δικτύου. Θα πραγματοποιηθεί πραγματικά ένα πολύ ενδιαφέρον βήμα γύρω από αυτό. Η παράμετρος -r είναι επίσης πολύ καλή: ελέγχει ένα πιστοποιητικό υπογραφής για επαλήθευση. Έτσι, γίνεται επαλήθευση των υπογραφών και αν το πιστοποιητικό ακυρώθηκε ή όχι.

Πίσω στην εγκατάσταση επιλέγοντας -i, -h για να καθοριστεί ότι θα γίνει σύνδεση με MD5, για παράδειγμα, και έπειτα -l για να γίνει καταγραφή των διαφορετικών τύπων των ενοτήτων που φορτώνονται, οι οποίες θα μπορούσαν, για παράδειγμα, να είναι ένα αρχείο DLL ή οποιοδήποτε άλλο πράγμα. Το επόμενο βήμα που θα καθορίσουμε είναι το -n. Αυτή θα είναι η εντολή εγκατάστασής στο Sysmon.



Σχήμα 35 Εκτέλεση του Sysmon.exe με τα επιθυμητά ορίσματα

Προς το παρόν, μπορεί να επαληθευτεί πώς καταγράφει τα αρχεία καταγραφής συμβάντων ξεκινώντας το πρόγραμμα προβολής συμβάντων. Η διαδρομή είναι αρχείο καταγραφής εφαρμογών και υπηρεσιών, Microsoft, Windows και στη συνέχεια στο Sysmon. Έχει δημιουργηθεί πλέον λειτουργικό αρχείο Sysmon όπου έχουμε όλες τις λεπτομέρειες που επιλέξαμε να φορτώσουμε.

Operational Number of events: 78,513 (!) New events available

Level	Date and Time	Source	Eve...	Task Category
Information	10/10/2016 7:10:22 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	10/10/2016 7:10:22 AM	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	10/10/2016 7:10:22 AM	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	10/10/2016 7:10:21 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	10/10/2016 7:10:21 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	10/10/2016 7:10:20 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	10/10/2016 7:10:20 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	10/10/2016 7:10:20 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	10/10/2016 7:10:19 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	10/10/2016 7:10:19 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	10/10/2016 7:10:19 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	10/10/2016 7:10:14 AM	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	10/10/2016 7:10:14 AM	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	10/10/2016 7:10:14 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	10/10/2016 7:10:14 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	10/10/2016 7:10:12 AM	Sysmon	3	Network connection detected (rule: NetworkConnect)

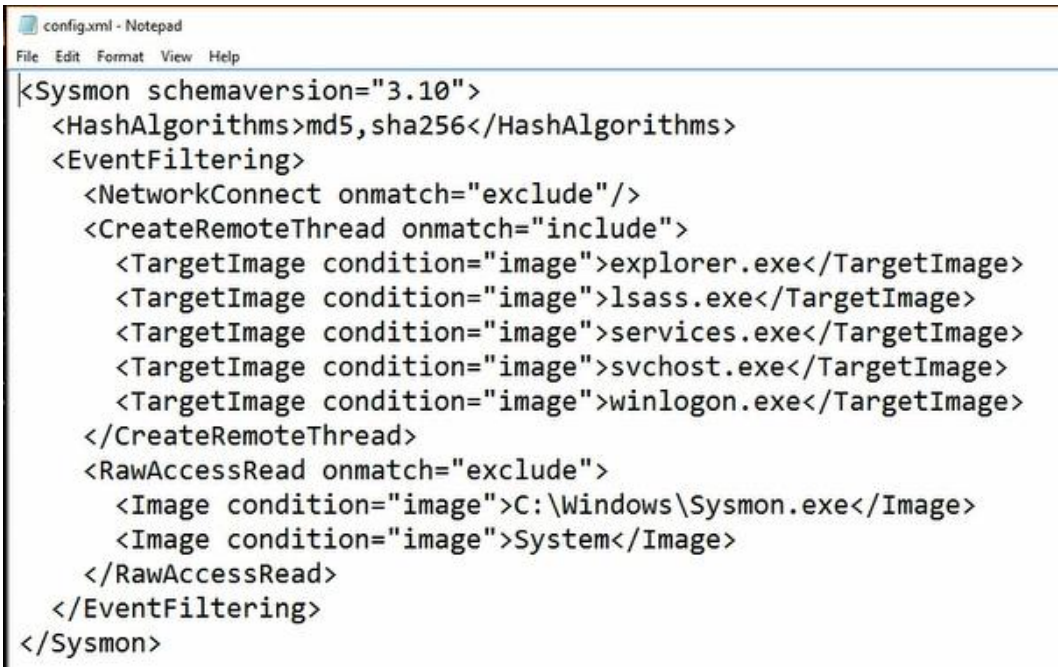
Σχήμα 36 Διάφοροι τύποι καταγεγραμμένων γεγονότων από το Sysmon

Φυσικά, υπάρχουν πολύ διαφορετικοί τύποι γεγονότων που θα μπορούσαν να χρησιμοποιηθούν εδώ. Υπάρχουν τώρα, δέκα γεγονότα που θα καταγραφούν. Από προεπιλογή, ορισμένα από αυτά δεν έχουν καταγραφεί. Προς το παρόν, θα εξεταστεί η εξαγωγή των hashes και των διευθύνσεων IP από το αρχείο καταγραφής.

Το Sysmon επιτρέπει στην παρακολούθηση της διαμόρφωσης αυτήν τη στιγμή, μια διαδικασία δημιουργεί ένα συμβάν και επίσης ένα τερματίζει το συμβάν. Όταν ξεκινάει για παράδειγμα μια διαδικασία, μπορεί να παρατηρηθεί ότι η συγκεκριμένη διαδικασία, για παράδειγμα, είχε τις ακόλουθες παραμέτρους εκτέλεσης.

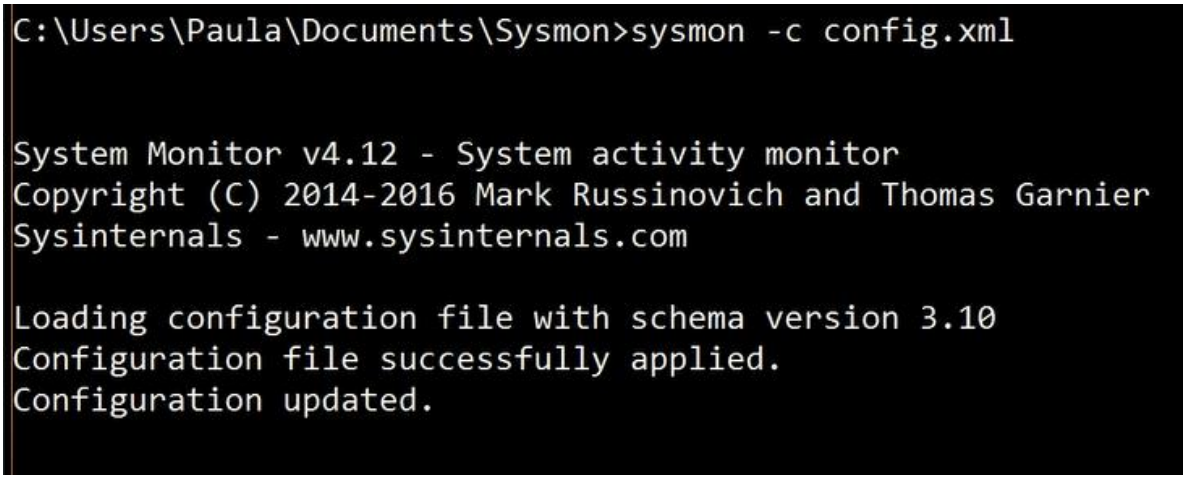
Επίσης, είναι γνωστό το ποιος εκτέλεσε αυτό το συμβάν και ποια ήταν η γονική εικόνα που ξεκίνησε αυτή η διαδικασία. Αυτό είναι πολύ ενδιαφέρον όταν αναλυθούν πολλά πράγματα όπως το ξεκίνημα ενός συγκεκριμένου εκτελέσιμου αρχείου, το οποίο μπορεί να είναι κακόβουλο λογισμικό.

Έχοντας πρόσβαση στο αρχείο καταγραφής, αυτό που έχει ενδιαφέρον μέχρι τώρα είναι η επαλήθευση για το ποια είναι η διαδρομή του αρχείου. Έτσι, πηγαίνοντας στις ιδιότητες του αρχείου καταγραφής και μπορεί κανείς να δει τη διαδρομή του η οποία είναι στο Windows \ System 32 \ Winevt \ logs. Γίνετε ενημέρωση της διαμόρφωσης του Sysmon.



Σχήμα 37 Αρχείο ρυθμίσεων του Sysmon

Το αρχείο ρυθμίσεών είναι το config.xml και στο αρχείο αυτό περιέχεται η έκδοση σχήματος που είναι αρκετά σημαντική ανάλογα με την έκδοση του Sysmon που τρέχει. Θα γίνει ενημέρωση της διαμόρφωσης με διαφορετικούς αλγόριθμους κατακερματισμού. Έτσι, σε αυτή την περίπτωση, πρόκειται όχι μόνο να συνδεθεί με το MD5, αλλά και με το SHA256, και θα συμπεριληφθούν εδώ όλα τα γεγονότα του δικτύου. Αυτό σημαίνει ότι γίνεται καταγραφή των πάντων, σε αυτό, αν δημιουργηθεί ένα απομακρυσμένο νήμα. Επίσης, η ακαθάριστη πρόσβαση διαβάζεται και αποκλείονται διαφορετικοί τύποι συμβάντων. Εδώ περιλαμβάνονται, για τη δημιουργία ενός απομακρυσμένου νήματος, διαφορετικοί τύποι γεγονότων. Ας γίνει ενημέρωση της διαμόρφωσης του συστήματος. Θα δοθεί η εντολή το Sysmon -c config.xml, η οποία είναι πολύ εύκολη και με βάση αυτή μπορούμε να ενημερώσουμε τη διαμόρφωση.



Σχήμα 38 Ενημέρωση του Sysmon με την εντολή Sysmon -c config .xml

Από τώρα και στο εξής, όταν πραγματοποιείται επαλήθευση στο αρχείο καταγραφής συμβάντων, θα πρέπει να μπορεί κάποιος να συνδεθεί με διαφορετικούς τύπους κατακερματισμού. Όχι μόνο MD5, αλλά και SHA256.

Σχήμα 39 Επαλήθευση αρχείου καταγραφής με 2 τρόπους κατακερματισμού

Αυτή είναι η διάταξη. Όπως φαίνεται, έχουμε μια διαφορά εδώ. Όταν εξεταστεί στο παλιό γεγονός, το μόνο πράγμα που υπάρχει είναι το MD5, αλλά όταν εξεταστεί το νέο γεγονός, υπάρχει και το SHA256. Αυτός είναι ο τρόπος με τον οποίο μπορεί κανείς να δει ότι η διαμόρφωση είναι ενημερωμένη.

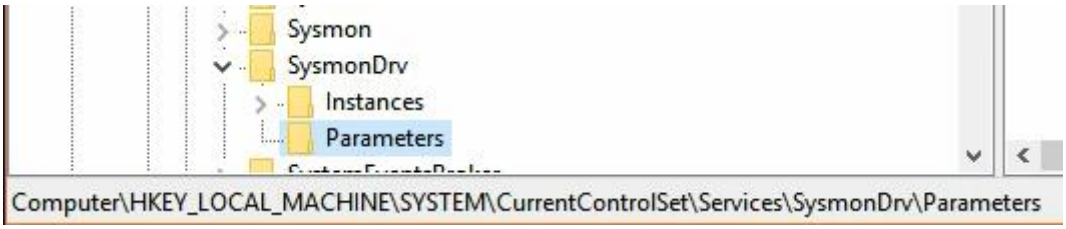
Ας κάνουμε κάτι προχωρημένο.

Ένα από τα πράγματα που πρόκειται να γίνουν είναι να γίνει εξαγωγή της διαμόρφωσης του συστήματος για να το αναπτύξουμε. Γιατί πρέπει να το κάνουμε αυτό; Μπορεί να χάθηκε ένα αρχείο ρυθμίσεων ή να υπάρχει ενημερωμένη διαμόρφωση με πολλούς διαφορετικούς τρόπους στην αρέσκεια του κάθε χρήστη. Δυστυχώς, το Sysmon, προς το παρόν, δεν παρέχει την επιλογή εξαγωγής του αρχείου ρυθμίσεων. Το μόνο που μπορεί να γίνει είναι η εντολή Sysmon - C και αυτό μας απεικονίζει τη διαμόρφωση που έχει γίνει με έναν ωραίο τρόπο. Δεν υπάρχει η δυνατότητα εξαγωγής αυτού του αρχείου σε ένα αρχείο κειμένου και ούτε μπορεί να εισαχθεί αλλού.

```
Administrator: Command Prompt

System Monitor v4.12 - System activity monitor
Copyright (C) 2014-2016 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Current configuration:
 - Service name:                 Sysmon
 - Driver name:                  SysmonDrv
 - HashingAlgorithms:            MD5,SHA256
 - Network connection:           enabled
 - Image loading:                disabled
 - CRL checking:                 disabled
 - Process Access:               disabled

Rule configuration (version 3.10):
 - NetworkConnect                    onmatch: exclude
 - CreateRemoteThread                onmatch: include
       TargetImage                    filter: image        value: 'explorer.exe'
       TargetImage                    filter: image        value: 'lsass.exe'
       TargetImage                    filter: image        value: 'services.exe'
       TargetImage                    filter: image        value: 'svchost.exe'
       TargetImage                    filter: image        value: 'winlogon.exe'
 - RawAccessRead                     onmatch: exclude
       Image                          filter: image        value: 'C:\Windows\Sysmon.exe'
       Image                          filter: image        value: 'System'
```

Σχήμα 40 Προβολή διαμόρφωσης του Sysmon

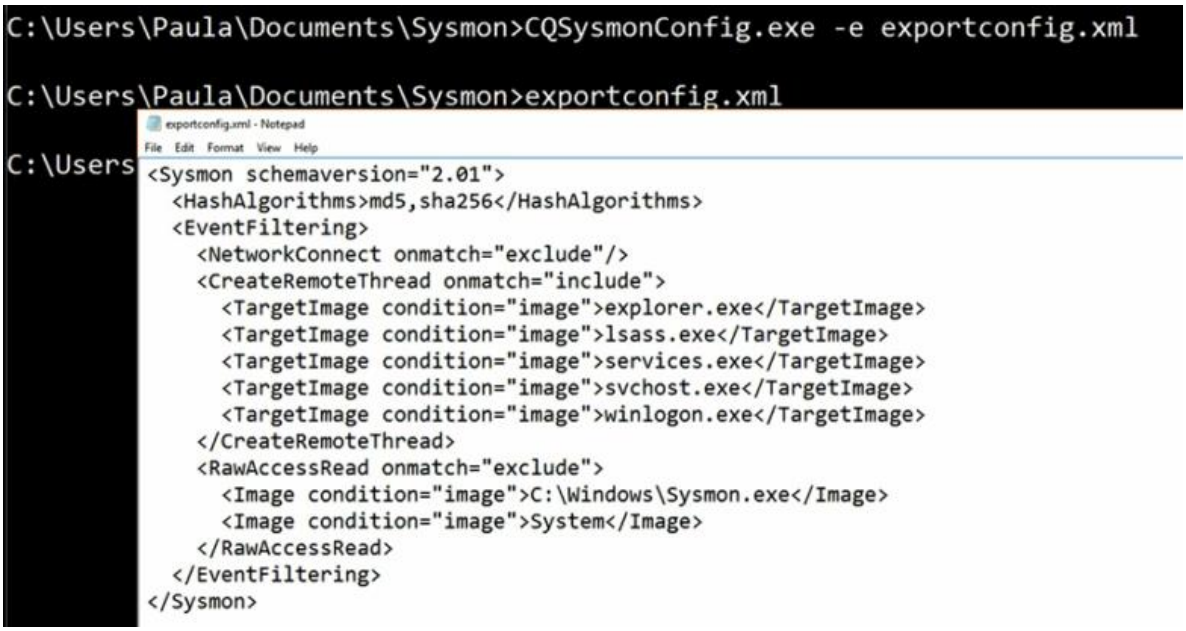
Μπορεί όμως να πάει κανείς στο μητρώο, regedit, και να βρει το Sysmon. Έχοντας αυτές τις ρυθμίσεις στο Σύστημα, Τρέχον Σύστημα Ελέγχου, μπορεί κάποιος να πάει στις Υπηρεσίες και μπορεί να εντοπίσει εδώ δύο πράγματα: το ένα είναι το Sysmon και ένα άλλο είναι το Sysmon driver.



Σχήμα 41 Εντοπισμός του Sysmon driver μέσω του αρχείου καταγραφής μητρώου

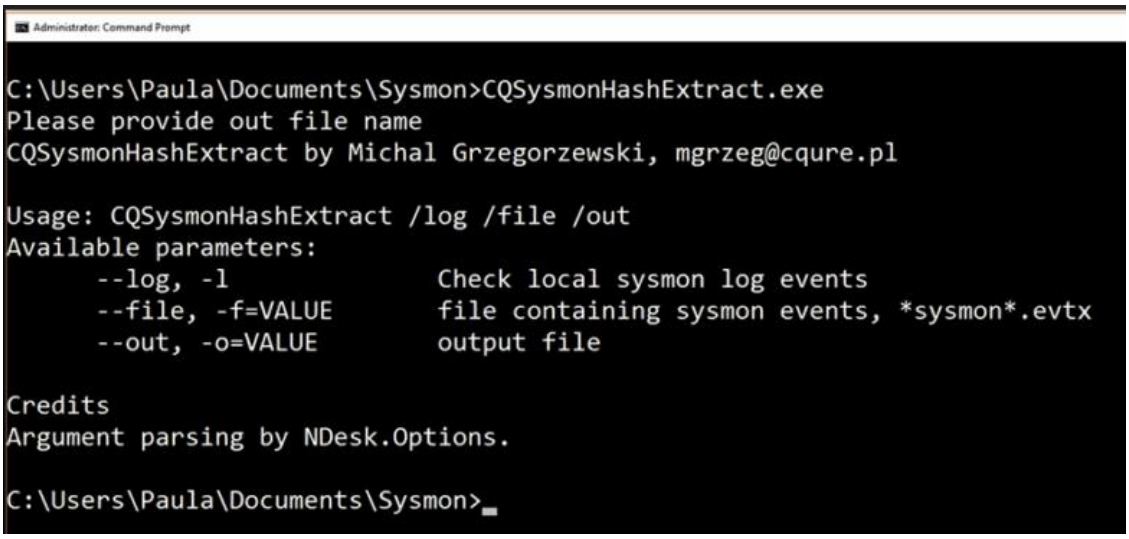
Εκεί μπορεί κανείς να εντοπίσει τη διαμόρφωση στην ομάδα παραμέτρων και να βρει τον αλγόριθμο κατακερματισμού, τις επιλογές και τους κανόνες. Μπορεί να γίνει εξαγωγή των ρυθμίσεων του μητρώου, αυτή όμως είναι μια άλλη επιλογή. Για αυτό υπάρχει ένα εργαλείο που ονομάζεται CQSysmonConfig.

Το CQSysmonconfig επιτρέπει την εξαγωγή της διαμόρφωσης σε ένα αρχείο. Αυτό γίνεται με την επιλογή -E config.xml. Αυτό το εξαγόμενο αρχείο config.xml είναι το αρχείο που μπορεί να χρησιμοποιηθεί για να παραμετροποιήσουμε τη διαμόρφωση. Αυτή είναι η διαμόρφωση μετά την εξαγωγή.



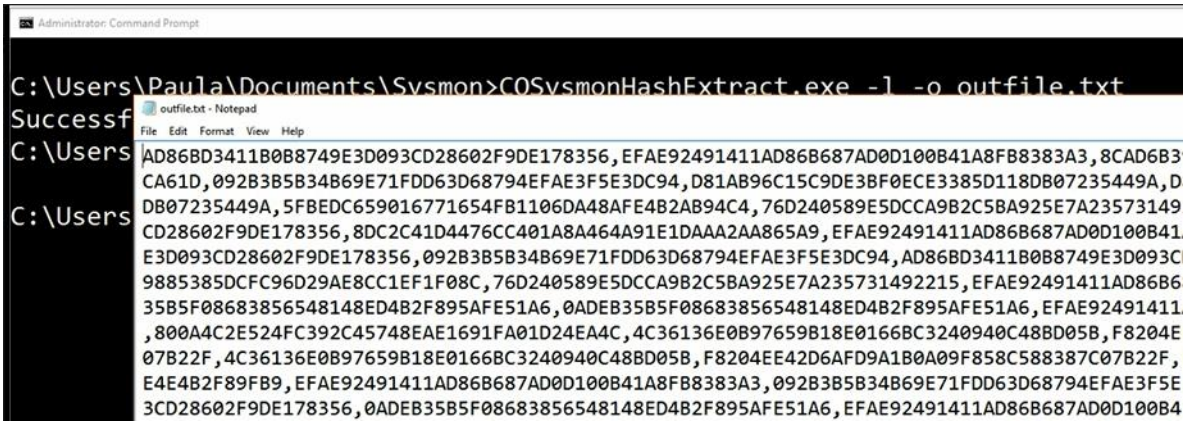
Σχήμα 42 Χρήση του CQSysmonConfig.exe

Αυτό που είναι ενδιαφέρον όταν θα παραμετροποιήσουμε τους διαφορετικούς τύπους αρχείων καταγραφής Sysmon είναι ότι είμαστε σε θέση να εξάγουμε τα hashes. Το CQSysmonHash το οποίο είναι ένα εργαλείο που μας επιτρέπει να καθορίσουμε το τρέχον αρχείο καταγραφής που έχουμε και επίσης μπορούμε να καθορίσουμε το αρχείο εξόδου όπου θα έχουμε τη λίστα των hashes μέσα στο αρχείο.



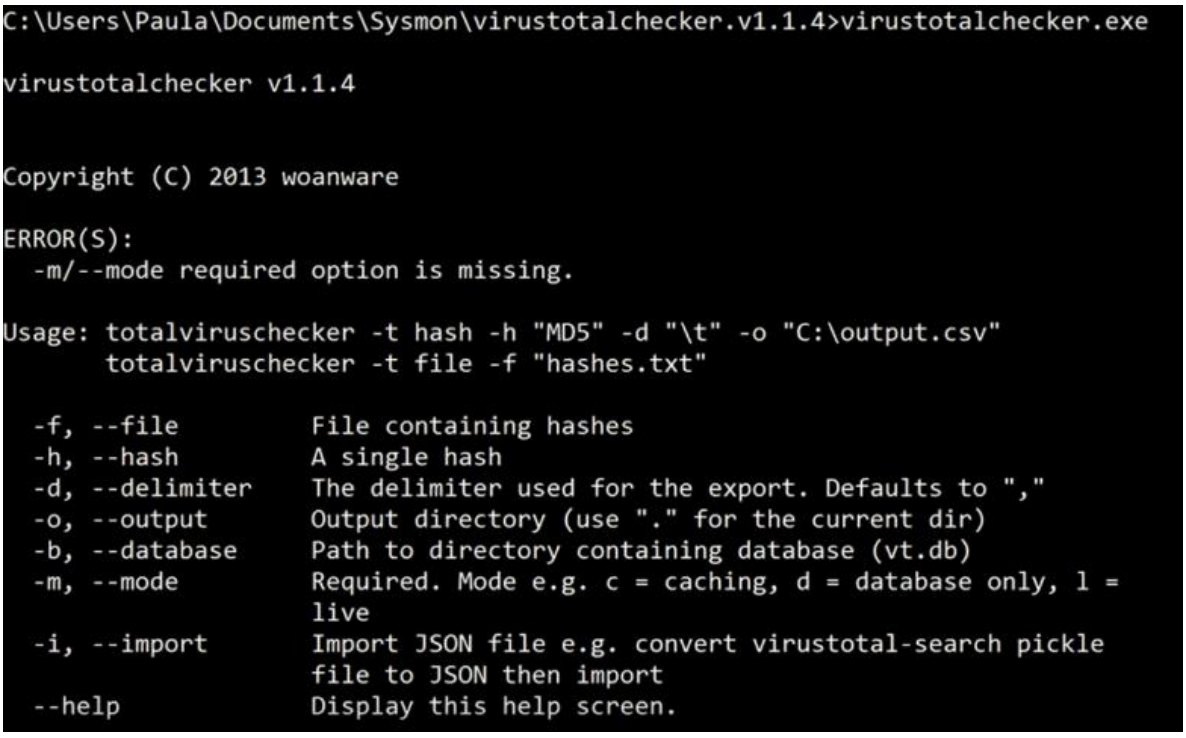
Σχήμα 43 Χρήση του CQSysmonHashExtract.exe

Στην περίπτωσή μας, πρόκειται να γίνει η εξαγωγή CQ Sysmon hash, με την επιλογή -L, και μπορεί να επιλεχθεί και το -O για την έξοδο. Μπορεί να καθοριστεί το συγκεκριμένο αρχείο που θα είναι outfile.txt. Προς το παρόν, όπως ανέφερα, θα χρειαστεί λίγος χρόνος, επειδή το αρχείο είναι μεγάλο. Στο outfile.txt μας, θα έχουμε μια λίστα με τα εξαγόμενα hashes. Αυτό το εξαγόμενο αρχείο μπορεί να ανέβει στο Virustotal για ανάλυση.



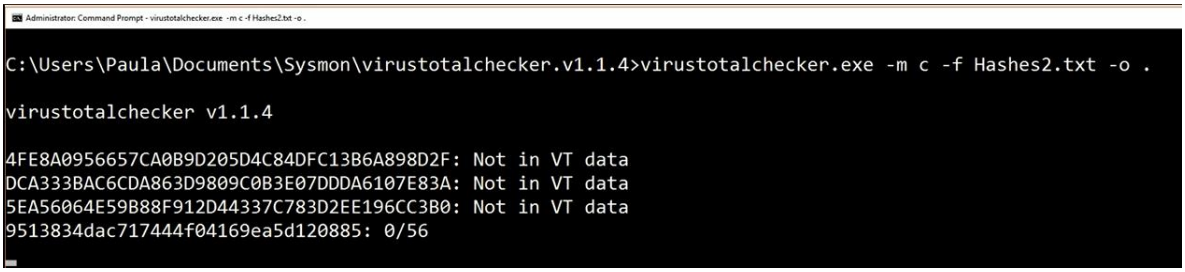
Σχήμα 44 Προβολή των hashes

Αυτά είναι τα hashes. Για παράδειγμα, αυτό που μπορεί να γίνει εδώ είναι η χρήση του ελεγκτή Virustotal. Το Virustotal checker επιτρέπει την υποβολή διαφορετικών τύπων hashes σε Virustotal.



Σχήμα 45 Χρήση του εκλεκτή virustotalchecker.exe

Ας δούμε πρώτα τις επιλογές. Από εδώ, μπορεί να καθοριστεί το αρχείο που περιέχει τα hashes προς χρήση. Θα οριστεί επίσης η έξοδος. Θα καθοριστεί επίσης η λειτουργία και θα γίνει επιλογή της προσωρινής αποθήκευσης του τρόπου λειτουργίας. Θα ανεβάσουμε τα hashes της λίστας στο Virustotal.

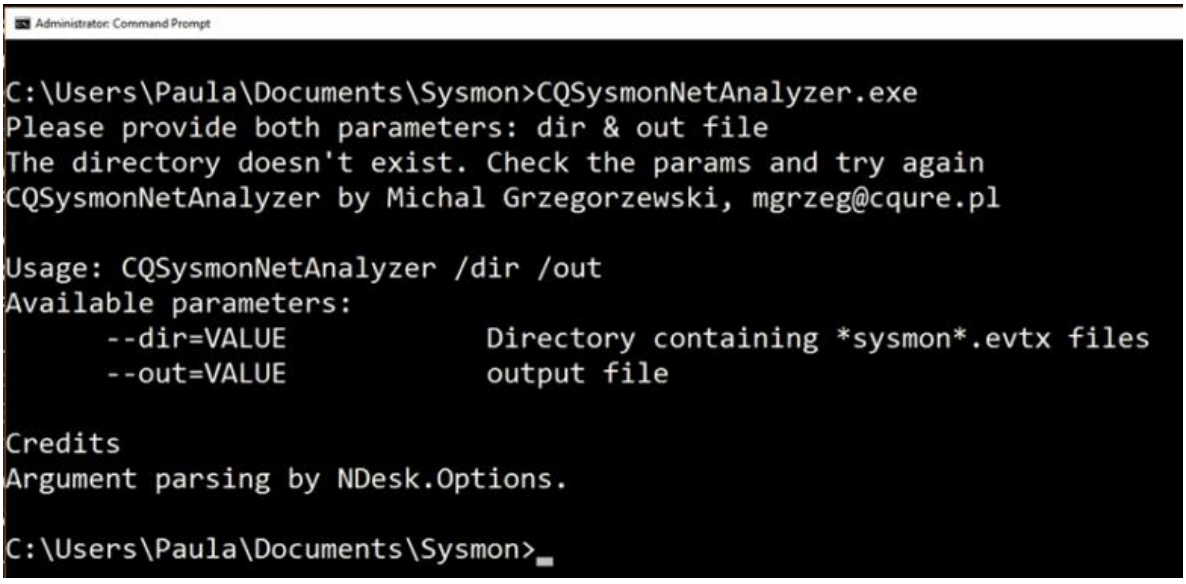


Σχήμα 46 Ανέβασμα του αρχείου των hashes στο virustotal

Έχουμε το Virustotal checker και θα καθοριστεί εδώ η επιλογή -m caching και -file hashes2.txt. Θα οριστεί η έξοδος και θα είμαστε έτοιμοι. Χρειάζεται λίγος χρόνος. Για να επιτευχθεί αυτό, θα πρέπει να μας αποσταλεί ένα κλειδί. Είναι το ιδιωτικό κλειδί από το Virustotal που επιτρέπει την υποβολή αυτών των δεδομένων. Θα χρειαστεί διαμόρφωση του ιδιωτικού κλειδιού στον ίδιο γονικό φάκελο όπου υπάρχει το Virustotalchecker.exe. Αυτό το κλειδί είναι δωρεάν, αλλά έχει τον περιορισμό φορτώσεις μόνο τεσσάρων στοιχείων ταυτόχρονα. Όταν αποκτά κανείς την πληρωμένη έκδοση, μπορεί να φορτώσει περισσότερα στοιχεία ταυτόχρονα.

Ορισμένα από αυτά τα hashes στον κατάλογο θα εντοπιστούν από το Virustotal ως κακόβουλο λογισμικό, οπότε πρόκειται να αφήσουμε αυτό το αποτέλεσμα προς το παρόν και μετά από λίγο, θα επιστρέψουμε σε αυτό και στη συνέχεια θα δούμε αν ανακάλυψε κάτι ή όχι.

Χρησιμοποιώντας αυτήν την ευκαιρία, ας δούμε ένα άλλο demo που θα σχετίζεται με την εξαγωγή πληροφοριών από τα αρχεία καταγραφής συμβάντων για διαφορετικούς τύπους διευθύνσεων IP με τους οποίους συνδεόμαστε. Διαφορετικές διαδικασίες που τρέχει ο χρήστης στα Windows συνδέονται μέσα στο δίκτυο και θα μάθουμε ακριβώς ποιες είναι αυτές οι IPs και με ποιες διευθύνσεις IPs συνδέονται. Για να γίνει αυτό, πρέπει φυσικά να αποκτήσουμε πρόσβαση στο αρχείο καταγραφής συμβάντων.Προς το παρόν, αυτό που θα παραμετροποιήσουμε θα το κάνουμε με ένα εργαλείο που ονομάζεται CQSysmonNetAnalyzer. Το CQSysmonNetAnalyzer είναι αυτό που μας επιτρέπει να αναλύουμε το αρχείο καταγραφής.



Σχήμα 47 Χρήση του CQSysmonNetAnalyzer

Υπάρχει μια τοποθεσία όπου υπάρχουν τα αρχεία του Sysmon και μία τοποθεσία που υπάρχουν τα αρχεία εξόδου. Στην περίπτωσή μας, πρόκειται να είναι στο C \ Windows \ System32 \ Winevt \ Logs. Θα το ονομάσουμε Sysmonnet.txt. Ας το εξάγουμε. Η εξαγωγή θα χρειαστεί λίγο

χρόνο, διότι αναλύει το ημερολόγιο και εξάγει τις διευθύνσεις IP ή τις πλήρεις πληροφορίες από το ημερολόγιο, αλλά εστιάζοντας στις IP διευθύνσεις με τις οποίες επικοινωνεί μέχρι τώρα. Το εξαγόμενο αρχείο θα εισαχθεί σε Excel. Προς το παρόν, το ημερολόγιο μοιάζει με αυτό. Υπάρχει το αρχείο καταγραφής και τώρα είναι εύκολο γίνει η εισαγωγή του.

	A	B	C	D	E	F	G	H	I	
1	MachineName	UtcTime	ProcessId	Image	User	Protocol	Initiated	SourceIsIpv6	SourceIp	Sour
2	____	10/10/2016 4:56	968	C:\Windows\System32\svchost.exe	NT AUTHORITY\SYSTEM	tcp	TRUE	FALSE	192.168.1.178	____
3	____	10/10/2016 4:56	6240	C:\Program Files\WindowsApps\Microsoft.Messaging_2.15.20002.0_x86__8wekyb3d8bbwe\	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____
4	____	10/10/2016 4:56	15948	C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____
5	____	10/10/2016 4:56	15948	C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____
6	____	10/10/2016 4:55	21712	C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____
7	____	10/10/2016 4:55	21712	C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____
8	____	10/10/2016 4:55	2892	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____
9	____	10/10/2016 4:55	2892	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____
10	____	10/10/2016 4:55	2596	C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeClickToRun.exe	NT AUTHORITY\SYSTEM	tcp	TRUE	FALSE	192.168.1.178	____
11	____	10/10/2016 4:55	2596	C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeClickToRun.exe	NT AUTHORITY\SYSTEM	tcp	TRUE	FALSE	192.168.1.178	____
12	____	10/10/2016 4:55	18756	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____
13	____	10/10/2016 4:55	18756	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____
14	____	10/10/2016 4:55	4	System	NT AUTHORITY\SYSTEM	udp	FALSE	FALSE	192.168.1.255	
15	____	10/10/2016 4:55	4	System	NT AUTHORITY\SYSTEM	udp	FALSE	FALSE	192.168.1.255	
16	____	10/10/2016 4:54	4	System	NT AUTHORITY\SYSTEM	tcp	FALSE	FALSE	192.168.1.178	____
17	____	10/10/2016 4:54	4	System	NT AUTHORITY\SYSTEM	tcp	FALSE	FALSE	192.168.1.178	____
18	____	10/10/2016 4:54	22480	C:\Windows\SysWOW64\dllhost.exe	____\Paula	tcp	TRUE	FALSE	192.168.1.178	____

Σχήμα 48 Προβολή του αρχείου καταγραφής

Έτσι φαίνεται το αρχείο καταγραφής. Εισάγουμε αυτήν τη στιγμή το μεγάλο αρχείο δεδομένων των διαφόρων τύπων συνδέσεων που έχουμε. Σε αυτό το σημείο υπάρχει η δυνατότητα να εξαιρέσουμε διαφορετικά είδη αντικειμένων που δεν χρειάζονται να πάρουν μέρος στην ανάλυση και θα μείνουν μόνο διαφορετικοί τύποι εκτελέσιμων αρχείων που έχουν ενδιαφέρουν στην ανάλυση και στην εξακρίβωση του γιατί επικοινωνούσαν μέσω του δικτύου.

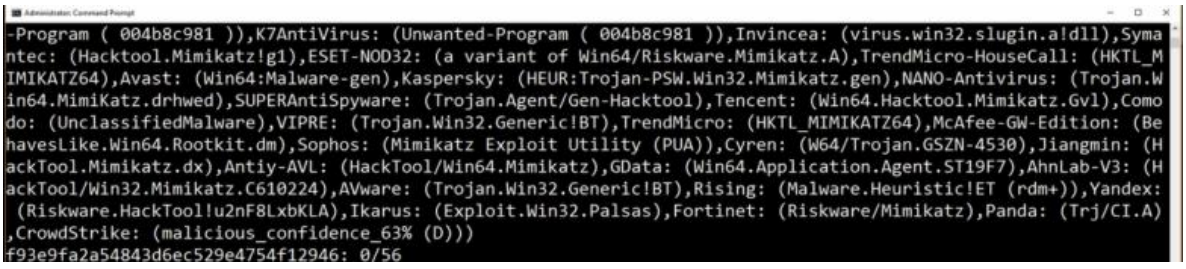
Το νόημα μου είναι ότι υπάρχει μια στήλη. Ονομάζεται IP προορισμού.. Θα γίνει αντιγραφή ολόκληρης της στήλης και θα επικολληθεί στο εργαλείο που ονομάζεται IPNetInfo. Αυτό που θα κάνει το εργαλείο είναι να φιλτράρει όλες τις εσωτερικές διευθύνσεις IP όπως 192.168 και ούτω καθεξής. Θα αφήσει μόνο τα εξωτερικά και θα τα αναλύσει επαληθεύοντας ποιος είναι ο ιδιοκτήτης μιας διεύθυνσης IP και ο τύπος της διεύθυνσης IP.

3	40.113.10.78	Succeed	USA - Washington	MSFT	Microsoft Corporation	40.74.0.0	40.125.127.255
4	23.96.240.104	Succeed	USA - Washington	MSFT	Microsoft Corporation	23.96.0.0	23.103.255.255
5	13.107.3.128	Succeed	USA - Washington	MSFT	Microsoft Corporation	13.64.0.0	13.107.255.255
6	23.97.209.97	Succeed	USA - Washington	MSFT	Microsoft Corporation	23.96.0.0	23.103.255.255
7	40.101.18.34	Succeed	USA - Washington	MSFT	Microsoft Corporation	40.74.0.0	40.125.127.255
8	23.59.97.117	Retrieving Dat...					
9	65.52.210.135	Waiting...					
10	168.63.18.79	Waiting...					
11	204.79.197.200	Waiting...					
12	65.52.26.28	Waiting					

Σχήμα 49 Ανάλυση των καταγεγραμμένων διευθύνσεων IP

Τώρα πραγματοποιείται η επαλήθευση αυτού που συνολικά επικοινωνήθηκε. Επιλέγοντας μία από τις πρώτες διευθύνσεις IP, δείχνει ότι πρόκειται για μια διεύθυνση IP της Microsoft Corporation και φυσικά του ποιος είναι ο ιδιοκτήτης. Μπορεί κάποιος να δει όλες τις πληροφορίες που έχει από το ARIN.net, και το πώς μπορεί να επικοινωνήσει με τον ιδιοκτήτη μιας διεύθυνσης IP κτλ. Υπάρχουν επίσης μερικά άλλα δίκτυα. Επίσης, γίνεται η επαλήθευση του τι και του ποιος είναι ο κάτοχος μιας συγκεκριμένης διεύθυνσης IP. Στο τέλος, υπάρχει μια πλήρη λίστα που η οποία μπορεί να χρησιμοποιηθεί ώστε να μπλοκαριστεί κάτι που δεν επιθυμεί ο χρήστης από το τείχος προστασίας.

Αυτή είναι η ανάλυση. Υπάρχει κάτι το ενδιαφέρον από τη λίστα των hashes που ανακαλύφθηκε;



Σχήμα 50 Προβολή καινούργιων ελέγχων

Απολύτως. Υπάρχουν 75 συνολικοί έλεγχοι. Φαίνεται η διάρκεια και επίσης φαίνονται οι πληροφορίες για το συγκεκριμένο εύρημα. Αυτό που τρέχει είναι το Mimikatz και επί του παρόντος, 33 από 57 διαφορετικούς τύπους παροχών μηχανών προστασίας από ιούς δήλωσαν ότι αυτό είναι πιθανώς κάτι που δεν είναι καλόβουλο. Εδώ έχουμε πληροφορίες για το τι ήταν αυτό.

5.4 Αρχείο παραμετροποίησης του Sysmon

Βασική διαμόρφωση

Υπάρχει η γρήγορη ρύθμιση του Sysmon για την παρακολούθηση επιλεγμένων συμβάντων με επιχειρήματα στη γραμμή εντολών.

- -h [hash, ...] = Καθορίζει τους τύπους κατακερματισμού που πρέπει να καταγραφούν. Χρήση του "*" για καταγραφή όλων ή το -h SHA256 για να ενεργοποιηθεί το SHA256 για παράδειγμα. Οι επιλογές είναι MD5, SHA1, SHA256 και IMPHASH.
- -n [process, ...] = Ενεργοποίηση καταγραφής των συνδέσεων δικτύου (πιθανή επίδραση επιτυχίας). Μπορεί να οριστεί μια ενιαία διαδικασία χρησιμοποιώντας ένα όνομα διαδικασίας όπως -n firefox.exe, cmd.exe, powershell.exe
- -l [process, ...] = Ενεργοποίηση καταγραφής συμβάντων που έχουν φορτωθεί με εικόνα (πιθανή επίδραση επιδόσεων). Μπορεί να οριστεί μια ενιαία διαδικασία χρησιμοποιώντας ένα όνομα διαδικασίας όπως το -l iexplore.exe, calc.exe
  Σημείωση: Εάν γίνει χρήση εντολών γραμμής εντολών για την ενεργοποίηση και την απενεργοποίηση του Sysmon, οι επιλογές αυτές δεν είναι πρόσθετες, οπότε πρέπει να καθοριστούν όλες οι επιθυμητές επιλογές ταυτόχρονα. sysmon.exe -c -n firefox.exe -h SHA1 για παράδειγμα. Η εντολή sysmon -c – θα επαναφέρει την προεπιλογή.

Προηγμένη διαμόρφωση

Οι προηγμένοι κανόνες για το Sysmon δημιουργούνται σε μορφή XML που είναι εύκολο να διαβαστεί και ιδιαίτερα είναι ο προτεινόμενος τρόπος για διαμόρφωση του Sysmon. Ένας κενός σκελετός για ένα αρχείο XML sysmon θα είναι ο ακόλουθος:

```
<Sysmon schemaversion="3.20">
  <!-- Capture all hash types -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
  ...conditions go here...
  </EventFiltering>
</Sysmon>
```

Οι συνθήκες που καθορίζουν τον έλεγχο για το τι θα εγγραφεί και τι δεν θα εγγραφεί. Ορίζονται ρητά οι λίστες των "ετικετών φίλτρων" που έχουν ενδιαφέρον χρησιμοποιώντας τις οδηγίες "include" και "exclude" και με βάση αυτές, όλα τα υπόλοιπα θα αντιστοιχούν ή όχι στον κατάλογο. Ουσιαστικά γίνεται ένα είδος whitelist / blacklist των συνθηκών που θα καταγραφούν. Για παράδειγμα, εάν επιθυμούμε καταγραφή μόνο προγραμμάτων οδήγησης που δεν έχουν υπογραφεί από τα "Microsoft Windows" ή περιέχουν τη λέξη "synaptics", μπορεί να γίνει χρήση της ετικέτας φίλτρου DriverLoad με μια συνθήκη υπογραφής όπως φαίνεται παρακάτω .

```
<DriverLoad onmatch="exclude">
  <Signature condition="is">Microsoft Windows</Signature>
  <Signature condition="contains">synaptics</Signature>
</DriverLoad>
```

Ένας παρόμοιος κανόνας που θα περιλαμβάνει την καταγραφή της κίνησης στη θύρα 80, IP 1.2.3.4, ή σε θύρες Kerberos μόνο θα μοιάζει έτσι :

```
<NetworkConnect onmatch="include">
   <DestinationPort condition="is">80</DestinationPort>
   <DestinationIp condition="is">1.2.3.4</DestinationIp>
   <DestionationPortName condition="is">kerberos</DestionationPortName>
</NetworkConnect>
```

Οι διαθέσιμες συνθήκες για τις καταχωρήσεις πεδίου είναι οι εξής:

is – Από προεπιλογή, οι τιμές είναι ίσες.

is not- Οι τιμές είναι διαφορετικές.

contains - Το πεδίο περιέχει αυτήν την τιμή.

excludes - Το πεδίο δεν περιέχει αυτήν την τιμή.

begin with - Το πεδίο αρχίζει με αυτήν την τιμή.

end with- Το πεδίο τελειώνει με αυτήν την τιμή.

less than- Η λεξικογραφική σύγκριση είναι μικρότερη από μηδέν.

more than- Η λεξικογραφική σύγκριση είναι περισσότερο από το μηδέν.

image - Ταιριάζει μια διαδρομή εικόνας (πλήρης διαδρομή ή μόνο όνομα εικόνας). Για παράδειγμα: Το lsass.exe θα ταιριάζει με το c: \ windows \ system32 \ lsass.exe.

Ένα παράδειγμα βασικής διαμόρφωσης για το Sysmon παρατίθεται στο παράτημα Α. Προσπαθεί να φιλτράρει ορισμένες από τις θύρες που μπορεί να μην έχουν ενδιαφέρον προβολής στην έξοδο από και ενεργοποιεί την εγγραφή για όλα τα συμβάντα δημιουργίας αρχείων.

Κεφάλαιο 6 Αρχεία καταγραφής των Windows

6.1 Ανάλυση των αρχείων καταγραφής

Το αρχείο καταγραφής συμβάντων των Windows είναι μια λεπτομερής καταγραφή των ειδοποιήσεων συστήματος, ασφάλειας και εφαρμογών που έχουν αποθηκευτεί από το λειτουργικό σύστημα των Windows που χρησιμοποιείται από τους διαχειριστές για τη διάγνωση προβλημάτων του συστήματος και την πρόβλεψη μελλοντικών ζητημάτων.

Οι εφαρμογές και το λειτουργικό σύστημα (OS) χρησιμοποιούν αυτά τα αρχεία καταγραφής συμβάντων για την καταγραφή σημαντικών ενεργειών υλικού και λογισμικού που μπορεί να χρησιμοποιήσει ο διαχειριστής για την αντιμετώπιση προβλημάτων με το λειτουργικό σύστημα. Το λειτουργικό σύστημα Windows παρακολουθεί συγκεκριμένα συμβάντα στα αρχεία καταγραφής του, όπως είναι οι εφαρμογές εγκατάστασης, η διαχείριση ασφάλειας, οι λειτουργίες ρύθμισης συστήματος κατά την αρχική εκκίνηση και τα προβλήματα ή τα σφάλματα.

Τα στοιχεία ενός αρχείου καταγραφής συμβάντων των Windows

- Κάθε συμβάν σε καταχώρηση αρχείου καταγραφής περιέχει τις ακόλουθες πληροφορίες: Ημερομηνία: Η ημερομηνία εμφάνισης του συμβάντος.
- Ώρα: Ο χρόνος που συνέβη το συμβάν.
- Χρήστης: Το όνομα χρήστη που καταγράφηκε στο μηχάνημα όταν συνέβη το συμβάν.
- Υπολογιστής: Το όνομα του υπολογιστή.
- Αναγνωριστικό συμβάντος: Αριθμός αναγνώρισης των Windows που καθορίζει τον τύπο συμβάντος.
- Πηγή: Το πρόγραμμα ή το στοιχείο που προκάλεσε το συμβάν.
- Τύπος: Ο τύπος συμβάντος, συμπεριλαμβανομένων πληροφοριών, προειδοποίησης, σφάλματος, ελέγχου επιτυχίας ασφαλείας ή ελέγχου αποτυχίας ασφαλείας.

Το λειτουργικό σύστημα Windows καταγράφει συμβάντα σε πέντε τομείς:

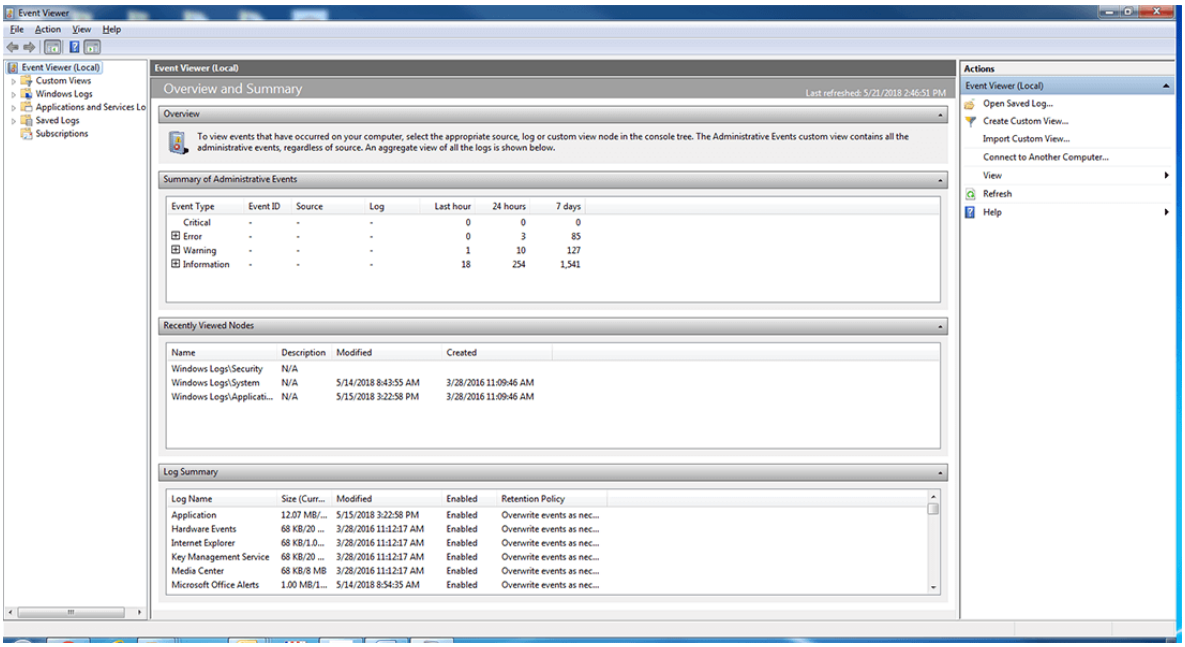
1. Εφαρμογή
2. Ασφάλεια
3. Ρύθμιση
4. Σύστημα
5. Προωθούμενα συμβάντα.

Τα Windows αποθηκεύουν τα αρχεία καταγραφής συμβάντων στο φάκελο C: \ WINDOWS \ system32 \ config \.

1. Τα συμβάντα εφαρμογής αφορούν σε συμβάντα με το λογισμικό που είναι εγκατεστημένο στον τοπικό υπολογιστή. Εάν μια εφαρμογή όπως το Microsoft Word διακοπεί, τότε το αρχείο καταγραφής συμβάντων των Windows θα δημιουργήσει μια καταχώρηση ημερολογίου σχετικά με το ζήτημα, το όνομα της εφαρμογής και γιατί διακόπηκε.
2. Τα συμβάντα ασφαλείας αποθηκεύουν πληροφορίες βάσει των πολιτικών ελέγχου του συστήματος των Windows και τα τυπικά αποθηκευμένα συμβάντα περιλαμβάνουν τις προσπάθειες σύνδεσης και την πρόσβαση σε πόρους. Για παράδειγμα, το αρχείο καταγραφής ασφαλείας αποθηκεύει μια εγγραφή όταν ο υπολογιστής επιχειρεί να επαληθεύσει τα διαπιστευτήρια λογαριασμού όταν ένας χρήστης προσπαθεί να συνδεθεί σε ένα μηχάνημα.
3. Τα συμβάντα ρύθμισης περιλαμβάνουν συμβάντα σχετικά με τον έλεγχο τομέων, όπως η θέση των αρχείων καταγραφής μετά από μια διαμόρφωση δίσκου.
4. Τα συμβάντα του συστήματος σχετίζονται με συμβάντα σε συγκεκριμένα συστήματα των Windows, όπως η κατάσταση των προγραμμάτων οδήγησης συσκευών.
5. Τα προωθούμενα συμβάντα φτάνουν από άλλα μηχανήματα στο ίδιο δίκτυο όταν ένας διαχειριστής θέλει να χρησιμοποιήσει έναν υπολογιστή που συγκεντρώνει πολλαπλά αρχεία καταγραφής.

6.2 Η χρήση του εργαλείου καταγραφής συμβάντων

Η Microsoft περιλαμβάνει το πρόγραμμα προβολής συμβάντων στο λειτουργικό σύστημα Windows Server και πελάτη για την προβολή αρχείων καταγραφής συμβάντων των Windows. Οι χρήστες έχουν πρόσβαση στο Πρόγραμμα προβολής συμβάντων κάνοντας κλικ στο κουμπί Έναρξη και εισάγοντας το Πρόγραμμα προβολής συμβάντων στο πεδίο αναζήτησης. Οι χρήστες μπορούν στη συνέχεια να επιλέξουν και να επιθεωρήσουν το επιθυμητό ημερολόγιο.



Σχήμα 51 Προβολή του ημερολογίου

Τα Windows κατηγοριοποιούν κάθε συμβάν με ένα επίπεδο σοβαρότητας.

Τα επίπεδα κατά σειρά σοβαρότητας είναι :

- Πληροφορίας

Τα περισσότερα αρχεία καταγραφής αποτελούνται από γεγονότα που βασίζονται σε πληροφορίες. Τα αρχεία καταγραφής με αυτήν την καταχώριση σημαίνουν συνήθως ότι στο γεγονός που συνέβη δεν υπήρχε συμβάν ή πρόβλημα. Ένα παράδειγμα συμβάντος πληροφοριών βάσει συστήματος είναι το Event 42, Kernel-Power, το οποίο υποδεικνύει ότι το σύστημα εισέρχεται σε κατάσταση αναστολής λειτουργίας.

- Προειδοποίησης

Τα συμβάντα επιπέδου προειδοποίησης βασίζονται σε συγκεκριμένα συμβάντα, όπως η έλλειψη χώρου αποθήκευσης. Τα προειδοποιητικά μηνύματα μπορούν να επιστήσουν την προσοχή σε πιθανά ζητήματα που ενδέχεται να μην απαιτούν άμεση δράση. Το συμβάν 51, ο δίσκος είναι ένα παράδειγμα μιας προειδοποίησης που βασίζεται στο σύστημα και σχετίζεται με σφάλμα σελιδοποίησης στη μονάδα του μηχανήματος.

- Σφάλματος

Ένα επίπεδο σφάλματος δείχνει ότι μια συσκευή ίσως δεν κατάφερε να φορτώσει ή να λειτουργήσει αναμενόμενα.

Το συμβάν 5719, το NETLOGON είναι ένα παράδειγμα σφάλματος συστήματος όταν ένας υπολογιστής δεν μπορεί να ρυθμίσει μια ασφαλή περίοδο σύνδεσης με έναν ελεγκτή τομέα.

- Κρίσιμο

Τα κρίσιμα συμβάντα επιπέδου υποδεικνύουν τα σοβαρότερα προβλήματα. Το αναγνωριστικό συμβάντος 41, το Kernel-Power είναι ένα παράδειγμα κρίσιμου συμβάντος συστήματος όταν ένα μηχάνημα κάνει επανεκκίνηση χωρίς καθαρό κλείσιμο.

Άλλα εργαλεία για την προβολή αρχείων καταγραφής συμβάντων των Windows

Η Microsoft παρέχει επίσης το wevtutil βοηθητικό πρόγραμμα γραμμής εντολών στο φάκελο System32 που ανακτά τα αρχεία καταγραφής συμβάντων, τα ερωτήματα εκτέλεσης, τα αρχεία καταγραφής των εξαγωγών, τα αρχεία καταγραφής αρχείων και τα διαγραμμένα αρχεία

καταγραφής. Τα βοηθητικά προγράμματα τρίτων που λειτουργούν επίσης με τα αρχεία καταγραφής συμβάντων των Windows περιλαμβάνουν το SolarWinds Log & Event Manager, το οποίο παρέχει συσχέτιση και αποκατάσταση πραγματικού χρόνου, παρακολούθηση ακεραιότητας αρχείων, παρακολούθηση συσκευών USB και την ανίχνευση απειλών.

Το Log & Event Manager συλλέγει αυτόματα αρχεία καταγραφής από διακομιστές, εφαρμογές και συσκευές δικτύου.

Το ManageEngine EventLog Analyzer δημιουργεί προσαρμοσμένες αναφορές από δεδομένα καταγραφής και αποστέλλει ειδοποιήσεις μηνυμάτων κειμένου και μηνύματα ηλεκτρονικού ταχυδρομείου σε πραγματικό χρόνο, βάσει συγκεκριμένων συμβάντων.

6.3 Κατανόηση του εργαλείου καταγραφής συμβάντων

Τα αρχεία καταγραφής συμβάντων είναι τοπικά αρχεία που καταγράφουν όλα τα «συμβάντα» στο σύστημα και περιλαμβάνοντας την πρόσβαση, τη διαγραφή, την προσθήκη ενός αρχείου ή μιας εφαρμογής, την τροποποίηση της ημερομηνίας του συστήματος, τη μείωση του συστήματος, την αλλαγή της διαμόρφωσης του συστήματος κλπ. , Οι καταγραφές κατηγοριοποιούνται στο σύστημα ως κατηγορίες ασφάλειας, εφαρμογής, υπηρεσίας καταλόγου, διακομιστών DNS και κατηγορίες αναπαραγωγής DFS. Οι υπηρεσίες καταλόγου, του διακομιστή DNS και των αρχείων καταγραφής αναπαραγωγής DFS ισχύουν μόνο για την υπηρεσία καταλόγου Active Directory. Τα συμβάντα που σχετίζονται με την ασφάλεια του συστήματος ή των δεδομένων ονομάζονται συμβάντα ασφαλείας και το αρχείο καταγραφής του ονομάζεται αρχείο καταγραφής ασφαλείας. Οι παρακάτω ενότητες παρέχουν περισσότερες λεπτομέρειες σχετικά με τα αρχεία καταγραφής συμβάντων των Windows και ποια εντολή παρακολούθησης:

Κατηγορίες καταγραφών συμβάντων

- Τύποι αρχείου συμβάντων
- Κατανόηση ενός γεγονότος
- Πώς μπορούν τα αρχεία καταγραφής ασφαλείας να αποτρέψουν την χειραγώγηση δεδομένων και την κλοπών αυτών;
- Εκδηλώσεις που απαιτούν έλεγχο και σχέδιο ελέγχου
- Ανάγκη για την παρακολούθηση αρχείων καταγραφής συμβάντων
- Άλλοι χρήσιμοι σύνδεσμοι

Κατηγορίες καταγραφών συμβάντων

Τα αρχεία καταγραφής συμβάντων ταξινομούνται ευρέως σε λίγες προκαθορισμένες κατηγορίες βάσει του κατασκευαστικού στοιχείου. Τα διάφορα στοιχεία για τα οποία καταγράφονται τα συμβάντα περιλαμβάνουν το σύστημα, την ασφάλεια του συστήματος, τις εφαρμογές που φιλοξενούνται στο σύστημα κ.λπ. Ορισμένες εφαρμογές καταγράφουν συμβάντα σε μια προσαρμοσμένη κατηγορία αντί να τα καταγράφουν στην προεπιλεγμένη κατηγορία εφαρμογών.

Τύπος αρχείου συμβάντων	Περιγραφή
Αρχείο καταγραφής εφαρμογών	Οποιοδήποτε συμβάν καταγράφεται από μια εφαρμογή. Αυτά καθορίζονται από τους προγραμματιστές κατά την ανάπτυξη της εφαρμογής. Π.χ.: Ένα σφάλμα κατά την εκκίνηση μιας εφαρμογής καταγράφεται στο αρχείο καταγραφής εφαρμογών.
Μητρώο συστήματος	Οποιοδήποτε συμβάν καταγράφεται από το λειτουργικό σύστημα. Π.χ.: Η αποτυχία εκκίνησης μιας μονάδας κατά την εκκίνηση καταγράφεται στο αρχείο καταγραφής συστήματος

Μητρώο ασφαλείας	Οποιοδήποτε γεγονός που έχει σημασία για την ασφάλεια του συστήματος. Π.χ. έγκυρες και άκυρες αίτησης σύνδεσης και αποσύνδεσης, οποιαδήποτε διαγραφή αρχείου κλπ. Καταγράφονται σε αυτή την κατηγορία.
Μητρώο υπηρεσίας καταλόγου	Καταγράφει γεγονότα των ενεργών αρχείων (Active Directory). Αυτό το αρχείο καταγραφής είναι διαθέσιμο μόνο σε ελεγκτές τομέα.
Μητρώο διακομιστή DNS	Καταγράφει συμβάντα για διακομιστές DNS και αναλύσεις ονομάτων. Αυτό το αρχείο καταγραφής είναι διαθέσιμο μόνο για διακομιστές DNS
Αρχείο καταγραφής υπηρεσιών αντιγραφής αρχείων	Καταγράφει τα συμβάντα της αναπαραγωγής ελεγκτή τομέα. Αυτό το αρχείο καταγραφής είναι διαθέσιμο μόνο σε ελεγκτές τομέα.

Τύποι αρχείου συμβάντων

Κάθε καταχώρηση συμβάντος ταξινομείται κατά τύπο για να προσδιορίσει τη σοβαρότητα του συμβάντος. Πρόκειται για πληροφορίες, προειδοποιήσεις, σφάλματα, ελέγχους επιτυχίας (αρχείο καταγραφής ασφαλείας) και ελέγχους αποτυχίας (αρχείο καταγραφής ασφαλείας).

Τύπος συμβάντων	Περιγραφή
Πληροφορίες	Ένα συμβάν που περιγράφει την επιτυχή λειτουργία μιας εργασίας, όπως μια εφαρμογή, ένας οδηγός ή μία υπηρεσία. Για παράδειγμα, ένα συμβάν πληροφοριών καταγράφεται όταν ένα πρόγραμμα οδήγησης δικτύου φορτώνεται με επιτυχία.
Προειδοποίηση	Ένα συμβάν που περιγράφει την επιτυχή λειτουργία μιας εργασίας, όπως μια εφαρμογή, ένας οδηγός ή μία υπηρεσία. Για παράδειγμα, ένα συμβάν πληροφοριών καταγράφεται όταν ένα πρόγραμμα οδήγησης δικτύου φορτώνεται με επιτυχία.
Λάθος	Ένα γεγονός που δεν είναι απαραίτητα σημαντικό, ωστόσο, μπορεί να υποδεικνύει την πιθανή εμφάνιση ενός μελλοντικού προβλήματος. Για παράδειγμα, ένα μήνυμα προειδοποίησης καταγράφεται όταν ο χώρος στο δίσκο αρχίζει να είναι χαμηλός.
Έλεγχος επιτυχίας (αρχείο καταγραφής ασφαλείας)	Ένα συμβάν που περιγράφει την επιτυχή ολοκλήρωση ενός ελεγχόμενου συμβάντος ασφαλείας. Για παράδειγμα, ένα συμβάν ελέγχου επιτυχίας καταγράφεται όταν ένας χρήστης συνδέεται σε έναν υπολογιστή.
Έλεγχος αποτυχίας (αρχείο καταγραφής ασφαλείας)	Ένα συμβάν που περιγράφει ένα ελεγχόμενο συμβάν ασφαλείας το οποίο δεν ολοκληρώθηκε με επιτυχία. Για παράδειγμα, ένας έλεγχος αποτυχίας μπορεί να καταγραφεί όταν ένας χρήστης δεν μπορεί να αποκτήσει πρόσβαση σε μια μονάδα δίσκου δικτύου.

Το πρόγραμμα προβολής συμβάντων παραθέτει τα αρχεία καταγραφής συμβάντων ως εξής:

Type	Date	Time	Source	Category	Event	User	Computer
Information	1/21/2010	10:34:15 ...	ESENT	General	100	N/A	VIDYAVASU
Error	1/18/2010	10:34:20 ...	crypt32	None	8	N/A	VIDYAVASU
Error	1/18/2010	10:34:20 ...	crypt32	None	8	N/A	VIDYAVASU
Error	1/18/2010	10:34:23 ...	crypt32	None	8	N/A	VIDYAVASU
Error	1/18/2010	10:34:25 ...	crypt32	None	8	N/A	VIDYAVASU
Error	1/18/2010	10:34:28 ...	crypt32	None	8	N/A	VIDYAVASU
Error	1/18/2010	10:34:30 ...	crypt32	None	8	N/A	VIDYAVASU
Information	1/18/2010	10:34:56 ...	EAPOL	None	2002	N/A	VIDYAVASU
Information	1/18/2010	10:34:56 ...	EAPOL	None	2003	N/A	VIDYAVASU
Information	1/18/2010	10:35:59 ...	iPod Service	None	0	N/A	VIDYAVASU
Error	1/18/2010	10:36:24 ...	crypt32	None	8	N/A	VIDYAVASU
Warning	1/15/2010	10:36:30 ...	crypt32	None	6	N/A	VIDYAVASU
Error	1/15/2010	10:36:30 ...	crypt32	None	8	N/A	VIDYAVASU
Information	1/18/2010	10:36:39 ...	DesktopCentral	None	103	N/A	VIDYAVASU
Error	1/18/2010	10:36:39 ...	crypt32	None	8	N/A	VIDYAVASU
Error	1/18/2010	10:37:31 ...	crypt32	None	8	N/A	VIDYAVASU
Information	12/24/2009	10:38:15 ...	ESENT	General	101	N/A	VIDYAVASU

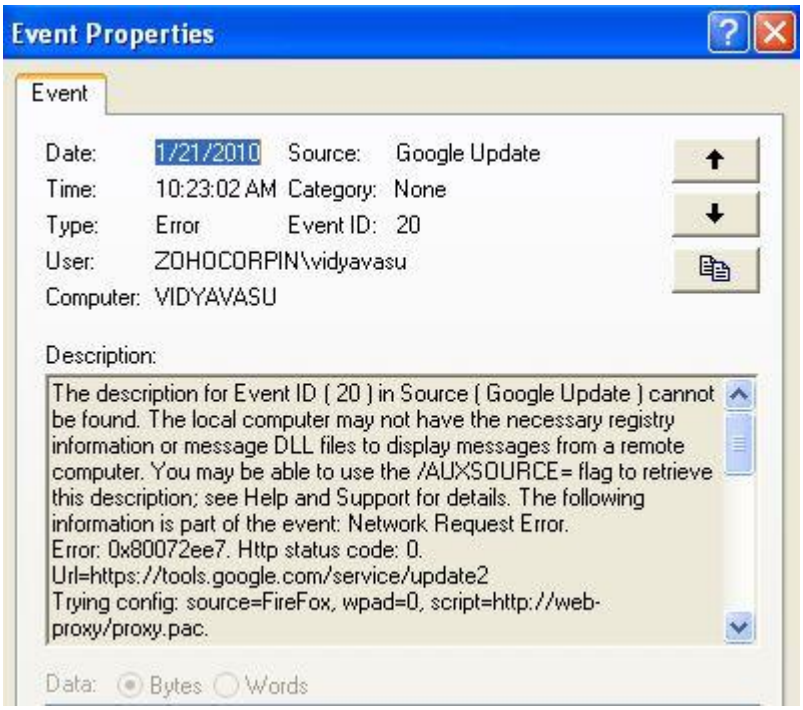
Σχήμα 52 Προβολή των συμβάντων

Κατανόηση ενός γεγονότος

Τα συμβάντα παρατίθενται με πληροφορίες κεφαλίδας και μια περιγραφή στο πρόγραμμα προβολής συμβάντων.

Κεφαλίδα	Περιγραφή
Ημερομηνία	Την ημερομηνία κατά την οποία συνέβη το συμβάν
Ώρα	Η ώρα που συνέβη το συμβάν
Χρήστης	Ο χρήστης που έχει συνδεθεί στον υπολογιστή όταν συνέβη το συμβάν
Υπολογιστής	Ο υπολογιστής στον οποίο συνέβη το συμβάν
Αναγνωριστικό γεγονότος	Αριθμός συμβάντος που προσδιορίζει τον τύπο συμβάντος. Βοηθά να μάθουμε περισσότερα για την εκδήλωση
Πηγή	Η πηγή που δημιούργησε το συμβάν. Θα μπορούσε να είναι μια εφαρμογή ή ένα στοιχείο του συστήματος
Τύπος	Τύπος συμβάντος (Πληροφορίες, προειδοποίηση, σφάλμα, έλεγχος επιτυχίας και έλεγχος αποτυχίας)

Κάνοντας διπλό κλικ σε ένα συμβάν προβάλλονται οι λεπτομέρειες:



Σχήμα 53 Προβολή λεπτομεριών ενός γεγονότος

Πώς μπορούν τα αρχεία καταγραφής ασφαλείας να αποτρέψουν τις κλοπές δεδομένων και κλοπών δεδομένων;

Η ασφάλεια είναι η μεγαλύτερη ανησυχία που αντιμετωπίζει κάθε επιχείρηση σήμερα. Τα περιστατικά όπως οι χειραγωγήσεις και οι κλοπές δεδομένων συνεχώς αυξάνονται, εκθέτοντας όλα τα τμήματα των επιχειρήσεων σε κινδύνους και αφήνοντας τους διαχειριστές άναυδους. Διάφορες βιομηχανικές έρευνες αποκαλύπτουν ότι η πλειοψηφία των προσπαθειών χειραγώγησης και κλοπής λαμβάνουν χώρα λόγω παράνομων προσπαθειών ελέγχου ταυτότητας. Ο έλεγχος των παράνομων ή αποτυχημένων προσπαθειών σύνδεσης θα μπορούσε να αποτρέψει (ή να μειώσει) κλοπές δεδομένων. Είναι σημαντικό να γνωρίζουμε τι μπορεί να προσφέρει ένα λειτουργικό σύστημα μέσω της ασφάλειας και τι πρέπει να κάνουμε για την υλοποίηση λειτουργικών συστημάτων με την απαιτούμενη ασφάλεια. Εκδηλώσεις που απαιτούν έλεγχο και σχέδιο ελέγχου. Τα συμβάντα δεν καταγράφονται από προεπιλογή για πολλές συνθήκες ασφαλείας, πράγμα που σημαίνει ότι οι πόροι εξακολουθούν να εκτίθενται σε χειραγωγήσεις Πρέπει να γίνει ρυθμίσει των πολιτικών ελέγχων για τον έλεγχο των συμβάντων ασφαλείας και να τα καταγραφούν τα κρίσιμα συμβάντα ασφαλείας που χρειάζονται τον έλεγχο:

- Σύνδεση χρήστη / αποσύνδεση
- Σύνδεση υπολογιστή / αποσύνδεση / επανεκκίνηση
- Πρόσβαση σε αντικείμενα, αρχεία και φακέλους
- Τροποποίηση του χρόνου συστήματος
- Εκκαθάριση των αρχείων καταγραφής ελέγχου

Δεν είναι απαραίτητο να ρυθμιστούν όλες τις πολιτικές ελέγχου. Κάτι τέτοιο θα είχε ως αποτέλεσμα την καταγραφή για κάθε ενέργεια που λαμβάνει χώρα και θα αυξήσει το μέγεθος της καταγραφής. Με την σωστή ρύθμιση των αρχείων καταγραφής και ανάλογα με το μέγεθος της ρύθμισης που έχει ρυθμιστεί, τα παλαιότερα αρχεία καταγραφής διαγράφονται. Η διαμόρφωση των σωστών πολιτικών που είναι πραγματικά κρίσιμες για το περιβάλλον θα βελτιώσει την ασφάλεια.

Οι έλεγχοι κρίσιμων συμβάντων είναι ενεργοποιημένοι από προεπιλογή για τους ελεγκτές τομέα. Για τις άλλες συσκευές των Windows, ρύθμιση των πολιτικών ελέγχου που είναι διαθέσιμες στην περιοχή Τοπικές ρυθμίσεις ασφαλείας. Οι διαθέσιμες ελεγκτικές πολιτικές είναι:

- Συμβάντα σύνδεσης λογαριασμού
- Διαχείριση λογαριασμών
- Πρόσβαση σε υπηρεσία καταλόγου
- Συμβάντα σύνδεσης
- Πρόσβαση στο αντικείμενο
- Αλλαγή πολιτικής
- Χρήση προνομίων
- Παρακολούθηση διαδικασιών
- Συμβάντα συστήματος

Ανάγκη για την παρακολούθηση αρχείων καταγραφής συμβάντων.

Η ανάγκη τήρησης των υποχρεώσεων ασφαλείας, όπως SOX, HIPAA κ.λπ. για τις εταιρείες που διαπραγματεύονται στο χρηματιστήριο, την βιομηχανία υγειονομικής περίθαλψης κ.λπ., απαιτεί την εφαρμογή διαδικασίας διαχείρισης ασφάλειας για την προστασία από απόπειρες ή επιτυχών μη εξουσιοδοτημένων προσβάσεων. Η διασφάλιση των πληροφοριών στο δίκτυό είναι κρίσιμη για την επιχείρησή με ή χωρίς τη συμμόρφωση με ορισμένα πρότυπα. Τα αρχεία καταγραφής συμβάντων των Windows είναι μια από τις πηγές με τις οποίες μπορούν να εντοπιστούν και να καταγραφούν οι προσπάθειες σύνδεσης. Ένας χειροκίνητος έλεγχος σε κάθε συσκευή των Windows είναι κουραστικό και αδύνατο και εγγυάται τον αυτοματοποιημένο έλεγχο και την παρακολούθηση των αρχείων καταγραφής συμβάντων σε τακτική βάση.

6.4 Κατανόηση του εργαλείου καταγραφής συμβάντων

Η έρευνα στοχεύει στην παροχή βασικών πληροφοριών που είναι χρήσιμες στην ανίχνευση γεγονότων με τη διερεύνηση στοιχείων των εργαλείων που χρησιμοποιούνται από πολλούς επιτιθέμενους. Πιο συγκεκριμένα, αυτή η αναφορά στοχεύει να είναι ένα λεξικό που μπορεί να χρησιμοποιηθεί ως οδηγός για την αποτελεσματική ανάλυση, προσδιορίζοντας τα εργαλεία που χρησιμοποιήθηκαν βάσει των ημερολογίων ή τι καταγράφεται όταν υλοποιείται ένα συγκεκριμένο εργαλείο. Σε αυτή την έρευνα, ερευνήθηκαν εργαλεία που χρησιμοποιούνται από πολλούς επιτιθέμενους. Τα ειδικά εργαλεία που χρησιμοποιούνται από πολλούς επιτιθέμενους περιγράφονται στην επόμενη ενότητα. Τα ακόλουθα γεγονότα ερευνήθηκαν έτσι ώστε τα άτομα που δεν είναι ειδικοί στην έρευνα περιστατικών να μπορούν να τα αναλύσουν ευκολότερα:

- Μητρώο συμβάντων
- Ιστορικό εκτέλεσης
- Καταχώρηση μητρώου

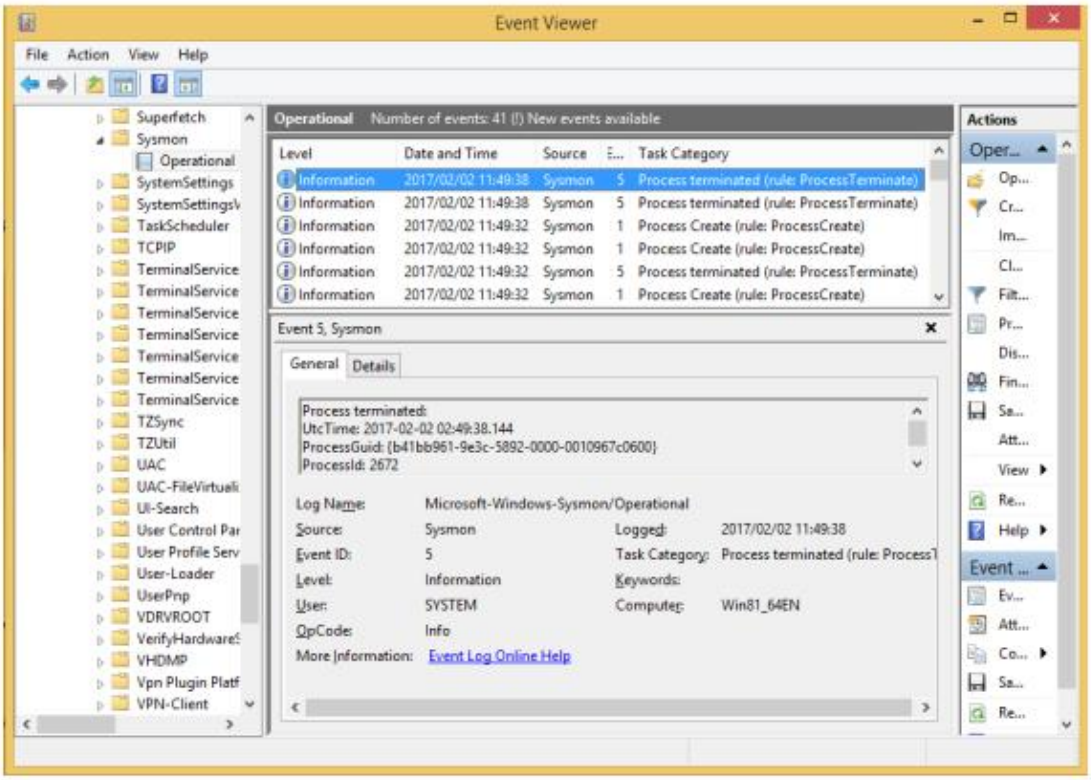
Σημειώστε ότι δεν είναι δυνατή η απόκτηση επαρκούς ποσότητας αρχείων καταγραφής συμβάντων με τις προεπιλεγμένες ρυθμίσεις των Windows. Σε αυτή την έρευνα ερευνήθηκαν, τα αρχεία που καταγράφονται με την προεπιλεγμένη ρύθμιση και την ακόλουθη ρύθμιση:

- Ενεργοποίηση της πολιτικής ελέγχου
- Εγκατάσταση Sysmon

Η πολιτική ελέγχου είναι μια προεπιλεγμένη ρύθμιση των Windows για την απόκτηση λεπτομερών αρχείων καταγραφής σχετικά με τη σύνδεση, την αποτύπωση, την πρόσβαση σε αρχεία κλπ. Η πολιτική ελέγχου μπορεί να επιβεβαιωθεί και οι ρυθμίσεις της να αλλάξουν από την πολιτική τοπικής ομάδας.

Το Sysmon είναι ένα εργαλείο που παρέχεται από τη Microsoft που επιτρέπει την καταγραφή των διαδικασιών εκκίνησης, επικοινωνίας δικτύου, αλλαγών αρχείων κ.λπ. Η εγκατάσταση του Sysmon

ενεργοποιεί την καταγραφή των αρχείων καταγραφής από το Πρόγραμμα προβολής συμβάντων όπως φαίνεται παρακάτω.



Σχήμα 54 Πρόγραμμα προβολής συμβάντων

Σε αυτήν την έρευνα, τα εργαλεία που αναφέρονται παρακάτω εκτελούνται στην πραγματικότητα σε ένα εικονικό δίκτυο αποτελούμενο από δύο συστήματα Windows 10. Ελέγχοντας τις αλλαγές στο σύστημα πριν και μετά την εκτέλεση κάθε εργαλείου, το ιστορικό εκτέλεσης, τα αρχεία καταγραφής συμβάντων και τα αρχεία καταχώρησης μητρώου συλλέχθηκαν και συνοψίστηκαν στο Κεφάλαιο 7. Το περιβάλλον δικτύου που χρησιμοποιήθηκε για την έρευνα αυτή περιγράφεται λεπτομερώς παρακάτω.

Μεταξύ των εργαλείων που παρατηρήθηκαν σε πολλαπλά περιστατικά που χειρίστηκαν, επιλέχθηκαν 10 εργαλεία που σχετίζονται άμεσα με τις επιχειρήσεις επίθεσης ως τυπικά εργαλεία, όπως εκτέλεση εντολών, απόκτηση κωδικού πρόσβασης και απομακρυσμένη σύνδεση. Ο παρακάτω πίνακας δείχνει αυτά τα εργαλεία που ομαδοποιούνται κατά το σκοπό χρησιμοποίησης από τον επιτιθέμενο.

Σκοπός χρήσης του εργαλείου από τον επιτιθέμενο	Εργαλείο
Εργαλεία απομακρυσμένων εντολών:	psexec
	smbexec
	wmiexec
	winrm
	wmic

Εργαλεία απομακρυσμένων εντολών:	WMImplant
Εργαλεία συλλογής πληροφοριών	project lazagne
	mimikatz
Εργαλείο ελέγχου συστήματος	empire

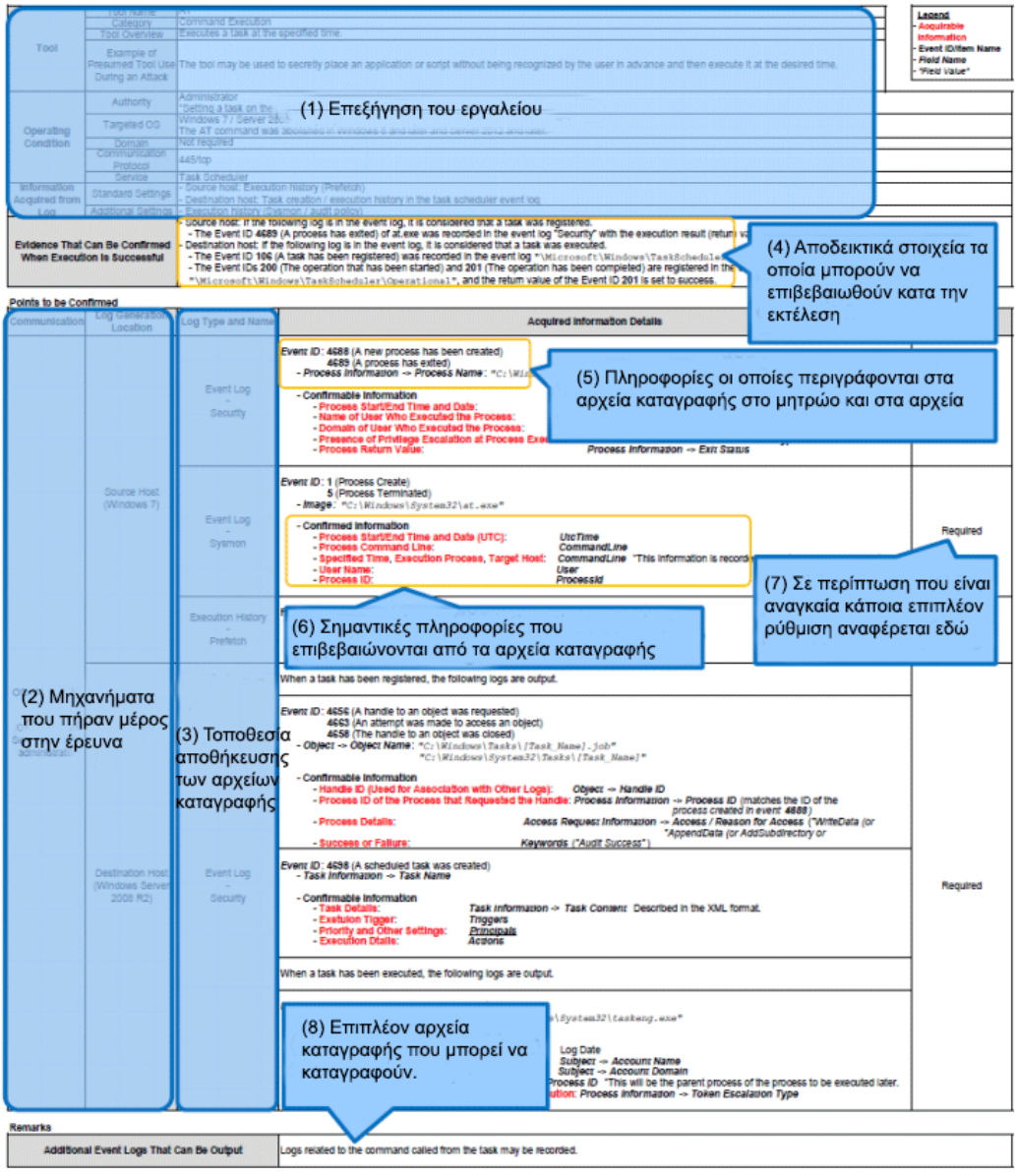
Περιβάλλον έρευνας

Ένα απλοποιημένο σύστημα με ένα ζεύγος πελάτη και διακομιστή, χτίστηκε σε ένα εικονικό δίκτυο ως στόχο. Τα επιλεγμένα εργαλεία εκτελέστηκαν στο περιβάλλον για να παρακολουθούν τις αλλαγές στα αρχεία και τα μητρώα που προκύπτουν από την εκτέλεση. Εγκαθιστώντας την ακόλουθη έκδοση των Windows στον υπολογιστή-πελάτη, ελέγχθηκαν συνολικά τέσσερις τύποι διαμορφώσεων συστημάτων.

- Εγκατεστημένο λειτουργικό σύστημα στον πελάτη
  - Windows 10

Κεφάλαιο 7 Αποτελέσματα έρευνας

Αυτό το κεφάλαιο συνοψίζει τις βασικές πληροφορίες, συμπεριλαμβανομένης της λειτουργικότητας των εργαλείων που δοκιμάστηκαν σε αυτή την έρευνα και των πληροφοριών καταγραφής που καταγράφηκαν κατά την εκτέλεση των σχετικών εργαλείων. Η προοπτική του επιτιθέμενου είχε επίσης ληφθεί υπόψη στην περιγραφή των βασικών πληροφοριών έτσι ώστε η σημασία κάθε εργαλείου σε μια ακολουθία επίθεσης να μπορεί εύκολα να γίνει κατανοητή. Αυτό το κεφάλαιο περιγράφει επίσης τις λεπτομέρειες των ημερολογίων που μπορούν να αποκτηθούν όταν διαμορφωθούν οι ρυθμίσεις που περιγράφονται στο κεφάλαιο 6.



Σχήμα 56 Επεξήγηση πίνακα με τα αποτελέσματα της έρευνας.

Τα παρακάτω περιγράφουν το περιεχόμενο που περιγράφεται για κάθε στοιχείο.

(1) Περιγραφή του εργαλείου

- Οι επιπτώσεις από τη χρήση του εργαλείου, τα προνόμια χρήσης του εργαλείου, το πρωτόκολλο επικοινωνίας, και οι σχετικές υπηρεσίες.

(2) Περιβάλλον δοκιμής

- Πληροφορίες για το λειτουργικό σύστημα του κεντρικού υπολογιστή της πηγής και του κεντρικού υπολογιστή προορισμού.

(3) Χώρος αποθήκευσης αρχείου καταγραφής

- Θέση αποθήκευσης μητρώων και ημερολογίων εκδηλώσεων.

(4) Στοιχεία που μπορούν να επιβεβαιωθούν εάν η εκτέλεση είναι επιτυχής

- Η μέθοδος επιβεβαίωσης της επιτυχούς εκτέλεσης του εργαλείου.

(5) Πληροφορίες που περιγράφονται στα αρχεία καταγραφής συμβάντων, στα μητρώα και στα αρχεία

- Εάν η εγγραφή σε ένα αρχείο καταγραφής συμβάντων, μητρώου ή αρχείου ταιριάζει με την περιγραφή αυτού του στοιχείου, είναι πιθανό ότι το αρχείο έγινε με την εκτέλεση του σχετικού εργαλείου και συνεπώς απαιτείται έρευνα.

(6) Σημαντικές πληροφορίες που μπορούν να επιβεβαιωθούν σε ένα ημερολόγιο

- Σημαντικές πληροφορίες που μπορούν να χρησιμοποιηθούν για τη διερεύνηση αρχείων στα στοχευμένα αρχεία καταγραφής

(Αυτό δεν σημαίνει απαραίτητα ότι όλες οι πληροφορίες που καταγράφονται περιγράφονται.)

(7) Το αν απαιτείται ή όχι πρόσθετη ρύθμιση για την απόκτηση του σχετικού αρχείου καταγραφής

- Αναφέρεται ως "-" όταν το αρχείο καταγραφής μπορεί να δημιουργηθεί στην τυπική ρύθμιση ή ως "Απαιτείται" όταν χρειάζεται πρόσθετη ρύθμιση.

(8) Πρόσθετα αρχεία καταγραφής συμβάντων που μπορεί να εξαχθούν

- Κάθε ημερολόγιο που μπορεί να καταγραφεί επιπρόσθετα.

7.1 Πίνακες αποτελεσμάτων για εργαλεία επαύξησης δικαιωμάτων

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	UAC BYPASS
	Κατηγορία	Επαύξηση Δικαιωμάτων
	Περιγραφή Εργαλείου	Εκτέλεση εφαρμογών με δικαιώματα διαχειριστή που κανονικά ελέγχονται από το UAC (ρυθμίσεις λογαριασμού χρήστη)
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο χρησιμοποιείται για την εκτέλεση εφαρμογών που κανονικά δεν θα έπρεπε να εκτελούνται με την προσποίηση ότι πρόκειται για μία τυπική εφαρμογή.
Κατάσταση λειτουργίας	Εξουσιοδότηση	Χρήστης ο οποίος έχει εξουσιοδότηση να χρησιμοποιεί προνόμια διαχειριστή σύμφωνα με το UAC χωρίς να χρησιμοποιεί τα διαπιστευτήρια του διαχειριστή. (Ένας χρήστης ο οποίος ανήκει στην ομάδα των διαχειριστών)
	Στοχευμένο Λογισμικό	Windows
	Τομέας	Δεν απαιτείται
	Πρωτόκολλο επικοινωνίας	-
	Υπηρεσία	-
Απαιτούμενη Πληροφορία	Ρυθμίσεις	Ιστορικό εκτελέσεων
	Επιπλέον ρυθμίσεις	Ιστορικό εκτελέσεων (Sysmon και πολιτική ελέγχου) • Μία διαδικασία που περιέχει στο όνομα γονικής διεργασίας μία εφαρμογή που κανονικά δεν θα έπρεπε να ξεκινά.

Απαιτούμενη Πληροφορία	Επιπλέον ρυθμίσεις	• Καταγράφονται τόσο η εφαρμογή που χρησιμοποιείται για παράκαμψη όσο και η εφαρμογή που εκτελείται μέσω της παράκαμψης.
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Καταγραφή της εκτέλεσης μιας διαδικασίας στην οποίας στο όνομα γονικής διεργασίας περιλαμβάνει μια εφαρμογή.

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Ασφάλεια	Καταγράφεται όταν πραγματοποιείται εγκατάσταση ενός προγράμματος.	Απαιτείται
			Event ID: 4688 (νέα διεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα που ξεκίνησε/τελείωσε η διεργασία: Log date • Το όνομα χρήστη που εκτέλεσε τη διεργασία.: → Account Name • Το όνομα τομέα του χρήστη που εκτέλεσε τη διεργασία.: Subject → Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type • Τιμή που επέστρεψε η διεργασία. : Process Information → Exit Status	Απαιτείται
			Event ID: 4656 (Ζητήθηκε ο χειρισμός ενός αντικειμένου) Event ID: 4663 (Πραγματοποιήθηκε προσπάθεια προσπέλασης του αντικειμένου) Event ID: 4658 (Ο χειρισμός του αντικειμένου ολοκληρώθηκε και τερματίστηκε) **Πληροφορίες Επιβεβαίωσης:** • Αναγνωριστικό Χειρισμού: Object → Handle ID • Αναγνωριστικό της διεργασίας που αιτήθηκε τον χειρισμό: Process Information →Process ID (ταιριάζει με τα αναγνωριστικά της διεργασίας που δημιουργήθηκαν στο Event 4688) • Λεπτομέρειες διεργασίας: Πληροφορίες της αίτησης εισόδου → Αιτιολογία της εισόδου • Επιτυχία ή Αποτυχία: Λέξεις κλειδιά (Επιτυχία ελέγχου)	Απαιτείται
			Εάν μία εφαρμογή εκτελεστεί με τη μέθοδο Bypass τότε θα καταγραφούν τα παρακάτω:	Απαιτείται

Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4688 (νέα διεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα που ξεκίνησε/τελείωσε η διεργασία: Log date • Το όνομα χρήστη που εκτέλεσε τη διεργασία.: → Account Name • Το όνομα τομέα του χρήστη που εκτέλεσε τη διεργασία.: Subject → Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type • Τιμή που επέστρεψε η διεργασία. : Process Information → Exit Status Εάν είναι επιτυχής επιστρέφει 0x0. Εάν αποτύχει επιστρέφει διαφορετική τιμή ανάλογα με το σφάλμα. Εξαρτάται από την εφαρμογή που χρησιμοποιήθηκε για το Bypass, εάν έχει εκτελεστεί από την γραμμή εντολών η τιμή μπορεί να μην είναι 0x0. Για αυτό το λόγο αυτό μπορεί να χρησιμοποιηθεί ώστε να ταξινομήσουμε εάν η εφαρμογή που εκτελέστηκε ήταν με παράκαμψη δικαιωμάτων ή για την παράκαμψη των δικαιωμάτων. Ανάλογα με το πως κλήθηκαν οι εφαρμογές μπορεί ή μία να τερματιστεί πιο νωρίς από την άλλη.	Απαιτείται
		Αρχείο καταγραφής - Sysmon	Καταγράφεται όταν πραγματοποιείται εγκατάσταση ενός προγράμματος.	Απαιτείται
			Event ID: 1 (Δημιουργία διεργασίας) Event ID: 2 (Τερματισμός διεργασίας) **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα που άρχισε/τελείωσε η διεργασία (UTC): Ώρα Utc • Διεργασία στη γραμμή εντολών: Γραμμή Εντολών • Όνομα χρήστη: Χρήστης • Αναγνωριστικό διεργασίας: ProcessId	Απαιτείται
			Εάν μία εφαρμογή εκτελεστεί με τη μέθοδο Bypass τότε θα καταγραφούν τα παρακάτω:	Απαιτείται
			Event ID: 1 (Δημιουργία διεργασίας) Event ID: 2 (Τερματισμός διεργασίας) **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα που άρχισε/τελείωσε η διεργασία (UTC): Ώρα Utc • Διεργασία στη γραμμή εντολών: Γραμμή Εντολών	

Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Sysmon	• Όνομα χρήστη: Χρήστης • Αναγνωριστικό διεργασίας: ProcessId • Γονικό όνομα διεργασίας: ParentImage • Γονικό αναγνωριστικό διεργασίας: ParentProcessId Εάν μία διεργασία αφορά σε αρχεία σεναρίων για επεξεργασία των δεσμών ενεργειών τότε η διαδικασία γίνεται γονική και θα ακολουθήσει μία διαδικασία παιδιού. Με το να ψάχνουμε τα αναγνωριστικά των διεργασιών μπορούμε να ανακαλύψουμε το δέντρο των εκτελεσμένων εφαρμογών.	Απαιτείται
		Καταγραφή εφαρμογών και υπηρεσιών	Event ID: 500 (Εφαρμογή επιδιόρθωσης συμβατότητας) **Πληροφορίες Επιβεβαίωσης:** • Εφαρμογή προγράμματος: Λεπτομέρειες → Καρτέλα UserData\CompatibilityFixEvent\ExePath • Επιδιόρθωση προγράμματος: Λεπτομέρειες → Καρτέλα: UserData\CompatibilityFixEvent\FixName	Απαιτείται
		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\’όνομα αρχείου’ Πληροφορίες Επιβεβαίωσης (Μπορούν να επιβεβαιωθούν χρησιμοποιώντας το εργαλείο WinPrefetchView): • Ώρα και ημερομηνία τελευταίας εκτέλεσης: Last Execution Time	Απαιτείται
			Παρατηρήσεις: Επιπλέον θα αλλάξει η ώρα και ημερομηνία της εφαρμογής που χρησιμοποιήθηκε για Bypass και αυτής που εκτελέστηκε.	Απαιτείται
		Ιστορικό Εκτέλεσης - Αρχείο μητρώου	Μητρώο Καταγραφής: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Uninstall\{[GUID]} **Πληροφορίες Επιβεβαίωσης:** • Περιεχόμενο: DisplayName (Το όνομα της εφαρμογής που χρησιμοποιήθηκε για το Bypass) • Εντολή διαγραφής: UninstallString (("%windir%\system32\’όνομα εφαρμογής’ -u "C:\Windows\AppPatch\Custom\{[GUID]}."))	Απαιτείται
			Μητρώο Καταγραφής: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\’όνομα αρχείου που χρησιμοποιήθηκε για το Bypass’ **Πληροφορίες Επιβεβαίωσης:** • Αποτύπωμα χρόνου της εγκατάστασης της εφαρμογής: DatabaseInstallTimeStamp (Δεκαεξαδική μορφή)	Απαιτείται

Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Ιστορικό Εκτέλεσης - Αρχείο μητρώου	Μητρώο Καταγραφής: HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\{[GUID]} **Πληροφορίες Επιβεβαίωσης:** • Διαδρομή αρχείου: DatabasePath → "C:\Windows\AppPatch\Custom\{[GUID]}. • Τύπος: DatabaseType • Περιεχόμενα αρχείου: DatabaseDescritpion → Το όνομα της εφαρμογής που χρησιμοποιήθηκε για το Bypass • Αποτύπωμα χρόνου της εγκατάστασης της εφαρμογής: DatabaseInstallTimeStamp (Δεκαεξαδική μορφή ίδια τιμή με παραπάνω)	Απαιτείται
			Παρατηρήσεις: Η παραπάνω τιμή του αρχείου μητρώου διαγράφετε όταν απεγκατασταθεί η εφαρμογή. Υπάρχουν εργαλεία που σβήνουν τα αποτυπώματα της εφαρμογής μόλις αυτή απεγκατασταθεί.	Απαιτείται

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	Καταγραφή τόσο της εφαρμογής που χρησιμοποιήθηκε για το Bypass όσο και της εφαρμογής που εκτελέστηκε με Bypass.

7.2 Πίνακες αποτελεσμάτων για εργαλεία απομακρυσμένων εντολών

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	psexec
	Κατηγορία	Εκτέλεση εντολών
	Περιγραφή Εργαλείου	Εκτέλεση διεργασιών σε ένα απομακρυσμένο σύστημα
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο μπορεί να χρησιμοποιηθεί για να εκτελεστούν απομακρυσμένες εντολές σε ένα πελάτη ή σε ένα διακομιστή στον τομέα ενός δικτύου. • Κεντρικός υπολογιστής πηγής: Psexec πηγή εκτέλεσης εντολών • Κεντρικός υπολογιστής προορισμού: Ο προορισμός που έχει συνδεθεί με την εντολή Psexec.
Κατάσταση λειτουργίας	Εξουσιοδότηση	• Κεντρικός υπολογιστής πηγής: Βασικός χρήστης • Κεντρικός υπολογιστής προορισμού: Διαχειριστής
	Στοχευμένο Λογισμικό	Windows
	Τομέας	Δεν απαιτείται
	Πρωτόκολλο επικοινωνίας	135/TCP, 445/TCP, μία τυχαία μεγάλη πόρτα Όταν εκτελείται σε ένα περιβάλλον τομέα, πραγματοποιείται επικοινωνία για έλεγχο ταυτότητας Kerberos με τον ελεγκτή τομέα.
	Υπηρεσία	-

Απαιτούμενη Πληροφορία	Ρυθμίσεις	• Κεντρικός υπολογιστής πηγής: Έχει καταχωρηθεί ένα μητρώο με το οποίο έχει εισαχθεί η Άδεια Χρήσης του PsExec. • Κεντρικός υπολογιστής προορισμού: Έχει καταχωρηθεί το γεγονός ότι έχει εγκατασταθεί, ξεκινήσει ή τελειώσει η υπηρεσία Psexesvc.
	Επιπλέον ρυθμίσεις	• Ιστορικό εκτέλεσης: (Sysmon/πολιτική ελέγχου) • Κεντρικός υπολογιστής πηγής: Το γεγονός ότι η διαδικασία PsExec εκτελέστηκε και έγινε σύνδεση στον προορισμό μέσω του δικτύου, καθώς και το όνομα της εντολής και το όρισμα για μια εντολή που εκτελέστηκε εξ 'αποστάσεως καταγράφονται • Κεντρικός υπολογιστής προορισμού: Το γεγονός ότι το δυαδικό αρχείο PSEXESVC δημιουργήθηκε και προσπεράστηκε και ότι η σύνδεση έγινε από την πηγή μέσω του δικτύου, καθώς και το όνομα εντολής και το όρισμα για μια εντολή που εκτελέστηκε εξ 'αποστάσεως καταγράφονται.
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Εάν κάποιο από τα παρακάτω παραιτηθεί τότε είναι πιθανόν να έχει εκτελεστεί το Psexec. • Κεντρικός υπολογιστής πηγής: Εάν υπάρχει η παρακάτω καταγραφή στις καταγραφές γεγονότων ➢ Event ID 4689 (μία διεργασία εξήλθε) από το Psexec.exe έχει καταγραφεί στις καταγραφές γεγονότων «Security» με τιμή αποτελέσματος εκτέλεσης 0x0. • Κεντρικός υπολογιστής προορισμού: Το Psexesvc.exe έχει εγκατασταθεί.

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4688 (νέα διεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) -Πληροφορίες διεργασίας → Όνομα διεργασίας: '[Αρχείο εκτέλεσης (psexec.exe)])' -Πληροφορίες Επιβεβαίωσης • Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής • Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject → Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject → Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type • Τιμή που επέστρεψε η διεργασία. : Process Information → Exit Status	Απαιτείται

Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Sysmon	Event ID: 1 (Δημιουργία διεργασίας) Event ID: 2 (Η διεργασία εξήλθε) -Image: '[Αρχείο εκτέλεσης(psexec.exe)]' -Πληροφορίες Επιβεβαίωσης • Ημερομηνία και ώρα έναρξης/τερματισμού της διεργασίας (UTC): UTCTime • Διεργασία στη γραμμή εντολών: Γραμμή εντολών 'Η εντολή που εκτελέστηκε απομακρυσμένα καταγράφτηκε στο στοιχείο της γραμμής εντολών.' • Όνομα χρήστη: Χρήστης • Αναγνωριστικό διεργασίας: ProcessId	Απαιτείται
		Ιστορικό Εκτέλεσης - Προετοιμασία	Καταγραφή στο αρχείο μητρώου: HKEY_USERS\[SID]\Software\Sysinternals\PsExec - EulaAccepted 'Εάν το αρχείο PsExec δεν εκτελέστηκε στο παρελθόν, εκδίδεται το μητρώο με την ένδειξη ότι έχει τεθεί η συμφωνία άδειας χρήσης. (Εάν η υπηρεσία εκτελέστηκε στο παρελθόν, το μητρώο θα παραμείνει αμετάβλητο.)'	Απαιτείται
	Προορισμός	Αρχείο καταγραφής - Σύστημα	Event ID: 7045 (Μία υπηρεσία εγκαταστάθηκε στο σύστημα) **Πληροφορίες Επιβεβαίωσης:** • Όνομα διεργασίας: 'Psexesvc' • Μονοπάτι: "%SystemRoot%\PSEXESVC.exe"	Απαιτείται
			Event ID: 7036 (Η κατάσταση της υπηρεσίας άλλαξε) * Η υπηρεσία "PSEXESVC" εισέρχεται στην κατάσταση "Executing" πριν εκτελέσει μια απομακρυσμένη διαδικασία και στην κατάσταση "Stopped" μετά την εκτέλεση.	
		Αρχείο καταγραφής - Ασφάλεια	Event ID: 5156 (Η πλατφόρμα φιλτραρίσματος των Windows έχει επιτρέψει μια σύνδεση) 'Η επικοινωνία γίνεται από τον κεντρικό υπολογιστή προέλευσης στον κεντρικό υπολογιστή προορισμού με πόρτες προορισμού 135 και 445,' (Παράδειγμα: Η πλατφόρμα φιλτραρίσματος Windows επέτρεψε την επικοινωνία από 192.168.0.10:49210 έως 192.168.0.2: 445) * Η επικοινωνία γίνεται από τον κεντρικό υπολογιστή προέλευσης στον κεντρικό υπολογιστή προορισμού με τυχαία υψηλή θύρα ως θύρα προορισμού. (1024 και πάνω)	Απαιτείται
			Event ID 5140 (Πρόσβαση σε αντικείμενο κοινόχρηστου δικτύου) -Πληροφορίες Επιβεβαίωσης • Ώρα και ημερομηνία σύνδεσης: Ημερομηνία καταγραφής 'Η ημερομηνία και η ώρα πριν την έναρξη του Psexesvc.exe'	

Λειτουρικό σύτημα : Χρήστης Windows ↓ Λειτουρικό σύτημα : Χρήστης Windows	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	• Ο χρήστης που χρησιμοποιήθηκε για τη δύνδεση: Subject → Security ID και Account Name • Κεντρικός υπολογιστής πηγής: Πληροφορίες διαδυκτίου → Διεύθυνση πηγής και πόρτες πηγής. • Κοινόχρηστη σύνδεση: "\??\C:\Windows" (administrative share)	Απαιτείται
			Event ID: 4672 (Ειδικά προνόμια ανατέθηκαν κατά τη σύνδεση): 'Πριν από αυτό το γεγονός, εμφανίζεται το γεγονός 4624. Ένας λογαριασμός που έχει συνδεθεί κατά την εμφάνιση του συμβάντος 4624 έχει ανατεθειμένα δικαιώματα.' **Πληροφορίες Επιβεβαίωσης:** • Ο λογαριασμός που χρησιμοποιήθηκε για τη σύνδεση: Subject → Security ID και Account Name • Ανατεθειμένα προνόμια: Privileges	
			Event ID: 4656 (Ζητήθηκε μια χειραγώγηση σε ένα αντικείμενο) Event ID: 4663 (Έγινε προσπάθεια πρόσβασης σε ένα αντικείμενο) • Object -> Object Name :"C:\Windows\PSEXESVC.exe"	
			Event ID: 5140 (Ένα κοινόχρηστο αντικείμενο στο δίκτυο προσπελάστηκε) -**Πληροφορίες Επιβεβαίωσης:** • Λογαριασμός που χρησιμοποιήθηκε για τη σύνδεση: Security ID και Account Name • Κεντρικός υπολογιστής πηγής; Πληροφορίες διαδικτύου → Διεύθυνση πηγής και πόρτες πηγής • Κοινόχρηστη σύνδεση: "*\IPC$" (administrative share)	
			Event ID: 5145 (Έχει επιλεγεί ένα αντικείμενο κοινής χρήσης δικτύου για να διαπιστωθεί εάν μπορεί να αποκτηθεί η επιθυμητή πρόσβαση από τον πελάτη) Το αναγνωριστικό του γεγονότος καταγράφετε πολλές φόρες. **Πληροφορίες Επιβεβαίωσης:** • Λογαριασμός που χρησιμοποιήθηκε για τη σύνδεση: Security ID και Account Name • Κεντρικός υπολογιστής πηγής; Πληροφορίες διαδυκτίου → Διεύθυνση πηγής και πόρτες πηγής • Κοινόχρηστος στόχος: Κοινόχρηστη πληροφορία → Κοινόχρηστο μονοπάτι Η διαδρομή κοινής χρήσης περιέχει "PSEXESVC" και "\\ ?? \ C: \ Windows".	

Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4656 (Ζητήθηκε μια χειραγώγηση σε ένα αντικείμενο) Event ID: 4660 (Ένα αντικείμενο διαγράφτηκε) Event ID: 4658 (Η χειραγώγηση του αντικειμένου τερματίστηκε) -Πληροφορίες διεργασίας → Αναγνωριστικό διεργασίας: '0x4' (System) -**Πληροφορίες Επιβεβαίωσης:** • Στοχευμένο αρχείο: Object → Object Name ("C:\Windows\PSEXESVC.exe") • Αναγνωριστικό χειραγώγησης: Object → Handle ID (Χρησιμοποιείται για συσχέτιση με άλλες καταγραφές) • Λεπτομέρειες διεργασίας: Access Request Information → Accces ('Delete','ReadAttributes') • Επιτυχία ή Αποτυχία: Keywords ('Επιτυχία ελέγχου')	Απαιτείται
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Δημιουργία διεργασίας) Event ID: 5 (Τερματισμός διεργασίας) - Image: "C:\Windows\PSEXESVC.exe" - Χρήστης: 'System' -**Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα που το PSexesvc.exe εκτελέστηκε: Ημερομηνία καταγραφής	Απαιτείται
			Event ID: 1 (Δημιουργία διεργασίας) Event ID: 5 (Τερματισμός διεργασίας) -**Πληροφορίες Επιβεβαίωσης:** • Πρόοδος απομακρυσμένης εκτέλεσης: Image • Επιχειρηματολογία: CommandLine • Ημερομηνία και ώρα έναρξης/τερματισμού της διεργασίας (UTC): UtcTime 'Η ημερομηνία και η ώρα μετά την έναρξη του PSEXESVC.exe και πριν από το τέλος του' • Λογαριασμός χρήστη που χρησιμοποιήθηκε για την απομακρυσμένη εκτέλεση: User	

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	Πληροφορίες σχετικά με την εκτέλεση της διαδικασίας χρησιμοποιώντας PsExec μπορεί να καταγραφούν στον "Destination Host".

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	smbexec
	Κατηγορία	Εκτέλεση εντολών
	Περιγραφή Εργαλείου	Εκτέλεση διεργασιών σε ένα απομακρυσμένο σύστημα
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο μπορεί να χρησιμοποιηθεί για να εκτελεστούν απομακρυσμένες εντολές σε ένα πελάτη ή σε ένα διακομιστή στον τομέα ενός δικτύου.
Κατάσταση λειτουργίας	Εξουσιοδότηση	• Κεντρικός υπολογιστής πηγής: Βασικός χρήστης • Κεντρικός υπολογιστής προορισμού: Διαχειριστής
	Στοχευμένο Λογισμικό	Windows
	Τομέας	-
	Πρωτόκολλο επικοινωνίας	135/TCP, 445/TCP, μία τυχαία μεγάλη πόρτα Όταν εκτελείται σε ένα περιβάλλον τομέα, πραγματοποιείται επικοινωνία για έλεγχο ταυτότητας Kerberos με τον ελεγκτή τομέα
	Υπηρεσία	-
Απαιτούμενη Πληροφορία	Ρυθμίσεις	• Κεντρικός υπολογιστής πηγής: Έχει καταχωρηθεί ένα μητρώο με το οποίο έχει εισαχθεί η Άδεια Χρήσης του Smbexec. • Κεντρικός υπολογιστής προορισμού: Έχει καταχωρηθεί το γεγονός ότι έχει εγκατασταθεί, ξεκινήσει ή τελειώσει η υπηρεσία Smbexec.
	Επιπλέον ρυθμίσεις	• Ιστορικό εκτέλεσης: (Sysmon/πολιτική ελέγχου) • Κεντρικός υπολογιστής πηγής: Το γεγονός ότι η διαδικασία Smbexec εκτελέστηκε και έγινε σύνδεση στον προορισμό μέσω του δικτύου, καθώς και το όνομα της εντολής και το όρισμα για μια εντολή που εκτελέστηκε εξ 'αποστάσεως καταγράφονται
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Όταν δημιουργείται το: • Event ID 5142 → Προσθήκη κοινόχρηστου αντικειμένου. Μπορούμε να ανιχνεύσουμε τη χρήση κρυφών κοινόχρηστων στοιχείων όπως το $Admin και το C$ τα οποία εμφανίζονται κυρίως σε συνθήκες επιθέσεις.

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα :	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	Event ID: 5140 (Ένα κοινόχρηστο αντικείμενο προσπελάστηκε) Event ID: 5142 (Ένα κοινόχρηστο αντικείμενο δημιουργήθηκε) Event ID: 5143 (Ένα κοινόχρηστο αντικείμενο επεξεργάστηκε) Event ID: 5144 (Ένα κοινόχρηστο αντικείμενο διαγράφτηκε)	Απαιτείται

Χρήστης Windows			Event ID: 5168 (Απέτυχε ο έλεγχος για SMB/SMB2)	
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Προορισμός	Αρχείο καταγραφής - Sysmon	Event ID: 4624 (Ενέργεια για χειραγώγηση του hash) Event ID: 13 (ImagePath) Event ID: 7045 (Εγκατάσταση υπηρεσίας στο σύστημα) Event ID: 1 (Εκτέλεση του Stager από το Services.exe) Event ID: 12 (Διαγραφή της υπηρεσίας keyNew από το αρχείο μητρώων) -**Πληροφορίες Επιβεβαίωσης:** • PackageName: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 • Συνδεδεμένος χρήστης: Διαχειριστής • Όνομα υπηρεσίας: ΄Υποπτο όνομα/τυχαίο • ParentImage: C:\Windows\system32\services.exe • TargetObject: "HKLM\System\CurrentControlSet\services\[Τυχαίο όνομα]"	Απαιτείται

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	Το Event ID: 13, το Image:services.exe, το TargetObject: ("HKLM\\System\\CurrentControlSet\\services\\", το "ImagePath") και το Details: /.{50,}/ θα πρέπει να δώσουν μεγάλες καταγραφές (ασυνήθιστη συμπεριφορά) οι οποίες ορίζονται ως τιμές των παραμέτρων (ImagePath) των νέων ή των τρεχουσών υπηρεσιών.

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	wmiexec
	Κατηγορία	Εκτέλεση εντολών
	Περιγραφή Εργαλείου	Εργαλείο διαχείρισης του συστήματος των Windows
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο εκτελεί μια δέσμη ενεργειών για άλλους κεντρικούς υπολογιστές. - Κεντρικός υπολογιστής πηγής: Η πηγή που εκτελεί το wmiexec.vbs - Κεντρικός υπολογιστής προορισμού: Το μηχάνημα που έχει πρόσβαση από το wmiexec.vbs
Κατάσταση λειτουργίας	Εξουσιοδότηση	Απλός χρήστης
	Στοχευμένο Λογισμικό	Windows
	Τομέας	Δεν απαιτείται
	Πρωτόκολλο επικοινωνίας	135/tcp, 445/tcp
	Υπηρεσία	-
Απαιτούμενη Πληροφορία	Ρυθμίσεις	Ιστορικό εκτέλεσης (Prefetch)
	Επιπλέον ρυθμίσεις	Ιστορικό δημιουργίας / διαγραφής αρχείου (Πολιτική ελέγχου)

		Ιστορικό εκτέλεσης (Sysmon)
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		- Κεντρικός υπολογιστής πηγής: Το κοινόχρηστο στοιχείο "WMI_SHARE" έχει δημιουργηθεί και διαγράφτηκε.

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4688 (νέα διεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) -Πληροφορίες διεργασίας → Όνομα διεργασίας: '[Αρχείο εκτέλεσης (psexec.exe)])' -**Πληροφορίες Επιβεβαίωσης:** • Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής • Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject → Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject → Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type Τιμή που επέστρεψε η διεργασία. : Process Information → Exit Status	Απαιτείται
			Event ID: 5156 (Η πλατφόρμα φιλτραρίσματος των Windows έχει επιτρέψει μια σύνδεση) -Πληροφορίες διεργασίας → Όνομα διεργασίας: "C:\Windows\System32\cscript.exe" -**Πληροφορίες Επιβεβαίωσης:** • Port πηγής: Πληροφορίες διαδικτύου → Port προορισμού "Ένας αριθμός θύρας μπορεί να αλλάξει καθορίζοντάς τον στον προορισμό"	Απαιτείται
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\cscript.exe" -**Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC) → UtcTime • Διεργασία στη γραμμή εντολών → Γραμμή εντολών • Όνομα χρήστη → User • Αναγνωριστικό διεργασίας → ProcessId	Απαιτείται
		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\CSCRIPT.EXE-D1EF4768.pf -**Πληροφορίες Επιβεβαίωσης:**	Απαιτείται

Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows			Η επιβεβαίωση μπορεί να γίνει χρησιμοποιώντας το εργαλείο WinPrefetchView • Ημερομηνία και ώρα τελευταίας εκτέλεσης → Last Execution Time	
	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4656 (Ζητήθηκε ο χειρισμός ενός αντικειμένου) Event ID: 4663 (Έγινε προσπάθεια προσπέλασης ενός αντικειμένου) Event ID: 4658 (Η χειραγώγηση του αντικειμένου τελείωσε) -Αντικείμενο → Object Name "(C:\Windows\Temp\wmi.dll)" -Πληροφορίες αιτήματος πρόσβασης → Access / Reason for Access: ("WriteData (ή AddFile)", "AppendData (ή AddSubdirectory ή CreatePipeInstance)") -**Πληροφορίες Επιβεβαίωσης:** • Όνομα διεργασίας: "C:\Windows\System32\cmd.exe" • Αναγνωριστικό χειραγώγησης: Object -> Handle ID Χρησιμοποιείται για σύνδεση με άλλα αρχεία καταγραφής	Απαιτείται
			Event ID: 5142 (Προστέθηκε ένα κοινόχρηστο αντικείμενο στο δίκτυο) -**Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού της διεργασίας: Log Date • Όνομα χρήστη που εκτέλεσε την διεργασία: Subject → Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject → Account Domain • Κοινόχρηστο όνομα: Share Information → Share name: ("*\WMI_SHARE") • Κοινόχρηστη διαδρομή: Share Information → Share Path: ("C:\Windows\Temp")	Απαιτείται
			Event ID: 5145 (Έχει επιλεγεί ένα αντικείμενο κοινόχρηστου δικτύου για να διαπιστωθεί εάν ο πελάτης μπορεί να λάβει την επιθυμητή πρόσβαση) -**Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού της διεργασίας: Log Date • Όνομα χρήστη που εκτέλεσε την διεργασία: Subject → Account Name	Απαιτείται

Λειτουρικό σύτημα : Χρήστης Windows ↓ Λειτουρικό σύτημα : Χρήστης Windows	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	• Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject → Account Domain • Κοινόχρηστο όνομα: Share Information → Share name: ("*\WMI_SHARE") • Κοινόχρηστη διαδρομή: Share Information → Share Path: ("C:\Windows\Temp") • Κοινόχρηστη διαδρομή: Share Information → Relative Target Name: (“wmi.dll”)	Απαιτείται
			Event ID: 4656 (Ζητήθηκε ο χειρισμός ενός αντικειμένου) Event ID: 4660 (Το αντικείμενο διαγράφτηκε) Event ID: 4658 (Η χειραγώγηση του αντικειμένου τελείωσε) -Αντικείμενο → Object Name: "(C:\Windows\Temp\wmi.dll)" -Πληροφορίες Αίτησης Πρόσβασης → Access/Reason for Access: "DELETE -**Πληροφορίες Επιβεβαίωσης:** • Όνομα διεργασίας: "(C:\Windows\System32\cmd.exe)"	Απαιτείται
			Event ID: 5144 (Ένα κοινόχρηστο με το δίκτυο αντικείμενο διαγράφτηκε) -**Πληροφορίες Επιβεβαίωσης:** • Κοινόχρηστο όνομα: Share Information → Share name: ("*\WMI_SHARE") • Κοινόχρηστη διαδρομή: Share Information → Share Path: ("C:\Windows\Temp")	Απαιτείται
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\wbem\WmiPrvSE.exe" "C:\Windows\System32\cmd.exe" -**Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC) → UtcTime • Διεργασία στη γραμμή εντολών → Γραμμή εντολών • Όνομα χρήστη → User • Αναγνωριστικό διεργασίας → ProcessId	Απαιτείται
		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\CSCRIPT.EXE-D1EF4768.pf -**Πληροφορίες Επιβεβαίωσης:** Η επιβεβαίωση μπορεί να γίνει χρησιμοποιώντας το εργαλείο WinPrefetchView	Απαιτείται

			• Last Execution Time and Date: Last Execution Time	

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	------

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	winrm
	Κατηγορία	Εκτέλεσης εντολών
	Περιγραφή Εργαλείου	Απομακρυσμένη εκτέλεση εντολών σε ένα κεντρικό υπολογιστή
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο χρησιμοποιείται για μια έρευνα πριν από την εκτέλεση μιας απομακρυσμένης εντολής. - Κεντρικός υπολογιστής πηγής: Πηγή εκτέλεσης εντολών WinRM - Κεντρικό υπολογιστής προορισμού: Το μηχάνημα που έχει πρόσβαση από την εντολή WinRM
Κατάσταση λειτουργίας	Εξουσιοδότηση	Διαχειριστής
	Στοχευμένο Λογισμικό	Windows
	Τομέας	-
	Πρωτόκολλο επικοινωνίας	5985/tcp (HTTP) or 5986/tcp (HTTPS)
	Υπηρεσία	Κεντρικός υπολογιστής προορισμού: Απομακρυσμένη διαχείριση των Windows (WS-Management)
Απαιτούμενη Πληροφορία	Ρυθμίσεις	Ιστορικό εκτέλεσης (Prefetch)
	Επιπλέον ρυθμίσεις	Κεντρικός υπολογιστής πηγής: Ιστορικό εκτέλεσης (Sysmon) Κεντρικός υπολογιστής προορισμού: Σύνδεση από τον κεντρικό υπολογιστή πηγής.
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Κεντρικός υπολογιστής πηγής: Εάν υπάρχει το ακόλουθο αρχείο καταγραφής, είναι δυνατό να εκτελεστεί το WinRM. • Καταγράφεται ένα γεγονός που υποδεικνύει ότι το cscript.exe έχει πρόσβαση στον κεντρικό υπολογιστή προορισμού με αναγνωριστικά συμβάντων 1 και 5 του αρχείου καταγραφής συμβάντων "Sysmon"

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουρικό σύτημα : Χρήστης			Event ID: 4688 (νέα διεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) -Πληροφορίες διεργασίας → Όνομα διεργασίας: '[Αρχείο εκτέλεσης (psexec.exe)])' -**Πληροφορίες Επιβεβαίωσης:** • Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής	

Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Ασφάλεια	• Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject → Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject → Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type Τιμή που επέστρεψε η διεργασία. : Process Information → Exit Status	Απαιτείται
		Αρχείο καταγραφής - Ασφάλεια	Event ID: 5156 (Η πλατφόρμα φιλτραρίσματος των Windows έχει επιτρέψει μια σύνδεση) -Πληροφορίες διεργασίας → Όνομα διεργασίας: "C:\Windows\System32\cscript.exe" -**Πληροφορίες Επιβεβαίωσης:** • Port πηγής: Πληροφορίες διαδικτύου → Port προορισμού "Ένας αριθμός θύρας μπορεί να αλλάξει καθορίζοντάς τον στον προορισμό"	Απαιτείται
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\cscript.exe"- **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC) → UtcTime • Διεργασία στη γραμμή εντολών → Γραμμή εντολών • Όνομα χρήστη → User • Αναγνωριστικό διεργασίας → ProcessId	Απαιτείται
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Εφαρμογές και υπηρεσίες Microsoft\Windows\Windows Remote Management	Event ID: 166 (Ο επιλεγμένος μηχανισμός ελέγχου ταυτότητας είναι διαπραγματεύσιμος) **Πληροφορίες Επιβεβαίωσης:** • Μέθοδος αυθεντικοποίησης: Authentication Mechanism (ο επιλεγμένος μηχανισμός ελέγχου ταυτότητας είναι Kerberos)	Απαιτείται
			Event ID: 80 (Αποστολή της αίτησης για λειτουργία λήψης στον κεντρικό υπολογιστή προορισμού και τη θύρα) **Πληροφορίες Επιβεβαίωσης:** • Αποστολή υπολογιστή προορισμού και θύρα: "[Host Name]:[Port]"	Απαιτείται
			Event ID: 143 (Λήψη απάντησης από το επίπεδο δικτύου) **Πληροφορίες Επιβεβαίωσης:** • Κατάσταση: Status (200 (HTTP_STATUS_OK))	Απαιτείται
			Event ID: 132 (Η λειτουργία WSMan εντοπίζεται επιτυχώς) **Πληροφορίες Επιβεβαίωσης:** • Χρόνος και ημερομηνία ολοκλήρωσης (UTC): UTCTime	Απαιτείται

Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\CSCRIPT.EXE-D1EF4768.pf **Πληροφορίες Επιβεβαίωσης:** • Χρόνος και ημερομηνία τελευταίας εκτέλεσης: Last Execution Time	Απαιτείται
	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	Event ID: 5156 (Το φιλτράρισμα των Windows επέτρεψε μία σύνδεση) -Πληροφορίες εφαρμογής → Όνομα εφαρμογής: “System” -Πληροφορίες διαδικτύου → Προορισμός: “Inbound” -Πληροφορίες διαδικτύου → Port πηγής: "5985" (HTTP) ή "5986" (HTTPS) -Πληροφορίες διαδικτύου → Πρωτόκολλο: "6" (TCP) **Πληροφορίες Επιβεβαίωσης:** • Κεντρικός υπολογιστής πηγής Πληροφορίες διαδικτύου → Διεύθυνση προορισμού • Κεντρικός υπολογιστής προορισμού: Πληροφορίες διαδικτύου → Port προορισμού	Απαιτείται
			Event ID: 4624 (Ένας λογαριασμός συνδέθηκε επιτυχώς) -Τύπος εισόδου: “3” **Πληροφορίες Επιβεβαίωσης:** • Αναγνωριστικό ασφαλείας: New Logon → Security ID • Αναγνωριστικό σύνδεσης: Subject → Logon ID • Λογαριασμός: Account Name → Account Domain	Απαιτείται
			Event ID: 4656 (Ζητήθηκε ο χειρισμός ενός αντικειμένου) Event ID: 4658 (Η χειραγώγηση του αντικειμένου τελείωσε) -Πληροφορίες διεργασίας → Όνομα διεργασίας: "C:\Windows\System32\svchost.exe" -Αντικείμενο → Όνομα αντικειμένου: "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Client" -Αντικείμενο → Όνομα αντικειμένου: "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Service" **Πληροφορίες Επιβεβαίωσης:**	Απαιτείται

			• Αναγνωριστικό χειρισμού: Object → Handle ID • Λεπτομέρειες αίτησης πρόσβασης: Access request information → Access ("READ_CONTROL", "Query key value", "Enumerate sub-keys", "Notify about changes to keys") * Αυτή η διαδικασία εκτελείται πολλές φορές.	

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Active Directory Domain Controller	Αρχείο καταγραφής - Ασφάλεια	Event ID: 5156 (Η πλατφόρμα φιλτραρίσματος των Windows επέτρεψε μία σύνδεση) -Πληροφορίες εφαρμογής → Όνομα εφαρμογής: "\device\harddiskvolume 2 \windows\system32\lsass.exe" -Πληροφορίες διαδικτύου → Κατεύθυνση: "Inbound" **Πληροφορίες Επιβεβαίωσης:** • Κεντρικός υπολογιστής πηγής: Network Information →Destination Address	Απαιτείται
			Event ID: 4769 (Ζητήθηκε εισιτήριο υπηρεσίας Kerberos) -Πληροφορίες διαδικτύου → Διεύθυνση πελάτη: "[Source Host]" **Πληροφορίες Επιβεβαίωσης:** • Χρήστης που χρησιμοποιήθηκε: Account Information → Account Name	Απαιτείται

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	----

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	wmic
	Κατηγορία	Εκτέλεσης εντολών
	Περιγραφή Εργαλείου	Ένα εργαλείο που χρησιμοποιείται για τη διαχείριση συστημάτων των Windows

	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο χρησιμοποιείται για μια έρευνα πριν από την εκτέλεση μιας απομακρυσμένης εντολής με το WMI. - Κεντρικός υπολογιστής πηγής: Πηγή εκτέλεσης εντολών wmic. - Κεντρικό υπολογιστής προορισμού: Το μηχάνημα που έχει πρόσβαση από την εντολή wmic.
Κατάσταση λειτουργίας	Εξουσιοδότηση	Απλός χρήστης “Ανάλογα με την εντολή που εκτελείται στην απομακρυσμένη πλευρά, ενδέχεται να απαιτούνται δικαιώματα διαχειριστή.”
	Στοχευμένο Λογισμικό	Windows
	Τομέας	Δεν απαιτείται
	Πρωτόκολλο επικοινωνίας	135 / tcp, 445 / tcp, μια τυχαία επιλεγμένη θύρα TCP 1024 ή μεγαλύτερη
	Υπηρεσία	Μέσα διαχείρισης παραθύρων, κλήση απομακρυσμένης διαδικασίας (RPC)
Απαιτούμενη Πληροφορία	Ρυθμίσεις	Ιστορικό εκτέλεσης (Prefetch)
	Επιπλέον ρυθμίσεις	Λεπτομέρειες εκτέλεσης διεργασίας (το όρισμα στο wmic) και η κατάσταση εκτέλεσης επιτυχία ή αποτυχία (η τιμή επιστροφής) (Sysmon και πολιτική ελέγχου)
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Εάν τα ακόλουθα αρχεία καταγραφής που έχουν τον ίδιο χρόνο καταγραφής βρίσκονται στο "host source" και "host destination", είναι πιθανό να γίνει μια απομακρυσμένη σύνδεση -Κεντρικός υπολογιστής πηγής: Εάν υπάρχει η παρακάτω εγγραφή στις καταγραφές συμβάντων: • Event ID: 4689 (μία διεργασία εξήλθε) -Κεντρικός υπολογιστής προορισμού: Εάν υπάρχει η παρακάτω εγγραφή στο Sysmon • Event ID: Καταγράφεται στο αρχείο καταγραφής συμβάντων "Sysmon" ότι εκτελέστηκε το αρχείο WmiPrvSE.exe με τα αναγνωριστικά συμβάντων 1 και 5

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουρικό σύτημα : Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4688 (νέα διεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) -Πληροφορίες διεργασίας → Όνομα διεργασίας: ‘[Αρχείο εκτέλεσης (WMImplant)]’ **-Πληροφορίες Επιβεβαίωσης:** • Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής • Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject → Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject → Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type	Απαιτείται

↓ Λειτουργικό σύτημα : Χρήστης Windows			• Τιμή που επέστρεψε η διεργασία. : Process Information → Exit Status	
		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\wbem\WMIC.exe" **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC) → UtcTime • Διεργασία στη γραμμή εντολών → Γραμμή εντολών ("C:\Windows\System32\wmiprvse.exe -secured -Embedding") • Όνομα χρήστη → User ("NT AUTHORITY\NETWORK SERVICE") • Αναγνωριστικό διεργασίας → ProcessId	Απαιτείται
	Πηγή	Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\WMIC.EXE-98223A30.pf **-Πληροφορίες Επιβεβαίωσης:** (τα παρακάτω μπορούν να επιβεβαιωθούν χρησιμοποιώντας αυτό το εργαλείο: WinPrefetchView) • Ημερομηνία και ώρα τελευταίας εκτέλεσης: Last Executed Time	Απαιτείται
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Προορισμός	Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\wbem\WmiPrvSE.exe" **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC) → UtcTime • Διεργασία στη γραμμή εντολών → Γραμμή εντολών ("C:\Windows\System32\wmiprvse.exe -secured -Embedding") • Όνομα χρήστη → User ("NT AUTHORITY\NETWORK SERVICE") • Αναγνωριστικό διεργασίας → ProcessId	Απαιτείται
		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf **-Πληροφορίες Επιβεβαίωσης:** (τα παρακάτω μπορούν να επιβεβαιωθούν χρησιμοποιώντας αυτό το εργαλείο: WinPrefetchView) • Ημερομηνία και ώρα τελευταίας εκτέλεσης: Last Executed Time	Απαιτείται

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	-Ανάλογα με τη διαδικασία που ονομάζεται wmic, τα συμβάντα για τη συγκεκριμένη διαδικασία μπορούν να καταγραφούν. -Εάν ο χρήστης υπάρχει στην υπηρεσία καταλόγου Active Directory, το αίτημα ελέγχου ταυτότητας μπορεί να καταγραφεί στον ελεγκτή τομέα

	-Ωστόσο, δεν είναι δυνατό να προσδιοριστεί εάν ένα τέτοιο αίτημα ελέγχου ταυτότητας έγινε από wmic ή άλλους.

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	WMImplant
	Κατηγορία	Εκτέλεση εντολών
	Περιγραφή Εργαλείου	Εκτέλεση διεργασιών σε ένα απομακρυσμένο σύστημα
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο μπορεί να χρησιμοποιηθεί για να εκτελεστούν απομακρυσμένες εντολές σε ένα πελάτη ή σε ένα διακομιστή στον τομέα ενός δικτύου.
Κατάσταση λειτουργίας Κατάσταση λειτουργίας	Εξουσιοδότηση	• Κεντρικός υπολογιστής πηγής: Βασικός χρήστης • Κεντρικός υπολογιστής προορισμού: Διαχειριστής
	Στοχευμένο Λογισμικό	Windows
	Τομέας	-
	Πρωτόκολλο επικοινωνίας Πρωτόκολλο επικοινωνίας	135/TCP, 445/TCP, μία τυχαία μεγάλη πόρτα Όταν εκτελείται σε ένα περιβάλλον τομέα, πραγματοποιείται επικοινωνία για έλεγχο ταυτότητας Kerberos με τον ελεγκτή τομέα
	Υπηρεσία	-
Απαιτούμενη Πληροφορία	Ρυθμίσεις	• Κεντρικός υπολογιστής πηγής: Έχει καταχωρηθεί ένα μητρώο με το οποίο έχει εισαχθεί η Άδεια Χρήσης του WMImplant. • Κεντρικός υπολογιστής προορισμού: Έχει καταχωρηθεί το γεγονός ότι έχει εγκατασταθεί, ξεκινήσει ή τελειώσει η υπηρεσία WMImplant.
	Επιπλέον ρυθμίσεις	Έλεγχος καταχώρησης: Για να εντοπιστεί η κακόβουλη δραστηριότητα ελέγχουμε το μητρώο που αποθηκεύονται αυτές οι ρυθμίσεις. Από το Regedit επιλέγουμε τα κλειδιά μητρώου που θέλουμε να παρακολουθήσουμε: • Δεξί κλικ στο Key – Permissions – Advanced – Auditing – Add – EVERYONE – (check names), OK. • Εφαρμογή σε – THIS KEY AND SUBKEYS (or what you want) • Επιλογή ‘Set Value’, ‘Create Subkey’, ‘Create Link’, ‘Delete’, ‘Write DAC’ & ‘Write Owner’ to start
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Reg.exe: Χρήση αυτού του βοηθητικού προγράμματος για να ελέγξουμε και να κάνουμε ερωτήσεις το μητρώο. • Αλλαγές στα Keys των υπηρεσιών: Ερώτηση στο μητρώο: "HKLM\System\CurrentControlSet\Services\eventlog\Windows PowerShell" • Ερώτηση στην τιμή ενός Key: Ερώτηση στο μητρώο: “HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell”

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις

	αρχείων καταγραφής			
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4688 (νέα διεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) -Πληροφορίες διεργασίας → Όνομα διεργασίας: '[Αρχείο εκτέλεσης (WMImplant)])' **-Πληροφορίες Επιβεβαίωσης:** • Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής • Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject → Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject → Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type Τιμή που επέστρεψε η διεργασία. : Process Information → Exit Status	Απαιτείται Απαιτείται
		Αρχείο καταγραφής - Ασφάλεια	Event ID: 500 (Εκτέλεση CommandName) Event ID: 501 (Εκτέλεση CommandLine) Event ID: 4104 (Οτιδήποτε παίρνει την παράμετρο get ή είναι κλήση iex) Event ID: 7 imageLoader Event ID: 4110 (Εκτέλεση εντολής με bypass) Event ID: 4104 (Εκτέλεση εντολής με πάνω από 1000 χαρακτήρες) Event ID: 400 (Εκτέλεση εντολής με μεγάλο αριθμό περιέργων χαρακτήρων)	Απαιτείται
		Αρχείο καταγραφής - Sysmon	Event ID: 19 (Ανιχνεύτηκε ενέργεια WmiEventFilter) Event ID: 20 (Ανιχνεύτηκε ενέργεια WmiEventConsumer) Event ID: 21 (Ανιχνεύτηκε ενέργεια WmiEventConsumerToFilter)	Απαιτείται
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Προορισμός	Ιστορικό Εκτέλεσης - Προετοιμασία	Μέγεθος των αρχείων καταγραφής: Αύξηση του μεγέθους των αρχείων καταγραφής. • Applications and Services Logs – 'Windows PowerShell' log ρύθμιση σε 500,000KB ή μεγαλύτερο • Applications and Services Logs / Microsoft-Windows - PowerShell/Operational' log ρύθμιση σε 500,000KB ή μεγαλύτερο WmiEventFilter (Καταγράφει ένα φίλτρο συμβάντων WMI) WmiEventConsumer (Καταγράφει έναν καταναλωτή συμβάντων WMI) WmiEventConsumerToFilter (Συνδέει τον καταναλωτή του συμβάντος στο φίλτρο συμβάντος)	Απαιτείται

Παρατηρήσεις

Windows Sysmon tool for lateral movement alerts.

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	Log Clear: Παρακολούθηση για την καταγραφή των μηνυμάτων Event ID: 104 System Log Αρχείο μητρώου: Παρακολούθηση των PS Keys για προσθήκες, αλλαγές και διαγραφές. Event ID: 4657 Security Log (Μία τιμή μητρώου τροποποιήθηκε) Εκτέλεση των παρακάτω στο Powershell για να γίνει προβολή του φίλτρου συμβάντων του WMI: # Reviewing WMI Subscriptions using Get-WMIObject # Event Filter Get-WMIObject -Namespace root\Subscription -Class __EventFilter -Filter “Name=’Updater’” # Event Consumer Get-WMIObject -Namespace root\Subscription -Class CommandLineEventConsumer -Filter “Name=’Updater’”
Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	# Binding Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding -Filter “__Path LIKE ‘%Updater%’”

7.3 Πίνακες αποτελεσμάτων για εργαλεία συλλογής πληροφοριών

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	project lazagne
	Κατηγορία	Συλλογή πληροφοριών
	Περιγραφή Εργαλείου	Απομακρυσμένη συλλογή πληροφορίων
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Είναι μια εφαρμογή ανοιχτού κώδικα που χρησιμοποιείται για την ανάκτηση πολλών κωδικών πρόσβασης που είναι αποθηκευμένα σε έναν τοπικό υπολογιστή.
Κατάσταση λειτουργίας	Εξουσιοδότηση	• Κεντρικός υπολογιστής πηγής: Βασικός χρήστης • Κεντρικός υπολογιστής προορισμού: Διαχειριστής
	Στοχευμένο Λογισμικό	Windows
	Τομέας	-
	Πρωτόκολλο επικοινωνίας	135/TCP, 445/TCP, μία τυχαία μεγάλη πόρτα Όταν εκτελείται σε ένα περιβάλλον τομέα, πραγματοποιείται επικοινωνία για έλεγχο ταυτότητας Kerberos με τον ελεγκτή τομέα
	Υπηρεσία	-
Απαιτούμενη Πληροφορία	Ρυθμίσεις	Δημιουργία συνδρομής μέσω του WEC Server Event Viewer
	Επιπλέον ρυθμίσεις	Χρήση προσαρμοσμένης διαμόρφωσης του Sysmon Αρχεία καταγραφής: • Φιλτράρισμα μέσω “Condition” • is, is not, contains, excludes, begin with, • end with, less than, more than, image

	• SwiftOnSecurity Sysmon Config
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής	Το αναγνωριστικό σύνδεσης είναι ένας μοναδικός (μοναδικός μεταξύ επανεκκινήσεων) αριθμός που προσδιορίζει τη συνεδρία σύνδεσης που μόλις ξεκίνησε. Οποιαδήποτε συμβάντα καταγράφονται στη συνέχεια κατά τη διάρκεια αυτής της περιόδου σύνδεσης θα αναφέρουν το ίδιο αναγνωριστικό σύνδεσης έως το συμβάν αποτύπωσης 4647 ή 4634.

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Windows	Πηγή	Αρχείο καταγραφής - Ασφάλεια Αρχείο καταγραφής - Ασφάλεια	Event ID: 4624 (Ένας λογαριασμός συνδέθηκε επιτυχώς) Event ID: 4648 (Πραγματοποιήθηκε μία σύνδεση χρησιμοποιώντας ειδικά διαπιστευτήρια) Event ID: 4768 (Μία νέα διεργασία ξεκίνησε) Event ID: 4656 (Ζητήθηκε ο χειρισμός ενός αντικειμένου) Event ID: 4672 (Ο χρήστης της νέας σύνδεσης έχει επαυξημένα προνόμια) **-Πληροφορίες Επιβεβαίωσης** • Αναγνωριστικό ασφαλείας: Το SID του λογαριασμού. • Όνομα λογαριασμού: Το όνομα σύνδεσης του λογαριασμού. • Τομέας λογαριασμού: Ο τομέας ή, στην περίπτωση των τοπικών λογαριασμών, το όνομα του υπολογιστή. • Αναγνωριστικό σύνδεσης: Αριθμός που προσδιορίζει την περίοδο σύνδεσης.	Απαιτείται
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows		Αρχείο καταγραφής - Sysmon	Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 10 (Μία νέα διεύθυνση IP έχει εκμισθωθεί) **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC) → UtcTime • Όνομα χρήστη → User ("NT AUTHORITY\NETWORK SERVICE") • Αναγνωριστικό διεργασίας → ProcessId	Απαιτείται
		Ιστορικό Εκτέλεσης - Προετοιμασία	**Πληροφορίες Επιβεβαίωσης:** (τα παρακάτω μπορούν να επιβεβαιωθούν χρησιμοποιώντας αυτό το εργαλείο: WinPrefetchView) Ημερομηνία και ώρα τελευταίας εκτέλεσης: Last Executed Time	Απαιτείται

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	-----

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	mimikatz
	Κατηγορία	Συλλογή πληροφοριών
	Περιγραφή Εργαλείου	Κλέβει τις καταγεγραμμένες πληροφορίες ελέγχου ταυτότητας
Εργαλείο	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Αυτό το εργαλείο εκτελείται για την απόκτηση κωδικών πρόσβασης ή την επαύξηση των δικαιωμάτων στα δικαιώματα διαχειριστή τομέα.
Κατάσταση λειτουργίας	Εξουσιοδότηση	Διαχειριστής
	Στοχευμένο Λογισμικό	Windows
	Τομέας	Δεν απαιτείται
	Πρωτόκολλο επικοινωνίας	-
	Υπηρεσία	-
Απαιτούμενη Πληροφορία	Ρυθμίσεις	Ιστορικό εκτέλεσης (Prefetch)
	Επιπλέον ρυθμίσεις	Ιστορικό εκτέλεσης (Sysmon / Πολιτική ελέγχου)
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Η επιτυχής εκτέλεση του εργαλείου δεν μπορεί να προσδιοριστεί από τα αρχεία καταγραφής συμβάντων ή το ιστορικό εκτέλεσης

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουρικό σύτημα : Χρήστης Windows ↓ Λειτουρικό σύτημα :	Πηγή	Αρχείο καταγραφής - Ασφάλεια	Event ID: 4688 (νέα διεργασία δημιουργήθηκε) Event ID: 4689 (μία διεργασία εξήλθε) -Πληροφορίες διεργασίας → Όνομα διεργασίας: "["[Όνομα αρχείου (mimikatz.exe)]" **-Πληροφορίες Επιβεβαίωσης:** • Όνομα και ημερομηνία έναρξης/τερματισμού διεργασίας: Ημερομηνία καταγραφής • Όνομα χρήστη που εκτέλεσε τη διεργασία: Subject → Account Name • Τομέας του χρήστη που εκτέλεσε τη διεργασία: Subject → Account Domain • Προβολή των προνομίων που είχε κατά την εκτέλεση της διεργασίας.: Process Information → Token Escalation Type • Τιμή που επέστρεψε η διεργασία. : Process Information → Exit Status	Απαιτείται
			Event ID: 1 (Μία διεργασία δημιουργήθηκε) Event ID: 5 (Μία διεργασία τερματίστηκε) -Image: "C:\Windows\System32\wbem\WmiPrvSE.exe"	

Χρήστης Windows	Πηγή	Αρχείο καταγραφής - Sysmon	**Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα έναρξης/τερματισμού διεργασίας (UTC) → UtcTime • Διεργασία στη γραμμή εντολών → Γραμμή εντολών ("C:\Windows\System32\wmiprvse.exe -secured -Embedding") • Όνομα χρήστη → User ("NT AUTHORITY\NETWORK SERVICE") • Αναγνωριστικό διεργασίας → ProcessId	Απαιτείται
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows		Ιστορικό Εκτέλεσης - Προετοιμασία	Όνομα αρχείου: C:\Windows\Prefetch\[Executable File(MIMIKATZ.EXE)]-[RANDOM].pf **Πληροφορίες Επιβεβαίωσης:** (τα παρακάτω μπορούν να επιβεβαιωθούν χρησιμοποιώντας αυτό το εργαλείο: WinPrefetchView) • Ημερομηνία και ώρα τελευταίας εκτέλεσης: Last Executed Time	Απαιτείται

Παρατηρήσεις

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	-----

7.4 Πίνακες αποτελεσμάτων για εργαλεία ελέγχου συστήματος

Βασικές Πληροφορίες

Εργαλείο	Όνομα Εργαλείου	Empire
	Κατηγορία	Εργαλείο ελέγχου συστήματος
	Περιγραφή Εργαλείου	Απομακρυσμένη χειραγώγηση/εκμετάλλευση ενός συστήματος
	Παράδειγμα υποτιθέμενης χρήσης του εργαλείου σε περίπτωση επίθεσης	Είναι ένας καθαρός πράκτορας PowerShell, ο οποίος εστιάζει αποκλειστικά σε python με κρυπτογραφικά ασφαλείς επικοινωνίες με την προσθήκη μιας ευέλικτης αρχιτεκτονικής. Το empire έχει τα μέσα να εκτελέσει πράκτορες PowerShell χωρίς την απαίτηση του PowerShell.exe
Κατάσταση λειτουργίας	Εξουσιοδότηση	• Κεντρικός υπολογιστής πηγής: Βασικός χρήστης • Κεντρικός υπολογιστής προορισμού: Διαχειριστής
	Στοχευμένο Λογισμικό	Windows
	Τομέας	-
	Πρωτόκολλο επικοινωνίας	80/TCP, 443/TCP
	Υπηρεσία	-
	Ρυθμίσεις	Ενεργοποίηση των αρχείων καταγραφής
		Αρχεία καταγραφής: Αύξηση του μεγέθους των αρχείων καταγραφής • Application, System logs - 256k ή μεγαλύτερο • PowerShell logs - 256k ή μεγαλύτερο

Απαιτούμενη Πληροφορία	Επιπλέον ρυθμίσεις	• Security Log - 512,000k Πολιτική Ασφαλείας: • Αλλαγή επιλογών ασφαλείας - "Έλεγχος: Ρυθμίστε τις ρυθμίσεις υποκατηγορίας πολιτικής ελέγχου" στο ΕΠΙΤΡΕΠΩ. Αυτό θέτει το σύστημα για να αναγκάσει τη χρήση του ""Advanced Audit Policies" Καταγραφές DNS: • Ενεργοποίηση καταγραφής DNS. Καταγράφει τα ερωτήματα DNS που συμβαίνουν. "systemroot\System32\Dns\Dns.log" a. Πακέτα καταγραφής για εντοπισμό σφαλμάτων b. Εισερχόμενα και εξερχόμενα c. UDP και TCP d. Πακέτα τύπου αίτησης και απάντησης e. Ερωτήματα / Μεταφορές και ενημερώσεις Καταγραφές DHCP: "%windir%\System32\Dhcp." Αυτό επιτρέπει την ανίχνευση συστημάτων στο δίκτυό που δεν εμπίπτουν στην ονοματοδοσία σας. • Event ID: 10 (Μία νέα διεύθυνση IP έχει εκμισθωθεί)
Απαιτούμενη Πληροφορία	Επιπλέον ρυθμίσεις	
Αποδεικτικά τα οποία μπορούν να επαληθευτούν όταν η εκτέλεση είναι επιτυχής		Event ID: 4698 Μία νέα διεργασία ξεκίνησε.

Στοιχεία που μπορούν να επαληθευτούν

Επικοινωνία	Τοποθεσία δημιουργίας των αρχείων καταγραφής	Τύπος και όνομα του αρχείου καταγραφής	Απαιτούμενες Πληροφορίες	Επιπλέον Ρυθμίσεις
Λειτουργικό σύτημα : Χρήστης Windows ↓ Λειτουργικό σύτημα : Χρήστης Windows	Προορισμός	Αρχείο καταγραφής - Ασφάλεια	Event ID: 400 (Αλλαγή της κατάστασης μηχανής) Event ID: 500 (Επιδώσεις των Windows) Event ID: 501 (EventTracker)	Απαιτείται
			Event ID: 4688 (Μία νέα διεργασία ξεκίνησε) **-Πληροφορίες Επιβεβαίωσης** • Αναγνωριστικό ασφαλείας: Το SID του λογαριασμού. • Όνομα λογαριασμού: Το όνομα σύνδεσης του λογαριασμού. • Τομέας λογαριασμού: Ο τομέας ή, στην περίπτωση των τοπικών λογαριασμών, το όνομα του υπολογιστή. • Αναγνωριστικό σύνδεσης: Αριθμός που προσδιορίζει την περίοδο σύνδεσης.	Απαιτείται
			Event ID: 1 (Δημιουργία διεργασίας) Event ID: 3 (Σύνδεση μέσω δικτύου) **Πληροφορίες Επιβεβαίωσης:** • Ημερομηνία και ώρα που άρχισε/τελείωσε η διεργασία (UTC): Ώρα Utc • Διεργασία στη γραμμή εντολών: Γραμμή Εντολών • Όνομα χρήστη: Χρήστης	

Λειτουρικό σύτημα : Χρήστης Windows ↓ Λειτουρικό σύτημα : Χρήστης Windows	Προορισμός	Αρχείο καταγραφής - Sysmon	• Αναγνωριστικό διεργασίας: ProcessId • Γονικό όνομα διεργασίας: ParentImage • Γονικό αναγνωριστικό διεργασίας: ParentProcessId Εάν μία διεργασία αφορά σε αρχεία σεναρίων για επεξεργασία των δεσμών ενεργειών τότε η διαδικασία γίνεται γονική και θα ακολουθήσει μία διαδικασία παιδιού. Με το να ψάχνουμε τα αναγνωριστικά των διεργασιών μπορούμε να ανακαλύψουμε το δέντρο των εκτελεσμένων εφαρμογών.	Απαιτείται
		Ιστορικό Εκτέλεσης - Προετοιμασία	• Computer Configuration > Policies > Administrative Templates > Windows Components > Powershell > Turn on Module Logging (Ενημέρωση των Windows για την καταγραφή δραστηριότητας Powershell στο δίσκο) • Computer Configuration > Policies > Administrative Templates > Windows Components > Powershell > Turn on PowerShell Script Block Logging (Δημιουργεί πιο λεπτομερή τα παραπάνω αρχεία καταγραφής) • Computer Configuration > Policies > Administrative Templates > Windows Components/Windows Remote Management (WinRM)/WinRM Service (Επιτρέπει την απομακρυσμένη συλλογή των παραπάνω αρχείων καταγραφής Powershell που μόλις δημιουργήσαμε)	Απαιτείται

Παρατηρήσεις:

Επιπλέον στοιχεία καταγραφής που μπορεί να εξαχθούν	Εκτέλεση των παρακάτω στο Powershell για να γίνει προβολή του φίλτρου συμβάντων του WMI: # Reviewing WMI Subscriptions using Get-WMIObject # Event Filter Get-WMIObject -Namespace root\Subscription -Class __EventFilter -Filter “Name=’Updater’” # Event Consumer Get-WMIObject -Namespace root\Subscription -Class CommandLineEventConsumer -Filter “Name=’Updater’” # Binding Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding -Filter “__Path LIKE ‘%Updater%’”

Κεφάλαιο 8 Μελλοντικές βλέψεις – Συμπεράσματα

8.1 Μελλοντικές βλέψεις

Ο στόχος σε αυτή την έρευνα είναι να γίνει μία ρύθμιση του Sysmon μέσω της παραμετροποίησης του xml αρχείου, το οποίο ευθύνεται για τη λειτουργία του Sysmon, ώστε με τη βοήθεια του αρχείου καταγραφής των Windows να γίνεται σωστό φιλτράρισμα των συμβάντων. Τα συμβάντα στα οποία επικεντρωθήκαμε σε αυτή την έρευνα αφορούν την ανίχνευση της εσωτερικής μετακίνησης σε ένα λειτουργικό σύστημα Windows 10. Ένα μελλοντικό πρόσθετο στην έρευνα μας θα ήταν ως συνέχεια των αποτελεσμάτων της έρευνας να χρησιμοποιηθεί η στοίβα ELK ως εργαλείο συλλογής και καταγραφής των συμβάντων. Αυτό θα βοηθήσει στη δημιουργία φίλτρων ανίχνευσης και ομαδοποίησης των εργαλείων που χρησιμοποιούνται ώστε να επιτευχθεί η εσωτερική μετακίνηση.

Στη συνέχεια θα μπορούσαμε να χρησιμοποιήσουμε το Kibana το οποίο είναι ένα εργαλείο απεικόνισης της στοίβας ELK. Είναι ανοιχτού κώδικα λογισμικό το οποίο στέλνει ερωτήσεις στην ελαστική αναζήτηση και σκοπό έχει την απεικόνιση του ερωτήματος σε πίνακες ελέγχου. Μερικές από τις οπτικοποιήσεις του Kibana είναι τα ιστογράμματα, γραφήματα γραμμής, διαγράμματα πίτας, χάρτες θερμότητας κ.α.

Επίσης θα μπορούσε να δημιουργηθεί ένα GUI στο οποίο θα μπορεί κάποιος από εκεί να ενεργοποιεί ή να απενεργοποιεί τα γεγονότα τα οποία θα καταγράφονται από το αρχείο καταγραφής των Windows ώστε να μπορεί να υπάρχει μια πιο γρήγορη και πιο καθαρή καταγραφή των γεγονότων των οποίων αποτελούν αποδεικτικά στοιχεία ενός συγκεκριμένου συμβάντος το οποί θα θέλαμε να ερευνήσουμε.

8.2 Συμπεράσματα

Σε αυτή την εργασία είδαμε το πώς μπορούμε να ανιχνεύσουμε και στη συνέχεια να περιορίσουμε – αποκλείσουμε την προσπάθεια εσωτερικής μετακίνησης τόσο από την πλευρά του επιτιθέμενου όσο και από την πλευρά του αμυνόμενου. Όπως είδαμε τόσο και το Sysmon όσο και το εργαλείο καταγραφής γεγονότων των Windows έχουν πάρα πολλές επιλογές παραμετροποίησης σαν μονάδες. Σε αυτή την έρευνα καταφέραμε να συνδυάσουμε τις επιλογές των δύο εργαλείων ώστε να επιτύχουμε το σκοπό μας σε ικανοποιητικό βαθμό και να έχουμε μία αρκετά ασφαλής αναφορά σχετικά με το τι πρέπει κανείς να προσέχει και ελέγχει σε ένα λειτουργικό σύστημα που δέχεται μία επίθεση εσωτερικής μετακίνησης.

Στη σύνταξη αυτής της αναφοράς χρειάστηκε να δοκιμάσουμε εμείς οι ίδιοι την επίθεση με μία ομάδα εργαλείων χειραγώγησης ενός λειτουργικού συστήματος. Οι ομάδες των εργαλείων που δοκιμάστηκαν αφορούν την επαύξηση των δικαιωμάτων, την εκτέλεση απομακρυσμένων εντολών, την συλλογή πληροφοριών και τέλος τον έλεγχο του συστήματος.

Στο τέλος παρουσιάσαμε το σύνολο των συμβάντων που καταγράψαμε ανάλογα με την ομάδα εργαλείων που ανήκουν και πραγματοποιήθηκε η ανάλυση αυτών ανάλογα με το εργαλείο που τα ενεργοποίησε.

Κεφάλαιο 9 Αναφορές

1) John H., (11 DECEMBER 2016). SANSInstitute
2) Randy Frantlin Smith, (2009). Ultimate Windows Security
3) Mike Jacobs and Michael Satran, (2018). Documents for Windows / Windows Event Colector
4) Toni Boger and Alexander Gillis, (2013). Search Windows Server
5) Jane Devry, (2017). Cybersecurity Insiders
6) Tom Ueltschi, (2017). Advance Incident Detection and Threat Hunting using Sysmon and Splunk
7) Dr. Christopher Kruegel (2019). Lateral Movement: What it is and How to block it.
8) Jane Devry, (2017). The Hunter's Den
9) Steve Anson, (2017). Lateral Movement Analysis
10) Nader Shalabi, (2018). Utilities for Sysmon tools.
11) SwiftOnSecurity, (2018). Sysmon-Configuration (Github)
12) Mark Russinovich and Thomas Garnier, (2017). Building A Perfect Sysmon Configuration File
13) Mark Russinovich and Thomas Garnier, (2017). Sysmon: how to set up, update and use
14) Matt Graeber, (2018). Working with Sysmon.
15) Roberto Rodriguez, (2017). Chronicles of a Threat Hunter: Hunting for Remotely Executed Code via Services & Lateral Movement with Sysmon, Win Event Logs.
16) Carlos Perez, (2014). Sysinternals Sysmon 6.10 Tracking of Permanent WMI Events
17) Massimo Bozza and Pietro Romano, (2018). ADVERSARIAL APPROACH TO IMPROVE DETECTION CAPABILITIES
18) Offensive Security, (2017). Mimikatz
19) John Savill, (2016). What is Mimikatz
20) Marry Trame, (2017). Threat Hunting: Catch these modules being loaded within 1-4 seconds to detect Invoke-Mimikatz
21) Panagiotis Gkatziroulis, (2018). Preventing Mimikatz Attacks
22) Allesandro Zanni, (2007). LaZagne
23) The MITRE Corporation, (2015). Bypass User Account Control
24) The MITRE Corporation, (2015). Lateral Movement
25) Mark Russinovich, (2016). PsExec
26) Eric Milam, 2013. Smbexec
27) Thomas McCarthy, 2013. Penetration Testing
28) Mark Russinovich and Thomas Garnier, (2019). Sysmon
29) Ethan Wilansky. (2009). WMIC - Take Command-line Control over WMI
30) Chris Truncer, (2017). Running WMImplant
31) Chris Truncer (2018). WMImplant
32) Michael C. Long II (2019). Disrupting the Empire: Identifying PowerShell Empire Command and Control Activity
33) Kent Ickler, (2017). Empire Bootstrapping v2 – How to Pre-Automate All the Things!

Παράρτημα Α

```
<!
--
        sysmon-config | A Sysmon configuration focused on default high-quality event
      tracing and easy customization by the community
        Master version:     64 | Date: 2018-01-30
        Master author:      @SwiftOnSecurity, other contributors also credited in-line
      or on Git
        Master project:     https://github.com/SwiftOnSecurity/sysmon-config
        Master license:     Creative Commons Attribution 4.0 | You may privatize,
      fork, edit, teach, publish, or deploy for commercial use - with attribution in
      the text.
        Fork version:       <N/A>
        Fork author: <N/A>
        Fork project:       <N/A>
        Fork license:       <N/A>
        REQUIRED: Sysmon version 7.01 or higher (due to changes in registry syntax and
      bug-fixes)
               https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
               Note that 6.03 and 7.01 have critical fixes for filtering, it's
      recommended you stay updated.
        NOTE: To collect Sysmon logs centrally for free, see https://aka.ms/WEF.
      Command to allow log access to the Network Service:
               wevtutil.exe sl Microsoft-Windows-Sysmon/Operational
      /ca:O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)
        NOTE: Do not let the size and complexity of this configuration discourage you
      from customizing it or building your own.
               This configuration is based around known, high-signal event tracing, and
      thus appears complicated, but it's only very
               detailed. Significant effort over years has been invested in front-
      loading as much filtering as possible onto the
               client. This is to make analysis of intrusions possible by hand, and to
      try to surface anomalous activity as quickly
               as possible to any technician armed only with Event Viewer. Its purpose
      is to democratize system monitoring for all organizations.
        NOTE: Sysmon is NOT a whitelist solution or HIDS engine, it is a computer
      change and event logging tool with very basic exclude rules.
               Do NOT ignore everything possible. Sysmon's purpose is providing context
      during a threat or problem investigation. Legitimate
```

```
        processes are routinely used by threats - do not blindly exclude them.
Additionally, be mindful of process-hollowing / imitation.
  NOTE: Sysmon is not hardened against an attacker with admin rights.
Additionally, this configuration offers an attacker, willing
        to study it, many ways to evade some of the logging. If you are in a
high-threat environment, you should consider a much broader
        log-most approach. However, in the vast majority of cases, an attacker
will bumble along through multiple behavioral traps which
        this configuration monitors, especially in the first minutes.
  TECHNICAL:
  - Run sysmon.exe -? for a briefing on Sysmon configuration.
  - Other languages may require localization. Registry and Filesystem paths can
change. For example, \shell\open\command\, where "open" is localized.
  - Sysmon does not support nested/multi-conditional rules. There are only
blanket INCLUDE and EXCLUDE. "Exclude" rules override "Include" rules.
  - If you only specify exclude for a filtering subsection, everything in that
subsection is logged by default.
  - Some Sysmon monitoring abilities are not meant for widely deployed general-
purpose use due to performance impact. Depends on environment.
  - Duplicate or overlapping "Include" rules do not result in duplicate events
being logged.
  - All characters enclosed by XML tags are always interpreted literally. Sysmon
does not support wildcards (*), alternate characters, or RegEx.
  - In registry events, the value name is appended to the full key path with a
"\" delimiter. Default key values are named "\(Default)"
  - "Image" is a technical term for a compiled binary file like an EXE or DLL.
Also, it can match just the filename, or entire path.
  - "ProcessGuid" is randomly generated, assigned, and tracked by Sysmon to
assist in tracing individual process launches. Cleared on service restart.
  - "LoginGuid" is randomly generated, assigned, and tracked by Sysmon to assist
in tracing individual user sessions. Cleared on service restart.
  - Sysmon does not track which rule caused an event to be logged.
  FILTERING: Filter conditions available for use are: is, is not, contains,
excludes, begin with, end with, less than, more than, image
  - The "image" filter is usable with any field. Same as "is" but can either
match the entire string, or only the text after the last "\" in the string.
Credit: @mattifestation
  PERFORMANCE: By using "end with" you can save performance by starting a string
match at the end of a line, which usually triggers earlier.
-->
```

```
<Sysmon schemaversion="4.00">
	<!--SYSMON META CONFIG-->
	<HashAlgorithms>md5,sha256</HashAlgorithms> <!-- Both MD5 and SHA256 are the industry-standard algorithms for identifying files -->
	<CheckRevocation/> <!-- Check loaded drivers, log if their code-signing certificate has been revoked, in case malware stole one to sign a kernel driver -->

	<!-- <ImageLoad/> --> <!-- Would manually force-on ImageLoad monitoring, even without configuration below. Included only documentation. -->
	<!-- <ProcessAccessConfig/> --> <!-- Would manually force-on ProcessAccess monitoring, even without configuration below. Included only documentation. -->
	<!-- <PipeMonitoringConfig/> --> <!-- Would manually force-on PipeCreated / PipeConnected events, even without configuration below. Included only documentation. -->

	<EventFiltering>

	<!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
		<!--COMMENT:  All process launched will be included, except for what matches a rule below. It's best to be as specific as possible, to
			avoid user-mode executables imitating other process names to avoid logging, or if malware drops files in an existing directory.
			Ultimately, you must weigh CPU time checking many detailed rules, against the risk of malware exploiting the blindness created.
			Beware of Masquerading, where attackers imitate the names and paths of legitimate tools. Ideally, you'd use both file path and
			code signatures to validate, but Sysmon does not support that. Look into Windows Device Guard for whitelisting support. -->

		<!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Description, Product, Company, CommandLine, CurrentDirectory, User, LogonGuid,
```

```
LogonId, TerminalSessionId, IntegrityLevel, Hashes, ParentProcessGuid,
ParentProcessId, ParentImage, ParentCommandLine-->
                <ProcessCreate onmatch="exclude">
                        <!--SECTION: Microsoft Windows-->
                        <CommandLine condition="begin
with">C:\Windows\system32\DllHost.exe /Processid</CommandLine> <!--
Microsoft:Windows-->
                        <CommandLine
condition="is">C:\Windows\system32\SearchIndexer.exe /Embedding</CommandLine>
<!--Microsoft:Windows: Search Indexer-->
                        <Image
condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--
Microsoft:Windows: Customer Experience Improvement-->
                        <Image
condition="is">C:\Windows\system32\audiodg.exe</Image> <!--Microsoft:Windows:
Launched constantly-->
                        <Image
condition="is">C:\Windows\system32\conhost.exe</Image> <!--Microsoft:Windows:
Command line interface host process-->
                        <Image
condition="is">C:\Windows\system32\musNotification.exe</Image> <!--
Microsoft:Windows: Update pop-ups-->
                        <Image
condition="is">C:\Windows\system32\musNotificationUx.exe</Image> <!--
Microsoft:Windows: Update pop-ups-->
                        <Image
condition="is">C:\Windows\system32\powercfg.exe</Image> <!--Microsoft:Power
configuration management-->
                        <Image
condition="is">C:\Windows\system32\sndVol.exe</Image> <!--Microsoft:Windows:
Volume control-->
                        <Image
condition="is">C:\Windows\system32\sppsvc.exe</Image> <!--Microsoft:Windows:
Software Protection Service-->
                        <Image
condition="is">C:\Windows\system32\wbem\WmiApSrv.exe</Image> <!--
Microsoft:Windows: WMI performance adapter host process-->
                        <Image
condition="is">C:\Windows\System32\plasrv.exe</Image> <!--Microsoft:Windows:
Performance Logs and Alerts DCOM Server-->
```

```
                    <Image
condition="is">C:\Windows\System32\wifitask.exe</Image> <!--Microsoft:Windows:
Wireless Background Task-->
                    <Image condition="is">C:\Program Files (x86)\Common
Files\microsoft shared\ink\TabTip32.exe</Image> <!--Microsoft:Windows: Touch
Keyboard and Handwriting Panel Helper-->
                    <Image
condition="is">C:\Windows\System32\smartscreen.exe</Image> <!--
Microsoft:Windows: Smartscreen, checks malicious websites and files
https://www.howtogeek.com/320711/what-is-smartscreen-and-why-is-it-running-on-
my-pc/ -->
                    <Image
condition="is">C:\Windows\System32\msfeedssync.exe</Image> <!--
Microsoft:Windows: Microsoft Feeds Synchronization
https://superuser.com/questions/445995/msfeedssync-exe-what-does-it-do -->
                    <Image
condition="is">C:\Windows\System32\RuntimeBroker.exe</Image> <!--
Microsoft:Windows: Runtime Broker https://www.howtogeek.com/268240/what-is-
runtime-broker-and-why-is-it-running-on-my-pc/ -->
                    <Image
condition="is">C:\Windows\System32\TokenBrokerCookies.exe</Image> <!--
Microsoft:Windows: SSO sign-in assistant for MicrosoftOnline.com-->
                    <CommandLine condition="is">C:\windows\system32\wermgr.exe
-queuereporting</CommandLine> <!--Microsoft:Windows:Windows error
reporting/telemetry-->
                    <ParentCommandLine
condition="is">C:\windows\system32\wermgr.exe -
queuereporting</ParentCommandLine> <!--Microsoft:Windows:Windows error
reporting/telemetry-->
                    <CommandLine condition="begin with">
"C:\Windows\system32\wermgr.exe" "-queuereporting_svc" </CommandLine> <!--
Microsoft:Windows:Windows error reporting/telemetry-->
                    <CommandLine condition="is">C:\WINDOWS\system32\wermgr.exe
-upload</CommandLine> <!--Microsoft:Windows:Windows error reporting/telemetry-->
                    <CommandLine
condition="is">\SystemRoot\System32\smss.exe</CommandLine> <!--Microsoft:Bootup:
Windows Session Manager-->
                    <CommandLine
condition="is">\??\C:\WINDOWS\system32\autochk.exe *</CommandLine> <!--
Microsoft:Bootup: Auto Check Utility-->
```

```
                    <IntegrityLevel
condition="is">AppContainer</IntegrityLevel> <!--Microsoft:Windows: Don't care
about sandboxed processes-->
                    <ParentCommandLine condition="begin
with">%%SystemRoot%%\system32\csrss.exe
ObjectDirectory=\Windows</ParentCommandLine> <!--Microsoft:Windows:CommandShell:
Triggered when programs use the command shell, but doesn't provide attribution
for what caused it-->
                    <ParentImage
condition="is">C:\Windows\system32\SearchIndexer.exe</ParentImage> <!--
Microsoft:Windows:Search: Launches many uninteresting sub-processes-->
                    <Image
condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Microsoft:Windows:
Network file syncing-->
                    <CommandLine condition="begin
with">C:\Windows\system32\wbem\wmiprvse.exe -Embedding</CommandLine> <!--
Microsoft:Windows: WMI provider host-->
                    <CommandLine condition="begin
with">C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding</CommandLine>
<!--Microsoft:Windows: WMI provider host-->
                    <Image
condition="is">C:\Windows\system32\SppExtComObj.Exe</Image> <!--
Microsoft:Windows: KMS activation-->
                    <Image
condition="is">C:\Windows\system32\PrintIsolationHost.exe</Image> <!--
Microsoft:Windows: Printing-->
                    <!--SECTION: Microsoft:Windows:Defender-->
                    <Image condition="begin with">C:\Program Files\Windows
Defender</Image> <!--Microsoft:Windows:Defender in Win10-->
                    <Image
condition="is">C:\Windows\system32\MpSigStub.exe</Image> <!--Microsoft:Windows:
Microsoft Malware Protection Signature Update Stub-->
                    <Image condition="begin
with">C:\Windows\SoftwareDistribution\Download\Install\AM_</Image> <!--
Microsoft:Defender: Signature updates-->
                    <!--SECTION: Microsoft:Windows:svchost-->
                           <!--COMMENT: These generally not exclude sub-
processes, which may be important. Do not exclude RemoteRegistry or Schedule.-->
```

```
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k appmodel -s
StateRepository</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k appmodel</CommandLine> <!--
Microsoft:Windows 10-->
                    <CommandLine
condition="is">C:\WINDOWS\system32\svchost.exe -k appmodel -p -s
tiledatamodelsvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k camera -s
FrameServer</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k dcomlaunch -s
LSM</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k dcomlaunch -s
PlugPlay</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k defragsvc</CommandLine> <!--
Microsoft:Windows defragmentation-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k devicesflow -s
DevicesFlowUserSvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k imgsvc</CommandLine> <!--
Microsoft:The Windows Image Acquisition Service-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localService -s
EventSystem</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localService -s
bthserv</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localService -s
nsi</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localService -s
w32Time</CommandLine>
```

```
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localServiceAndNoImpersonation</CommandLine> <!--Microsoft:Windows: Network
services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localServiceNetworkRestricted
-s Dhcp</CommandLine> <!--Microsoft:Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localServiceNetworkRestricted
-s EventLog</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localServiceNetworkRestricted
-s TimeBrokerSvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localServiceNetworkRestricted
-s WFDSConMgrSvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localServiceNetworkRestricted</CommandLine> <!--Microsoft:Windows: Network
services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localServiceAndNoImpersonation
-s SensrSvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localServiceNoNetwork</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localSystemNetworkRestricted -
p -s WPDBusEnum</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localSystemNetworkRestricted -
p -s fhsvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localSystemNetworkRestricted -
s DeviceAssociationService</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localSystemNetworkRestricted -
s NcbService</CommandLine>
```

```
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localSystemNetworkRestricted -
s SensorService</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localSystemNetworkRestricted -
s TabletInputService</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localSystemNetworkRestricted -
s UmRdpService</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localSystemNetworkRestricted -
s WPDBusEnum</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k localSystemNetworkRestricted -
s WdiSystemHost</CommandLine> <!--Microsoft:Windows: Diagnostic System Host [
http://www.blackviper.com/windows-services/diagnostic-system-host/ ] -->
                    <CommandLine
condition="is">C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -
p -s WdiSystemHost</CommandLine> <!--Microsoft:Windows: Diagnostic System Host [
http://www.blackviper.com/windows-services/diagnostic-system-host/ ] -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted</CommandLine> <!--Microsoft:Windows-->
                    <CommandLine
condition="is">C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s
wlidsvc</CommandLine> <!--Microsoft:Windows: Windows Live Sign-In Assistant [
https://www.howtogeek.com/howto/30348/what-are-wlidsvc.exe-and-wlidsvcm.exe-and-
why-are-they-running/ ] -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -s
ncaSvc</CommandLine> <!--Microsoft:Windows: Network Connectivity Assistant [
http://www.blackviper.com/windows-services/network-connectivity-assistant/ ] -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
BDESVC</CommandLine> <!--Microsoft:Windows:Network: BitLocker Drive Encryption--
>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s BITS</CommandLine>
<!--Microsoft:Windows:Network: Background Intelligent File Transfer (BITS) -->
```

```
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
CertPropSvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
DsmSvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s Gpsvc</CommandLine>
<!--Microsoft:Windows:Network: Group Policy -->
                    <CommandLine
condition="is">C:\Windows\System32\svchost.exe -k netsvcs -p -s
NetSetupSvc</CommandLine> <!--Microsoft:Windows: Network Setup Service, manages
the installation of network drivers -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
ProfSvc</CommandLine> <!--Microsoft:Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s SENS</CommandLine>
<!--Microsoft:Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
SessionEnv</CommandLine> <!--Microsoft:Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
Themes</CommandLine> <!--Microsoft:Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
Winmgmt</CommandLine> <!--Microsoft:Windows: Windows Management Instrumentation
(WMI) -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs</CommandLine> <!--
Microsoft:Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k networkService -p -s
DoSvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k networkService -s
Dnscache</CommandLine> <!--Microsoft:Windows:Network: DNS caching, other uses --
>
```

```
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k networkService -s
LanmanWorkstation</CommandLine> <!--Microsoft:Windows:Network: "Workstation"
service, used for SMB file-sharing connections and RDP-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k networkService -s
NlaSvc</CommandLine> <!--Microsoft:Windows:Network: Network Location Awareness--
>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k networkService -s
TermService</CommandLine> <!--Microsoft:Windows:Network: Terminal Services
(RDP)-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k networkService</CommandLine>
<!--Microsoft:Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
networkServiceNetworkRestricted</CommandLine> <!--Microsoft:Windows: Network
services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k rPCSS</CommandLine> <!--
Microsoft:Windows Services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k secsvcs</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k swprv</CommandLine> <!--
Microsoft:Software Shadow Copy Provider-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k unistackSvcGroup</CommandLine>
<!--Microsoft:Windows 10-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k utcsvc</CommandLine> <!--
Microsoft:Windows Services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k wbioSvcGroup</CommandLine> <!-
-Microsoft:Windows Services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k werSvcGroup</CommandLine> <!--
Microsoft:Windows: ErrorReporting-->
```

```
                    <CommandLine
condition="is">C:\WINDOWS\System32\svchost.exe -k wsappx -p -s
ClipSVC</CommandLine> <!--Microsoft:Windows:Apps: Client License Service-->
                    <CommandLine
condition="is">C:\WINDOWS\system32\svchost.exe -k wsappx -p -s
AppXSvc</CommandLine> <!--Microsoft:Windows:Apps: AppX Deployment Service-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k wsappx -s
ClipSVC</CommandLine> <!--Microsoft:Windows:Apps: Client License Service-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k wsappx</CommandLine> <!--
Microsoft:Windows:Apps [ https://www.howtogeek.com/320261/what-is-wsappx-and-
why-is-it-running-on-my-pc/ ] -->
                    <ParentCommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs</ParentCommandLine>
<!--Microsoft:Windows: Network services: Spawns Consent.exe-->
                    <ParentCommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted</ParentCommandLine> <!--Microsoft:Windows-->
                    <!--SECTION: Microsoft:dotNet-->
                    <CommandLine condition="begin
with">C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe</CommandLine> <!--
Microsoft:DotNet-->
                    <Image
condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe</Ima
ge> <!--Microsoft:DotNet-->
                    <Image
condition="is">C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe</Image
> <!--Microsoft:DotNet-->
                    <Image
condition="is">C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCac
he.exe</Image> <!--Microsoft:Windows: Font cache service-->
                    <ParentCommandLine
condition="contains">C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngentask.ex
e</ParentCommandLine>
                    <ParentImage
condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe</Par
entImage> <!--Microsoft:DotNet-->
```

```
                    <ParentImage
condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngentask.exe</Par
entImage> <!--Microsoft:DotNet-->
                    <ParentImage
condition="is">C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe</Paren
tImage> <!--Microsoft:DotNet-->
                    <ParentImage
condition="is">C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe</Paren
tImage> <!--Microsoft:DotNet: Spawns thousands of ngen.exe processes-->
                    <!--SECTION: Microsoft:Office-->
                    <Image condition="is">C:\Program Files\Microsoft
Office\Office16\MSOSYNC.EXE</Image> <!--Microsoft:Office: Background process for
SharePoint/Office365 connectivity-->
                    <Image condition="is">C:\Program Files (x86)\Microsoft
Office\Office16\MSOSYNC.EXE</Image> <!--Microsoft:Office: Background process for
SharePoint/Office365 connectivity-->
                    <Image condition="is">C:\Program Files\Microsoft
Office\Office15\MSOSYNC.EXE</Image> <!--Microsoft:Office: Background process for
SharePoint/Office365 connectivity-->
                    <Image condition="is">C:\Program Files\Common
Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE</Image> <!--
Microsoft:Office: Licensing service-->
                    <Image condition="is">C:\Program Files\Microsoft
Office\Office16\msoia.exe</Image> <!--Microsoft:Office: Telemetry collector-->
                    <Image condition="is">C:\Program Files (x86)\Microsoft
Office\root\Office16\officebackgroundtaskhandler.exe</Image>
                    <!--SECTION: Microsoft:Office:Click2Run-->
                    <Image condition="is">C:\Program Files\Common
Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe</Image> <!--
Microsoft:Office: Background process-->
                    <ParentImage condition="end with">C:\Program Files\Common
Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe</ParentImage> <!--
Microsoft:Office: Background process-->
                    <ParentImage condition="is">C:\Program Files\Common
Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe</ParentImage> <!--
Microsoft:Office: Background process-->
                    <!--SECTION: Microsoft:Windows: Media player-->
                    <Image condition="is">C:\Program Files\Windows Media
Player\wmpnscfg.exe</Image> <!--Microsoft:Windows: Windows Media Player Network
Sharing Service Configuration Application-->
```

```
                    <!--SECTION: Google-->
                    <CommandLine condition="begin with">"C:\Program Files
(x86)\Google\Chrome\Application\chrome.exe" --type=</CommandLine> <!--
Google:Chrome: massive command-line arguments-->
                    <CommandLine condition="begin with">"C:\Program
Files\Google\Chrome\Application\chrome.exe" --type=</CommandLine> <!--
Google:Chrome: massive command-line arguments-->
                    <Image condition="begin with">C:\Program Files
(x86)\Google\Update\</Image> <!--Google:Chrome:Updater: You should experiment
with this line since attackers sometimes hide in this folder-->
                    <ParentImage condition="begin with">C:\Program Files
(x86)\Google\Update\</ParentImage> <!--Google:Chrome:Updater: You should
experiment with this line since attackers sometimes hide in this folder-->
                    <!--SECTION: Firefox-->
                    <CommandLine condition="begin with">"C:\Program
Files\Mozilla Firefox\plugin-container.exe" --channel</CommandLine> <!--
Mozilla:Firefox: Large command-line arguments | Credit @Darkbat91 -->
                    <CommandLine condition="begin with">"C:\Program Files
(x86)\Mozilla Firefox\plugin-container.exe" --channel</CommandLine> <!--
Mozilla:Firefox: Large command-line arguments | Credit @Darkbat91 -->
                    <!--SECTION: Adobe-->
                    <CommandLine condition="contains">AcroRd32.exe" /CR
</CommandLine> <!--Adobe:AcrobatReader: Uninteresting sandbox subprocess-->
                    <CommandLine condition="contains">AcroRd32.exe" --
channel=</CommandLine> <!--Adobe:AcrobatReader: Uninteresting sandbox
subprocess-->
                    <ParentImage condition="end with">C:\Program Files
(x86)\Common Files\Adobe\AdobeGCClient\AGSService.exe</ParentImage>
                    <!--SECTION: Adobe:Acrobat DC-->
                    <Image condition="end with">C:\Program Files
(x86)\Adobe\Acrobat DC\Acrobat\AcroCEF\AcroCEF.exe</Image> <!--Adobe:Acrobat:
Sandbox subprocess, still evaluating security exposure-->
                    <Image condition="end with">C:\Program Files
(x86)\Adobe\Acrobat DC\Acrobat\LogTransport2.exe</Image> <!--Adobe: Telemetry [
https://forums.adobe.com/thread/1006701 ] -->
                    <!--SECTION: Adobe:Acrobat 2015-->
                    <Image condition="end with">C:\Program Files
(x86)\Adobe\Acrobat 2015\Acrobat\AcroCEF\AcroCEF.exe</Image> <!--Adobe:Acrobat:
Sandbox subprocess, still evaluating security exposure-->
```

```
                    <Image condition="end with">C:\Program Files
(x86)\Adobe\Acrobat 2015\Acrobat\LogTransport2.exe</Image> <!--Adobe: Telemetry
[ https://forums.adobe.com/thread/1006701 ] -->
                    <!--SECTION: Adobe:Acrobat Reader DC-->
                    <Image condition="end with">C:\Program Files
(x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe</Image> <!--
Adobe:AcrobatReader: Sandbox subprocess, still evaluating security exposure-->
                    <Image condition="end with">C:\Program Files
(x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe</Image> <!--Adobe:
Telemetry [ https://forums.adobe.com/thread/1006701 ] -->
                    <!--SECTION: Adobe:Flash-->
                    <Image condition="end
with">C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe</Image>
<!--Adobe:Flash: Properly hardened updater, not a risk-->
                    <!--SECTION: Adobe:Updater-->
                    <Image condition="end with">C:\Program Files (x86)\Common
Files\Adobe\ARM\1.0\AdobeARM.exe</Image> <!--Adobe:Updater: Properly hardened
updater, not a risk-->
                    <ParentImage condition="end with">C:\Program Files
(x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe</ParentImage> <!--Adobe:Updater:
Properly hardened updater, not a risk-->
                    <Image condition="end with">C:\Program Files (x86)\Common
Files\Adobe\ARM\1.0\armsvc.exe</Image> <!--Adobe:Updater: Properly hardened
updater, not a risk-->
                    <!--SECTION: Adobe:Supporting processes-->
                    <Image condition="end with">C:\Program Files
(x86)\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe</Image>
                    <Image condition="end with">C:\Program Files (x86)\Common
Files\Adobe\Adobe Desktop Common\HEX\Adobe CEF Helper.exe</Image>
                    <Image condition="end with">C:\Program Files (x86)\Common
Files\Adobe\AdobeGCClient\AdobeGCClient.exe</Image> <!--Adobe:Creative Cloud-->
                    <Image condition="end with">C:\Program Files (x86)\Common
Files\Adobe\OOBE\PDApp\P6\adobe_licutil.exe</Image> <!--Adobe:License utility-->
                    <Image condition="end with">C:\Program Files (x86)\Common
Files\Adobe\OOBE\PDApp\P7\adobe_licutil.exe</Image> <!--Adobe:License utility-->
                    <ParentImage condition="end with">C:\Program Files
(x86)\Common Files\Adobe\OOBE\PDApp\P7\adobe_licutil.exe</ParentImage> <!--
Adobe:License utility-->
                    <Image condition="end with">C:\Program Files (x86)\Common
Files\Adobe\OOBE\PDApp\UWA\updaterstartuputility.exe</Image>
```

```
                    <ParentImage condition="end with">C:\Program Files
(x86)\Common Files\Adobe\OOBE\PDApp\UWA\updaterstartuputility.exe</ParentImage>
                    <!--SECTION: Adobe:Creative Cloud-->
                    <Image condition="end with">C:\Program Files
(x86)\Adobe\Adobe Creative Cloud\ACC\Creative Cloud.exe</Image>
                    <ParentImage condition="end with">C:\Program Files
(x86)\Adobe\Adobe Creative Cloud\ACC\Creative Cloud.exe</ParentImage>
                    <ParentImage condition="end with">C:\Program Files
(x86)\Adobe\Adobe Creative Cloud\CCXProcess\CCXProcess.exe</ParentImage>
                    <ParentImage condition="end with">C:\Program Files
(x86)\Adobe\Adobe Creative Cloud\CoreSync\CoreSync.exe</ParentImage>
                    <!--SECTION: Cisco-->
                    <ParentImage condition="end with">C:\Program Files
(x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnagent.exe</ParentImage>
<!--Cisco: Calls netsh to change settings on connect-->
                    <!--SECTION: Drivers-->
                           <!--COMMENT: Attackers sometimes hide themselves in
the folders of drivers, be careful to only exclude what is clogging events-->
                    <CommandLine condition="begin with">"C:\Program
Files\DellTPad\ApMsgFwd.exe" -s{</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\igfxsrvc.exe -Embedding</CommandLine>
                    <ParentImage condition="end with">C:\Program
Files\DellTPad\HidMonitorSvc.exe</ParentImage>
                    <ParentImage condition="end with">C:\Program
Files\Realtek\Audio\HDA\RtkAudioService64.exe</ParentImage> <!--Realtek:Driver:
routine actions-->
                    <!--SECTION: Dropbox-->
                    <Image condition="end with">C:\Program Files
(x86)\Dropbox\Update\DropboxUpdate.exe</Image> <!--Dropbox:Updater: Lots of
command-line arguments-->
                    <ParentImage condition="end with">C:\Program Files
(x86)\Dropbox\Update\DropboxUpdate.exe</ParentImage>
                    <!--SECTION: Dell-->
                    <ParentImage condition="is">C:\Program Files
(x86)\Dell\CommandUpdate\InvColPC.exe</ParentImage> <!--Dell:CommandUpdate:
Detection process-->
                    <Image condition="is">C:\Program
Files\Dell\SupportAssist\pcdrcui.exe</Image> <!--Dell:SupportAssist: routine
actions-->
```

```
                    <Image condition="is">C:\Program
Files\Dell\SupportAssist\koala.exe</Image> <!--Dell:SupportAssist: routine
actions-->
                    <ParentCommandLine condition="end with">"-
outc=C:\ProgramData\Dell\CommandUpdate\inventory.xml" "-
logc=C:\ProgramData\Dell\CommandUpdate\scanerrs.xml" "-lang=en" "-enc=UTF-16"
</ParentCommandLine>
             </ProcessCreate>


      <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE
FILESYSTEM [FileCreateTime]-->
             <!--COMMENT:   [ https://attack.mitre.org/wiki/Technique/T1099 ] -
->


             <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename,
CreationUtcTime, PreviousCreationUtcTime-->
             <FileCreateTime onmatch="include">
                    <Image condition="begin with">C:\Users</Image> <!--Look
for timestomping in user area-->
             </FileCreateTime>


             <FileCreateTime onmatch="exclude">
                    <Image condition="image">OneDrive.exe</Image> <!--OneDrive
constantly changes file times-->
                    <Image
condition="image">C:\Windows\system32\backgroundTaskHost.exe</Image>
                    <Image condition="contains">setup</Image> <!--Ignore
setups-->
                    <Image condition="contains">install</Image> <!--Ignore
setups-->
                    <Image condition="contains">Update\</Image> <!--Ignore
setups-->
                    <Image condition="end with">redist.exe</Image> <!--Ignore
setups-->
                    <Image condition="is">msiexec.exe</Image> <!--Ignore
setups-->
```

```
                <Image condition="is">TrustedInstaller.exe</Image> <!--
Ignore setups-->
                </FileCreateTime>


        <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
                <!--COMMENT:   By default this configuration takes a very
conservative approach to network logging, limited to only extremely high-signal
events.-->
                <!--COMMENT:   [ https://attack.mitre.org/wiki/Command_and_Control
] [ https://attack.mitre.org/wiki/Exfiltration ] [
https://attack.mitre.org/wiki/Lateral_Movement ] -->
                <!--TECHNICAL: For the DestinationHostname, Sysmon uses the
GetNameInfo API, which will often not have any information, and may just be a
CDN. This is NOT reliable for filtering.-->
                <!--TECHNICAL: For the DestinationPortName, Sysmon uses the
GetNameInfo API for the friendly name of ports you see in logs.-->
                <!--TECHNICAL: These exe do not initiate their connections, and
thus includes do not work in this section: BITSADMIN NLTEST-->

                <!-- https://www.first.org/resources/papers/conf2017/APT-Log-
Analysis-Tracking-Attack-Tools-by-Audit-Policy-and-Sysmon.pdf -->


                <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, User, Protocol,
Initiated, SourceIsIpv6, SourceIp, SourceHostname, SourcePort, SourcePortName,
DestinationIsIpV6, DestinationIp, DestinationHostname, DestinationPort,
DestinationPortName-->
                <NetworkConnect onmatch="include">
                        <!--Suspicious sources for network-connecting binaries-->
                        <Image condition="begin with">C:\Users</Image> <!--Tools
downloaded by users can use other processes for networking, but this is a very
valuable indicator.-->
                        <Image condition="begin with">C:\ProgramData</Image> <!--
Normally, network communications should be sourced from "Program Files" not from
ProgramData, something to look at-->
                        <Image condition="begin with">C:\Windows\Temp</Image> <!--
Suspicious anything would communicate from the system-level temp directory-->
                        <!--Suspicious Windows tools-->
```

```
                    <Image condition="image">at.exe</Image> <!--
Microsoft:Windows: Remote task scheduling, removed in Win10 | Credit @ion-storm
-->
                    <Image condition="image">certutil.exe</Image> <!--
Microsoft:Windows: Certificate tool can contact outbound | Credit @ion-storm
@FVT [ https://twitter.com/FVT/status/834433734602530817 ] -->
                    <Image condition="image">cmd.exe</Image> <!--
Microsoft:Windows: Remote command prompt-->
                    <Image condition="image">cmstp.exe</Image> <!--
Microsoft:Windows: Connection manager profiles can launch executables from
WebDAV [ https://twitter.com/NickTyrer/status/958450014111633408 ] | Credit
@NickTyrer @Oddvarmoe @KyleHanslovan @subTee -->
                    <Image condition="image">cscript.exe</Image> <!--
Microsoft:WindowsScriptingHost: | Credit @Cyb3rOps [
https://gist.github.com/Neo23x0/a4b4af9481e01e749409 ] -->
                    <Image condition="image">driverquery.exe</Image> <!--
Microsoft:Windows: Remote recognisance of system configuration,
oudated/vulnerable drivers -->
                    <Image condition="image">dsquery.exe</Image> <!--
Microsoft: Query Active Directory -->
                    <Image condition="image">hh.exe</Image> <!--
Microsoft:Windows: HTML Help Executable, opens CHM files -->
                    <Image condition="image">infDefaultInstall.exe</Image> <!
-Microsoft: [ https://github.com/huntresslabs/evading-autoruns ] | Credit
@KyleHanslovan -->
                    <Image condition="image">java.exe</Image> <!--Java:
Monitor usage of vulnerable application and init from JAR files | Credit @ion-
storm -->
                    <Image condition="image">javaw.exe</Image> <!--Java:
Monitor usage of vulnerable application and init from JAR files -->
                    <Image condition="image">javaws.exe</Image> <!--Java:
Monitor usage of vulnerable application and init from JAR files -->
                    <Image condition="image">mmc.exe</Image> <!--
Microsoft:Windows: -->
                    <Image condition="image">msbuild.exe</Image> <!--
Microsoft:Windows: [ https://www.hybrid-
analysis.com/sample/a314f6106633fba4b70f9d6ddbee452e8f8f44a72117749c21243dc93c7e
d3ac?environmentId=100 ] -->
```

```
                    <Image condition="image">mshta.exe</Image> <!--
Microsoft:Windows: HTML application executes scripts without IE protections |
Credit @ion-storm [ https://en.wikipedia.org/wiki/HTML_Application ] -->
                    <Image condition="image">msiexec.exe</Image> <!--
Microsoft:Windows: Can install from http:// paths | Credit @vector-sec -->
                    <Image condition="image">nbtstat.exe</Image> <!--
Microsoft:Windows: NetBIOS statistics, attackers use to enumerate local network
-->
                    <Image condition="image">net.exe</Image> <!--
Microsoft:Windows: Note - May not detect anything, net.exe is a front-end to
lower APIs | Credit @ion-storm -->
                    <Image condition="image">net1.exe</Image> <!--
Microsoft:Windows: Launched by "net.exe", but it may not detect connections
either -->
                    <Image condition="image">notepad.exe</Image> <!--
Microsoft:Windows: [ https://secrary.com/ReversingMalware/CoinMiner/ ] [
https://blog.cobaltstrike.com/2013/08/08/why-is-notepad-exe-connecting-to-the-
internet/ ] -->
                    <Image condition="image">nslookup.exe</Image> <!--
Microsoft:Windows: Retrieve data over DNS -->
                    <Image condition="image">powershell.exe</Image> <!--
Microsoft:Windows: PowerShell interface-->
                    <Image condition="image">qprocess.exe</Image> <!--
Microsoft:Windows: [ https://www.first.org/resources/papers/conf2017/APT-Log-
Analysis-Tracking-Attack-Tools-by-Audit-Policy-and-Sysmon.pdf ] -->
                    <Image condition="image">qwinsta.exe</Image> <!--
Microsoft:Windows: Query remote sessions | Credit @ion-storm -->
                    <Image condition="image">qwinsta.exe</Image> <!--
Microsoft:Windows: Remotely query login sessions on a server or workstation |
Credit @ion-storm -->
                    <Image condition="image">reg.exe</Image> <!--
Microsoft:Windows: Remote Registry editing ability | Credit @ion-storm -->
                    <Image condition="image">regsvcs.exe</Image> <!--
Microsoft:Windows: [ https://www.hybrid-
analysis.com/sample/3f94d7080e6c5b8f59eeecc3d44f7e817b31562caeba21d02ad705a0bfc6
3d67?environmentId=100 ] -->
                    <Image condition="image">regsvr32.exe</Image> <!--
Microsoft:Windows: [ https://subt0x10.blogspot.com/2016/04/bypass-application-
whitelisting-script.html ] -->
```

```
                    <Image condition="image">rundll32.exe</Image> <!--
Microsoft:Windows: [ https://blog.cobaltstrike.com/2016/07/22/why-is-rundll32-
exe-connecting-to-the-internet/ ] -->
                    <Image condition="image">rwinsta.exe</Image> <!--
Microsoft:Windows: Disconnect remote sessions | Credit @ion-storm -->
                    <Image condition="image">sc.exe</Image> <!--
Microsoft:Windows: Remotely change Windows service settings | Credit @ion-storm
-->
                    <Image condition="image">schtasks.exe</Image> <!--
Microsoft:Windows: Command-line interface to local and remote tasks -->
                    <Image condition="image">taskkill.exe</Image> <!--
Microsoft:Windows: Kill processes, has remote ability -->
                    <Image condition="image">tasklist.exe</Image> <!--
Microsoft:Windows: List processes, has remote ability -->
                    <Image condition="image">wmic.exe</Image> <!--
Microsoft:WindowsManagementInstrumentation: Credit @Cyb3rOps [
https://gist.github.com/Neo23x0/a4b4af9481e01e749409 ] -->
                    <Image condition="image">wscript.exe</Image> <!--
Microsoft:WindowsScriptingHost: | Credit @arekfurt -->
                    <!--Relevant 3rd Party Tools-->
                    <Image condition="image">nc.exe</Image> <!-- Nmap's modern
version of netcat [ https://nmap.org/ncat/guide/index.html#ncat-overview ] [
https://securityblog.gr/1517/create-backdoor-in-windows-with-ncat/ ] -->
                    <Image condition="image">ncat.exe</Image> <!-- Nmap's
modern version of netcat [ https://nmap.org/ncat/guide/index.html#ncat-overview
] [ https://securityblog.gr/1517/create-backdoor-in-windows-with-ncat/ ] -->
                    <Image condition="image">psexec.exe</Image> <!--
Sysinternals:PsExec client side | Credit @Cyb3rOps -->
                    <Image condition="image">psexesvc.exe</Image> <!--
Sysinternals:PsExec server side | Credit @Cyb3rOps -->
                    <Image condition="image">tor.exe</Image> <!--Tor [
https://www.hybrid-
analysis.com/sample/800bf028a23440134fc834efc5c1e02cc70f05b2e800bbc285d7c92a4b12
6b1c?environmentId=100 ] -->
                    <Image condition="image">vnc.exe</Image> <!-- VNC client |
Credit @Cyb3rOps -->
                    <Image condition="image">vncservice.exe</Image> <!-- VNC
server | Credit @Cyb3rOps -->
                    <Image condition="image">vncviewer.exe</Image> <!-- VNC
client | Credit @Cyb3rOps -->
```

```
                    <Image condition="image">winexesvc.exe</Image> <!-- Winexe
service executable | Credit @Cyb3rOps -->
                    <Image condition="image">nmap.exe</Image>
                    <Image condition="image">psinfo.exe</Image>
                    <!--Ports: Suspicious-->
                    <DestinationPort condition="is">22</DestinationPort> <!--
SSH protocol, monitor admin connections-->
                    <DestinationPort condition="is">23</DestinationPort> <!--
Telnet protocol, monitor admin connections, insecure-->
                    <DestinationPort condition="is">25</DestinationPort> <!--
SMTP mail protocol port, insecure, used by threats-->
                    <DestinationPort condition="is">142</DestinationPort> <!--
IMAP mail protocol port, insecure, used by threats-->
                    <DestinationPort condition="is">3389</DestinationPort> <!-
-Microsoft:Windows:RDP: Monitor admin connections-->
                    <DestinationPort condition="is">5800</DestinationPort> <!-
-VNC protocol: Monitor admin connections, often insecure-->
                    <DestinationPort condition="is">5900</DestinationPort> <!-
-VNC protocol Monitor admin connections, often insecure-->
                    <!--Ports: Proxy-->
                    <DestinationPort condition="is">1080</DestinationPort> <!-
-Socks proxy port | Credit @ion-storm-->
                    <DestinationPort condition="is">3128</DestinationPort> <!-
-Socks proxy port | Credit @ion-storm-->
                    <DestinationPort condition="is">8080</DestinationPort> <!-
-Socks proxy port | Credit @ion-storm-->
                    <!--Ports: Tor-->
                    <DestinationPort condition="is">1723</DestinationPort> <!-
-Tor protocol [ https://attack.mitre.org/wiki/Technique/T1090 ] | Credit @ion-
storm-->
                    <DestinationPort condition="is">4500</DestinationPort> <!-
-Tor protocol, also triggers on IPsec [
https://attack.mitre.org/wiki/Technique/T1090 ] | Credit @ion-storm-->
                    <DestinationPort condition="is">9001</DestinationPort> <!-
-Tor protocol [ http://www.computerworlduk.com/tutorial/security/tor-enterprise-
2016-blocking-malware-darknet-use-rogue-nodes-3633907/ ] -->
                    <DestinationPort condition="is">9030</DestinationPort> <!-
-Tor protocol [ http://www.computerworlduk.com/tutorial/security/tor-enterprise-
2016-blocking-malware-darknet-use-rogue-nodes-3633907/ ] -->
                </NetworkConnect>
```

```
		<NetworkConnect onmatch="exclude">
			<!--COMMENT: Unfortunately, these exclusions are very broad and easily abused, but it's a limitation of Sysmon rules that they can't be more specific as they're in user folders-->
			<Image condition="image">Spotify.exe</Image> <!--Spotify-->
			<Image condition="end with">AppData\Roaming\Dropbox\bin\Dropbox.exe</Image> <!--Dropbox-->
			<Image condition="image">g2ax_comm_expert.exe</Image> <!--GoToMeeting-->
			<Image condition="image">g2mcomm.exe</Image> <!--GoToMeeting-->
			<!--SECTION: Microsoft-->
			<Image condition="image">OneDrive.exe</Image> <!--Microsoft:OneDrive-->
			<Image condition="image">OneDriveStandaloneUpdater.exe</Image> <!--Microsoft:OneDrive-->
			<Image condition="end with">AppData\Local\Microsoft\Teams\current\Teams.exe</Image> <!--Microsoft: Teams-->
			<DestinationHostname condition="end with">microsoft.com</DestinationHostname> <!--Microsoft:Update delivery-->
			<DestinationHostname condition="end with">microsoft.com.akadns.net</DestinationHostname> <!--Microsoft:Update delivery-->
			<DestinationHostname condition="end with">microsoft.com.nsatc.net</DestinationHostname> <!--Microsoft:Update delivery-->
			<!--Section: Loopback Addresses-->
			<DestinationIp condition="is">127.0.0.1</DestinationIp>
			<DestinationIp condition="begin with">fe80:0:0:0</DestinationIp>
		</NetworkConnect>


	<!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON STATUS MESSAGES-->
```

```
		<!--DATA: UtcTime, State, Version, SchemaVersion-->
		<!--Cannot be filtered.-->


	<!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
		<!--COMMENT:  Useful data in building infection timelines.-->


		<!--DATA: UtcTime, ProcessGuid, ProcessId, Image-->
		<ProcessTerminate onmatch="include">
			<Image condition="begin with">C:\Users</Image> <!--Process
terminations by user binaries-->
		</ProcessTerminate>


		<ProcessTerminate onmatch="exclude">
		</ProcessTerminate>


	<!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
		<!--COMMENT:  Because drivers with bugs can be used to escalate
to kernel permissions, be extremely selective
			about what you exclude from monitoring. Low event volume,
little incentive to exclude.
			[ https://attack.mitre.org/wiki/Technique/T1014 ] -->
		<!--TECHNICAL: Sysmon will check the signing certificate
revocation status of any driver you don't exclude.-->


		<!--DATA: UtcTime, ImageLoaded, Hashes, Signed, Signature,
SignatureStatus-->
		<DriverLoad onmatch="exclude">
			<Signature condition="contains">microsoft</Signature> <!--
Exclude signed Microsoft drivers-->
			<Signature condition="contains">windows</Signature> <!--
Exclude signed Microsoft drivers-->
			<Signature condition="begin with">Intel </Signature> <!--
Exclude signed Intel drivers-->
		</DriverLoad>
```

```
		<!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
			<!--COMMENT:  Can cause high system load, disabled by default.-->
			<!--COMMENT:  [ https://attack.mitre.org/wiki/Technique/T1073 ] [
https://attack.mitre.org/wiki/Technique/T1038 ] [
https://attack.mitre.org/wiki/Technique/T1034 ] -->

			<!--DATA: UtcTime, ProcessGuid, ProcessId, Image, ImageLoaded,
Hashes, Signed, Signature, SignatureStatus-->
			<ImageLoad onmatch="include">
			</ImageLoad>

		<!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
			<!--COMMENT:  Monitor for processes injecting code into other
processes. Often used by malware to cloak their actions. Also when Firefox loads
Flash.
			[ https://attack.mitre.org/wiki/Technique/T1055 ] -->

			<!--DATA: UtcTime, SourceProcessGuid, SourceProcessId,
SourceImage, TargetProcessId, TargetImage, NewThreadId, StartAddress,
StartModule, StartFunction-->
			<CreateRemoteThread onmatch="exclude">
				<!--COMMENT: Exclude mostly-safe sources and log anything
else.-->
				<SourceImage
condition="is">C:\Windows\system32\wbem\WmiPrvSE.exe</SourceImage>
				<SourceImage
condition="is">C:\Windows\system32\svchost.exe</SourceImage>
				<SourceImage
condition="is">C:\Windows\system32\wininit.exe</SourceImage>
				<SourceImage
condition="is">C:\Windows\system32\csrss.exe</SourceImage>
				<SourceImage
condition="is">C:\Windows\system32\services.exe</SourceImage>
				<SourceImage
condition="is">C:\Windows\system32\winlogon.exe</SourceImage>
```

```
                    <SourceImage
condition="is">C:\Windows\system32\audiodg.exe</SourceImage>
                    <StartModule
condition="is">C:\Windows\system32\kernel32.dll</StartModule>
                    <TargetImage condition="end
with">Google\Chrome\Application\chrome.exe</TargetImage>
                    <SourceImage condition="is">C:\Program Files
(x86)\Webroot\WRSA.exe</SourceImage>
             </CreateRemoteThread>


      <!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
             <!--EVENT 9: "RawAccessRead detected"-->
             <!--COMMENT:  Can cause high system load, disabled by default.-->
             <!--COMMENT:  Monitor for raw sector-level access to the disk,
often used to bypass access control lists or access locked files.
                    Disabled by default since including even one entry here
activates this component. Reward/performance/rule maintenance decision.
                    Encourage you to experiment with this feature yourself. [
https://attack.mitre.org/wiki/Technique/T1067 ] -->
             <!--COMMENT:  You will likely want to set this to a full capture
on domain controllers, where no process should be doing raw reads.-->


             <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, Device-->
             <RawAccessRead onmatch="include">
             </RawAccessRead>


      <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
             <!--EVENT 10: "Process accessed"-->
             <!--COMMENT:  Can cause high system load, disabled by default.-->
             <!--COMMENT:  Monitor for processes accessing other process'
memory.-->


             <!--DATA: UtcTime, SourceProcessGuid, SourceProcessId,
SourceThreadId, SourceImage, TargetProcessGuid, TargetProcessId, TargetImage,
GrantedAccess, CallTrace-->
             <ProcessAccess onmatch="include">
```

```
		</ProcessAccess>


	<!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
		<!--EVENT 11: "File created"-->
		<!--NOTE:	Other filesystem "minifilters" can make it appear to Sysmon that some files are being written twice. This is not a Sysmon issue, per Mark Russinovich.-->
		<!--NOTE:	You may not see files detected by antivirus. Other filesystem minifilters, like antivirus, can act before Sysmon receives the alert a file was written.-->


		<!--DATA: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename, CreationUtcTime-->
		<FileCreate onmatch="include">
			<TargetFilename condition="contains">\Start Menu</TargetFilename> <!--Microsoft:Windows: Startup links and shortcut modification [ https://attack.mitre.org/wiki/Technique/T1023 ] -->
			<TargetFilename condition="contains">\Startup\</TargetFilename> <!--Microsoft:Office: Changes to user's auto-launched files and shortcuts-->
			<TargetFilename condition="contains">\Content.Outlook\</TargetFilename> <!--Microsoft:Outlook: attachments-->
			<TargetFilename condition="contains">\Downloads\</TargetFilename> <!--Downloaded files. Does not include "Run" files in IE-->
			<TargetFilename condition="end with">.application</TargetFilename> <!--Microsoft:ClickOnce: [ https://blog.netspi.com/all-you-need-is-one-a-clickonce-love-story/ ] -->
			<TargetFilename condition="end with">.appref-ms</TargetFilename> <!--Microsoft:ClickOnce application | Credit @ion-storm -->
			<TargetFilename condition="end with">.bat</TargetFilename> <!--Batch scripting-->
			<TargetFilename condition="end with">.chm</TargetFilename>
			<TargetFilename condition="end with">.cmd</TargetFilename> <!--Batch scripting: Batch scripts can also use the .cmd extension | Credit: @mmazanec -->
```

```
                    <TargetFilename condition="end
with">.cmdline</TargetFilename> <!--Microsoft:dotNet: Executed by cvtres.exe-->
                    <TargetFilename condition="end with">.dmp</TargetFilename>
<!--Process dumps [ (fr) http://blog.gentilkiwi.com/securite/mimikatz/minidump ]
-->
                    <TargetFilename condition="end
with">.docm</TargetFilename> <!--Microsoft:Office:Word: Macro-->
                    <TargetFilename condition="end with">.exe</TargetFilename>
<!--Executable-->
                    <TargetFilename condition="end with">.jar</TargetFilename>
<!--Java applets-->
                    <TargetFilename condition="end
with">.jnlp</TargetFilename> <!--Java applets-->
                    <TargetFilename condition="end with">.jse</TargetFilename>
<!--Scripting [ Example: https://www.sophos.com/en-us/threat-center/threat-
analyses/viruses-and-spyware/Mal~Phires-C/detailed-analysis.aspx ] -->
                    <TargetFilename condition="end with">.hta</TargetFilename>
<!--Scripting-->
                    <TargetFilename condition="end
with">.pptm</TargetFilename> <!--Microsoft:Office:Word: Macro-->
                    <TargetFilename condition="end with">.ps1</TargetFilename>
<!--PowerShell [ More information:
http://www.hexacorn.com/blog/2014/08/27/beyond-good-ol-run-key-part-16/ ] -->
                    <TargetFilename condition="end with">.sys</TargetFilename>
<!--System driver files-->
                    <TargetFilename condition="end with">.scr</TargetFilename>
<!--System driver files-->
                    <TargetFilename condition="end with">.vbe</TargetFilename>
<!--VisualBasicScripting-->
                    <TargetFilename condition="end with">.vbs</TargetFilename>
<!--VisualBasicScripting-->
                    <TargetFilename condition="end
with">.xlsm</TargetFilename> <!--Microsoft:Office:Word: Macro-->
                    <TargetFilename condition="end
with">proj</TargetFilename><!--Microsoft:MSBuild:Script: More information:
https://twitter.com/subTee/status/885919612969394177-->
                    <TargetFilename condition="end
with">.sln</TargetFilename><!--Microsoft:MSBuild:Script: More information:
https://twitter.com/subTee/status/885919612969394177-->
```

```
                    <TargetFilename condition="begin
with">C:\Users\Default</TargetFilename> <!--Microsoft:Windows: Changes to
default user profile-->
                    <TargetFilename condition="begin
with">C:\Windows\system32\Drivers</TargetFilename> <!--Microsoft: Drivers
dropped here-->
                    <TargetFilename condition="begin
with">C:\Windows\SysWOW64\Drivers</TargetFilename> <!--Microsoft: Drivers
dropped here-->
                    <TargetFilename condition="begin
with">C:\Windows\system32\GroupPolicy\Machine\Scripts</TargetFilename> <!--Group
policy [ More information: http://www.hexacorn.com/blog/2017/01/07/beyond-good-
ol-run-key-part-52/ ] -->
                    <TargetFilename condition="begin
with">C:\Windows\system32\GroupPolicy\User\Scripts</TargetFilename> <!--Group
policy [ More information: http://www.hexacorn.com/blog/2017/01/07/beyond-good-
ol-run-key-part-52/ ] -->
                    <TargetFilename condition="begin
with">C:\Windows\system32\Wbem</TargetFilename> <!--Microsoft:WMI: [ More
information:
http://2014.hackitoergosum.org/slides/day1_WMI_Shell_Andrei_Dumitrescu.pdf ] -->
                    <TargetFilename condition="begin
with">C:\Windows\SysWOW64\Wbem</TargetFilename> <!--Microsoft:WMI: [ More
information:
http://2014.hackitoergosum.org/slides/day1_WMI_Shell_Andrei_Dumitrescu.pdf ] -->
                    <TargetFilename condition="begin
with">C:\Windows\system32\WindowsPowerShell</TargetFilename> <!--
Microsoft:Powershell: Look for modifications for persistence [
https://www.malwarearchaeology.com/cheat-sheets ] -->
                    <TargetFilename condition="begin
with">C:\Windows\SysWOW64\WindowsPowerShell</TargetFilename> <!--
Microsoft:Powershell: Look for modifications for persistence [
https://www.malwarearchaeology.com/cheat-sheets ] -->
                    <TargetFilename condition="begin
with">C:\Windows\Tasks\</TargetFilename> <!--Microsoft:ScheduledTasks [
https://attack.mitre.org/wiki/Technique/T1053 ] -->
                    <TargetFilename condition="begin
with">C:\Windows\system32\Tasks</TargetFilename> <!--Microsoft:ScheduledTasks [
https://attack.mitre.org/wiki/Technique/T1053 ] -->
                    <!--Windows application compatibility-->
```

```
                    <TargetFilename condition="begin
with">C:\Windows\AppPatch\Custom</TargetFilename> <!--Microsoft:Windows:
Application compatibility shims [ https://www.fireeye.com/blog/threat-
research/2017/05/fin7-shim-databases-persistence.html ] -->
                    <TargetFilename
condition="contains">VirtualStore</TargetFilename> <!--Microsoft:Windows: UAC
virtualization [ https://blogs.msdn.microsoft.com/oldnewthing/20150902-
00/?p=91681 ] -->
                    <!--Exploitable file names-->
                    <TargetFilename condition="end with">.xls</TargetFilename>
<!--Legacy Office files are often used for attacks-->
                    <TargetFilename condition="end with">.ppt</TargetFilename>
<!--Legacy Office files are often used for attacks-->
                    <TargetFilename condition="end with">.rft</TargetFilename>
<!--RTF files often 0day malware vectors when opened by Office-->
             </FileCreate>


             <FileCreate onmatch="exclude">
                    <!--SECTION: Microsoft-->
                    <Image condition="is">C:\Program Files (x86)\EMET
5.5\EMET_Service.exe</Image> <!--Microsoft:EMET: Writes to C:\Windows\AppPatch\-
->
                    <!--SECTION: Microsoft:Office-->
                    <TargetFilename
condition="is">C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRes
tartTask</TargetFilename>
                    <!--SECTION: Microsoft:Office:Click2Run-->
                    <Image condition="is">C:\Program Files\Common
Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe</Image> <!--
Microsoft:Office Click2Run-->
                    <!--SECTION: Microsoft:Windows-->
                    <Image condition="is">C:\Windows\system32\smss.exe</Image>
<!-- Microsoft:Windows: Session Manager SubSystem: Creates
swapfile.sys,pagefile.sys,hiberfile.sys-->
                    <Image
condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--
Microsoft:Windows: Windows 10 app, creates tons of cache files-->
```

```
                    <Image
condition="is">\\?\C:\Windows\system32\wbem\WMIADAP.EXE</Image> <!--
Microsoft:Windows: WMI Performance updates-->
                    <Image
condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Microsoft:Windows:
Network file syncing-->
                    <TargetFilename condition="begin
with">C:\Windows\system32\DriverStore\Temp\</TargetFilename> <!--
Microsoft:Windows: Temp files by DrvInst.exe-->
                    <TargetFilename condition="begin
with">C:\Windows\system32\wbem\Performance\</TargetFilename> <!--
Microsoft:Windows: Created in wbem by WMIADAP.exe-->
                    <TargetFilename condition="end
with">WRITABLE.TST</TargetFilename> <!-- Microsoft:Windows: Created in wbem by
svchost-->
                    <TargetFilename condition="begin
with">C:\Windows\Installer\</TargetFilename> <!--Microsoft:Windows:Installer:
Ignore MSI installer files caching-->
                    <!--SECTION: Microsoft:Windows:Updates-->
                    <TargetFilename condition="begin
with">C:\$WINDOWS.~BT\Sources\</TargetFilename> <!-- Microsoft:Windows: Feature
updates containing lots of .exe and .sys-->
                    <Image condition="begin
with">C:\Windows\winsxs\amd64_microsoft-windows</Image> <!-- Microsoft:Windows:
Windows update-->
                    <!--SECTION: Dell-->
                    <Image condition="is">C:\Program Files
(x86)\Dell\CommandUpdate\InvColPC.exe</Image>
                    <!--SECTION: Intel-->
                    <Image
condition="is">C:\Windows\system32\igfxCUIService.exe</Image> <!--Intel: Drops
bat and other files in \Windows in normal operation-->
                    <!--SECTION: Adobe-->
                    <TargetFilename
condition="is">C:\Windows\System32\Tasks\Adobe Acrobat Update
Task</TargetFilename>
                    <TargetFilename
condition="is">C:\Windows\System32\Tasks\Adobe Flash Player
Updater</TargetFilename>
                </FileCreate>
```

```
		<!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-
->
			<!--EVENT 12: "Registry object added or deleted"-->
			<!--EVENT 13: "Registry value set-->
			<!--EVENT 14: "Registry objected renamed"-->


			<!--NOTE:	Windows writes hundreds or thousands of registry
keys a minute, so just because you're not changing things, doesn't mean these
rules aren't being run.-->
			<!--NOTE:	You do not have to spend a lot of time worrying
about performance, CPUs are fast, but it's something to consider. Every rule and
condition type has a small cost.-->
			<!--NOTE:	"contains" works by finding the first letter, then
matching the second, etc, so the first letters should be as low-occurrence as
possible.-->
			<!--NOTE:	[ https://attack.mitre.org/wiki/Technique/T1112 ] -
->


			<!--TECHNICAL: You cannot filter on the "Details" attribute, due
to performance issues when very large keys are written, and variety of data
formats-->
			<!--TECHNICAL: Possible prefixes are HKLM, HKCR, and HKU-->
			<!--CRITICAL:  Schema version 3.30 and higher change
HKLM\="\REGISTRY\MACHINE\" and HKU\="\REGISTRY\USER\" and
HKCR\="\REGISTRY\MACHINE\SOFTWARE\Classes\" and
CurrentControlSet="ControlSet001"-->
			<!--CRITICAL:  Due to a bug, Sysmon versions BEFORE 7.01 may not
properly log with the new prefix style for registry keys that was originally
introduced in schema version 3.30-->
			<!--NOTE:	Because Sysmon runs as a service, it has no
filtering ability for, or concept of, HKCU or HKEY_CURRENT_USER. Use "contains"
or "end with" to get around this limitation-->
```

```
		<!-- ! CRITICAL NOTE !:	It may appear this section is MISSING important entries, but SOME RULES MONITOR MANY KEYS, so look VERY CAREFULLY to see if something is already covered.-->


		<!--DATA: EventType, UtcTime, ProcessGuid, ProcessId, Image, TargetObject, Details (can't filter on), NewName (can't filter on)-->
		<RegistryEvent onmatch="include">
			<!--Autorun or Startups-->
				<!--ADDITIONAL REFERENCE: [ http://www.ghacks.net/2016/06/04/windows-automatic-startup-locations/ ] -->
				<!--ADDITIONAL REFERENCE: [ https://view.officeapps.live.com/op/view.aspx?src=https://arsenalrecon.com/downloads/resources/Registry_Keys_Related_to_Autorun.ods ] -->
				<!--ADDITIONAL REFERENCE: [ http://www.silentrunners.org/launchpoints.html ] -->
				<!--ADDITIONAL REFERENCE: [ https://www.microsoftpressstore.com/articles/article.aspx?p=2762082&seqNum=2 ] -->
			<TargetObject condition="contains">CurrentVersion\Run</TargetObject> <!--Microsoft:Windows: Wildcard for Run keys, including RunOnce, RunOnceEx, RunServices, RunServicesOnce [Also covers terminal server] -->
			<TargetObject condition="contains">Policies\Explorer\Run</TargetObject> <!--Microsoft:Windows: Alternate runs keys | Credit @ion-storm-->
			<TargetObject condition="contains">Group Policy\Scripts</TargetObject> <!--Microsoft:Windows: Group policy scripts-->
			<TargetObject condition="contains">Windows\System\Scripts</TargetObject> <!--Microsoft:Windows: Wildcard for Logon, Loggoff, Shutdown-->
			<TargetObject condition="contains">CurrentVersion\Windows\Load</TargetObject> <!--Microsoft:Windows: [ https://msdn.microsoft.com/en-us/library/jj874148.aspx ] -->
			<TargetObject condition="contains">CurrentVersion\Windows\Run</TargetObject> <!--Microsoft:Windows: [ https://msdn.microsoft.com/en-us/library/jj874148.aspx ] -->
```

```
                    <TargetObject
condition="contains">CurrentVersion\Winlogon\Shell</TargetObject> <!--
Microsoft:Windows: [ https://msdn.microsoft.com/en-
us/library/ms838576(v=winembedded.5).aspx ] -->
                    <TargetObject
condition="contains">CurrentVersion\Winlogon\System</TargetObject> <!--
Microsoft:Windows [ https://www.exterminate-it.com/malpedia/regvals/zlob-dns-
changer/118 ] -->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\Notify</TargetObject> <!--Microsoft:Windows: Autorun
location [ https://attack.mitre.org/wiki/Technique/T1004 ] [
https://www.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-
search-order ] -->
                    <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\Shell</TargetObject> <!--Microsoft:Windows: [
https://technet.microsoft.com/en-us/library/ee851671.aspx ] -->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\Userinit</TargetObject> <!--Microsoft:Windows:
Autorun location [ https://www.cylance.com/windows-registry-persistence-part-2-
the-run-keys-and-search-order ] -->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows
NT\CurrentVersion\Drivers32</TargetObject> <!--Microsoft:Windows: Legacy driver
loading | Credit @ion-storm -->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\BootExecute</TargetObject> <!--Microsoft:Windows: Autorun | Credit @ion-
storm | [ https://www.cylance.com/windows-registry-persistence-part-2-the-run-
keys-and-search-order ] -->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug</TargetObject>
<!--Microsoft:Windows: Automatic program crash debug program [
https://www.symantec.com/security_response/writeup.jsp?docid=2007-050712-5453-
99&tabid=2 ] -->
                    <TargetObject
condition="contains">UserInitMprLogonScript</TargetObject> <!--
```

```
Microsoft:Windows: Legacy logon script environment variable [
http://www.hexacorn.com/blog/2014/11/14/beyond-good-ol-run-key-part-18/ ] -->
                    <!--Services-->
                    <TargetObject condition="end
with">\ServiceDll</TargetObject> <!--Microsoft:Windows: Points to a service's
DLL [ https://blog.cylance.com/windows-registry-persistence-part-1-introduction-
attack-phases-and-windows-services ] -->
                    <TargetObject condition="end
with">\ServiceManifest</TargetObject> <!--Microsoft:Windows: Manifest pointing
to service's DLL [
https://www.geoffchappell.com/studies/windows/win32/services/svchost/index.htm ]
-->
                    <TargetObject condition="end
with">\ImagePath</TargetObject> <!--Microsoft:Windows: Points to a service's EXE
[ https://attack.mitre.org/wiki/Technique/T1050 ] -->
                    <TargetObject condition="end with">\Start</TargetObject>
<!--Microsoft:Windows: Services start mode changes (Disabled, Automatically,
Manual)-->
                    <!--CLSID launch commands and Default File Association
changes-->
                    <TargetObject
condition="contains">shell\open\command\</TargetObject> <!--Microsoft:Windows:
Sensitive sub-key under file associations and CLSID that map to launch command--
>
                    <TargetObject
condition="contains">shell\open\ddeexec\</TargetObject> <!--Microsoft:Windows:
Sensitive sub-key under file associations and CLSID that map to launch command--
>
                    <TargetObject
condition="contains">shell\install\command\</TargetObject> <!--
Microsoft:Windows: Sensitive sub-key under file associations and CLSID that map
to launch command-->
                    <TargetObject
condition="contains">Explorer\FileExts\</TargetObject> <!--Microsoft:Windows:
Changes to file extension mapping-->
                    <TargetObject condition="contains">{86C86720-42A0-1069-
A2E8-08002B30309D}</TargetObject> <!--Microsoft:Windows: Tooltip handler-->
                    <TargetObject condition="contains">exefile</TargetObject>
<!--Microsoft:Windows Executable handler, to ensure any changes not generally
monitored, for less-common shell command types like "runas"-->
```

```
                    <!--Windows COM-->
                    <TargetObject condition="end
with">\InprocServer32\(Default)</TargetObject> <!--Microsoft:Windows:COM Object
Hijacking [ https://blog.gdatasoftware.com/2014/10/23941-com-object-hijacking-
the-discreet-way-of-persistence ] | Credit @ion-storm -->
                    <!--Windows shell visual modifications-->
                    <TargetObject condition="end with">\Hidden</TargetObject>
<!--Microsoft:Windows:Explorer: Some types of malware try to hide their hidden
system files from the user, good signal event -->
                    <TargetObject condition="end
with">\ShowSuperHidden</TargetObject> <!--Microsoft:Windows:Explorer: Some types
of malware try to hide their hidden system files from the user, good signal
event [ Example:
https://www.symantec.com/security_response/writeup.jsp?docid=2007-061811-4341-
99&tabid=2 ] -->
                    <TargetObject condition="end
with">\HideFileExt</TargetObject> <!--Microsoft:Windows:Explorer: Some malware
hides file extensions to make diagnosis/disinfection more daunting to novice
users -->
                    <!--Windows shell hijack and modifications-->
                    <TargetObject
condition="contains">Classes\*\</TargetObject> <!--Microsoft:Windows:Explorer: [
http://www.silentrunners.org/launchpoints.html ] -->
                    <TargetObject
condition="contains">Classes\AllFilesystemObjects\</TargetObject> <!--
Microsoft:Windows:Explorer: [ http://www.silentrunners.org/launchpoints.html ] -
->
                    <TargetObject
condition="contains">Classes\Directory\</TargetObject> <!--
Microsoft:Windows:Explorer: [
https://stackoverflow.com/questions/1323663/windows-shell-context-menu-option ]
-->
                    <TargetObject
condition="contains">Classes\Drive\</TargetObject> <!--
Microsoft:Windows:Explorer: [
https://stackoverflow.com/questions/1323663/windows-shell-context-menu-option ]
-->
                    <TargetObject
condition="contains">Classes\Folder\</TargetObject> <!--
Microsoft:Windows:Explorer: ContextMenuHandlers, DragDropHandlers,
```

```
CopyHookHandlers, [ https://stackoverflow.com/questions/1323663/windows-shell-context-menu-option ] -->
                    <TargetObject condition="contains">ContextMenuHandlers\</TargetObject> <!--Microsoft:Windows: [ http://oalabs.openanalysis.net/2015/06/04/malware-persistence-hkey_current_user-shell-extension-handlers/ ] -->
                    <TargetObject condition="contains">CurrentVersion\Shell</TargetObject> <!--Microsoft:Windows: Shell Folders, ShellExecuteHooks, ShellIconOverloadIdentifers, ShellServiceObjects, ShellServiceObjectDelayLoad [ http://oalabs.openanalysis.net/2015/06/04/malware-persistence-hkey_current_user-shell-extension-handlers/ ] -->
                    <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\ShellExecuteHooks</TargetObject> <!--Microsoft:Windows: ShellExecuteHooks-->
                    <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\ShellServiceObjectDelayLoad</TargetObject> <!--Microsoft:Windows: ShellExecuteHooks-->
                    <TargetObject condition="begin with">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\ShellIconOverlayIdentifiers</TargetObject> <!--Microsoft:Windows: ShellExecuteHooks-->
                    <!--AppPaths hijacking-->
                    <TargetObject condition="begin with">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\</TargetObject> <!--Microsoft:Windows: Credit to @Hexacorn [ http://www.hexacorn.com/blog/2013/01/19/beyond-good-ol-run-key-part-3/ ] -->
                    <!--Terminal service boobytrap-->
                    <TargetObject condition="begin with">HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\InitialProgram</TargetObject> <!--Microsoft:Windows:RDP: Note other Terminal Server run keys are handled by another wildcard already-->
                    <!--Group Policy integrity-->
                    <TargetObject condition="begin with">HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\</TargetObject> <!--Microsoft:Windows: Group Policy internally uses a plug-in architecture that nothing should be modifying-->
                    <!--Winsock and Winsock2-->
```

```
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Services\WinSock\</TargetObject> <!--
Microsoft:Windows: Wildcard, includes Winsock and Winsock2-->
                    <TargetObject condition="end
with">\ProxyServer</TargetObject> <!--Microsoft:Windows: System and user proxy
server-->
                    <!--Credential providers-->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Provider</TargetObject> <!--Wildcard, includes Credential Providers and
Credential Provider Filters-->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\</TargetObject> <!-- [
https://attack.mitre.org/wiki/Technique/T1131 ] [
https://attack.mitre.org/wiki/Technique/T1101 ] -->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\</TargetObject>
<!--Microsoft:Windows: Changes to WDigest-UseLogonCredential for password
scraping [ https://www.trustedsec.com/april-2015/dumping-wdigest-creds-with-
meterpreter-mimikatzkiwi-in-windows-8-1/ ] -->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Netsh</TargetObject> <!--Microsoft:Windows: Netsh
helper DLL [ https://attack.mitre.org/wiki/Technique/T1128 ] -->
                    <!--Networking-->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order\</TargetObject
> <!--Microsoft:Windows: Order of network providers that are checked to connect
to destination [ https://www.malwarearchaeology.com/cheat-sheets ] -->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\NetworkList\Profiles</TargetObject> <!--Microsoft:Windows: |
Credit @ion-storm -->
                    <TargetObject condition="end
with">\EnableFirewall</TargetObject> <!--Microsoft:Windows: Monitor for firewall
disablement, all firewall profiles [
https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject condition="end
with">\DoNotAllowExceptions</TargetObject> <!--Microsoft:Windows: Monitor for
firewall disablement, all firewall profiles [
https://attack.mitre.org/wiki/Technique/T1089 ] -->
```

```
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPol
icy\StandardProfile\AuthorizedApplications\List</TargetObject> <!--Windows
Firewall authorized applications for all networks| Credit @ion-storm -->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPol
icy\DomainProfile\AuthorizedApplications\List</TargetObject> <!--Windows
Firewall authorized applications for domain networks -->
                    <!--DLLs that get injected into every process at launch-->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Windows\Appinit_Dlls\</TargetObject> <!--Microsoft:Windows:
Feature disabled by default [ https://attack.mitre.org/wiki/Technique/T1103 ] --
>
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows
NT\CurrentVersion\Windows\Appinit_Dlls\</TargetObject> <!--Microsoft:Windows:
Feature disabled by default [ https://attack.mitre.org/wiki/Technique/T1103 ] --
>
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\AppCertDlls\</TargetObject> <!--Microsoft:Windows: Credit to @Hexacorn [
http://www.hexacorn.com/blog/2013/01/19/beyond-good-ol-run-key-part-3/ ] [
https://blog.comodo.com/malware/trojware-win32-trojanspy-volisk-a/ ] -->
                    <!--Office-->
                    <TargetObject
condition="contains">Microsoft\Office\Outlook\Addins\</TargetObject> <!--
Microsoft:Office: Outlook add-ins, access to sensitive data and often cause
issues-->
                    <TargetObject condition="contains">Office
Test\</TargetObject> <!-- Microsoft:Office: Persistence method [
http://www.hexacorn.com/blog/2014/04/16/beyond-good-ol-run-key-part-10/ ] |
Credit @Hexacorn -->
                    <TargetObject condition="contains">Security\Trusted
Documents\TrustRecords</TargetObject> <!--Microsoft:Office: Monitor when "Enable
editing" or "Enable macros" is used | Credit @OutflankNL | [
https://outflank.nl/blog/2018/01/16/hunting-for-evil-detect-macros-being-
executed/ ] -->
                    <!--IE-->
```

```
                    <TargetObject condition="contains">Internet
Explorer\Toolbar\</TargetObject> <!--Microsoft:InternetExplorer: Machine and
user [ Example: https://www.exterminate-it.com/malpedia/remove-mywebsearch ] -->
                    <TargetObject condition="contains">Internet
Explorer\Extensions\</TargetObject> <!--Microsoft:InternetExplorer: Machine and
user [ Example: https://www.exterminate-it.com/malpedia/remove-mywebsearch ] -->
                    <TargetObject condition="contains">Browser Helper
Objects\</TargetObject> <!--Microsoft:InternetExplorer: Machine and user [
https://msdn.microsoft.com/en-us/library/bb250436(v=vs.85).aspx ] -->
                    <TargetObject condition="end
with">\DisableSecuritySettingsCheck</TargetObject>
                    <TargetObject condition="end with">\3\1206</TargetObject>
<!--Microsoft:InternetExplorer: Malware sometimes assures scripting is on in
Internet Zone [ https://support.microsoft.com/en-us/help/182569/internet-
explorer-security-zones-registry-entries-for-advanced-users ] -->
                    <TargetObject condition="end with">\3\2500</TargetObject>
<!--Microsoft:InternetExplorer: Malware sometimes disables Protected Mode in
Internet Zone [ https://blog.avast.com/2013/08/12/your-documents-are-corrupted-
from-image-to-an-information-stealing-trojan/ ] -->
                    <TargetObject condition="end with">\3\1809</TargetObject>
<!--Microsoft:InternetExplorer: Malware sometimes disables Pop-up Blocker in
Internet Zone [ https://support.microsoft.com/en-us/help/182569/internet-
explorer-security-zones-registry-entries-for-advanced-users ] -->
                    <!--Magic registry keys-->
                    <TargetObject condition="contains">{AB8902B4-09CA-4bb6-
B78D-A8F59079A8D5}\</TargetObject> <!--Microsoft:Windows: Thumbnail cache
autostart [ http://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-
levels-up-with-new-autostart-mechanism/ ] -->
                    <!--Install/Infection artifacts-->
                    <TargetObject condition="end
with">\UrlUpdateInfo</TargetObject> <!--Microsoft:ClickOnce: Source URL is
stored in this value [ https://subt0x10.blogspot.com/2016/12/mimikatz-delivery-
via-clickonce-with.html ] -->
                    <TargetObject condition="end
with">\InstallSource</TargetObject> <!--Microsoft:Windows: Source folder for
certain program and component installations-->
                    <!--Windows UAC tampering-->
                    <TargetObject condition="end
with">HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA</
TargetObject> <!--Detect: UAC Tampering | Credit @ion-storm -->
```

```
                    <TargetObject condition="end
with">HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccoun
tTokenFilterPolicy</TargetObject> <!--Detect: UAC Tampering | Credit @ion-storm
-->
                    <!--Microsoft Security Center tampering | Credit @ion-
storm -->
                    <TargetObject condition="end
with">HKLM\SOFTWARE\Microsoft\Security Center\AllAlertsDisabled</TargetObject>
<!-- [ https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject condition="end
with">HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusOverride</TargetObject>
<!-- [ https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject condition="end
with">HKLM\SOFTWARE\Microsoft\Security
Center\AntiVirusDisableNotify</TargetObject> <!-- [
https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject condition="end
with">HKLM\SOFTWARE\Microsoft\Security Center\DisableMonitoring</TargetObject>
<!-- [ https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject condition="end
with">HKLM\SOFTWARE\Microsoft\Security
Center\FirewallDisableNotify</TargetObject> <!-- [
https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject condition="end
with">HKLM\SOFTWARE\Microsoft\Security Center\FirewallOverride</TargetObject>
<!-- [ https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject condition="end
with">HKLM\SOFTWARE\Microsoft\Security Center\UacDisableNotify</TargetObject>
<!-- [ https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject condition="end
with">HKLM\SOFTWARE\Microsoft\Security
Center\UpdatesDisableNotify</TargetObject> <!-- [
https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\HideSCAHealth<
/TargetObject> <!--Microsoft:Windows:Security Center: Malware sometimes disables
[ https://blog.avast.com/2013/08/12/your-documents-are-corrupted-from-image-to-
an-information-stealing-trojan/ ] -->
                    <!--Windows application compatibility-->
```

```
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Custom</TargetObject> <!--Microsoft:Windows:
AppCompat [ https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-
databases-persistence.html ] -->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\InstalledSDB</TargetObject> <!--
Microsoft:Windows: AppCompat [ https://attack.mitre.org/wiki/Technique/T1138 ] -
->
                    <TargetObject
condition="contains">VirtualStore</TargetObject> <!--Microsoft:Windows: Registry
virtualization [ https://msdn.microsoft.com/en-
us/library/windows/desktop/aa965884(v=vs.85).aspx ] -->
                    <!--Windows internals integrity monitoring-->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\</TargetObject> <!--Microsoft:Windows: Malware likes changing IFEO, like
adding Debugger to disable antivirus EXE-->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\</TargetObject> <!--
Microsoft:Windows: Event log system integrity and ACLs-->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\Safeboot\</TargetObject> <!--
Microsoft:Windows: Services approved to load in safe mode-->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\Winlogon\</TargetObject> <!--
Microsoft:Windows: Providers notified by WinLogon-->
                    <TargetObject condition="end
with">\FriendlyName</TargetObject> <!--Microsoft:Windows: New devices connected
and remembered-->
                    <TargetObject
condition="is">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\InProgre
ss\(Default)</TargetObject> <!--Microsoft:Windows: See when WindowsInstaller is
engaged, useful for timeline matching with other events-->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32</TargetObject> <!--
Microsoft:Windows: Malware sometimes disables tracing to obfuscate tracks-->
                </RegistryEvent>
```

```
            <RegistryEvent onmatch="exclude">
            <!--COMMENT:  Remove low-information noise. Often these hide a
procress recreating an empty key and do not hide the values created
subsequently.-->
                  <!--SECTION: Microsoft binaries-->
                  <Image condition="end
with">Office\root\integration\integrator.exe</Image> <!--Microsoft:Office: C2R
client-->
                  <Image
condition="is">C:\Windows\system32\backgroundTaskHost.exe</Image> <!--
Microsoft:Windows: Changes association registry keys-->
                  <Image condition="is">C:\Program Files\Common
Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe</Image> <!--
Microsoft:Office: C2R client-->
                  <Image condition="is">C:\Program Files\Windows
Defender\MsMpEng.exe</Image> <!--Microsoft:Windows:Defender-->
                  <Image
condition="is">C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\Sea
rchUI.exe</Image> <!--Microsoft:Cortana-->
                  <Image condition="is">C:\Program Files (x86)\EMET
5.5\EMET_Service.exe</Image> <!--Microsoft:EMET: Routinely refreshes EMET
configuration keys from Group Policy-->
                  <!--Misc-->
                  <TargetObject condition="end
with">Toolbar\WebBrowser</TargetObject> <!--Microsoft:IE: Extraneous activity-->
                  <TargetObject condition="end
with">Toolbar\WebBrowser\ITBar7Height</TargetObject> <!--Microsoft:IE:
Extraneous activity-->
                  <TargetObject condition="end
with">Toolbar\WebBrowser\ITBar7Layout</TargetObject> <!--Microsoft:IE:
Extraneous activity-->
                  <TargetObject condition="end
with">Toolbar\ShellBrowser\ITBar7Layout</TargetObject> <!--
Microsoft:Windows:Explorer: Extraneous activity-->
                  <TargetObject condition="end with">Internet
Explorer\Toolbar\Locked</TargetObject> <!--Microsoft:Windows:Explorer:
Extraneous activity-->
```

```
                    <TargetObject condition="end
with">Toolbar\WebBrowser\{47833539-D0C5-4125-9FA8-0819E2EAAC93}</TargetObject>
<!--Microsoft:Windows:Explorer: Extraneous activity-->
                    <TargetObject condition="end
with">ShellBrowser</TargetObject> <!--Microsoft:InternetExplorer: Noise-->
                    <TargetObject condition="end
with">\CurrentVersion\Run</TargetObject> <!--Microsoft:Windows: Remove noise
from the "\Windows\CurrentVersion\Run" wildcard-->
                    <TargetObject condition="end
with">\CurrentVersion\RunOnce</TargetObject> <!--Microsoft:Windows: Remove noise
from the "\Windows\CurrentVersion\Run" wildcard-->
                    <TargetObject condition="end with">\CurrentVersion\App
Paths</TargetObject> <!--Microsoft:Windows: Remove noise from the
"\Windows\CurrentVersion\App Paths" wildcard-->
                    <TargetObject condition="end with">\CurrentVersion\Image
File Execution Options</TargetObject> <!--Microsoft:Windows: Remove noise from
the "\Windows\CurrentVersion\Image File Execution Options" wildcard-->
                    <TargetObject condition="end with">\CurrentVersion\Shell
Extensions\Cached</TargetObject> <!--Microsoft:Windows: Remove noise from the
"\CurrentVersion\Shell Extensions\Cached" wildcard-->
                    <TargetObject condition="end with">\CurrentVersion\Shell
Extensions\Approved</TargetObject> <!--Microsoft:Windows: Remove noise from the
"\CurrentVersion\Shell Extensions\Approved" wildcard-->
                    <TargetObject condition="end
with">}\PreviousPolicyAreas</TargetObject> <!--Microsoft:Windows: Remove noise
from \Winlogon\GPExtensions by svchost.exe-->
                    <TargetObject
condition="contains">\Control\WMI\Autologger\</TargetObject> <!--
Microsoft:Windows: Remove noise from monitoring "\Start"-->
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Services\UsoSvc\Start</TargetObject> <!--
Microsoft:Windows: Remove noise from monitoring "\Start"-->
                    <TargetObject condition="end
with">\Lsa\OfflineJoin\CurrentValue</TargetObject> <!--Microsoft:Windows:
Sensitive value during domain join-->
                    <TargetObject condition="end
with">\Components\TrustedInstaller\Events</TargetObject> <!--Microsoft:Windows:
Remove noise monitoring Winlogon-->
```

```
                    <TargetObject condition="end
with">\Components\TrustedInstaller</TargetObject> <!--Microsoft:Windows: Remove
noise monitoring Winlogon-->
                    <TargetObject condition="end
with">\Components\Wlansvc</TargetObject> <!--Microsoft:Windows: Remove noise
monitoring Winlogon-->
                    <TargetObject condition="end
with">\Components\Wlansvc\Events</TargetObject> <!--Microsoft:Windows: Remove
noise monitoring Winlogon-->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\</TargetObject> <!--Microsoft:Windows: Remove noise monitoring installations
run as system-->
                    <TargetObject condition="end
with">\Directory\shellex</TargetObject> <!--Microsoft:Windows: Remove noise
monitoring Classes-->
                    <TargetObject condition="end
with">\Directory\shellex\DragDropHandlers</TargetObject> <!--Microsoft:Windows:
Remove noise monitoring Classes-->
                    <TargetObject condition="end
with">\Drive\shellex</TargetObject> <!--Microsoft:Windows: Remove noise
monitoring Classes-->
                    <TargetObject condition="end
with">\Drive\shellex\DragDropHandlers</TargetObject> <!--Microsoft:Windows:
Remove noise monitoring Classes-->
                    <TargetObject
condition="contains">_Classes\AppX</TargetObject> <!--Microsoft:Windows: Remove
noise monitoring "Shell\open\command"--> <!--Win8+-->
                    <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\</TargetO
bject> <!--Microsoft:Windows: SvcHost Noise-->
                    <Image
condition="is">C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\Sea
rchUI.exe</Image> <!--Microsoft:Windows: Remove noise from Windows 10 Cortana |
Credit @ion-storm--> <!--Win10-->
                    <Image condition="is">C:\Program Files (x86)\Cisco\Cisco
AnyConnect Secure Mobility Client\vpnagent.exe</Image>
                    <!--Bootup Control noise-->
```

```
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Audit</TargetObject> <!--
Microsoft:Windows:lsass.exe: Boot noise--> <!--Win8+-->
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Audit\AuditPolicy</TargetObject>
<!--Microsoft:Windows:lsass.exe: Boot noise--> <!--Win8+-->
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Audit\PerUserAuditing\System</Ta
rgetObject> <!--Microsoft:Windows:lsass.exe: Boot noise--> <!--Win8+-->
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\LsaPid</TargetObject> <!--
Microsoft:Windows:lsass.exe: Boot noise-->
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SspiCache</TargetObject> <!--
Microsoft:Windows:lsass.exe: Boot noise--> <!--Win8+-->
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Domains</TargetObject>
<!--Microsoft:Windows:lsass.exe: Boot noise--> <!--Win8+-->
                    <TargetObject condition="end
with">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit</Targ
etObject> <!--Microsoft:Windows:lsass.exe: Boot noise--> <!--Win8+-->
                    <!--Services startup settings noise, some low-risk
services routinely change it and this can be ignored-->
                    <TargetObject condition="end
with">\services\bits\Start</TargetObject> <!--Microsoft:Windows: Remove noise
from monitoring "\Start"-->
                    <TargetObject condition="end
with">\services\clr_optimization_v2.0.50727_32\Start</TargetObject> <!--
Microsoft:dotNet: Windows 7-->
                    <TargetObject condition="end
with">\services\clr_optimization_v2.0.50727_64\Start</TargetObject> <!--
Microsoft:dotNet: Windows 7-->
                    <TargetObject condition="end
with">\services\clr_optimization_v4.0.30319_32\Start</TargetObject> <!--
Microsoft:dotNet: Windows 10-->
                    <TargetObject condition="end
with">\services\clr_optimization_v4.0.30319_64\Start</TargetObject> <!--
Microsoft:dotNet: Windows 10-->
```

```
                    <TargetObject condition="end
with">\services\deviceAssociationService\Start</TargetObject> <!--
Microsoft:Windows: Remove noise from monitoring "\Start"-->
                    <TargetObject condition="end
with">\services\fhsvc\Start</TargetObject> <!--Microsoft:Windows: File History
Service-->
                    <TargetObject condition="end
with">\services\nal\Start</TargetObject> <!--Intel: Network adapter diagnostic
driver-->
                    <TargetObject condition="end
with">\services\trustedInstaller\Start</TargetObject> <!--Microsoft:Windows:
Remove noise from monitoring "\Start"-->
                    <TargetObject condition="end
with">\services\tunnel\Start</TargetObject> <!--Microsoft:Windows: Remove noise
from monitoring "\Start"-->
                    <TargetObject condition="end
with">\services\usoSvc\Start</TargetObject> <!--Microsoft:Windows: Remove noise
from monitoring "\Start"-->
                    <!--FileExts noise filtering-->
                    <TargetObject
condition="contains">\OpenWithProgids</TargetObject> <!--Microsoft:Windows:
Remove noise from monitoring "FileExts"-->
                    <TargetObject condition="end
with">\OpenWithList</TargetObject> <!--Microsoft:Windows: Remove noise from
monitoring "FileExts"-->
                    <TargetObject condition="end
with">\UserChoice</TargetObject> <!--Microsoft:Windows: Remove noise from
monitoring "FileExts"-->
                    <TargetObject condition="end
with">\UserChoice\ProgId</TargetObject> <!--Microsoft:Windows: Remove noise from
monitoring "FileExts"--> <!--Win8+-->
                    <TargetObject condition="end
with">\UserChoice\Hash</TargetObject> <!--Microsoft:Windows: Remove noise from
monitoring "FileExts"--> <!--Win8+-->
                    <TargetObject condition="end
with">\OpenWithList\MRUList</TargetObject> <!--Microsoft:Windows: Remove noise
from monitoring "FileExts"-->
                    <TargetObject condition="end with">} 0xFFFF</TargetObject>
<!--Microsoft:Windows: Remove noise generated by explorer.exe on monitored
ShellCached binary keys--> <!--Win8+-->
```

```
                    <!--Group Policy noise-->
                    <TargetObject condition="end
with">HKLM\System\CurrentControlSet\Control\Lsa\Audit\SpecialGroups</TargetObjec
t> <!--Microsoft:Windows: Routinely set through Group Policy, not especially
important to log-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts</TargetObject> <!--Microsoft:Windows:Group Policy: Noise below
the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup</TargetObject> <!--Microsoft:Windows:Group Policy: Noise
below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup\0</TargetObject> <!--Microsoft:Windows:Group Policy:
Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup\0\PSScriptOrder</TargetObject> <!--
Microsoft:Windows:Group Policy: Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup\0\SOM-ID</TargetObject> <!--Microsoft:Windows:Group
Policy: Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup\0\GPO-ID</TargetObject> <!--Microsoft:Windows:Group
Policy: Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup\0\0\IsPowershell</TargetObject> <!--
Microsoft:Windows:Group Policy: Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup\0\0\ExecTime</TargetObject> <!--Microsoft:Windows:Group
Policy: Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
```

```
Policy\Scripts\Shutdown</TargetObject> <!--Microsoft:Windows:Group Policy: Noise
below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Shutdown\0</TargetObject> <!--Microsoft:Windows:Group Policy:
Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Shutdown\0\PSScriptOrder</TargetObject> <!--
Microsoft:Windows:Group Policy: Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Shutdown\0\SOM-ID</TargetObject> <!--Microsoft:Windows:Group
Policy: Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Shutdown\0\GPO-ID</TargetObject> <!--Microsoft:Windows:Group
Policy: Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Shutdown\0\0\IsPowershell</TargetObject> <!--
Microsoft:Windows:Group Policy: Noise below the actual key while building-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Shutdown\0\0\ExecTime</TargetObject> <!--Microsoft:Windows:Group
Policy: Noise below the actual key while building-->
                    <TargetObject
condition="contains">\safer\codeidentifiers\0\HASHES\{</TargetObject> <!--
Microsoft:Windows: Software Restriction Policies. Can be used to disable
security tools, but very noisy to monitor if you use it-->
                    <!--SECTION: 3rd party-->
                    <Image condition="is">C:\Program Files\WIDCOMM\Bluetooth
Software\btwdins.exe</Image> <!--Constantly writes to HKLM-->
                    <TargetObject condition="begin
with">HKCR\VLC.</TargetObject> <!--VLC update noise-->
                    <TargetObject condition="begin
with">HKCR\iTunes.</TargetObject> <!--Apple: iTunes update noise-->
                </RegistryEvent>
```

```
        <!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED
[FileCreateStreamHash]-->
                <!--EVENT 15: "File stream created"-->
                <!--COMMENT:   Any files created with an NTFS Alternate Data
Stream which match these rules will be hashed and logged.
                        [
https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-
in-ntfs/ ]
                        ADS's are used by browsers and email clients to mark files
as originating from the Internet or other foreign sources.
                        [ https://textslashplain.com/2016/04/04/downloads-and-the-
mark-of-the-web/ ] -->
                <!--NOTE: Other filesystem minifilters can make it appear to
Sysmon that some files are being written twice. This is not a Sysmon issue, per
Mark Russinovich.-->


                <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename,
CreationUtcTime, Hash-->
                <FileCreateStreamHash onmatch="include">
                        <TargetFilename
condition="contains">Downloads</TargetFilename> <!--Downloaded files. Does not
include "Run" files in IE-->
                        <TargetFilename
condition="contains">Temp\7z</TargetFilename> <!--7zip extractions-->
                        <TargetFilename
condition="contains">Startup</TargetFilename> <!--ADS startup | Example: [
https://www.hybrid-
analysis.com/sample/a314f6106633fba4b70f9d6ddbee452e8f8f44a72117749c21243dc93c7e
d3ac?environmentId=100 ] -->
                        <TargetFilename condition="end with">.bat</TargetFilename>
<!--Batch scripting-->
                        <TargetFilename condition="end with">.cmd</TargetFilename>
<!--Batch scripting | Credit @ion-storm -->
                        <TargetFilename condition="end with">.hta</TargetFilename>
<!--Scripting-->
                        <TargetFilename condition="end with">.lnk</TargetFilename>
<!--Shortcut file | Credit @ion-storm -->
                        <TargetFilename condition="end with">.ps1</TargetFilename>
<!--PowerShell-->
```

```
                    <TargetFilename condition="end with">.ps2</TargetFilename>
<!--PowerShell-->
                    <TargetFilename condition="end with">.reg</TargetFilename>
<!--Registry File-->
                    <TargetFilename condition="end with">.jse</TargetFilename>
<!--Registry File-->
                    <TargetFilename condition="end with">.vb</TargetFilename>
<!--VisualBasicScripting files-->
                    <TargetFilename condition="end with">.vbe</TargetFilename>
<!--VisualBasicScripting files-->
                    <TargetFilename condition="end with">.vbs</TargetFilename>
<!--VisualBasicScripting files-->
             </FileCreateStreamHash>


             <FileCreateStreamHash onmatch="exclude">
             </FileCreateStreamHash>


      <!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
             <!--EVENT 16: "Sysmon config state changed"-->
             <!--COMMENT:  This ONLY logs if the hash of the configuration
changes. Running "sysmon.exe -c" with the current configuration will not be
logged with Event 16-->

             <!--DATA: UtcTime, Configuration, ConfigurationFileHash-->
             <!--Cannot be filtered.-->


      <!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]--
>
             <!--EVENT 17: "Pipe Created"-->
             <!--EVENT 18: "Pipe Connected"-->


             <!--ADDITIONAL REFERENCE: [ https://www.cobaltstrike.com/help-smb-
beacon ] -->
             <!--ADDITIONAL REFERENCE: [
https://blog.cobaltstrike.com/2015/10/07/named-pipe-pivoting/ ] -->
```

```
            <!--DATA: UtcTime, ProcessGuid, ProcessId, PipeName, Image-->
            <PipeEvent onmatch="include">
            </PipeEvent>


      <!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
            <!--EVENT 19: "WmiEventFilter activity detected"-->
            <!--EVENT 20: "WmiEventConsumer activity detected"-->
            <!--EVENT 21: "WmiEventConsumerToFilter activity detected"-->


            <!--ADDITIONAL REFERENCE: [
https://www.darkoperator.com/blog/2017/10/15/sysinternals-sysmon-610-tracking-
of-permanent-wmi-events ] -->
            <!--ADDITIONAL REFERENCE: [
https://rawsec.lu/blog/posts/2017/Sep/19/sysmon-v610-vs-wmi-persistence/ ] -->


            <!--DATA: EventType, UtcTime, Operation, User, Name, Type,
Destination, Consumer, Filter-->
            <WmiEvent onmatch="include">
            </WmiEvent>


      <!--SYSMON EVENT ID 255 : ERROR-->
            <!--"This event is generated when an error occurred within Sysmon.
They can happen if the system is under heavy load
                  and certain tasked could not be performed or a bug exists
in the Sysmon service. You can report any bugs on the
                  Sysinternals forum or over Twitter (@markrussinovich)."-->
            <!--Cannot be filtered.-->


      </EventFiltering>
</Sysmon>
```