Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Κατανεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Χρήση του εργαλείου sysmon για τον εντοπισμό επιθέσεων εσωτερικής μετακίνησης ενός επιτιθέμενου** **Application of the sysmon tool for the identification of internal lateral movements of an attacker**
Ονοματεπώνυμο Φοιτητή	**Δράκος Μιχαήλ**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**ΜΠΚΣΑ18009**
Επιβλέπων	**Κοτζανικολάου Παναγιώτης, Αναπληρωτής Καθηγητής**

Ημερομηνία Παράδοσης: **Νοέμβριος 2022**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Παναγιώτης Κοτζανικολάου Αναπληρωτής Καθηγητής	Δέσποινα Πολέμη Καθηγήτρια	Κωσταντίνος Πατσάκης Αναπληρωτής Καθηγητής

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω τον καθηγητή Κο Παπαγεωργίου Σπυρίδων για τη σημαντικότατη καθοδήγηση του καθώς και για τη συνεργασία του με την οποία κατάφερα να ολοκληρώσω τη διπλωματική μου εργασία.

Επιπρόσθετα, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στους γονείς μου για την διαρκή τους υποστήριξη καθώς και για την παρότρυνση που μου έδιναν σε όλο αυτό το ακαδημαϊκό ταξίδι.

Τέλος, θα ήθελα να εκφράσω τις ευχαριστίες μου για την εταιρία Vitex S.A. στην οποία εργαζόμουν καθ' όλη τη διάρκεια αυτού του ακαδημαϊκού ταξιδιού, για όλη την υποστήριξη της προκειμένου να παρακολουθήσω και να ολοκληρώσω το συγκεκριμένο μεταπτυχιακό πρόγραμμα σπουδών.

Δράκος Μιχαήλ,

Νοέμβριος 2022

Περίληψη

Μέσα από την παρούσα διπλωματική διατριβή, ο αναγνώστης μπορεί να ενημερωθεί για τη χρήση, το τρόπο λειτουργίας και τις δυνατότητες του εργαλείου Sysmon καθώς επίσης παρουσιάζεται ένας τρόπος εγκατάστασης και παραμετροποίησης του εργαλείου. Το Sysmon παρέχει αναλυτικές πληροφορίες σχετικά με τις δημιουργίες διαδικασιών, τις συνδέσεις δικτύου και τις αλλαγές στο χρόνο δημιουργίας των αρχείων στα Windows συστήματα. Όλες αυτές οι πληροφορίες που παράγει το Symon συλλέγονται σε συμβάντα που παράγονται από το ίδιο το εργαλείο χρησιμοποιώντας τη συλλογή συμβάντων των Windows και στη συνέχεια μπορεί να γίνει η ανάλυση τους από εκεί. Ο αναγνώστης ενημερώνεται ταυτόχρονα για τους τρόπους με τους οποίους μπορούν να εντοπιστούν επιθέσεις εσωτερικής μετακίνησης ενός επιτιθέμενου μέσα σε ένα δίκτυο με Windows Domain.

Επιπλέον κατά τη διάρκεια της συγκεκριμένης αναφοράς γίνεται μια αναλυτική παρουσίαση και ανάλυση όσο αναφορά στις μεθοδολογίες, στις τεχνικές και στα εργαλεία που χρησιμοποιεί ένας επιτιθέμενος με σκοπό να μετακινηθεί εσωτερικά (Lateral Movement) σε ένα δίκτυο με Windows Domain, έχοντας ως τελικό σκοπό να γίνει domain admin είτε να υποκλέψει δεδομένα.

Abstract

Through this dissertation, the reader can be informed about the use, operation and capabilities of the Sysmon tool as well as a way to install and configure the tool. Sysmon provides detailed information on process creations, network connections, and changes in file creation time in Windows systems. All of this information generated by Symon is collected in events generated by the tool itself using the Windows event collection and then can be analyzed from there. At the same time, the reader is informed about the ways in which an attacker's internal movements can be detected in a network with Windows Domain.

In addition, during this report, a detailed presentation and analysis of the methodologies, techniques and tools used by an attacker in order to move internally (Lateral Movement) in a network with Windows Domain, with the ultimate goal of becoming a domain admin or steal data.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη 4

Abstract 4

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ 5

1 Εισαγωγή 7

1.1 Στόχος και σκοπός διατριβής 7

1.2 Δομή διατριβής 7

2 Εργαλείο Παρακολούθησης Συμβάντων - Sysmon 9

2.1 Παρουσίαση του εργαλείου Sysmon 9

2.2 Λειτουργίες και Δυνατότητες του εργαλείου Sysmon 11

2.3 Εγκατάσταση, Χρήση και Ρύθμιση του Sysmon 17

2.4 Ρύθμιση του Sysmon με χρήση αρχείου .xml configuration file 21

3 Αρχεία Καταγραφής συμβάντων σε συστήματα Windows 24

3.1 Διαχωρισμός των αρχείων καταγραφής 24

3.2 Κατηγορίες των αρχείων καταγραφής βάσει κρισιμότητας 25

3.3 Πρόγραμμα Προβολής των αρχείων καταγραφής 26

3.4 Αξιοσημείωτα αρχεία καταγραφής για την ανίχνευση εσωτερικής μετακίνησης 29

3.5 Παραμετροποίηση αρχείων καταγραφής Windows 36

4 Τεχνικές και Τακτικές Εσωτερικής Μετακίνησης βάσει MITRE ATT&CK 40

4.1 Λογισμικό ανάπτυξης εφαρμογών 41

4.2 Component Object Model and Distributed COM 42

4.3 Εκμετάλλευση απομακρυσμένων υπηρεσιών 44

4.4 Εσωτερικό Spearphishing 47

4.5 Logon Scripts 48

4.6 Pass the Hash 49

4.7 Pass the Ticket 50

4.8 Πρωτόκολλο Remote Desktop 52

4.9 Απομακρυσμένη αντιγραφή αρχείου 56

4.10 Απομακρυσμένες Υπηρεσίες 58

4.11 Αναπαραγωγή μέσω αφαιρούμενων μέσων 60

4.12 Κοινόχρηστο Webroot 61

4.13 Παραβίαση κοινόχρηστου περιεχομένου 63

4.14 Λογισμικό τρίτων κατασκευαστών 64
4.15 Windows Admin Shares 67
4.16 Εργαλείο Windows Remote Management 70
5 Ανίχνευση και τρόποι προστασίας κατά της εσωτερικής μετακίνησης 71
5.1 Ανάπτυξη ορθών πρακτικών επαλήθευσης ταυτότητας 72
5.2 Προστασία κωδικών πρόσβασης 73
5.3 Προστασία των λογαριασμών με υψηλά προνόμια 74
5.4 Εφαρμογή της αρχής του λιγότερου προνομίου 74
5.5 Κλείδωμα συσκευών 75
5.6 Διαχωρισμός δικτύου 75
5.7 Παρακολούθηση δικτύου 76
5.8 Εξέταση χρήσης honeypots 76
6 Κυνήγι απειλών εσωτερικής μετακίνησης μέσω παρακολούθησης συγκεκριμένων εργαλείων 77
6.1 PsExec 77
6.2 RemCom 79
6.3 PAExec 79
7 Μεθοδολογία επιτιθέμενου 80
7.1 Αναγνώριση 80
7.2 Συλλογή διαπιστευτηρίων και κλιμάκωση προνομίων 81
7.3 Απόκτηση Πρόσβασης 81
8 Χρήση Εργαλείων και Προσομοίωση επίτευξης Εσωτερικής Μετακίνησης 82
8.1 WMI 82
8.2 SMBExec 84
8.3 Mimikatz (Pass-the-hash) 86
8.4 psexec 88
9 Αποτελέσματα, Συμπεράσματα και Μελλοντικές Επεκτάσεις 92
9.1 Πιθανές μελλοντικές επεκτάσεις 92
10 Βιβλιογραφικές Πηγές 93
Παράρτημα [10] 94

1 Εισαγωγή

Στην συγκεκριμένη διπλωματική διατριβή γίνεται αναφορά και παρουσίαση των τεχνικών καθώς και των πλέον γνωστών εργαλείων που χρησιμοποιούν οι επιτιθέμενοι για να μετακινηθούν εσωτερικά σε ένα δίκτυο με Windows Domain. Η εσωτερική ή αλλιώς πλευρική μετακίνηση(Lateral Movement) είναι η διαδικασία κατά την οποία ένας εισβολέας παίρνει τον έλεγχο ενός στοιχείου-τερματικού μέσα σε ένα τομέα ενός δικτύου και στη συνέχεια επεκτείνει την προσέγγισή του μέσα από τη συγκεκριμένη συσκευή σε άλλα στοιχεία-τερματικά εντός του ίδιου δικτύου ή τομέα δικτύου.

Όσο αναφορά στον εντοπισμό αυτού του είδους επιθέσεων προτείνεται η χρήση του εργαλείου Sysmon της Microsoft σε συνεργασία των αρχείων καταγραφής Windows. Παρακάτω όπως θα δείτε στην αναφορά αυτή γίνεται αναλυτική παρουσίαση του συγκεκριμένου εργαλείου όπως επίσης δίνεται και μια προτεινόμενη ρύθμιση του Sysmon με σκοπό να εντοπίζονται τόσο η χρήση των εργαλείων, όσο και οι εντολές που δίνει κάποιος επιτιθέμενος για να μετακινηθεί εσωτερικά (Lateral Movement) σε ένα δίκτυο με Windows Domain. Οι λόγοι που έχουν συνήθως οι επιτιθέμενοι και εκτελούν τέτοιου είδους επιθέσεις είναι να υποκλέψουν δεδομένα είτε έχουν ως τελικό σκοπό να γίνουν Domain Admin.

1.1 Στόχος και σκοπός διατριβής

Η συγκεκριμένη αναφορά σκοπεύει στην παροχή βασικών πληροφοριών που είναι χρήσιμες για την ανίχνευση και τη διερεύνηση στοιχείων και εργαλείων που χρησιμοποιούνται από τους περισσότερους επιτιθέμενους. Πιο συγκεκριμένα, αυτή η αναφορά στοχεύει στο να αποτελεί ένα λεξικό που να μπορεί να χρησιμοποιηθεί ως οδηγός για την αποτελεσματική ανάλυση του αρχείου καταγραφής συμβάντων των Windows, προσδιορίζοντας ποια εργαλεία χρησιμοποιήθηκαν με βάση τα αρχεία καταγραφής ή ποια καταγραφή έγινε κατά την εκτέλεση ενός συγκεκριμένου εργαλείου από έναν επιτιθέμενο.

Ο τελικός βέβαια στόχος της συγκεκριμένης αναφοράς είναι αφού παρουσιαστούν αναλυτικά ορισμένες τεχνικές και εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, να αναδείξει τις ικανότητες και την χρήση του εργαλείου Sysmon όπως επίσης και την αποτελεσματικότητα του στον εντοπισμό τέτοιου είδους επιθέσεων σε συνεργασία με τα αρχεία καταγραφής (Event Logs) των Windows.

1.2 Δομή διατριβής

Κάθε κεφάλαιο αποτελεί συνέχεια του προηγούμενου και όλα μαζί έχουν ως στόχο να αναδείξουν τελικά την αξία και τη μεγάλη σημασία της ορθής λειτουργίας του εργαλείου Sysmon σε Windows συστήματα για την ανίχνευση επιθέσεων εσωτερικής μετακίνησης σε αυτά.

Πιο συγκεκριμένα, στα κεφάλαια που ακολουθούν:

- Γίνεται αναλυτική παρουσίαση των τεχνικών και των πλέον γνωστών εργαλείων εσωτερικής μετακίνησης σε ένα δίκτυο με Windows Domain.

- Γίνεται παρουσίαση και ανάλυση του τρόπου λειτουργίας καθώς και των δυνατοτήτων του εργαλείου Sysmon.
- Δίνεται μια προτεινόμενη και ορθή ρύθμιση του εργαλείου Sysmon για τον εντοπισμό επιθέσεων εσωτερικής μετακίνησης σε ένα δίκτυο με Windows Domain.
- Δίνεται μια προτεινόμενη γενική ρύθμιση των Event Logs των Windows σε συνεργασία με το Sysmon.
- Γίνεται προσομοίωση ορισμένων επιθέσεων εσωτερικής μετακίνησης με συγκεκριμένα εργαλεία και ανίχνευση αυτών μέσω της καταγραφής αρχείων συμβάντων των Windows.

2 Εργαλείο Παρακολούθησης Συμβάντων - Sysmon

Όπως έχει παρατηρηθεί, είναι αρκετά συχνά εμφανιζόμενο το φαινόμενο της εσωτερικής μετακίνησης ενός επιτιθέμενου μέσα σε ένα δίκτυο με Windows Domain, όπως επίσης και η προσπάθεια κατάκτησης δικαιωμάτων και προνομίων διαχειριστή από τον επιτιθέμενο με κύριο σκοπό να υποκλέψει δεδομένα ή και να επιφέρει σημαντικές αλλαγές στο σύστημα προς όφελός του πάντα.

Οι μέθοδοι και οι τεχνικές που χρησιμοποιούν οι επιτιθέμενοι είναι αρκετές για να εκπληρώσουν τον σκοπό αυτό και οι περισσότερες από αυτές είναι πλέον γνωστές. Κάνοντας ορθή χρήση διαφόρων συνήθως OpenSource εργαλείων οι επιτιθέμενοι επιταχύνουν και επιτυγχάνουν τον σκοπό τους. Ωστόσο, αρκετές φορές το κύριο πρόβλημά των επιτιθέμενων είναι ότι αφήνουν ίχνη πίσω τους και μπορούν να γίνουν αντιληπτοί από τον αμυνόμενο.

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 μεταβληθούν από την πολιτική κάθε τοπικής ομάδας ενός δικτύου.

Για τον εντοπισμό των ιχνών ενός επιτιθέμενου μέσα σε ένα δίκτυο μια πολύ καλή πρόταση είναι το εργαλείο Sysmon (System Monitor).

2.1 Παρουσίαση του εργαλείου Sysmon

Το Sysmon ένα εργαλείο της σουίτας Sysinternals το οποίο διατίθεται δωρεάν από την Microsoft και έχει δημιουργηθεί ή αλλιώς γραφτεί από τον Mark Roussinovich [2].

Το Σύστημα Παρακολούθησης (Sysmon) είναι ένα βοηθητικό πρόγραμμα που γράφτηκε για την παρακολούθηση των δυνητικών κακόβουλων δραστηριοτήτων σε κάποιο άτομο ή σε υπολογιστές ή ακόμη και σε ένα ολόκληρο δίκτυο υπολογιστών.

Το Sysmon βασίζεται στους ίδιους μηχανισμούς παρακολούθησης που διαθέτει το εργαλείο Procmon, αλλά διαφέρει από Procmon σε διάφορους βασικούς τρόπους για να καταστεί έτσι δυνατή την ύπαρξή του και να επιβεβαιώνεται ως πιο κατάλληλο εργαλείο για την παρακολούθηση ενός ενεργού παρείσακτος.

Πρώτον, σε αντίθεση με κάθε βοηθητικό πρόγραμμα διαγνωστικού ελέγχου της σουίτας Sysinternals που τέθηκε πριν από αυτό, το Sysmon είναι εγκατεστημένο και διαρρυθμισμένο για συνεχή, μακροπρόθεσμη παρακολούθηση που επιβιώνει και ξεκινά να τρέχει μετά από κάθε επανεκκίνηση τους συστήματος.

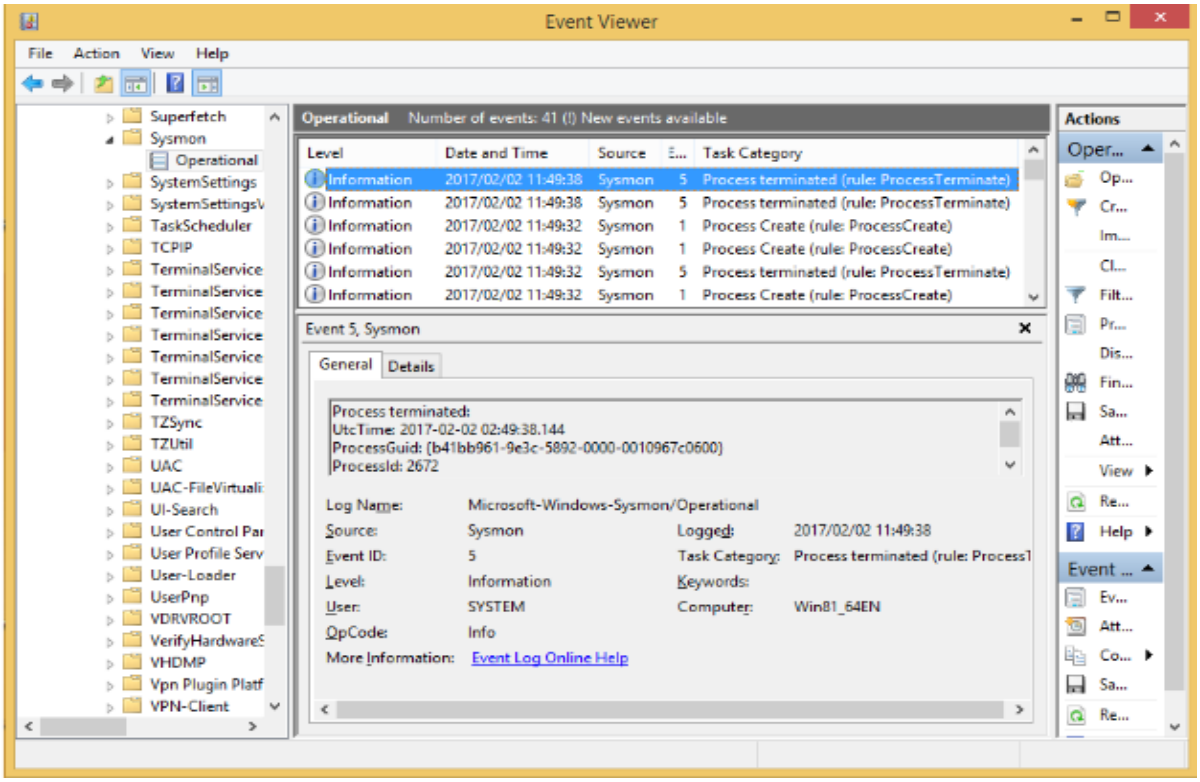
Δεύτερον, το Sysmon επικεντρώνεται μόνο σε ένα υποσύνολο γεγονότων, αρχείων, διεργασιών και δικτύων που ενδιαφέρουν, ενώ ταυτόχρονα καταγράφει πρόσθετες πληροφορίες πέρα από τις καταγραφές του Procmon.

Τέλος, αντί να γράφει τα Logs του σε ένα ιδιόκτητο αρχείο καταγραφής το οποίο μπορεί να επιθεωρηθεί μόνο μετά τη διακοπή της καταγραφής, το Sysmon καταγράφει τα δεδομένα του στα Windows αρχεία της καταγραφής των συμβάντων των Windows. Με αυτό τον τρόπο καταγραφής που χρησιμοποιεί το Sysmon τα δεδομένα που συλλέγει μπορούν να προωθηθούν σε έναν συλλέκτη συμβάντων των Windows ή σε μια πλατφόρμα ελέγχου

ασφάλειας (SIEM), προσφέροντας σχεδόν σε πραγματικό χρόνο ορατότητα στη δραστηριότητα ενός εισβολέα σε όλο το φάσμα ενός δικτύου.

Το Sysmon παρέχει λεπτομερείς πληροφορίες σχετικά με τις δημιουργίες των διαδικασιών στο σύστημα που είναι εγκατεστημένο, τις συνδέσεις δικτύου που γίνονται από και προς το σύστημα αυτό, αλλά και τις αλλαγές στο χρόνο δημιουργίας των αρχείων. Συλλέγοντας τα Logs που παράγει χρησιμοποιώντας τη συλλογή συμβάντων των Windows(Event Viewer) και στη συνέχεια κάνοντας ανάλυση αυτών, είναι εύκολο να εντοπιστεί κακόβουλη ή ανώμαλη δραστηριότητα σε ένα σύστημα Windows. Με αυτό τον τρόπο μπορεί να γίνει εμφανές ο τρόπος με τον οποίο λειτουργούν οι εισβολείς όπως και το κακόβουλο λογισμικό που χρησιμοποιούν [2].

Κάνοντας χρήση του Event Viewer των Windows μπορούμε να δούμε αναλυτικά στοιχεία για την κάθε πληροφορία των Logs που παράγει το Sysmon (Βλ. Εικόνα 1).



Εικόνα 1 [7] - Checking Sysmon Logs from Event Viewer

Το Sysmon είναι ουσιαστικά ένα Service και ένας Driver του συστήματος των Windows, όπου αφού εγκατασταθεί σε ένα σύστημα παραμένει ενεργό και λειτουργεί ασταμάτητα ακόμη και μετά όλων των επανεκκινήσεων που μπορούν να γίνουν σε ένα σύστημα με σκοπό να παρακολουθεί και να καταγράφει τη δραστηριότητα του συστήματος στο αρχείο καταγραφής συμβάντων των Windows.

Αν και το Sysmon δεν έχει τη δυνατότητα να αναλύει ή να ερμηνεύει τα δεδομένα που συλλαμβάνει, εκεί έξω υπάρχουν πολλά εργαλεία που μπορούν να επεξεργαστούν τα δεδομένα των αρχείων καταγραφής συμβάντων των Windows.

Γενικά το Sysmon έχει τη δυνατότητα να παρακολουθήσει:

- Τη δημιουργία και τον τερματισμό μιας διαδικασίας του συστήματος.
- Τη φόρτωση των προγραμμάτων οδήγησης πυρήνα, DLL αρχείων όπως και άλλα αρχεία εικόνων.
- Εισερχόμενες και εξερχόμενες συνδέσεις δικτύου TCP και UDP.
- Τη διαδικασία δημιουργίας ενός νήματος σε μια διαφορετική Process.
- Τη πρόσβαση σε ακατέργαστο δίσκο.
- Την αλλαγή των χρονικών σημείων δημιουργίας αρχείων, ένα τέχνασμα με το οποίο το κακόβουλο λογισμικό προσπαθεί συχνά να καλύψει τις διαδρομές του ή να κρύψει την ύπαρξή του.

Το Sysmon μπορεί επίσης να καταγράψει σε ψηφιακές υπογραφές έως και τέσσερα διαφορετικά Hashes για κάθε είδος αρχείου κατά την φόρτωσή του.

Να σημειωθεί ωστόσο εδώ πως το Sysmon δεν παρέχει ανάλυση των συμβάντων που δημιουργεί το ίδιο καθώς επίσης δεν προσπαθεί να προστατευτεί ή να κρυφτεί από τους επιτιθέμενους.

Το πρόγραμμα οδήγησης του Sysmon έχει ρυθμιστεί ως πρόγραμμα εκκίνησης και αρχίζει να συλλαμβάνει πληροφορίες από την εκκίνηση του εκάστοτε συστήματος στο οποίο είναι εγκατεστημένο. Μόλις ξεκινήσει η υπηρεσία, καταναλώνει τα δεδομένα που παράγει ο Driver, συλλαμβάνει πρόσθετες πληροφορίες όπως hashes αρχείων που περιεγράφηκαν προηγουμένως και γράφει γεγονότα στο αρχείο καταγραφής συμβάντων των Windows.

Το Sysmon μπορεί επίσης αφού δημιουργήσει αυτόματα Hashes από όλα (ή επιλεγμένα) δυαδικά αρχεία που εκτελούνται σε ένα σύστημα Windows να επιτρέπει την υποβολή αυτών σε υπηρεσίες όπως το VirusTotal για τον έλεγχο τους.

Η Microsoft ενημερώνει συνεχώς το Sysmon, οπότε προτείνεται η αναζήτηση ανά τακτά χρονικά διαστήματα νέων εκδόσεων ή νέων λειτουργιών που προστίθενται σε αυτό.

2.2 Λειτουργίες και Δυνατότητες του εργαλείου Sysmon

Το Sysmon όπως αναφέρθηκε και παραπάνω είναι ένα βοηθητικό πρόγραμμα κονσόλας που εγκαθιστά μια υπηρεσία και ένα πρόγραμμα οδήγησης στο σύστημά σας με σκοπό την παρακολούθηση πιθανών προβλημάτων ασφάλειας καθώς και σχετικών Events για μεγάλο χρονικό διάστημα και σε όλες τις επανεκκινήσεις του συστήματός σας. Συνδέοντας τα Events αυτά στο δίκτυό σας, μπορείτε να εντοπίσετε στοιχεία μη εξουσιοδοτημένης δραστηριότητας και να κατανοήσετε πώς οι εισβολείς λειτουργούν στο δίκτυό σας.

Συνολικά οι δυνατότητες και οι λειτουργίες του Sysmon αναφέρονται μία προς μία παρακάτω [2]:

- Καταγραφή της διαδικασίας δημιουργίας με πλήρη γραμμή εντολών για τρέχουσες και γονικές διαδικασίες.
- Καταγραφή του Hash των αρχείων χρησιμοποιώντας αλγόριθμους κρυπτογράφησης SHA1 (προεπιλογή), MD5, SHA256 ή IMPHASH.
- Δυνατότητα χρήσης πολλαπλών ταυτόχρονα Hashes.

- Περιλαμβάνει μια διεργασία GUID διαδικασίας η οποία δημιουργεί συμβάντα για να επιτρέψει τη συσχέτιση των συμβάντων ακόμα και όταν τα Windows επαναχρησιμοποιήσουν αναγνωριστικά διεργασίας.
- Συμπεριλαμβάνει έναν οδηγό GUID σε κάθε εκδήλωση για να επιτρέπεται η συσχέτιση των συμβάντων στην ίδια περίοδο σύνδεσης.
- Καταγράφει τη φόρτωση των προγραμμάτων οδήγησης ή των DLLs με τις υπογραφές και τα Hashes τους.
- Τα αρχεία καταγραφής ανοίγουν για πρόσβαση πρώτης ανάγνωσης δίσκων και τόμων.
- Προαιρετικά διαθέτει δυνατότητα καταγραφής συνδέσεων δικτύου, συμπεριλαμβανομένης της πηγής κάθε σύνδεσης, των διευθύνσεων IP, των αριθμών θυρών, των ονομάτων κεντρικών υπολογιστών και των ονομάτων των θυρών.
- Δυνατότητα εντοπισμού αλλαγών στο χρόνο δημιουργίας αρχείων για να καταλάβουμε πότε δημιουργήθηκε πραγματικά ένα αρχείο. Η τροποποίηση του αρχείου δημιουργίας timestamps είναι μια τεχνική που συνήθως χρησιμοποιείται από κακόβουλο λογισμικό με σκοπό να καλύψει τα ίχνη του.
- Δυνατότητα αυτόματης επαναφόρτωσης της διαμόρφωσης αν αλλάξει η Registry των Windows.
- Φιλτράρισμα κανόνων για την αποδοχή ή τον αποκλεισμό δυναμικά ορισμένων συμβάντων.
- Δυνατότητα δημιουργίας Logs από την αρχή της διαδικασίας εκκίνησης του συστήματος για τη λήψη δραστηριότητας από ακόμη και εξελιγμένου κακόβουλου λογισμικού πυρήνα(kernel-mode malware).

Στα Windows Vista και σε όλες τι νεότερες εκδόσεις των Windows, το Sysmon καταγράφει τα Events του συστήματος και τα εμφανίζει στην τοποθεσία: **"Applications and Services Logs/Microsoft/Windows/Sysmon/Operational"** του Microsoft Event Viewer και τα οποία αποθηκεύει στην τοποθεσία: **"C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx"**. Όλα τα Events του Sysmon είναι σε επίπεδο πληροφοριών (Informational) και αναφέρουν την πηγή τους ως "Sysmon". Κάθε κατηγορία εργασιών έχει ένα αναγνωριστικό συμβάντος (Event ID), το οποίο απλοποιεί το φιλτράρισμα των Events. Αυτά παρατίθενται στον παρακάτω πίνακα και στη συνέχεια περιγράφονται το καθένα ξεχωριστά και λεπτομερώς [2].

Task Category	Event ID
Process Creation	1
A process changed a file creation time	2
Network connection	3

Sysmon service state changed	4
Process terminated	5
Driver loaded	6
Image loaded	7
CreateRemoteThread detected	8
RawAccessRead detected	9
ProcessAccess	10
FileCreate	11
RegistryEvent (Object create and delete)	12
RegistryEvent (Value Set)	13
RegistryEvent (Key and Value Rename)	14
FileCreateStreamHash	15
Sysmon configuration change	16
PipeEvent (Pipe Created)	17
PipeEvent (Pipe Connected)	18
WmiEvent (WmiEventFilter activity detected)	19
WmiEvent (WmiEventConsumer activity detected)	20
WmiEvent (WmiEventConsumerToFilter activity detected)	21
DNSEvent (DNS query)	22
FileDelete (A file delete was detected)	23
ClipboardChange (New content in the clipboard)	24
ProcessTampering (Process image change)	25
Error report	255

Sysmon event categories and IDs

Παρακάτω αναφέρονται πιο αναλυτικά καθώς και ορισμένα παραδείγματα για κάθε τύπου συμβάντος που δημιουργεί το Sysmon.

- **Event ID 1: 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: A process changed a file creation time:** Το συμβάν αλλαγής του χρόνου δημιουργίας ενός αρχείου καταγράφεται όταν ένας 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 για να φανούν σαν να έχουν εγκατασταθεί μέσω του λειτουργικό σύστημα. Σημειώστε βέβαια ότι πολλές διαδικασίες αλλάζουν νόμιμα το χρόνο δημιουργίας ενός αρχείου, γεγονός το οποίο δεν δηλώνει απαραίτητα κακόβουλη δραστηριότητα.
- **Event ID 3: Network Connection:** Το συμβάν δικτυακής σύνδεσης καταγράφει συνδέσεις TCP / UDP στο μηχάνημα όπου είναι εγκατεστημένο το Sysmon. Η λειτουργία αυτή είναι απενεργοποιημένη από προεπιλογή. Κάθε δικτυακή σύνδεση συνδέεται με μια διεργασία μέσω των πεδίων ProcessId και ProcessGUID. Το συμβάν περιέχει επίσης τις διευθύνσεις IP, τους αριθμούς των θυρών καθώς και την IPv6.
- **Event ID 4: Sysmon service state changed:** Το συμβάν αλλαγής της κατάστασης της υπηρεσίας αναφέρει την κατάσταση της υπηρεσίας του Sysmon (ξεκίνησε ή σταμάτησε αντίστοιχα).
- **Event ID 5: Process terminated:** Η διαδικασία τερματίζει τις αναφορές συμβάντων όταν τερματίζεται μια διαδικασία. Παρέχει το UtcTime, ProcessGuid και ProcessId της συγκεκριμένης διαδικασίας.
- **Event ID 6: Driver loaded:** Τα συμβάντα που φορτώνονται από κάποιον Driver παρέχουν πληροφορίες σχετικά με το αντίστοιχο πρόγραμμα οδήγησης που φορτώνεται στο σύστημα. Τα διαμορφωμένα Hashes παρέχονται καθώς και πληροφορίες υπογραφής. Η υπογραφή δημιουργείται ασύγχρονα για λόγους απόδοσης του συστήματος και υποδεικνύει εάν το αρχείο αφαιρέθηκε μετά τη φόρτωση του.
- **Event ID 7: Image loaded:** Το συμβάν φορτωμένης εικόνας καταγράφεται όταν μια ενότητα φορτώνεται σε μια συγκεκριμένη διαδικασία. Αυτό το συμβάν είναι απενεργοποιημένο από προεπιλογή κατά την εγκατάσταση του Sysmon σε ένα σύστημα Windows και πρέπει να ρυθμιστεί με την παράμετρο -l. Υποδεικνύει τη διαδικασία στην οποία φορτώνεται η ενότητα και διαθέτει πληροφορίες υπογραφής. Η υπογραφή δημιουργείται ασύγχρονα για λόγους απόδοσης του συστήματος 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 συμβάντων.
- **Event ID 8: CreateRemoteThread:** Το συμβάν CreateRemoteThread ανιχνεύει πότε μια διαδικασία δημιουργεί ένα νήμα σε μια άλλη διαδικασία. Αυτή η τεχνική χρησιμοποιείται συνήθως από κάποιο κακόβουλο λογισμικό για την έγχυση κώδικα και την απόκρυψη του σε άλλες διαδικασίες. Το συμβάν υποδεικνύει τη διαδικασία της πηγής και του στόχου. Παρέχει πληροφορίες σχετικά με τον κώδικα που θα εκτελεστεί στο νέο νήμα: StartAddress, StartModule και StartFunction. Σημειώστε ότι τα πεδία StartModule και StartFunction συνάγονται και ενδέχεται να είναι κενά

αν η διεύθυνση εκκίνησης βρίσκεται εκτός των φορτωμένων μονάδων ή των γνωστών εξαγόμενων λειτουργιών.

- **Event ID 9: RawAccessRead:** 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 αυτό υποδεικνύει τη διαδικασία προέλευσης και τη συσκευή προορισμού.
- **Event ID 10: ProcessAccess:** Η διαδικασία αυτή προσεγγίζει αναφορές γεγονότων 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 διαδικασίας στόχου. Αυτό επιτρέπει την ανίχνευση εργαλείων hacking που διαβάζουν τα περιεχόμενα μνήμης διαδικασιών όπως το Local Security Authority (Lsass.exe) για να κλέψουν τα διαπιστευτήρια για χρήση σε επιθέσεις με την τεχνική του Pass-the-Hash. Η ενεργοποίησή της συγκεκριμένης λειτουργίας μπορεί να δημιουργήσει σημαντικά ποσά καταγραφής εάν υπάρχουν ενεργοποιημένα διαγνωστικά βοηθητικά προγράμματα που ανοίγουν επανειλημμένα διεργασίες για την αναζήτηση της κατάστασής τους, οπότε γενικά θα πρέπει να γίνεται μόνο με φίλτρα που καταργούν τις προσδοκώμενες προσπελάσεις**.**
- **Event ID 11: FileCreate:** Οι εγγραφές δημιουργίας αρχείων καταγράφονται όταν ένα αρχείο δημιουργείται ή αντικαθίσταται. Αυτό το συμβάν είναι χρήσιμο για την παρακολούθηση των τοποθεσιών autostart, όπως το φάκελο "Εκκίνηση", καθώς και προσωρινών αλλά και κατεβασμένων καταλόγων, οι οποίοι είναι κοινές θέσεις κακόβουλων προγραμμάτων που εισέρχονται σε ένα σύστημα κατά την αρχική μόλυνση.
- **Event ID 12: RegistryEvent (Object create and delete):** Τα κλειδιά μητρώου και οι τιμές τους δημιουργούν και διαγράφουν χάρτες 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 του μητρώου από κάποιο κακόβουλο λογισμικό.

Το Sysmon χρησιμοποιεί συντομευμένες εκδόσεις στα ονόματα των ριζικών καταλόγων του μητρώου, με τις ακόλουθες αντιστοιχίσεις:

Όνομα κλειδιού	**Συντομογραφία**
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_LOCAL_MACHINE\System\ControlSet00x	HKLM\System\CurrentControlSet
HKEY_LOCAL_MACHINE\Classes	HKCR

- **Event ID 13: RegistryEvent (Value Set):** Αυτός ο τύπος συμβάντος μητρώου αναγνωρίζει τις τροποποιήσεις στις τιμές του μητρώου. Το συμβάν καταγράφει την τιμή που έχει εγγραφεί για τις τιμές μητρώου τύπου DWORD και QWORD**.**
- **Event ID 14: RegistryEvent (Key and Value Rename):** Το κλειδί μητρώου και η τιμή της μετονομασίας λειτουργιών σε αυτόν τον τύπο συμβάντος, λειτουργούν καταγράφοντας το νέο όνομα του κλειδιού ή της τιμής που μετονομάστηκε**.**
- **Event ID 15: FileCreateStreamHash:** Αυτό το συμβάν καταγράφεται όταν μια ονομαστική ροή αρχείου δημιουργείται και δημιουργεί συμβάντα που καταγράφουν το hash των περιεχομένων του αρχείου στο οποίο έχει εκχωρηθεί η ροή (η ονομαστική ροή), καθώς και τα περιεχόμενα της ροής που έχει ονομάσει. Υπάρχουν παραλλαγές κακόβουλου λογισμικού που ρίχνουν τα εκτελέσιμα τους ή τις ρυθμίσεις διαμόρφωσης μέσω λήψεων του προγράμματος περιήγησης και αυτό το συμβάν έχει ως στόχο να καταγράψει αυτό που βασίζεται στο πρόγραμμα περιήγησης που συνδέει μια ροή "σήμα του διαδικτύου" του Zone.Identifier.
- **Event ID 16: Sysmon configuration change:** Αυτό το συμβάν δημιουργείται όταν αλλάξει η κατάσταση διαμόρφωσης του Sysmon στο σύστημα το οποίο είναι εγκατεστημένο και μπορεί να περιλαμβάνει ή όχι κάποια τιμή κατακερματισμό. Εάν είχε καθοριστεί μια διαμόρφωση του Sysmon με αρχείο τύπου XML, τότε θα καταγραφεί μια τιμή κατακερματισμού του αρχείου, ώστε να μπορεί να εντοπιστεί εάν κάποιος αναδιαμορφώσει το Sysmon με ένα μη εξουσιοδοτημένο αρχείο διαμόρφωσης το οποίο θα παράγει διαφορετικό κατακερματισμό.
- **Event ID 17: PipeEvent (Pipe Created):** Αυτό το συμβάν δημιουργείται όταν δημιουργηθεί ένας ονομασμένος σωλήνας (Pipe). Το κακόβουλο λογισμικό χρησιμοποιεί συχνά ονομασμένους σωλήνες(Pipes) για επικοινωνία μεταξύ των διαδικασιών.
- **Event ID 18: PipeEvent (Pipe Connected):** Αυτό το συμβάν καταγράφεται όταν πραγματοποιείται μια ορισμένη σύνδεση σωλήνα (Pipe) μεταξύ ενός προγράμματος-πελάτη και ενός διακομιστή.
- **Event ID 19: WmiEvent (WmiEventFilter activity detected):** Όταν καταγράφεται ένα φίλτρο συμβάντος WMI, το οποίο είναι μια μέθοδος που χρησιμοποιείται από κάποιο κακόβουλο συνήθως λογισμικό για εκτέλεση, το συμβάν αυτό καταγράφει το χώρο ονομάτων WMI, το όνομα του φίλτρου και την έκφραση του φίλτρου.
- **Event ID 20: WmiEvent (WmiEventConsumer 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: WmiEvent (WmiEventConsumerToFilter 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: DNSEvent (DNS query):** Αυτό το συμβάν δημιουργείται όταν μια διεργασία εκτελεί ένα ερώτημα DNS, είτε το αποτέλεσμα είναι επιτυχές είτε αποτυγχάνει, αποθηκευμένο προσωρινά ή όχι. Η τηλεμετρία για αυτό το συμβάν

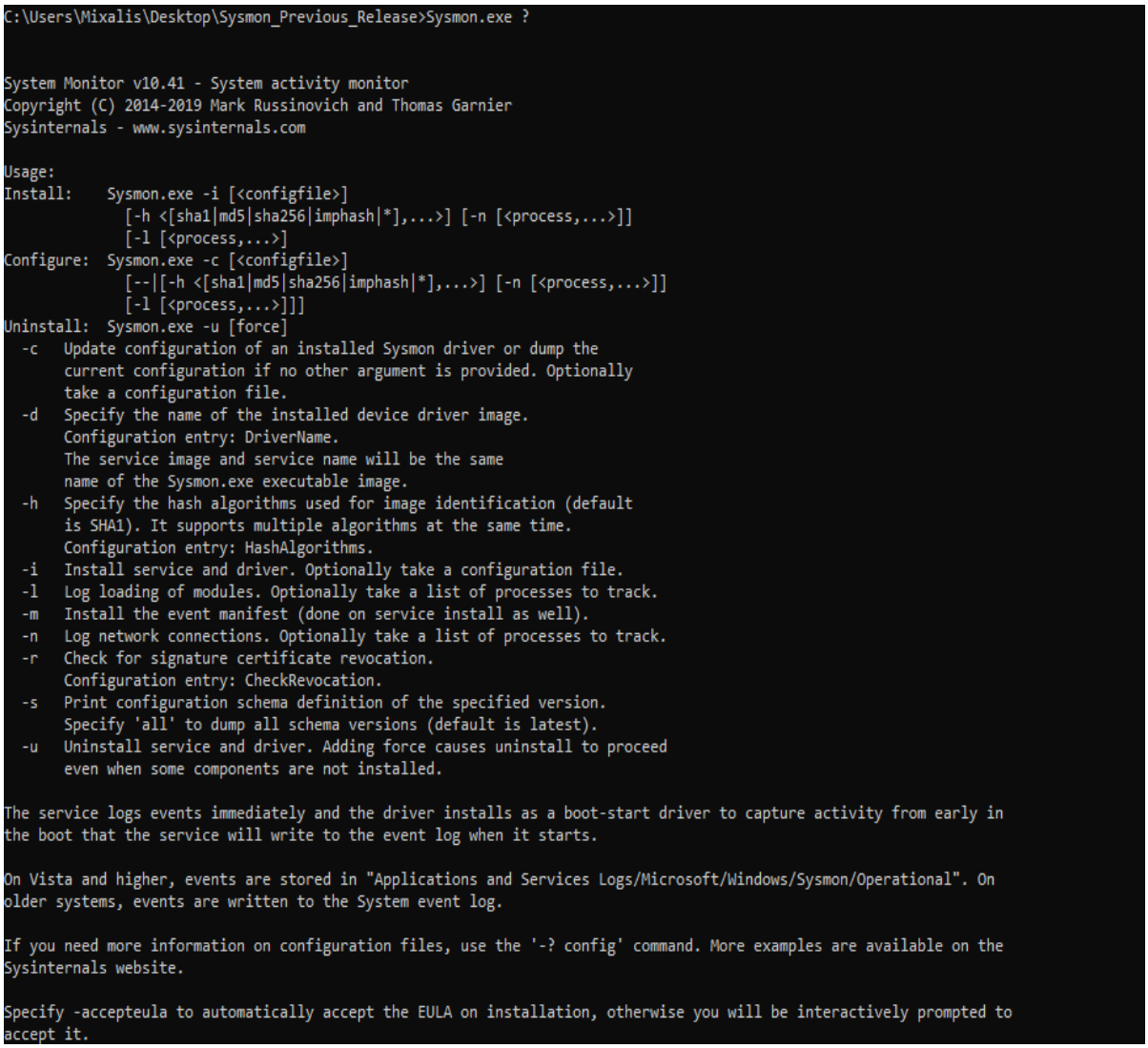
προστέθηκε ως δυνατότητα για τα Windows 8.1 και έπειτα, έτσι λοιπόν δεν είναι διαθέσιμη στα Windows 7 και σε όλα τα νωρίτερα από αυτό λειτουργικά συστήματα Windows.

- **Event ID 23: FileDelete (A file delete was detected):** Αυτό το συμβάν δημιουργείται όταν ένα αρχείο διαγράφεται εντός ενός συστήματος.
- **Event ID 24: ClipboardChange (New content in the clipboard):** Αυτό το συμβάν δημιουργείται όταν αλλάζουν τα περιεχόμενα του πρόχειρου στο εκάστοτε σύστημα.
- **Event ID 25: ProcessTampering (Process image change):** Αυτό το συμβάν δημιουργείται όταν η εικόνα μια διαδικασίας αλλάζει από μια εξωτερική πηγή, όπως μια διαφορετική διαδικασία.
- **Event ID 255: Error:** Αυτό το συμβάν δημιουργείται όταν έχει παρουσιαστεί κάποιο σφάλμα στο Sysmon. Τέτοια σφάλματα μπορούν να συμβούν αν το σύστημα βρίσκεται σε μεγάλο φορτίο και ορισμένες εντολές δεν μπορούν να εκτελεστούν ή υπάρχει σφάλμα στην υπηρεσία του Sysmon. Μπορείτε να αναφέρετε τυχόν σφάλματα του Sysmon στο φόρουμ Sysinternals ή στο Twitter (@markrussinovich).

2.3 Εγκατάσταση, Χρήση και Ρύθμιση του Sysmon

Το εργαλείο Sysmon των δημιουργών Mark Russinovich και Thomas Garnier μπορούμε να το βρούμε και να το κατεβάσουμε από τον ιστότοπο: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon . Όπως θα δείτε και παρακάτω παρουσιάζεται αρχικά ο τρόπος εγκατάστασης του Sysmon σε ένα Windows σύστημα και στη συνέχεια παρουσιάζεται ο τρόπος με τον οποίο μπορεί να ρυθμιστεί σωστά το Sysmon, καθώς και το πώς μπορεί να ενημερωθεί μέσω κάποιας προσαρμοσμένης διαμόρφωσης.

Ξεκινώντας με την εγκατάσταση του Sysmon, αφού έχουμε το αρχείο εγκατάστασης **`Sysmon.exe`** μπορούμε απλώς μέσα από τη γραμμή εντολών των Windows (cmd) να τρέξουμε την εντολή **`Sysmon.exe`** σε συνέχεια με ένα ερωτηματικό για να μάθουμε τι είδους επιλογές έχουμε. Αντίστοιχο παράδειγμα για αυτό μπορείτε να δείτε στη παρακάτω εικόνα που παραθέτουμε (Βλ. ***Εικόνα 2***) [3].



Εικόνα 2 – Εκτέλεση εντολής "Sysmon.exe?"

Ένα από τα αξιοσημείωτα θέματα είναι ότι ακόμα κι αν δεν καθορίσουμε συγκεκριμένες ρυθμίσεις, το Sysmon θα εγκατασταθεί χωρίς προβλήματα στο σύστημά μας. Όπως βλέπετε, υπάρχει μια επιλογή **-c** με την οποία μπορούμε να ενημερώσουμε τη διαμόρφωση του Sysmon, οποιαδήποτε στιγμή εμείς θέλουμε ακόμη και αν το Sysmon είναι ήδη εγκατεστημένο στο σύστημά μας. Μέσα από τη συγκεκριμένη επιλογή μπορούμε να καθορίσουμε ένα σωρό πράγματα τα οποία αναφέρονται αναλυτικότερα το καθένα παρακάτω.

Αρχικά μπορούμε να καθορίσουμε τους αλγόριθμους κατακερματισμού που θα δημιουργεί και που θα καταγράφει το Sysmon. Σαν βασικό αλγόριθμο κατακερματισμού μπορούμε να καθορίσουμε τον SHA1, αλλά έχουμε πολλές ακόμη επιλογές. Ένας ιδιαίτερα ενδιαφέρον αλγόριθμος κατακερματισμού είναι ο imphash που μοιάζει με κατακερματισμό εισαγωγής. Μπορούμε ακόμη να βασιστούμε στη λίστα των εισαγωγών για ένα συγκεκριμένο αρχείο εικόνας. Αυτό είναι αρκετά ενδιαφέρον ειδικά όταν οι

προγραμματιστές αλλάζουν την έκδοση του αρχείου και ούτω καθεξής, αλλά η λίστα των εισαγωγών παραμένει η ίδια.

Επιπλέον, έχουμε την πολύ σημαντική επιλογή **-l**, για τη καταγραφή των διαφόρων ενοτήτων του Sysmon.

Έχουμε επίσης την επιλογή **-n**, η οποία χρησιμοποιείται για την καταγραφή διαφορετικών τύπων συνδέσεων δικτύου και μπορούμε να κάνουμε πραγματικά πολύ ενδιαφέρον πράγματα γύρω από αυτή την επιλογή.

Μια ακόμη πολύ ενδιαφέρον επιλογή του Sysmon είναι ο διακόπτης **-r** με τον οποίο ενεργοποιώντας τον μπορούμε να ελέγξουμε για πιστοποιητικά υπογραφής με σκοπό την επαλήθευση τους. Έτσι, μπορούμε να επαληθεύσουμε τις υπογραφές και αν το πιστοποιητικό ανακαλείται ή όχι.

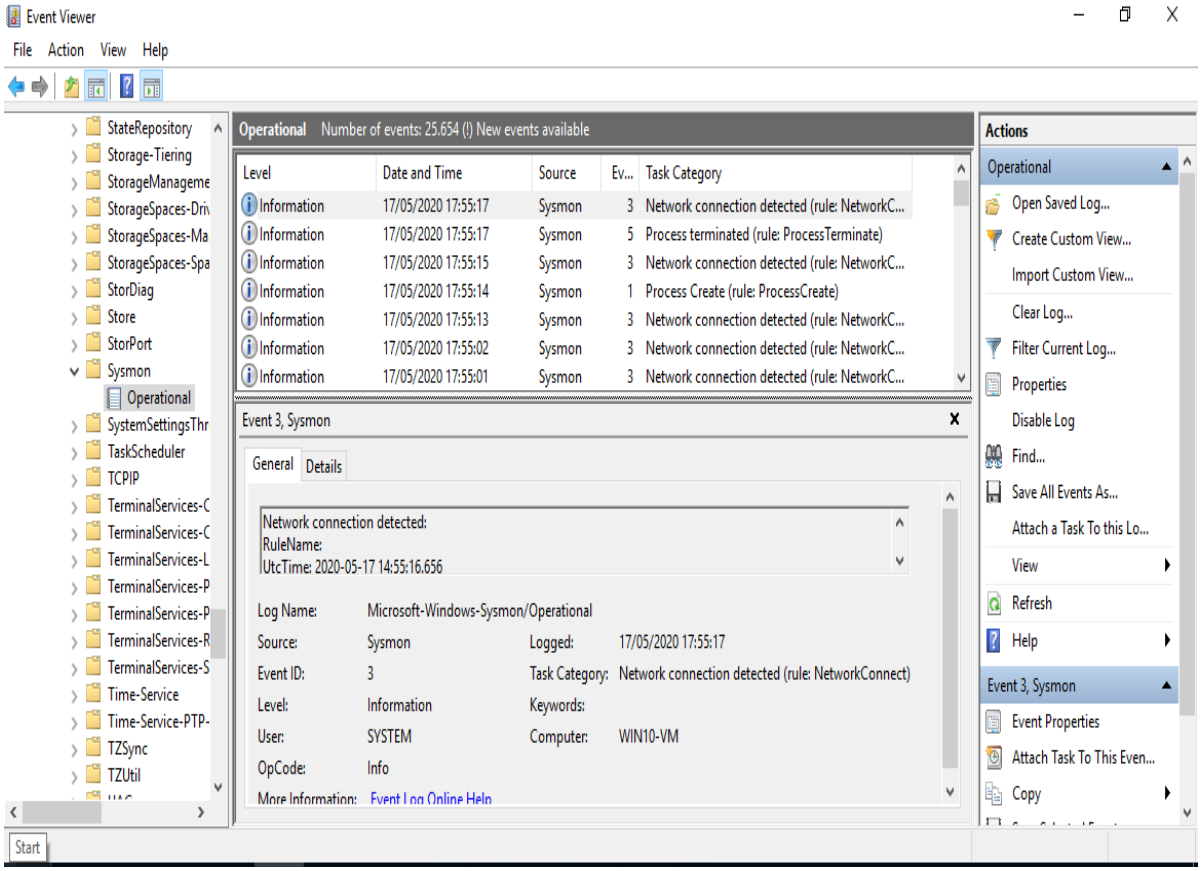
Ξεκινώντας λοιπόν με την εγκατάσταση του Sysmon στο σύστημά μας πληκτρολογούμε στη γραμμή εντολών (cmd) των Windows την εντολή **Sysmon.exe -i** για την εγκατάσταση του, **-h SHA1** για να καθορίσουμε ότι θα καταγράφονται οι SHA1(για παράδειγμα) κατακερματισμένες τιμές των αρχείων και μετά με την επιλογή **-l** για την ενεργοποίηση της καταγραφής διαφορετικών τύπων ενοτήτων που φορτώνονται στο σύστημα, για παράδειγμα DLL αρχεία. Η επόμενη και τελευταία επιλογή που θα καθορίσουμε είναι το **-n**, για τη καταγραφή των δικτυακών συνδέσεων. Αυτή είναι και αρχική εγκατάσταση του Sysmon, την εκτέλεση της οποίας μπορείτε να δείτε και παρακάτω (Βλ. ***Εικόνα 3***).

```
C:\Users\IEUser\Downloads\Sysmon>Sysmon.exe -i -h SHA1 -l -n

System Monitor v10.42 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.

C:\Users\IEUser\Downloads\Sysmon>
```

Εικόνα 3 – Εκτέλεση εντολής για την εγκατάσταση του Sysmon

Προς το παρόν, αφού ολοκληρώθηκε επιτυχώς η εγκατάσταση του Sysmon μπορούμε να επαληθεύσουμε τον τρόπο καταγραφής της δραστηριότητας του στα αρχεία καταγραφής των συμβάντων των Windows. Αυτά μπορούμε να τα βρούμε και να τα διαβάσουμε ανοίγοντας το Event Viewer των Windows. Για τη διαδικασία αυτή λοιπόν θα πρέπει να μεταβούμε στα αρχεία καταγραφής εφαρμογών και υπηρεσιών της Microsoft μέσα στο εκάστοτε Windows σύστημά μας και στη συνέχεια στο πεδίο του Sysmon. Αφού δώσουμε λίγο χρόνο λοιπόν σε αυτό για να ανοίξει έως ότου φορτώσει με όλα τα δεδομένα παρατηρούμε πως έχουμε όλες τις λεπτομέρειες που έχουμε επιλέξει να φορτώσουμε

μέσα από την εγκατάσταση του Sysmon. Ένα αντίστοιχο παράδειγμα αυτής της διαδικασίας εμφάνισης δίνεται παρακάτω (Βλ. ***Εικόνα 4***) [3].



Εικόνα 4 – Προβολή των αρχείων καταγραφής του Sysmon μέσω του Windows Event Viewer

Όσο αναφορά στην ανάλυση, το Sysmon είναι ένα υπέροχο εργαλείο, διότι μας επιτρέπει να παρακολουθούμε κατά τη συγκεκριμένη διαμόρφωσή που του έχουμε δώσει αυτή τη στιγμή, μια διαδικασία η οποία δημιουργεί ένα συμβάν και επίσης ένα συμβάν που τερματίζει τη διαδικασία. Όποτε, για παράδειγμα, ξεκινά μια διαδικασία, μπορούμε να εντοπίσουμε ότι η συγκεκριμένη διαδικασία είχε τις ακόλουθες παραμέτρους εκτέλεσης (Βλ. ***Εικόνα 5***).

Εικόνα 5 – Προβολή των αρχείων καταγραφής του Sysmon για την δημιουργία μιας διεργασίας

Επίσης, μπορούμε να γνωρίζουμε ποιος το έκανε και ποια ήταν η γονική εικόνα που ξεκίνησε αυτή τη διαδικασία. Αυτό είναι αρκετά ενδιαφέρον όταν αναλύουμε πολλά πράγματα, όπως για παράδειγμα ποιος ξεκίνησε ένα συγκεκριμένο εκτελέσιμο που μπορεί να είναι κακόβουλο λογισμικό.

Έχοντας αποκτήσει πρόσβαση στο αρχείο καταγραφής των Windows, αυτό που μας ενδιαφέρει τώρα είναι να επαληθεύσουμε ποια είναι και η διαδρομή του. Έτσι, μπορούμε να πάμε στις ιδιότητες του αρχείου καταγραφής των Windows και να δούμε τη διαδρομή στην οποία βρίσκονται τα αρχεία καταγραφής η οποία είναι: **`Windows\System 32\Winevt\`**. Επομένως, μπορούμε να αντιγράψουμε αυτό το μονοπάτι και παίξουμε λίγο σε αυτό, αλλά πρώτα απ' όλα, θα πάμε να ενημερώσουμε τη διαμόρφωση του Sysmon μέσω ενός .xml Configuration File. Αναλυτικότερα σχετικά με αυτή τη διαδικασία ενημέρωσης της διαμόρφωσης του Sysmon παρουσιάζονται στην παρακάτω ενότητα.

2.4 Ρύθμιση του Sysmon με χρήση αρχείου .xml configuration file

Για την εγκατάσταση του Sysmon χωρίς τις προεπιλεγμένες ρυθμίσεις του, αλλά κάνοντας χρήση συγκεκριμένου αρχείου διαμόρφωσης (.xml configuration file) χρησιμοποιούμε τη γραμμή εντολών των Windows και κάνουμε χρήση της παρακάτω εντολής:

```
sysmon -accepteula -i c:\Users\IEUser\Documents\config_file.xml
```

Το αρχείο διαμόρφωσης (.xml configuration file) που δίνεται ως όρισμα στη παραπάνω εντολή καθορίζει όλες τις ρυθμίσεις του Sysmon στο εκάστοτε σύστημα που θα γίνει η εγκατάσταση. Όπως παρατηρούμε ως όρισμα στη συγκεκριμένη εντολή δίνεται η απόλυτη διαδρομή του αρχείου διαμόρφωσης στην οποία είναι αποθηκευμένο στο εκάστοτε σύστημα [11].

Για να αλλάξουμε ή να ενημερώσουμε τη διαμόρφωση του ήδη εγκατεστημένου Sysmon σε ένα σύστημα με ένα αρχείο διαμόρφωσης (.xml configuration file) κάνουμε χρήση της παρακάτω εντολής [3]:

```
sysmon -c c:\Users\IEUser\Documents\config_file.xml
```

Η διαμόρφωση του Sysmon επηρεάζεται άμεσα από το αρχείο διαμόρφωσης που δίνεται κάθε φορά και σχεδιάζεται ώστε να βοηθήσει σε κάθε είδους προσαρμογή το αντίστοιχο περιβάλλον ή σύστημα να εντοπιστούν οι αντίστοιχες κακόβουλες ή ύποπτες δραστηριότητες που επιθυμούμε.

Ένα πολύ απλό παράδειγμα αρχείου διαμόρφωσης του Sysmon δίνεται παρακάτω (Βλ. ***Εικόνα 6***).

config.xml - Notepad

File Edit Format View Help

```
<Sysmon schemaversion="3.30">
  <HashAlgorithms>md5,sha256</HashAlgorithms>
  <EventFiltering>
    <NetworkConnect onmatch="exclude"/>
    <CreateRemoteThread onmatch="include">
      <TargetImage condition="image">explorer.exe</TargetImage>
      <TargetImage condition="image">lsass.exe</TargetImage>
      <TargetImage condition="image">services.exe</TargetImage>
      <TargetImage condition="image">svchost.exe</TargetImage>
      <TargetImage condition="image">winlogon.exe</TargetImage>
    </CreateRemoteThread>
    <RawAccessRead onmatch="exclude">
      <Image condition="image">C:\Windows\Sysmon.exe</Image>
      <Image condition="image">System</Image>
    </RawAccessRead>
    <!-- Event ID = 10 -->
    <ProcessAccess onmatch="include">
        <TargetImage condition="image">lsass.exe</TargetImage>
        </ProcessAccess>
    <FileCreate onmatch="include"/>
  </EventFiltering>
</Sysmon>
```

Εικόνα 6 – Παράδειγμα αρχείου διαμόρφωσης του Sysmon

Όπως θα καταλάβατε δεν είναι απαραίτητο να διαμορφώσετε τα πάντα, μπορείτε να διαμορφώσετε κατ' επιλογήν μόνο μερικά πράγματα. Και, με λίγα λόγια, μπορείτε επίσης να ορίσετε τι θα θέλατε να συμπεριλάβετε για ορισμένα συμβάντα ή να εξαιρέσετε. Για τις συνδέσεις δικτύου, για παράδειγμα στην παραπάνω περίπτωσή, παρακολουθούμε όλους τους τύπους συμβάντων. Μπορείτε ωστόσο να δημιουργήσετε ένα απομακρυσμένο νήμα, σε αυτήν τη συγκεκριμένη περίπτωση, παρακολουθώντας μόνο εξερευνητές, LSASS, υπηρεσίες, svchost, Winlogon και αντίστοιχα άλλα παρόμοια πράγματα. Η ακατέργαστη πρόσβαση ανάγνωσης ενεργοποιήθηκε, αποκλείοντας, φυσικά, το Sysmon και το σύστημα, αλλά τα υπόλοιπα παρακολουθούνται. Και φυσικά πράγματα όπως η πρόσβαση στη διαδικασία, η οποία είναι καλή για τον εντοπισμό επιθέσεων τύπου **pass-the-hash**, συμπεριλαμβάνουμε μόνο την LSASS. Αντιθέτως, στην περίπτωση του **FileCreate**

onmatch = "include", δεν παρακολουθώ τα πάντα και συγκεκριμένα δεν παρακολουθείται τίποτα στο παραπάνω παράδειγμα αρχείου διαμόρφωσης. Αυτός είναι γενικά ο τρόπος με τον οποίο δουλεύουμε σε ένα αρχείο διαμόρφωσης τύπου .xml του Sysmon.

Στα πλαίσια της συγκεκριμένης εργασίας επειδή έχουμε ως στόχο να εντοπίσουμε την εσωτερική μετακίνηση ενός επιτιθέμενου σε δίκτυο με Windows Domain κάνοντας χρήση του εργαλείου Sysmon, χρησιμοποιήσαμε μια κατάλληλη διαμόρφωση η οποία παρατίθεται ως παράτημα στο τελευταίο κεφάλαιο της συγκεκριμένης εργασίας. Πρόκειται για ένα πρότυπο αρχείου διαμόρφωσης του Sysmon με προεπιλεγμένη παρακολούθηση συμβάντων σε υψηλό βαθμό [11]. Το αρχείο διαμόρφωσης θα πρέπει να λειτουργεί ως σημείο εκκίνησης για την παρακολούθηση αλλαγών του συστήματος σε ένα αυτόνομο και προσβάσιμο πακέτο. Σημειώστε ότι η διαμόρφωση αυτή του Sysmon δεν παρακολουθεί πράγματα όπως έλεγχο ταυτότητας και άλλα συμβάντα των Windows που είναι επίσης ζωτικής σημασίας για την έρευνα συμβάντων. Για τον λόγο αυτό έχουμε παραθέσει παρακάτω ορισμένες κατάλληλες ρυθμίσεις για τα αρχεία καταγραφής των Windows όπου σε συνδυασμό με το Sysmon έχουν ως σκοπό τον εντοπισμό της εσωτερικής μετακίνησης ενός επιτιθέμενου.

3 Αρχεία Καταγραφής συμβάντων σε συστήματα Windows

Η Microsoft αύξησε σταδιακά την αποδοτικότητα και την αποτελεσματικότητα των ελεγκτικών εγκαταστάσεων της με τα χρόνια. Τα σύγχρονα συστήματα Windows μπορούν να καταγράψουν τεράστιες ποσότητες πληροφοριών με ελάχιστο αντίκτυπο στο σύστημα. Η διαμόρφωση επαρκούς καταγραφής στα συστήματα Windows και η ιδανική συγκέντρωση αυτών των αρχείων καταγραφής σε SIEM ή σε άλλο αθροιστή καταγραφής, είναι ένα κρίσιμο βήμα προς τη διασφάλιση του ότι ένα περιβάλλον Windows μπορεί να υποστηρίξει μια αποτελεσματική απόκριση συμβάντων. Τα σύγχρονα συστήματα Windows αποθηκεύουν αρχεία καταγραφής στον κατάλογο **%SystemRoot%\System32\winevt\logs** από προεπιλογή στη δυαδική μορφή καταγραφής συμβάντων των Windows XML, που ορίζεται από την επέκταση **.evtx**. Τα αρχεία καταγραφής μπορούν επίσης να αποθηκευτούν εξ' αποστάσεως χρησιμοποιώντας συνδρομές καταγραφής. Για απομακρυσμένη καταγραφή, ένα απομακρυσμένο σύστημα που εκτελεί την υπηρεσία Windows Event Collector εγγράφεται σε συνδρομές αρχείων καταγραφής που παράγονται από άλλα συστήματα. Οι τύποι αρχείων καταγραφής που θα συλλεχθούν μπορούν να καθοριστούν σε επίπεδο κοκκώδους και η μεταφορά πραγματοποιείται μέσω HTTPS στη θύρα 5986 χρησιμοποιώντας WinRM. Τα GPO μπορούν να χρησιμοποιηθούν για τη διαμόρφωση των απομακρυσμένων εγκαταστάσεων καταγραφής σε κάθε υπολογιστή. Τα συμβάντα μπορούν να καταγραφούν στα αρχεία καταγραφής συμβάντων ασφαλείας, συστήματος και εφαρμογών ή, σε σύγχρονα συστήματα Windows, ενδέχεται επίσης να εμφανίζονται σε πολλά άλλα αρχεία καταγραφής. Αναλυτικότερα παρακάτω στην ενότητα "Διαχωρισμός των αρχείων καταγραφής" περιγράφονται οι κατηγορίες στις οποίες κατηγοριοποιούν τα Windows τα αρχεία καταγραφής τους.

3.1 Διαχωρισμός των αρχείων καταγραφής

Ένα αρχείο καταγραφής είναι ένα αρχείο δεδομένων που δημιουργείται από έναν υπολογιστή και περιέχει πληροφορίες σχετικά με μοτίβα χρήσης, δραστηριότητες και λειτουργίες εντός λειτουργικού συστήματος, εφαρμογής, διακομιστή ή άλλης συσκευής.

Τα αρχεία καταγραφής των Windows είναι αρχεία των συμβάντων που συμβαίνουν στον υπολογιστή σας, είτε από ένα άτομο είτε από μια διαδικασία ή διεργασία που εκτελείται στο σύστημα. Το αρχείο καταγραφής συμβάντων των Windows περιέχει αρχεία καταγραφής από το λειτουργικό σύστημα και εφαρμογές, όπως SQL Server ή Internet Information Services (IIS). Τα αρχεία καταγραφής χρησιμοποιούν μια δομημένη μορφή δεδομένων, καθιστώντας τα εύκολα στην αναζήτηση και ανάλυση.

Τα Windows αποθηκεύουν τα αρχεία καταγραφής συμβάντων και διαχωρίζονται στις παρακάτω πέντε υποκατηγορίες:

- *Application (Εφαρμογή)*

  Περιλαμβάνουν τις καταγραφές από τη λειτουργία των εφαρμογών που βρίσκονται εγκατεστημένες στο σύστημα. Το τι θα καταγραφεί, καθορίζεται από το δημιουργό της κάθε επιμέρους εφαρμογής.

- *Security (Ασφάλεια)*

  Περιλαμβάνουν συμβάντα συστήματος που αφορούν την προστασία του συστήματος, όπως για παράδειγμα συμβάντα αυθεντικοποίησης, μεταβολές αντικειμένων, χρήση πόρων κ.ά. Η επιλογή των συμβάντων που θα καταγράφονται καθορίζεται από το διαχειριστή του συστήματος.

- *Setup (Ρύθμιση)*

  Περιλαμβάνουν συμβάντα σχετικά με τον έλεγχο τομέων, όπως η θέση των αρχείων καταγραφής μετά από μια διαμόρφωση δίσκου.

- *System (Σύστημα)*

  Καταγράφονται συμβάντα σχετικά με τη λειτουργία του συστήματος, όπως αστοχία ενός οδηγού συσκευής ή ενός υποσυστήματος κ.ά. Η επιλογή των συμβάντων που θα καταγράφονται είναι προκαθορισμένη από το εκάστοτε σύστημα.

- *Forwarded Events (Προωθούμενα συμβάντα)*

  Τα προωθούμενα συμβάντα αφορούν συμβάντα διαφορετικών μηχανημάτων του ίδιου δικτύου και χρησιμοποιούνται από έναν διαχειριστή στην περίπτωση που θέλει να χρησιμοποιήσει έναν υπολογιστή που να συγκεντρώνει πολλαπλά αρχεία καταγραφής από διαφορετικά μηχανήματα στο ίδιο δίκτυο.

3.2 Κατηγορίες των αρχείων καταγραφής βάσει κρισιμότητας

Τα Windows επίσης κατηγοριοποιούν κάθε συμβάν σύμφωνα με ένα επίπεδο κρισιμότητας το οποίο τα ίδια έχουν ορίσει εξ' αρχής. Τα επίπεδα αυτά κατά σειρά κρισιμότητας είναι τα εξής [9]:

- *Συμβάντα Πληροφορίας*

Τα αρχεία καταγραφής με αυτήν την κατηγοριοποίηση σημαίνουν συνήθως ότι στο γεγονός που συνέβη δεν υπήρχε κάποιο πρόβλημα. Τα περισσότερα αρχεία καταγραφής αποτελούνται από γεγονότα που βασίζονται σε πληροφορίες. Ένα τέτοιο παράδειγμα συμβάντος πληροφορίας βάσει συστήματος είναι το Event με το αναγνωριστικό νούμερο: 1042, MsiInstaller, το οποίο υποδεικνύει τον τερματισμό μιας συναλλαγής Windows Installer στο σύστημα.

- *Συμβάντα Προειδοποίησης*

Τα συμβάντα με την κατηγοριοποίηση της προειδοποίησης βασίζονται σε συγκεκριμένα μονάχα συμβάντα. Τα προειδοποιητικά μηνύματα μπορούν να επιστήσουν την προσοχή σε πιθανά ζητήματα που ενδέχεται να μην απαιτούν άμεση δράση. Το Event για παράδειγμα με το αναγνωριστικό νούμερο: 4003, μας δείχνει ότι η λειτουργία της αυτόματης διαμόρφωσης του WLAN εντόπισε περιορισμένη συνδεσιμότητα, επιχειρώντας αυτόματη ανάκτηση.

- *Συμβάντα Σφάλματος*

Τα συμβάντα επιπέδου σφάλματος δείχνουν ότι κάποια λειτουργία του συστήματος δεν κατάφερε να φορτώσει ή να λειτουργήσει αναμενόμενα. Το Event με το αναγνωριστικό

νούμερο: 36, το Volsnap είναι ένα παράδειγμα σφάλματος συστήματος όταν ένας υπολογιστής δεν μπορεί να δημιουργήσει σκιώδη αντίγραφα του τόμου C: επειδή ο αποθηκευτικός χώρος σκιώδους αντιγράφου δεν μπόρεσε να αυξηθεί λόγω του ορίου που επέβαλε ο χρήστης.

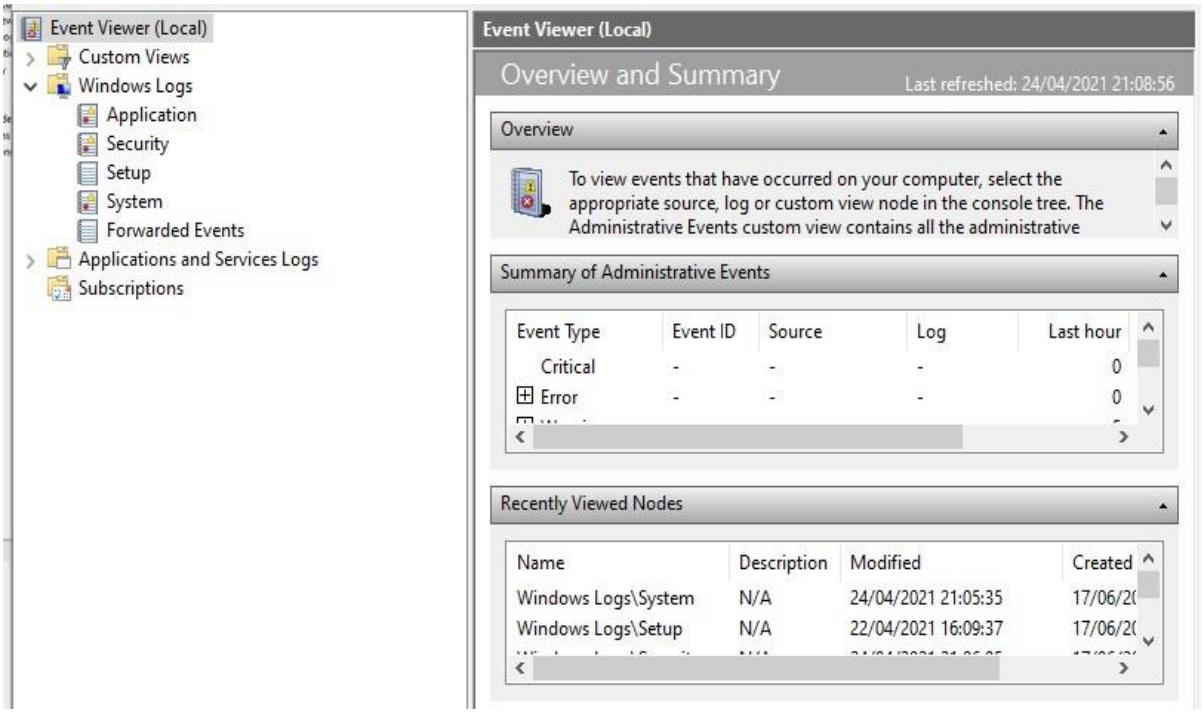
- *Κρίσιμα Συμβάντα*

Τα κρίσιμα συμβάντα υποδεικνύουν τα σοβαρότερα προβλήματα του συστήματος. Ένα αντίστοιχο παράδειγμα είναι το συμβάν με το αναγνωριστικό νούμερο: 41, το Kernel-Power το οποίο δημιουργείται όταν ένα σύστημα επανεκκινηθεί χωρίς να κλείσει καθαρά πρώτα. Αυτό το σφάλμα θα μπορούσε να προκληθεί στην περίπτωση που το σύστημα σταμάτησε να ανταποκρίνεται ή έχασε ενέργεια απροσδόκητα.

3.3 Πρόγραμμα Προβολής των αρχείων καταγραφής

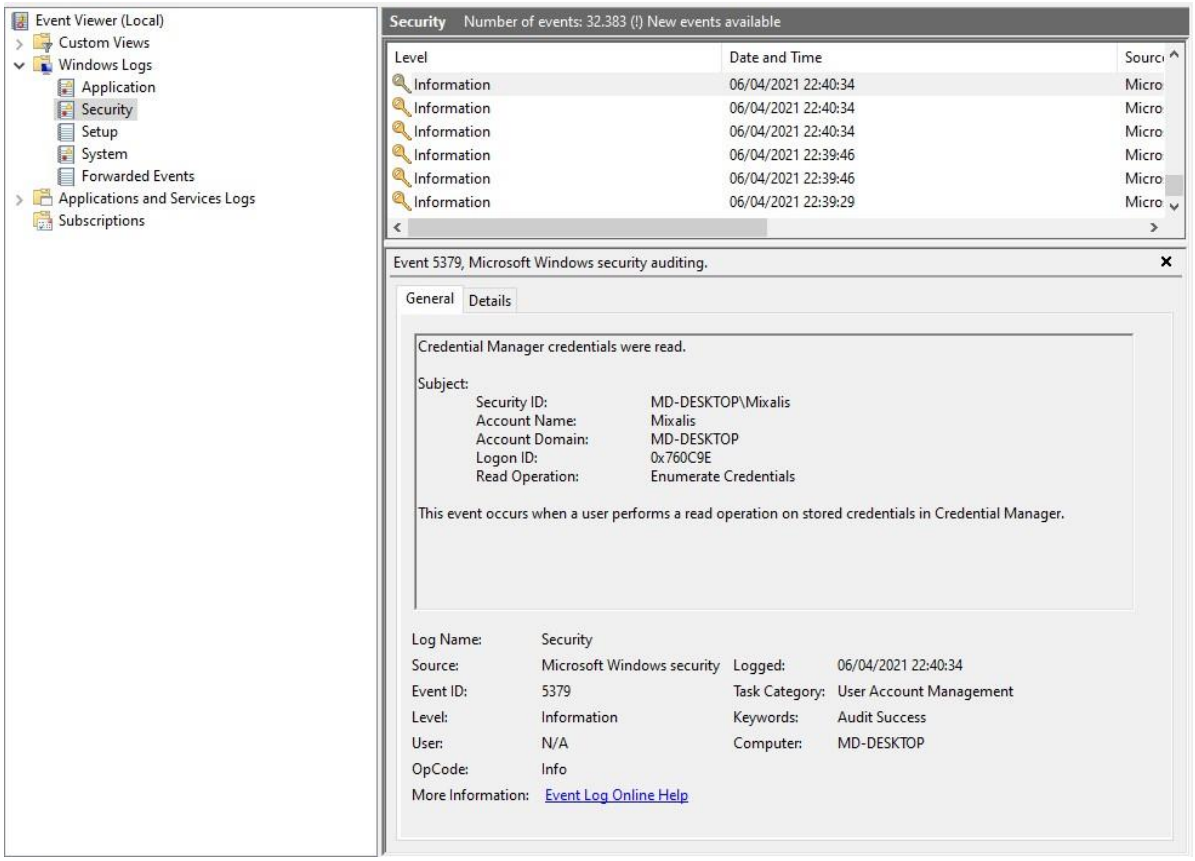
Το Windows Event Viewer είναι το ενσωματωμένο εργαλείο των Windows το οποίο εμφανίζει όλο το αρχείο καταγραφής μηνυμάτων εφαρμογής και συστήματος, συμπεριλαμβανομένων σφαλμάτων, μηνυμάτων με πληροφορίες και προειδοποιήσεων. Είναι ένα χρήσιμο εργαλείο για την αντιμετώπιση όλων των ειδών διαφορετικών προβλημάτων των Windows καθώς και θεμάτων ασφάλειας. Να σημειωθεί ότι ακόμη και ένα σωστά λειτουργικό σύστημα θα εμφανίζει διάφορες προειδοποιήσεις και σφάλματα στα αρχεία καταγραφής που μπορείτε να δείτε με του Event Viewer.

Παρακάτω ανοίγοντας τον Event Viewer των Windows μπορούμε να δούμε τη δομή που έχουμε και η οποία περιεγράφηκε παραπάνω (Βλ. ***Εικόνα 7***) [9].



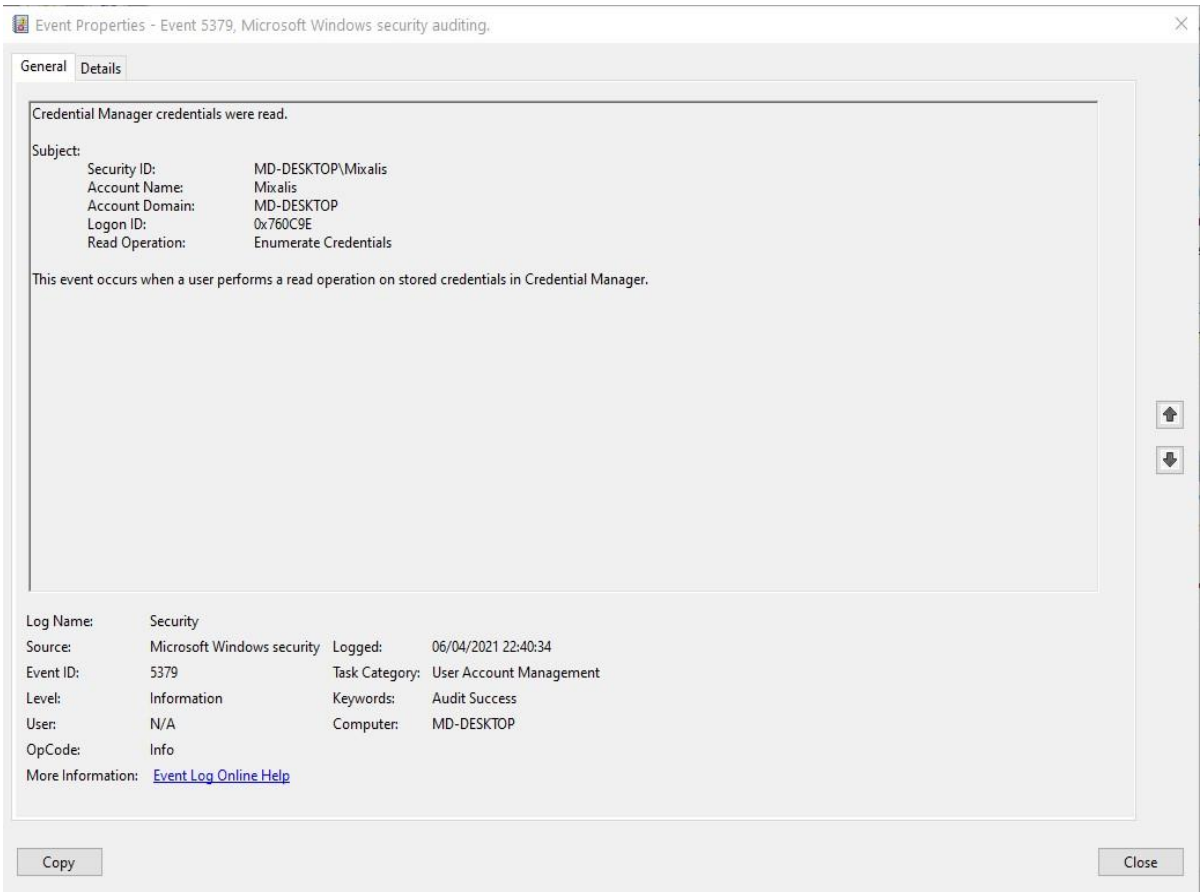
Εικόνα 7 [9] – Κατηγορίες των Windows Logs

Από την λίστα στο αριστερό τμήμα, αναπτύξτε την επιλογή Windows Logs και επιλέξτε Security. Παρατηρήστε στο κεντρικό τμήμα τα συμβάντα (Events) που έχουν καταγραφεί. Επιλέγοντας ένα Event, μπορούμε, στο κάτω μέρος, να παρατηρήσουμε γενικές πληροφορίες, καθώς και αναλυτικότερα στοιχεία του συμβάντος (Βλ. ***Εικόνα 8***).



Εικόνα 8 – Επιλογή συμβάντος

Κάνοντας διπλό κλικ στο συμβάν θα ανοίξει παράθυρο όπου μπορούμε πιο εύκολα να μελετήσουμε όλες τις λεπτομέρειες σχετικά με αυτό. Παρακάτω παρουσιάζονται αναλυτικά όλες οι πληροφορίες από ένα καταγεγραμμένο συμβάν (Βλ. ***Εικόνα 9***).



Εικόνα 9 – Προβολή πληροφοριών συμβάντος

Κάθε συμβάν καταχώρησης του αρχείου καταγραφής περιέχει τις ακόλουθες πληροφορίες [9]:

- *Ημερομηνία*: Η ημερομηνία εμφάνισης του συμβάντος.
- *Όνομα καταγραφής*: Το όνομα του αρχείου καταγραφής συμβάντων όπου είναι αποθηκευμένο το συμβάν. Χρήσιμο κατά την επεξεργασία πολλών αρχείων καταγραφής που τραβήχτηκαν από το ίδιο σύστημα.
- *Ώρα*: Η ημερομηνία και ώρα του τοπικού συστήματος κατά την οποία καταγράφηκε το συμβάν.
- *Χρήστης*: Το όνομα χρήστη που καταγράφηκε στο σύστημα τη στιγμή που συνέβη το συμβάν.
- *Υπολογιστής*: Το όνομα του υπολογιστή στον οποίο καταγράφηκε το συμβάν. Αυτό είναι χρήσιμο κατά την εξέταση των αρχείων καταγραφής που συλλέγονται από πολλά συστήματα, αλλά δεν πρέπει να θεωρείται ως η συσκευή που προκάλεσε ένα συμβάν.
- *Αναγνωριστικό συμβάντος*: Αναγνωριστικός αριθμός 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.
- *Επίπεδο*: Η κρισιμότητα που αποδίδεται στο εν λόγω συμβάν.
- *Περιγραφή*: Ένα μπλοκ κειμένου όπου καταγράφονται πρόσθετες πληροφορίες ειδικά για το συμβάν που καταγράφεται. Αυτό είναι συχνά το πιο σημαντικό πεδίο για τον αναλυτή.

3.4 Αξιοσημείωτα αρχεία καταγραφής για την ανίχνευση εσωτερικής μετακίνησης

Αξίζει σε αυτό το σημείο να σημειωθούν ορισμένες κατηγορίες συμβάντων καθώς και συμβάντα των Windows τα οποία είναι μείζονος σημασίας για την ανίχνευση της εσωτερικής μετακίνησης ενός επιτιθέμενου μέσα σε ένα δίκτυο με Windows Domain. Ορισμένα από αυτά του είδους τα συμβάντα είναι η πρόσβαση σε κοινόχρηστα αντικείμενα. Οι επιτιθέμενοι αξιοποιούν συχνά έγκυρα διαπιστευτήρια που έχουν υποκλέψει για απομακρυσμένη πρόσβαση σε δεδομένα και υπολογιστές μέσω κοινών στοιχείων που δημιουργούνται από χρήστες ή διαχειριστές. Με αυτόν τον τρόπο θα δημιουργηθούν συμβάντα σύνδεσης λογαριασμού και σύνδεσης γενικά, αλλά και πρόσθετη καταγραφή για τέτοιου είδους συμβάντα μπορεί επίσης να ενεργοποιηθεί στην κονσόλα διαχείρισης πολιτικής ομάδας μεταβαίνοντας στο: **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies -> Object Access -> Audit File Share**. Μόλις ενεργοποιηθεί η επιλογή αυτή, τα ακόλουθα αναγνωριστικά συμβάντων θα καταγραφούν στο αρχείο καταγραφής συμβάντων ασφαλείας [4].

Αναγνωριστικά συμβάντος κοινής χρήσης δικτύου:

Αναγνωριστικό Συμβάντος	Περιγραφή
5140	Προσπελάστηκε ένα αντικείμενο κοινής χρήσης δικτύου. Η καταχώριση συμβάντος παρέχει το όνομα λογαριασμού και τη διεύθυνση προέλευσης του λογαριασμού που έχει πρόσβαση στο αντικείμενο. Λάβετε υπόψη ότι σε αυτήν την καταχώριση θα εμφανίζεται ότι έγινε πρόσβαση στο κοινόχρηστο στοιχείο, αλλά όχι σε ποια αρχεία στο κοινόχρηστο. Ένας μεγάλος αριθμός αυτών των συμβάντων από έναν μόνο λογαριασμό μπορεί να αποτελεί ένδειξη ενός λογαριασμού που χρησιμοποιείται για τη συλλογή ή χαρτογράφηση δεδομένων στο δίκτυο.
5142	Προστέθηκε ένα αντικείμενο κοινής χρήσης δικτύου.
5143	Ένα αντικείμενο κοινής χρήσης δικτύου τροποποιήθηκε.
5144	Ένα αντικείμενο κοινής χρήσης δικτύου διαγράφηκε.
5145	Έγινε έλεγχος ενός αντικειμένου κοινής χρήσης δικτύου για να δει εάν μπορεί να παραχωρηθεί στον πελάτη

	επιθυμητή πρόσβαση. Η αποτυχία καταγράφεται μόνο εάν απορριφθεί η άδεια σε επίπεδο κοινής χρήσης αρχείων. Εάν η άδεια απορριφθεί σε επίπεδο NTFS τότε δεν καταγράφεται καταχώριση.

Εάν είναι ενεργοποιημένος ο λεπτομερής έλεγχος μεριδίου αρχείων στην κονσόλα διαχείρισης πολιτικής ομάδας, μεταβαίνοντας στο: **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies -> Object Access -> Audit Detailed Share Share** κάθε αρχείο σε κάθε κοινόχρηστο στοιχείο στο οποίο έχει πρόσβαση θα δημιουργήσει μια καταχώριση καταγραφής συμβάντος με αναγνωριστικό: **5145**. Όπως μπορείτε να φανταστείτε, αυτό το επίπεδο καταγραφής ενδέχεται να δημιουργήσει μεγάλο όγκο αποτελεσμάτων. Το σύστημα που ξεκινά την πρόσβαση ενδέχεται επίσης να εμφανίζει στοιχεία για τις συνδέσεις στο κλειδί μητρώου: **NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2**.

Παρά το γεγονός ότι είναι ένα υποσύνολο της κλοπής διαπιστευτηρίων, υπάρχουν αρκετές επιπλέον εκτιμήσεις που πρέπει να ληφθούν υπόψη όταν τα διαπιστευτήρια αξιοποιούνται για να αποκτήσουν πρόσβαση οι επιτιθέμενοι σε ένα σύστημα μέσω του Remote Desktop Protocol (RDP). Εάν το RDP χρησιμοποιείται τακτικά από τους διαχειριστές ή από το γραφείο βοήθειας χρηστών ενός τομέα Windows, παρέχει ένα ελκυστικό φορέα επίθεσης για τους επιτιθέμενους που προσπαθούν να προσομοιώσουν μια τυπική δραστηριότητα μέσα σε ένα δίκτυο. Μόλις βρεθεί σε σύστημα πελάτη, ο επιτιθέμενος μπορεί απλά να αξιοποιήσει τα ενσωματωμένα εργαλεία της Microsoft για να επιτρέψει την απομακρυσμένη πρόσβαση του σε άλλα συστήματα χρησιμοποιώντας την υπηρεσία RDP σε συνδυασμό με έγκυρα διαπιστευτήρια. Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει το εργαλείο Microsoft Remote Desktop Connection (mstsc.exe) για να αποκτήσει πρόσβαση σε ένα σύστημα ενός θύματος. Ενώ ελπίζουμε ότι δεν εκτίθεται η προεπιλεγμένη θύρα 3389 στο Διαδίκτυο, εάν η προώθηση θύρας έχει ρυθμιστεί ως άξονας σε άλλα συστήματα προσβάσιμα στο διαδίκτυο το καθιστούν δυνατό από εξωτερικούς ή εσωτερικούς κεντρικούς υπολογιστές. Ανάλογα με το διαθέσιμο εύρος ζώνης, αυτή η προσέγγιση που βασίζεται στο γραφικό περιβάλλον μπορεί να είναι λιγότερο από ιδανική για τον εισβολέα, αλλά εάν αυτή είναι μια μέθοδος που χρησιμοποιείται συνήθως στο περιβάλλον σας, οι επιτιθέμενοι είναι πιθανό να το χρησιμοποιήσουν για να ταιριάξουν με την κανονική κίνηση του δικτύου. Από την πλευρά των αμυνόμενων τώρα η υπηρεσία RDP αξιοποιεί τον τυπικό έλεγχο ταυτότητας της Microsoft για τον έλεγχο της πρόσβασης σε πόρους, επομένως τα αρχεία καταγραφής που σχετίζονται με τη σύνδεση λογαριασμού και τα συμβάντα σύνδεσης που περιγράφονται παραπάνω θα ισχύουν για συνδέσεις RDP. Εκτός από τα συμβάντα σύνδεσης λογαριασμού, άλλες καταχωρήσεις καταγραφής συμβάντων που μπορεί να είναι χρήσιμες για τον εντοπισμό και την παρακολούθηση κακόβουλης χρήσης του RDP στο περιβάλλον σας περιλαμβάνουν τα παρακάτω αναγνωριστικά [4]:

- **4624** - Το συμβάν σύνδεσης θα εμφανίσει είτε τον τύπο 10 είτε τον τύπο 3 όταν χρησιμοποιείται το RDP, ανάλογα με τις εκδόσεις των Windows που χρησιμοποιούνται και τη συγκεκριμένη διαμόρφωσή τους.

- **4778** - Αυτό το συμβάν καταγράφεται όταν μια περίοδος σύνδεσης επανασυνδέεται σε κάποιο σταθμό εργασίας Windows. Αυτό μπορεί να συμβεί τοπικά όταν το περιβάλλον χρήστη αλλάζει μέσω γρήγορης εναλλαγής χρηστών. Μπορεί επίσης να συμβεί όταν μια περίοδος σύνδεσης επανασυνδεθεί μέσω RDP. Για να γίνει διάκριση μεταξύ εναλλαγής RDP και τοπικής περιόδου σύνδεσης, ανατρέξτε στο πεδίο Όνομα περιόδου σύνδεσης στην περιγραφή του συμβάντος. Εάν είναι τοπικό, το πεδίο θα περιέχει Κονσόλα και, εάν είναι απομακρυσμένο, θα ξεκινήσει με RDP. Για συνεδρίες RDP, οι απομακρυσμένες πληροφορίες κεντρικού υπολογιστή θα βρίσκονται στην ενότητα Πληροφορίες δικτύου της περιγραφής του συμβάντος.
- **4779** - Αυτό το συμβάν καταγράφεται όταν αποσυνδέεται μια περίοδος σύνδεσης. Αυτό μπορεί να συμβεί τοπικά όταν το περιβάλλον χρήστη αλλάζει μέσω γρήγορης εναλλαγής χρηστών. Μπορεί επίσης να συμβεί όταν μια περίοδος σύνδεσης επανασυνδεθεί μέσω RDP. Μια πλήρης αποσύνδεση από μια περίοδο λειτουργίας RDP καταγράφεται με το Αναγνωριστικό συμβάντος **4637** ή **4647** όπως αναφέρθηκε προηγουμένως. Για να γίνει διάκριση μεταξύ εναλλαγής RDP και τοπικής περιόδου σύνδεσης, ανατρέξτε στο πεδίο Όνομα περιόδου σύνδεσης στην περιγραφή του συμβάντος. Εάν είναι τοπικό, το πεδίο θα περιέχει Κονσόλα και εάν είναι απομακρυσμένο, θα ξεκινήσει με RDP. Για συνεδρίες RDP, οι πληροφορίες απομακρυσμένου κεντρικού υπολογιστή θα βρίσκονται στην ενότητα Πληροφορίες δικτύου της περιγραφής συμβάντος.

Στο μηχάνημα που λαμβάνει τη σύνδεση, ενδέχεται να βρεθούν πρόσθετα αρχεία καταγραφής και συγκεκριμένα των υπηρεσιών RDP. Το αρχείο καταγραφής: **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4** μπορεί να περιέχει τη διεύθυνση IP και το όνομα χρήστη σύνδεσης του υπολογιστή προέλευσης στα αναγνωριστικά συμβάντων 21, 22 ή 25. Το Αναγνωριστικό συμβάντος 41 μπορεί επίσης να περιέχει το όνομα χρήστη σύνδεσης. Το λειτουργικό αρχείο καταγραφής: **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4** ενδέχεται να εγγράψει το Αναγνωριστικό συμβάντος **1149** που περιέχει τη διεύθυνση IP έναρξης και το όνομα χρήστη σύνδεσης. Τέλος, το αρχείο καταγραφής: **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational** μπορεί να εγγράψει το Αναγνωριστικό συμβάντος **131** που περιέχει την αρχική διεύθυνση IP και το όνομα χρήστη σύνδεσης.

Μια ακόμη κατηγορία συμβάντων η οποία μπορεί να φανεί αρκετά χρήσιμη για τον εντοπισμό πλευρικής μετακίνησης ενός επιτιθέμενου είναι η καταγραφή των συμβάντων για τις προγραμματισμένες εργασίες ενός συστήματος Windows. Εάν το ιστορικό είναι ενεργοποιημένο στην εφαρμογή Task Scheduler, μέσω του Event Viewer των Windows ή με την εντολή: **wevtutil** τότε στο αρχείο καταγραφής: **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Operationa**l θα καταγράφεται όλη η δραστηριότητα σχετικά με τις προγραμματισμένες εργασίες στο τοπικό σύστημα.

Αναγνωριστικά συμβάντων δραστηριότητας προγραμματισμένων εργασιών:

Αναγνωριστικό Συμβάντος	Περιγραφή
106	Δημιουργήθηκε προγραμματισμένη εργασία. Στην καταχώριση εμφανίζεται ο λογαριασμός χρήστη που προγραμματίζει την εργασία και το όνομα του χρήστη που έχει εκχωρηθεί στην εργασία. Η καταγεγραμμένη ημερομηνία και ώρα δείχνουν πότε προγραμματίστηκε η εργασία. Αναζητώντας το συσχετισμένο Αναγνωριστικό συμβάντος 200 και 201 μπορούμε να πάρουμε επιπλέον πληροφορίες.
140	Ενημερώθηκε η προγραμματισμένη εργασία. Στην καταχώριση εμφανίζεται ο λογαριασμός χρήστη που ενημέρωσε την εργασία και το όνομα της εργασίας. Η καταγεγραμμένη ημερομηνία και ώρα δείχνουν πότε ενημερώθηκε η εργασία. Αναζητώντας το συσχετισμένο Αναγνωριστικό συμβάντος 200 και 201 μπορούμε να πάρουμε επιπλέον πληροφορίες σχετικά.
141	Η προγραμματισμένη εργασία διαγράφηκε. Η καταχώρηση εμφανίζει τον λογαριασμό χρήστη που διέγραψε την εργασία και το όνομα της εργασίας.
200	Εκτελέστηκε προγραμματισμένη εργασία. Εμφανίζει το όνομα της εργασίας και την πλήρη διαδρομή προς το εκτελέσιμο σε δίσκο που εκτελέστηκε (αναφέρεται ως η ενέργεια). Συσχετίζοντάς το με το συσχετισμένο Αναγνωριστικό συμβάντος 106 μπορεί να προσδιοριστεί ο λογαριασμός χρήστη που προγραμματίζει την εργασία.
201	Η προγραμματισμένη εργασία ολοκληρώθηκε. Εμφανίζει το όνομα της εργασίας και την πλήρη διαδρομή προς το εκτελέσιμο σε δίσκο που εκτελέστηκε (αναφέρεται ως η ενέργεια). Συσχετίζοντάς το με το συσχετισμένο Αναγνωριστικό συμβάντος 106 μπορεί να προσδιοριστεί ο λογαριασμός χρήστη που προγραμματίζει την εργασία.

Οι κακόβουλοι εισβολείς μπορούν να αξιοποιήσουν τις ενσωματωμένες εντολές των Windows: **at** και **schtasks** και να επεκτείνουν την επιρροή τους καθώς και να διατηρήσουν την επιμονή τους σε κάποιο περιβάλλον θύματος. Η εντολή **at**, ενώ έχει καταργηθεί στις τελευταίες εκδόσεις των Windows, εξακολουθεί να χρησιμοποιείται σε παλαιότερες εκδόσεις των Windows. Η εντολή επιτρέπει την εκτέλεση μιας διαδικασίας σε τακτά χρονικά διαστήματα σε τοπικό είτε σε απομακρυσμένο μηχάνημα. Η σύνταξη της είναι: **`at [\\targetIP] [HH:MM][A|P] [command]`**.

Όπου **targetIP** καθορίζεται το απομακρυσμένο σύστημα όπως ονομάζεται, ο χρόνος με καθορισμένο AM ή PM και η εντολή που θα εκτελεστεί λαμβάνεται ως επιλογή.

Ομοίως, τα νεότερα συστήματα Windows υποστηρίζουν την εντολή **schtasks**, αν και με ελαφρώς πιο εμπλεκόμενη σύνταξη: **schtasks /create /tn [taskname] /s [targetIP] /u [user] /p [password] /sc [frequency] /st [starttime] /sd [startdate] /tr [command]**

Για άλλη μια φορά, αυτή η εντολή επιτρέπει την εκτέλεση μιας διαδικασίας σε ένα τοπικό ή απομακρυσμένο σύστημα σε μια καθορισμένη ώρα. Επιπλέον, εάν εκτελείται με διαπιστευτήρια διαχειριστή, η επιλογή **/ru SYSTEM** επιτρέπει την εκτέλεση του συγκεκριμένου προγράμματος με δικαιώματα σε επίπεδο συστήματος. Επομένως, οι επιτιθέμενοι με έγκυρα διαπιστευτήρια είναι σε θέση να προγραμματίσουν εντολές για εκτέλεση σε συστήματα ως μέσο εξάλειψης δεδομένων, διατήρηση μόνιμης πρόσβασης, επέκταση ελέγχου ή άλλες εργασίες που θεωρούν κατάλληλες.

Όσο αναφορά στον εντοπισμό των προγραμματισμένων εργασιών που δημιουργούνται μέσω της εντολής: **schtasks** για κάθε σύστημα όπου έχει προγραμματιστεί μια τέτοιου είδους εργασία, μπορείτε να βρείτε πρόσθετες λεπτομέρειες στο φάκελο: **%SystemRoot%\System32\Tasks**. Κάθε εργασία που δημιουργείται μέσω της εντολής: **schtasks** δημιουργεί στο εκάστοτε σύστημα ένα αρχείο XML με το ίδιο όνομα με την εργασία σε αυτήν την τοποθεσία. Σε αυτά τα αρχεία XML υπάρχουν αρκετά πεδία με χρήσιμες πληροφορίες. Στην ενότητα "RegistrationInfo", το πεδίο "Author" εμφανίζει τον λογαριασμό που χρησιμοποιήθηκε για τον προγραμματισμό της εργασίας και το πεδίο "Date" εμφανίζει την ημερομηνία και την ώρα του τοπικού συστήματος κατά την οποία καταγράφηκε η δημιουργία της εργασίας. Στην ενότητα "Principals", το πεδίο "UserID" δείχνει το περιβάλλον χρήστη στο οποίο θα εκτελεστεί η εργασία. Η ενότητα "Triggers" παρέχει λεπτομέρειες σχετικά με το πότε θα εκτελεστεί η εργασία και το πεδίο "Exec" στην ενότητα "Actions" περιγράφει τι θα εκτελεστεί.

Επίσης, οποιαδήποτε χρήση πιστοποιημένων διαπιστευτηρίων για τον προγραμματισμό εργασιών σε απομακρυσμένα συστήματα θα αφήσει τα συσχετισμένα συμβάντα σύνδεσης λογαριασμού και σύνδεσης όπως αναφέρθηκε προηγουμένως.

Τέλος, μπορούμε να ανατρέξουμε στην ενότητα Έλεγχος πρόσβασης αντικειμένου για επιπλέον αναγνωριστικά συμβάντων που ενδέχεται να καταγραφούν σε σχέση με τις προγραμματισμένες εργασίες. Ο έλεγχος πρόσβασης αντικειμένου δεν είναι ενεργοποιημένος από προεπιλογή, αλλά πρέπει να ενεργοποιείται ειδικά σε ευαίσθητα συστήματα. Για να το κάνετε αυτό, απλώς χρησιμοποιήστε την Πολιτική τοπικής ασφάλειας για να ορίσετε στις: **Ρυθμίσεις ασφάλειας -> Τοπικές πολιτικές -> Πολιτική ελέγχου -> Πρόσβαση αντικειμένου ελέγχου** την Ενεργοποίηση για επιτυχία και αποτυχία. Όταν είναι ενεργοποιημένος ο έλεγχος πρόσβασης αντικειμένων, ορισμένες δραστηριότητες καταγράφονται από προεπιλογή και άλλες πρέπει να ρυθμιστούν ρητά. Ο λόγος για αυτό είναι ότι η πρόσβαση σε αντικείμενα πραγματοποιείται συνεχώς σε ένα σύστημα, επομένως αυτό το αρχείο καταγραφής έχει σχεδιαστεί για να είναι πιο κοκκώδες ώστε να επιτρέπει σε αντικείμενα που έχουν σημασία να λαμβάνουν επιπλέον έλεγχο χωρίς να κατακλύζουν τα αρχεία καταγραφής προσπαθώντας να καταγράψουν όλη την πρόσβαση αντικειμένων στο σύστημα. Τα συμβάντα ελέγχου πρόσβασης αντικειμένου αποθηκεύονται στο αρχείο καταγραφής ασφαλείας. Εάν είναι ενεργοποιημένος ο έλεγχος πρόσβασης αντικειμένων, οι προγραμματισμένες εργασίες λαμβάνουν πρόσθετη καταγραφή.

Μια ακόμη κατηγορία αρχείων καταγραφής των Windows που παίζουν σημαντικό ρόλο στον εντοπισμό επιθέσεων και ειδικότερα στην εσωτερική μετακίνηση ενός επιτιθέμενου είναι τα αρχεία καταγραφής που περιέχουν τις αλλαγές πολιτικών ελέγχου. Όταν αλλάζει μια πολιτική ελέγχου, επηρεάζει τα διαθέσιμα αποδεικτικά στοιχεία για τους ανακριτές και τους χειριστές συμβάντων για το εάν η αλλαγή έγινε κακόβουλα από έναν εισβολέα ή νόμιμα από έναν διαχειριστή. Ευτυχώς, τα σύγχρονα συστήματα Windows κάνουν καλή δουλειά καταγραφής αυτών των αλλαγών όταν συμβαίνουν. Το αναγνωριστικό συμβάντος που χρησιμοποιείται για αυτόν τον έλεγχο κατέχει το αναγνωριστικό: **4719**.

- **4719** - Η πολιτική ελέγχου συστήματος άλλαξε. Η ενότητα Αλλαγή πολιτικής ελέγχου θα απαριθμήσει τις συγκεκριμένες αλλαγές που έγιναν στην πολιτική ελέγχου. Η ενότητα Θέμα της περιγραφής συμβάντος ενδέχεται να εμφανίζει τον λογαριασμό που έκανε την αλλαγή, αλλά συχνά (όπως όταν η αλλαγή γίνεται μέσω της Πολιτικής ομάδας) αυτή η ενότητα απλώς αναφέρει το όνομα του τοπικού συστήματος. Δυστυχώς, ο έλεγχος της πρόσβασης στις Υπηρεσίες καταλόγου είναι ένας τομέας όπου τα Windows είναι ακόμη λιγότερο από σαφή.
- **1102** - Ανεξάρτητα από τις ρυθμίσεις στην πολιτική ελέγχου, εάν διαγραφεί το αρχείο καταγραφής συμβάντων ασφαλείας, το αναγνωριστικό συμβάντος: 1102 θα καταγραφεί ως η πρώτη καταχώριση στο νέο, κενό αρχείο καταγραφής. Μπορείτε να πείτε το όνομα του λογαριασμού χρήστη που διέγραψε το αρχείο καταγραφής των λεπτομερειών της καταχώρησης. Ένα παρόμοιο συμβάν, με το αναγνωριστικό συμβάντος: 104, δημιουργείται στο αρχείο καταγραφής συστήματος εάν διαγραφεί.

Τέλος, τα αρχεία καταγραφής των Windows που αφορούν στον έλεγχο χρήσης PowerShell παίζουν σημαντικό ρόλο στον εντοπισμό επιθέσεων και ειδικότερα στην εσωτερική μετακίνηση ενός επιτιθέμενου. Η Microsoft συνεχίζει να αυξάνει τον αριθμό των διαθέσιμων αρχείων καταγραφής γύρω από το PowerShell για να βοηθήσει στην καταπολέμηση της παράνομης χρήσης του. Για άλλη μια φορά, αυτές οι εγκαταστάσεις καταγραφής πρέπει να ενεργοποιηθούν μέσω της Πολιτικής ομάδας, συγκεκριμένα στο **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows PowerShell**. Υπάρχουν τρεις βασικές κατηγορίες καταγραφής που ενδέχεται να είναι διαθέσιμες, ανάλογα με την έκδοση των εν λόγω Windows και αυτές αναφέρονται παρακάτω:

- Καταγραφή ενότητας
    1. Καταγράφει συμβάντα εκτέλεσης αγωγού.
    2. Καταγράφεται σε αρχεία καταγραφής συμβάντων.
- Καταγραφή μπλοκ σεναρίων
    1. Καταγράφει ασαφείς εντολές που αποστέλλονται στο PowerShell.
    2. Καταγράφει μόνο τις εντολές, όχι την προκύπτουσα έξοδο.
    3. Καταγράφεται σε αρχεία καταγραφής συμβάντων.
- Μεταγραφή
    1. Καταγράφει την είσοδο και την έξοδο του PowerShell.

2. Δεν θα καταγράψει την έξοδο εξωτερικών προγραμμάτων που εκτελούνται, μόνο το PowerShell.
3. Καταγράφεται σε αρχεία κειμένου καθορισμένης τοποθεσίας από τον χρήστη.

Μόλις ενεργοποιηθούν, αυτά τα αρχεία καταγραφής μπορούν να παρέχουν πληθώρα πληροφοριών σχετικά με τη χρήση του PowerShell στα συστήματά Windows. Εάν εκτελείτε συστηματικά πολλά σενάρια PowerShell, αυτό μπορεί να παράγει μεγάλο όγκο δεδομένων, οπότε φροντίστε να δοκιμάσετε και να συντονίσετε τις εγκαταστάσεις ελέγχου για να επιτύχετε μια ισορροπία μεταξύ ορατότητας και φόρτωσης πριν αναπτύξετε τέτοιες αλλαγές στην παραγωγή. Οι καταχωρήσεις καταγραφής συμβάντων PowerShell εμφανίζονται σε διαφορετικά αρχεία καταγραφής συμβάντων. Στο εσωτερικό της τοποθεσίας: **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx** θα βρείτε τα παρακάτω δύο συμβάντα συγκεκριμένης σημείωσης [4]:

Αναγνωριστικό Συμβάντος	**Περιγραφή**
4103	Δείχνει την εκτέλεση αγωγών από τη μονάδα καταγραφής λειτουργικής μονάδας. Περιλαμβάνει το περιβάλλον χρήστη που χρησιμοποιείται για την εκτέλεση των εντολών. Το πεδίο Όνομα Υπολογιστή θα περιέχει την Κονσόλα εάν εκτελεστεί τοπικά ή θα εμφανιστεί εάν εκτελείται από ένα απομακρυσμένο σύστημα.
4104	Εμφανίζει καταχωρήσεις καταγραφής μπλοκ σεναρίων. Καταγράφει τις εντολές που αποστέλλονται στο PowerShell, αλλά όχι την έξοδο. Καταγράφει όλες τις λεπτομέρειες κάθε μπλοκ μόνο κατά την πρώτη χρήση για εξοικονόμηση χώρου. Θα εμφανιστεί ως συμβάν επιπέδου προειδοποίησης εάν η Microsoft θεωρήσει τη δραστηριότητα ύποπτη.

Μπορείτε να βρείτε πρόσθετες σχετικές καταχωρίσεις στο αρχείο καταγραφής: **%SystemRoot%\System32\winevt\Logs\Windows PowerShell.evtx** όπως αναφέρεται και στο παρακάτω πίνακα [4]:

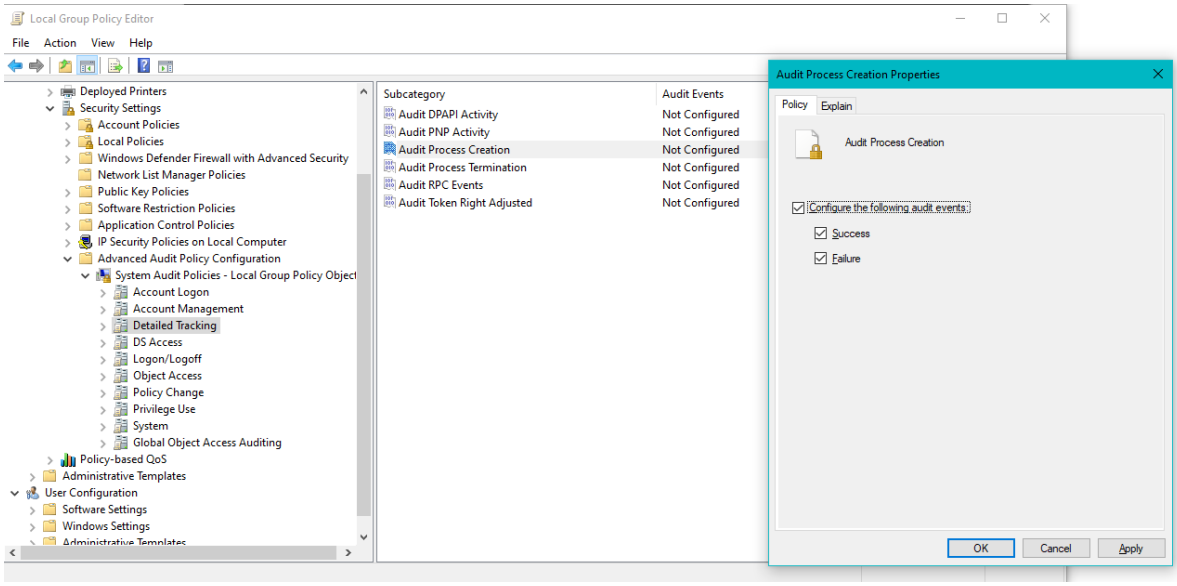
Αναγνωριστικό Συμβάντος	**Περιγραφή**
400	Υποδεικνύει την έναρξη εκτέλεσης εντολών ή περιόδου σύνδεσης. Το πεδίο Όνομα Υπολογιστή εμφανίζει εάν (τοπική) Κονσόλα ή την απομακρυσμένη περίοδο λειτουργίας που προκάλεσε την εκτέλεση.
800	Εμφανίζει λεπτομέρειες εκτέλεσης αγωγού. Το UserID εμφανίζει τον λογαριασμό που χρησιμοποιείται. Το πεδίο Όνομα Υπολογιστή εμφανίζει εάν (τοπική) Κονσόλα ή την απομακρυσμένη περίοδο λειτουργίας που προκάλεσε την εκτέλεση. Δεδομένου ότι πολλά κακόβουλα σενάρια κωδικοποιούν επιλογές με κωδικοποίηση τύπου Base64,

	ελέγξτε το πεδίο HostApplication για επιλογές που κωδικοποιούνται με την παράμετρο **-enc** ή **-EncodedCommand**.

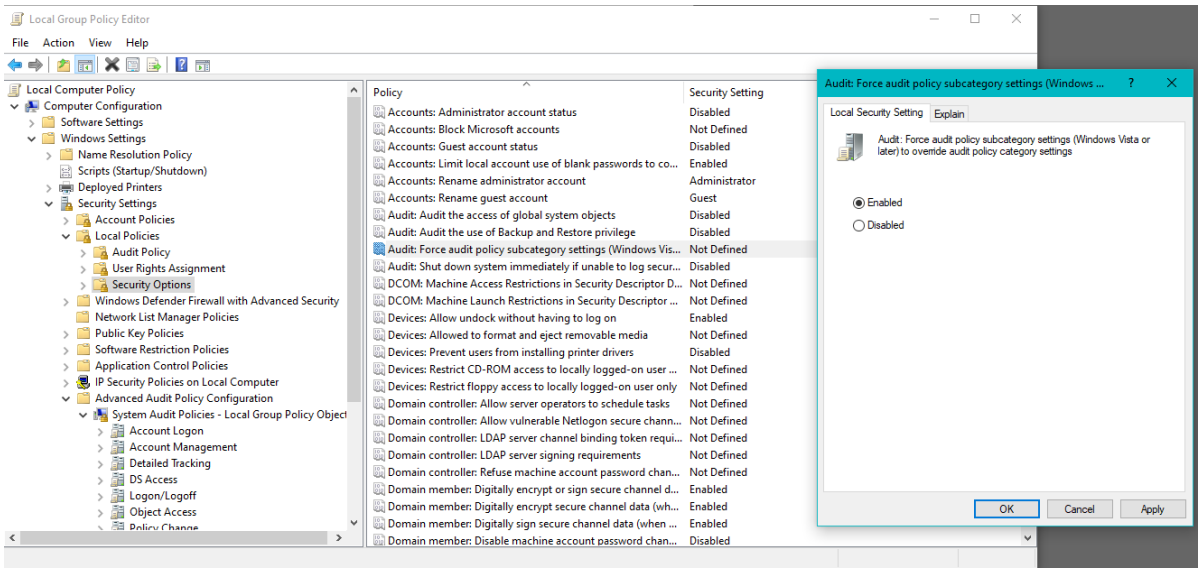
Αξίζει να σημειωθεί ότι η εκτέλεση απομακρυσμένου PowerShell απαιτεί έλεγχο ταυτότητας, οπότε αναζητήστε και τα σχετικά συμβάντα σύνδεσης λογαριασμού και σύνδεσης γενικότερα για τον εντοπισμό χρήσης του.

3.5 Παραμετροποίηση αρχείων καταγραφής Windows

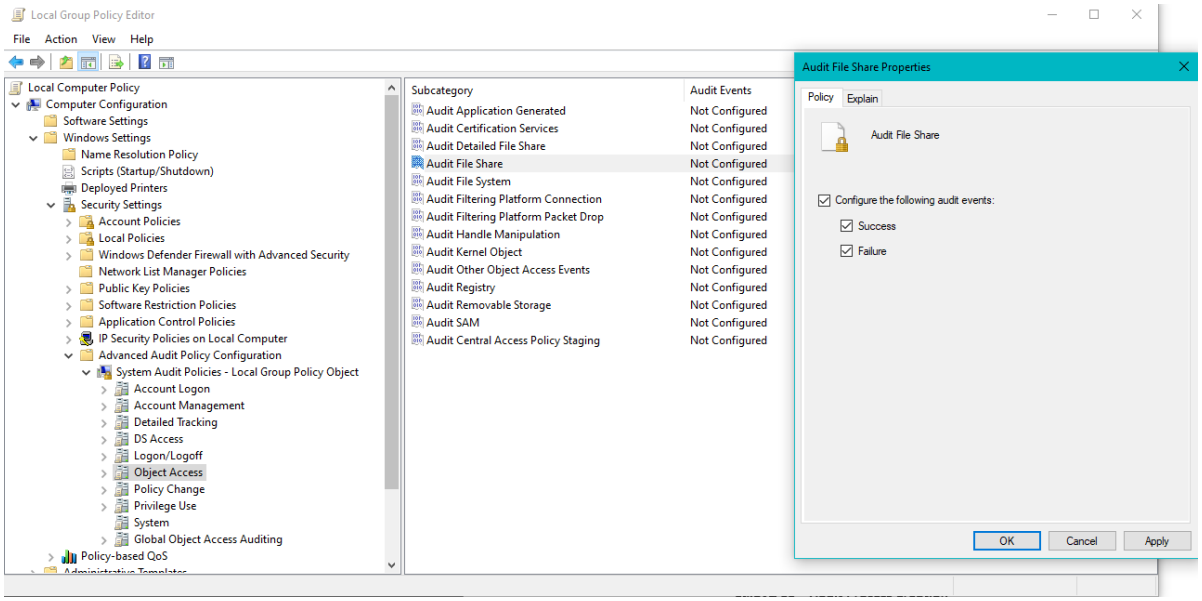
Τα αρχεία καταγραφής σε συστήματα Windows μπορούν να παραμετροποιηθούν με σκοπό να βοηθούν στον ευκολότερο εντοπισμό κακόβουλης δραστηριότητας και πιο συγκεκριμένα εσωτερικής μετακίνησης. Παρακάτω παρατίθενται ορισμένα στιγμιότυπα εικόνων από συγκεκριμένη παραμετροποίηση που έγινε σε ένα σύστημα με Windows 10 λειτουργικό σύστημα (Βλ. ***Εικόνα 10-16***). Σκοπός αυτής της παραμετροποίησης είναι η καταγραφή επιπλέον πληροφοριών του συστήματος, έτσι ώστε σε περίπτωση επίθεσης να μπορέσουμε να εντοπίσουμε και να ιχνηλατήσουμε τις κινήσεις του επιτιθέμενου στον υπολογιστή μας. Πιο συγκεκριμένα ενεργοποιήθηκαν στο σύστημα μας ορισμένες ακόμα παράμετροι προκειμένου να καταγράφονται και να παραμένουν πληροφορίες όπως Process and File Share Auditing, Command line logging, Task Scheduler logging και Powershell logging.



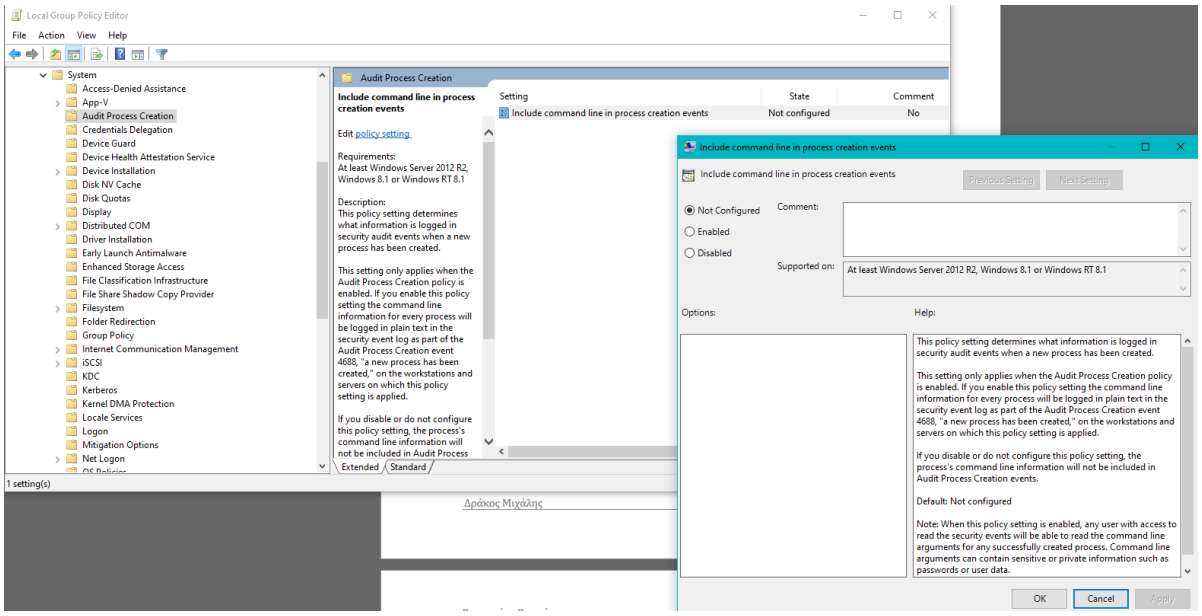
Εικόνα 10 – Audit Process Creation



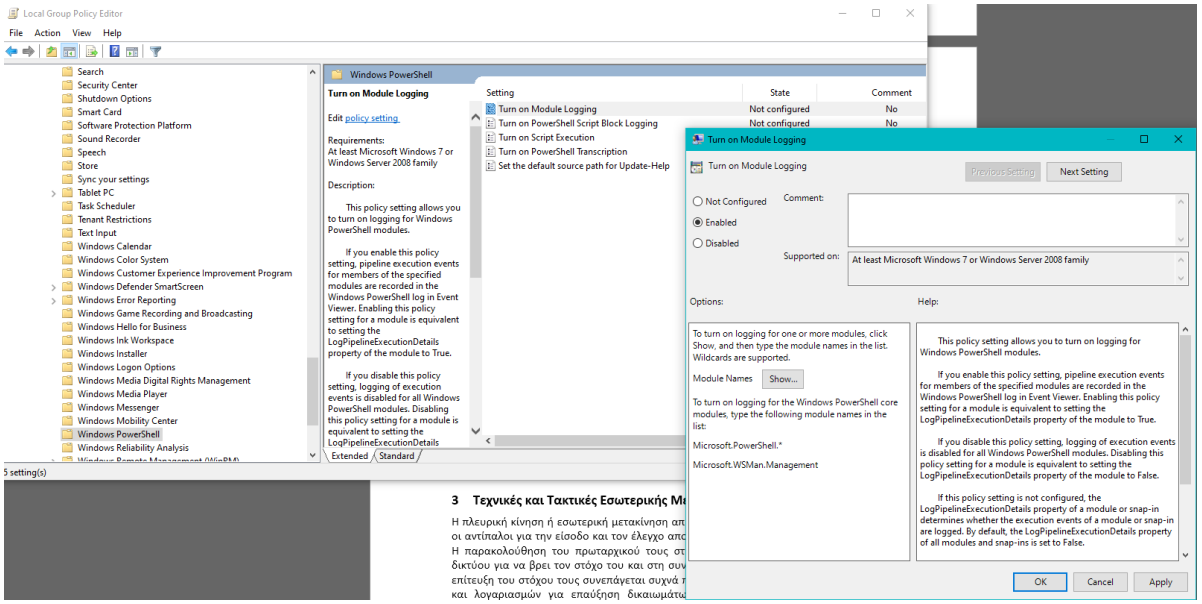
Εικόνα 11 – Audit Policy subcategory settings



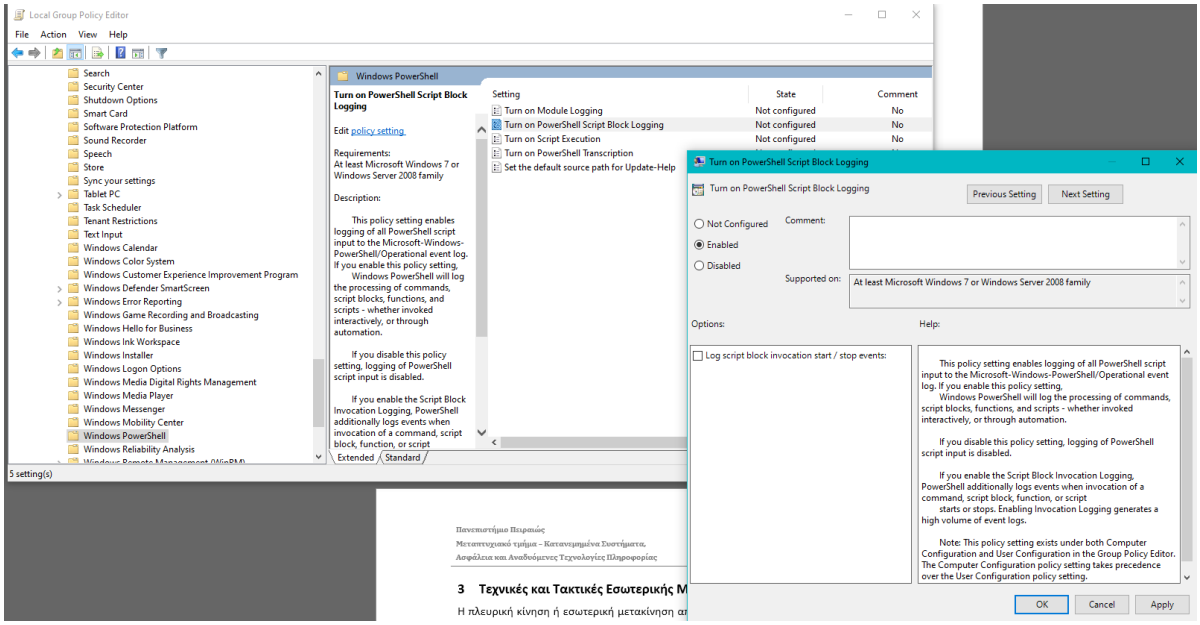
Εικόνα 12 – Command Line Logging



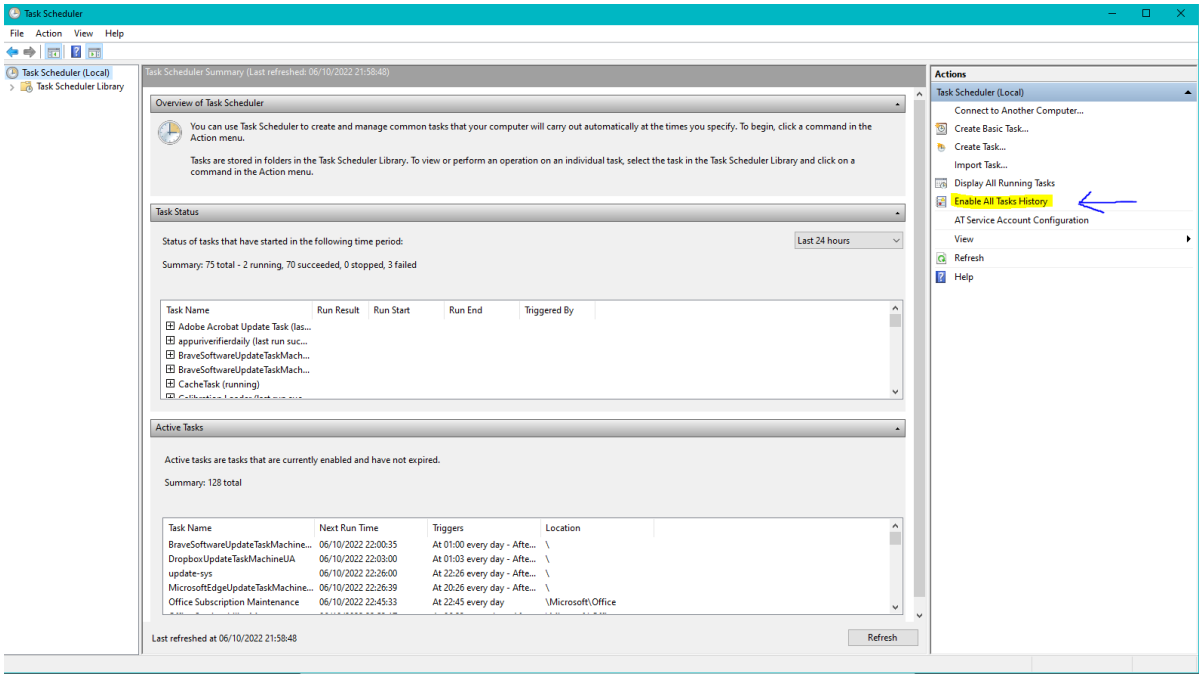
Εικόνα 13 – Audit File Share



Εικόνα 14 – PowerShell Logging



Εικόνα 15 – PowerShell Script Logging



Εικόνα 16 – Task Scheduler Logging

4 Τεχνικές και Τακτικές Εσωτερικής Μετακίνησης βάσει MITRE ATT&CK

Η πλευρική ή εσωτερική κίνηση αναφέρεται στις τεχνικές που χρησιμοποιεί ένας επιτιθέμενος, αφού αποκτήσει αρχική πρόσβαση, για να προχωρήσει βαθύτερα σε ένα δίκτυο αναζητώντας ευαίσθητα δεδομένα και άλλα περιουσιακά στοιχεία υψηλής αξίας. Μετά την είσοδό του στο δίκτυο, ο εισβολέας διατηρεί συνεχή πρόσβαση μεταβαίνοντας στο παραβιασμένο περιβάλλον και αποκτώντας αυξημένα προνόμια χρησιμοποιώντας διάφορα εργαλεία. Η πλευρική κίνηση είναι μια βασική τακτική που διακρίνει τις σημερινές προηγμένες επίμονες απειλές (APT) από τις απλοϊκές κυβερνοεπιθέσεις του παρελθόντος. Η εσωτερική μετακίνηση επιτρέπει σε έναν παράγοντα απειλής να αποφύγει τον εντοπισμό και να διατηρήσει την πρόσβαση, ακόμη και αν ανακαλυφθεί στο μηχάνημα που μολύνθηκε για πρώτη φορά. Και με παρατεταμένο χρόνο παραμονής, η κλοπή δεδομένων ενδέχεται να μην συμβεί πέραν από μόνο εβδομάδες ή και μήνες μετά την αρχική παραβίαση. Αφού ένας επιτιθέμενος αποκτήσει αρχική πρόσβαση σε ένα τελικό σημείο, όπως μέσω μιας επίθεσης ηλεκτρονικού ψαρέματος ή μόλυνσης από κακόβουλο λογισμικό, στη συνέχεια υποδύεται έναν νόμιμο χρήστη και μετακινείται σε πολλά συστήματα του δικτύου μέχρι να επιτευχθεί ο τελικός στόχος. Η επίτευξη αυτού του στόχου περιλαμβάνει τη συλλογή πληροφοριών σχετικά με πολλαπλά συστήματα και λογαριασμούς, την απόκτηση διαπιστευτηρίων, την κλιμάκωση των προνομίων και τελικά την απόκτηση πρόσβασης στο προσδιορισμένο ωφέλιμο φορτίο. Παρακάτω φαίνονται αυτές οι φάσεις με τη σειρά που πραγματοποιούνται από έναν επιτιθέμενο για να φτάσει στο τελικό του στόχο.

Η παρακολούθηση του πρωταρχικού στόχου ενός επιτιθέμενου απαιτεί συχνά την εξερεύνηση του δικτύου για να βρει τον στόχο του και στη συνέχεια να αποκτήσει πρόσβαση σε αυτό. Η επίτευξη του στόχου τους συνεπάγεται συχνά περιστροφή μέσω πολλαπλών συστημάτων και λογαριασμών για επαύξηση δικαιωμάτων ή προνομίων όπως και για εξαγωγή δεδομένων. Οι επιτιθέμενοι ενδέχεται να εγκαταστήσουν τα δικά τους εργαλεία απομακρυσμένης πρόσβασης για να ολοκληρώσουν την πλευρική κίνηση ή να χρησιμοποιούν νόμιμα διαπιστευτήρια με εγγενή εργαλεία δικτύου και λειτουργικού συστήματος, τα οποία μπορεί να είναι πιο κρυφά. Οι τεχνικές καθώς και τα εργαλεία είναι αρκετά που μπορεί να χρησιμοποιήσει κάποιος επιτιθέμενος έχοντας ως σκοπό να μετακινηθεί εσωτερικά-πλευρικά ενός δικτύου με Windows Domain. Παρακάτω λοιπόν παρουσιάζονται αναλυτικά μία προς μία οι τεχνικές αυτές σε συνδυασμό με τα αντίστοιχα εργαλεία καθώς αναφέρονται και συγκεκριμένα παραδείγματα αυτών των τεχνικών επιθέσεων. Επιπλέον αναφέρονται τρόποι με τους οποίους μπορεί κανείς να μειώσει και να αντιμετωπίσει τις συγκεκριμένες τεχνικές επιθέσεων, αλλά και τρόποι με τους οποίους μπορεί κανείς να τις εντοπίσει. Πιο συγκεκριμένα παρακάτω ακολουθούν όλες οι τακτικές και οι τεχνικές των επιθέσεων που αντιπροσωπεύουν το πίνακα MITRE ATT&CK για Επιχειρήσεις και συγκεκριμένα για την πλατφόρμα των συστημάτων Windows.

4.1 Λογισμικό ανάπτυξης εφαρμογών

Οι επιτιθέμενοι μπορούν να αναπτύξουν κακόβουλο λογισμικό σε συστήματα εσωτερικά ενός δικτύου χρησιμοποιώντας λογισμικό και συστήματα ανάπτυξης εφαρμογών που χρησιμοποιούνται από τους διαχειριστές των επιχειρήσεων. Τα δικαιώματα που απαιτούνται για αυτήν τη δράση ποικίλλουν ανάλογα με τη διαμόρφωση του κάθε συστήματος. Τα τοπικά διαπιστευτήρια μπορεί να επαρκούν για άμεση πρόσβαση στον εξυπηρετητή ανάπτυξης λογισμικού ή ενδέχεται να απαιτούνται διαπιστευτήρια συγκεκριμένου Domain. Ωστόσο, το σύστημα μπορεί να απαιτεί έναν λογαριασμό διαχειριστή για να συνδεθεί ή να εκτελέσει την ανάπτυξη του λογισμικού.

Η πρόσβαση σε ένα σύστημα ανάπτυξης λογισμικού σε ένα τοπικό δίκτυο ή σε ολόκληρο το εταιρικό δίκτυο επιτρέπει σε έναν επιτιθέμενο να έχει δικαιώματα απομακρυσμένης εκτέλεσης κώδικα σε όλα τα συστήματα που είναι συνδεδεμένα με ένα τέτοιο σύστημα. Η πρόσβαση αυτή μπορεί να χρησιμοποιηθεί για την πλευρική μετακίνηση σε άλλα συστήματα, τη συγκέντρωση πληροφοριών ή την πρόκληση συγκεκριμένου Impact, όπως για παράδειγμα την εκκαθάριση των σκληρών δίσκων σε όλα τα τερματικά του δικτύου.

Ένα αντίστοιχο παράδειγμα μιας τέτοιας τεχνικής επίθεσης η οποία έχει πραγματοποιηθεί είναι το **APT32** το οποίο παραβίασε το McAfee ePO για να κινηθεί εσωτερικά με τη διανομή κακόβουλου λογισμικού ως εργασία ανάπτυξης λογισμικού [1].

Για την αντιμετώπιση και τη μείωση αυτών των μεθόδων επιθέσεων προτείνεται η εφαρμογή των διαδικασιών που αναφέρονται και περιγράφονται παρακάτω στο ***Πίνακα 1***.

Υπογραφή κώδικα	Εάν το σύστημα ανάπτυξης εφαρμογών μπορεί να ρυθμιστεί ώστε να αναπτύξει μόνο υπογεγραμμένα δυαδικά αρχεία, βεβαιωθείτε ότι τα αξιόπιστα πιστοποιητικά υπογραφής δεν βρίσκονται στο ίδιο σύστημα με το σύστημα ανάπτυξης εφαρμογών και αντιθέτως βρίσκονται σε ένα σύστημα στο οποίο δεν είναι δυνατή η πρόσβαση από απόσταση ή σε μια απομακρυσμένη πρόσβαση η οποία είναι σφιχτά ελεγχόμενη.
Έλεγχος ταυτότητας πολλαπλών παραγόντων	Χρησιμοποιήστε έλεγχο ταυτότητας πολλαπλών παραγόντων για λογαριασμούς που χρησιμοποιούνται για την πρόσβαση στο σύστημα και στο λογισμικό ανάπτυξης εφαρμογών.
Τμηματοποίηση δικτύου	Βεβαιωθείτε ότι υπάρχει σωστή απομόνωση συστήματος και πρόσβασης για κρίσιμα συστήματα εντός του δικτύου μέσω της χρήσης τείχους προστασίας, διαχωρισμού προνομίων λογαριασμού, πολιτικής ομάδας και πιστοποίησης πολλαπλών παραγόντων.
Προνομιακή διαχείριση λογαριασμού	Αποκτήστε πρόσβαση σε συστήματα ανάπτυξης εφαρμογών μόνο σε περιορισμένο αριθμό εξουσιοδοτημένων διαχειριστών. Βεβαιωθείτε ότι τα διαπιστευτήρια των λογαριασμών που μπορούν να χρησιμοποιηθούν για την πρόσβαση σε συστήματα ανάπτυξης λογισμικού είναι μοναδικά και δεν χρησιμοποιούνται σε όλο το εταιρικό δίκτυο.

Ενημέρωση λογισμικού	Να γίνεται τακτικά η εγκατάσταση των ενημερωμένων εκδόσεων στα συστήματα ανάπτυξης εφαρμογών για να αποτρέψετε πιθανή απομακρυσμένη πρόσβαση μέσω εκμετάλλευσης αδυναμιών για την προσαύξηση προνομίων.

Πίνακας 1

Για τον εντοπισμό αυτού του είδους τεχνικής επιτιθέμενων μπορούμε να παρακολουθούμε τις εφαρμογές ανάπτυξης λογισμικού από ένα δευτερεύον σύστημα.

Επιπλέον μπορούμε να εκτελούμε την ανάπτυξη του λογισμικού και των εφαρμογών σε τακτά χρονικά διαστήματα, ώστε να ξεχωρίζει η δραστηριότητα παράνομης ανάπτυξης λογισμικού.

Τέλος, μπορούμε να παρακολουθούμε τη δραστηριότητα της διαδικασίας που δεν συσχετίζεται με το γνωστό καλό λογισμικό όπως επίσης και να παρακολουθούμε τη δραστηριότητα σύνδεσης των λογαριασμών στο σύστημα ανάπτυξης λογισμικού.

4.2 Component Object Model and Distributed COM

Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν το μοντέλο των Components Objects των Windows (COM) καθώς και το μοντέλο των κατανεμημένων Objects (DCOM) των Windows για να εκτελούν τοπικά κώδικα ή για να εκτελούν κώδικα σε απομακρυσμένα συστήματα ως μέρος πλευρικής κίνησης.

Το COM είναι ένα στοιχείο της φυσικής διεπαφής προγραμματισμού εφαρμογών των Windows (API) που επιτρέπει την αλληλεπίδραση μεταξύ αντικειμένων λογισμικού ή εκτελέσιμου κώδικα που υλοποιεί μία ή περισσότερες διεπαφές. Μέσω του COM, ένα αντικείμενο πελάτη μπορεί να καλέσει μεθόδους αντικειμένων διακομιστή, οι οποίες είναι συνήθως βιβλιοθήκες δυναμικής σύνδεσης (ddl) ή εκτελέσιμα αρχεία (.exe). Το DCOM είναι ένα λογισμικό που επεκτείνει τη λειτουργικότητα του Component Object Model (COM) πέρα από έναν τοπικό υπολογιστή χρησιμοποιώντας την τεχνολογία κλήσης από απόσταση (RPC).

Τα δικαιώματα αλληλεπίδρασης με τοπικά και απομακρυσμένα αντικείμενα COM του διακομιστή καθορίζονται από τις λίστες ελέγχου πρόσβασης (ACL) στο μητρώο των Windows (Registry). Από προεπιλογή, μόνο οι διαχειριστές του εκάστοτε συστήματος μπορούν να ενεργοποιήσουν από απόσταση και να εκκινήσουν αντικείμενα COM μέσω DCOM [1].

Οι επιτιθέμενοι μπορούν να καταχραστούν το COM για τοπική εκτέλεση εντολών ή / και φόρτωσης ωφέλιμου φορτίου (Payload). Διάφορες διασυνδέσεις COM είναι εκτεθειμένες και μπορούν να χρησιμοποιηθούν για την επίκληση της αυθαίρετης εκτέλεσης κώδικα μέσω διαφόρων γλωσσών προγραμματισμού όπως C, C ++, Java και VBScript. Συγκεκριμένα αντικείμενα COM υπάρχουν επίσης για να εκτελούν απευθείας λειτουργίες πέρα από την εκτέλεση κώδικα, όπως τη δημιουργία προγραμματισμένης εργασίας, τη λήψη / εκτέλεση αρχείων και άλλες συμπεριφορές των επιτιθέμενων, όπως την επαύξηση δικαιωμάτων και την διατήρηση τους.

Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν το DCOM για πλευρική μετακίνηση μέσα σε ένα δίκτυο με Windows Domain. Μέσω του DCOM, οι επιτιθέμενοι που λειτουργούν στο

πλαίσιο ενός κατάλληλα προνομιούχου χρήστη μπορούν να αποκτήσουν εξ αποστάσεως αυθαίρετη ή και άμεση εκτέλεση shell code μέσω εφαρμογών του Office καθώς και άλλων εφαρμογών των Windows που περιέχουν ανασφαλείς μεθόδους. Το DCOM μπορεί επίσης να εκτελεί μακροεντολές σε υπάρχοντα έγγραφα όπως επιπλέον μπορεί να ζητήσει την εκτέλεση δυναμικής ανταλλαγής δεδομένων (DDE) απευθείας μέσω μιας στιγμιότυπου δημιουργούμενης από COM μιας εφαρμογής του Microsoft Office παρακάμπτοντας την ανάγκη για ένα κακόβουλο έγγραφο [1].

Οι περιπτώσεις όπου έχουν χρησιμοποιηθεί οι μέθοδοι και τα εργαλεία αντίστοιχα για την εκτέλεση τέτοιου είδους επιθέσεων είναι αρκετές εκ των οποίων ενδεικτικά ορισμένες αναφέρονται παρακάτω:

- Cobalt Strike: Το Cobalt Strike είναι ένα εργαλείο το οποίο μπορεί να παραδώσει ωφέλιμα φορτία "**beacon**" για πλευρική κίνηση, εκμεταλλευόμενο την απομακρυσμένη εκτέλεση COM.
- Empire: Το Empire είναι ένα άλλο εργαλείο το οποίο μπορεί να χρησιμοποιήσει **Invoke-DCOM** και να αξιοποιήσει την απομακρυσμένη εκτέλεση COM για πλευρική κίνηση.
- MuddyWater: Το MuddyWater χρησιμοποίησε κακόβουλο λογισμικό που έχει τη δυνατότητα εκτέλεσης κακόβουλου λογισμικού μέσω του COM και του Outlook.
- POWERSTATS: Το POWERSTATS είναι ένα Backdoor γραμμένο σε PowerShell Code το οποίο μπορεί να χρησιμοποιήσει το DCOM (στοχεύοντας την διεύθυνση loopback 127.0.0.1) για την εκτέλεση πρόσθετων ωφέλιμων φορτίων σε υποβαθμισμένους κεντρικούς υπολογιστές.
- Ursnif: Τα Ursnif droppers έχουν χρησιμοποιήσει αντικείμενα COM για να εκτελέσουν το πλήρες εκτελέσιμο φορτίο ενός κακόβουλου λογισμικού.

Για την αντιμετώπιση και τη μείωση αυτών των μεθόδων επιθέσεων προτείνεται η εφαρμογή των διαδικασιών που αναφέρονται και περιγράφονται παρακάτω στο ***Πίνακα 2*** [1].

Απομόνωση Εφαρμογής και Sandboxing	Βεβαιωθείτε ότι είναι ενεργοποιημένες όλες οι ειδοποιήσεις για κάθε COM καθώς και η προστατευμένη προβολή.
Απενεργοποίηση ή κατάργηση δυνατότητας ή προγράμματος	Εξετάστε την απενεργοποίηση κάθε DCOM μέσω του Dcomcnfg.exe.
Τμηματοποίηση δικτύου	Ενεργοποιήστε το τείχος προστασίας των Windows, το οποίο αποτρέπει την εκδοχή κάθε DCOM από προεπιλογή.
Προνομιακή διαχείριση λογαριασμού	Τροποποιήστε τις ρυθμίσεις του μητρώου (απευθείας ή με χρήση του Dcomcnfg.exe) ως εξής: **HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{{AppID_GUID}}** σε συνδυασμό με την ασφάλεια ολόκληρης της διαδικασίας των επιμέρους εφαρμογών COM και ως εξής: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole** σε συνδυασμό με τις προεπιλογές ασφαλείας ολόκληρου του συστήματος για

	όλες τις εφαρμογές COM που δεν ρυθμίζουν τη δική τους ασφάλεια σε επίπεδο process.

Πίνακας 2

Για τον εντοπισμό και την ανίχνευση αυτών των τεχνικών επιθέσεων μπορούμε να παρακολουθούμε το οτιδήποτε COM που φορτώνει αρχεία DLL και άλλα στοιχεία τα οποία συνήθως δεν σχετίζονται με την εκάστοτε εφαρμογή. Η απαρίθμηση αντικειμένων COM, μέσω του Query Registry ή του PowerShell , μπορεί επίσης να προχωρήσει σε κακόβουλη χρήση.

Επιπλέον μπορούμε να παρακολουθούμε την αναπαραγωγή των διαδικασιών που σχετίζονται με αντικείμενα COM, ειδικά αυτές που επικαλούνται από ένα χρήστη διαφορετικό από αυτόν που είναι συνδεδεμένος αυτήν την εκάστοτε στιγμή.

Τέλος μπορούμε να παρακολουθούμε για τυχόν εισροές ή μη φυσιολογικές αυξήσεις της κίνησης Distributed Computing Environment / Remote Procedure Call (DCE / RPC).

4.3 Εκμετάλλευση απομακρυσμένων υπηρεσιών

Η εκμετάλλευση μιας ευπάθειας λογισμικού συμβαίνει όταν ένας επιτιθέμενος εκμεταλλεύεται ένα σφάλμα προγραμματισμού που υπάρχει σε μια εφαρμογή, σε μια υπηρεσία, εντός του λογισμικού του λειτουργικού συστήματος ή εντός του ίδιου του πυρήνα του συστήματος για να εκτελέσει κώδικα που ελέγχεται από τον ίδιο. Ένας κοινός στόχος για την Post-Compromised εκμετάλλευση απομακρυσμένων υπηρεσιών είναι η πλευρική μετακίνηση για την ενεργοποίηση της πρόσβασης σε ένα απομακρυσμένο σύστημα.

Ένας επιτιθέμενος ίσως χρειαστεί να καθορίσει εάν το απομακρυσμένο σύστημα βρίσκεται σε ευάλωτη κατάσταση και αυτό μπορεί να γίνει μέσω σάρωσης της υπηρεσίας δικτύου ή άλλων μεθόδων ανακάλυψης που αναζητούν κοινό, ευάλωτο λογισμικό που μπορεί να αναπτυχθεί στο δίκτυο, έλλειψη ορισμένων επιδιορθώσεων σε ευπάθειες ή λογισμικό ασφαλείας που μπορεί να χρησιμοποιείται για την ανίχνευση ή την απομακρυσμένη εκμετάλλευση. Οι διακομιστές είναι πιθανώς στόχος υψηλής αξίας για την εκμετάλλευση πλευρικής κίνησης, αλλά τα τερματικά συστήματα σε ένα δίκτυο ενδέχεται επίσης να διατρέχουν κίνδυνο εάν παρέχουν κάποια πλεονέκτημα ή κάποια πρόσβαση σε πρόσθετους πόρους.

Υπάρχουν αρκετά καλά πλέον γνωστές ευπάθειες που διατρέχουν σε κοινές υπηρεσίες όπως το SMB και το RDP, καθώς και γνωστές εφαρμογές που μπορούν να χρησιμοποιηθούν σε εσωτερικά δίκτυα όπως η MySQL καθώς και υπηρεσίες διακομιστή web.

Ανάλογα με το επίπεδο των permissions της ευάλωτης απομακρυσμένης υπηρεσίας, ένας επιτιθέμενος μπορεί να επιτύχει εκμετάλλευση για την εξέλιξη των προνομίων του ως αποτέλεσμα της εκμετάλλευσης της πλευρικής κίνησης.

Οι περιπτώσεις όπου έχουν χρησιμοποιηθεί οι μέθοδοι και τα εργαλεία για την εκτέλεση τέτοιου είδους επιθέσεων είναι αρκετές εκ των οποίων ενδεικτικά ορισμένες αναφέρονται παρακάτω:

- APT28: Μια ομάδα απειλών η οποία εκμεταλλεύτηκε μια ευπάθεια εκτέλεσης απομακρυσμένου κώδικα του πρωτοκόλλου SMB των Windows για τη διεξαγωγή πλευρικής κίνησης.
- Emotet: Ένα modular malware που έχει εκμεταλλευτεί το SMB μέσω εκμετάλλευσης μιας ευπάθειας όπως το ETERNALBLUE (MS17-010) για την επίτευξη πλευρικής μετακίνησης και διάδοσης.
- Empire: Ένα Open Source εργαλείο απομακρυσμένης διαχείρισης και Post Exploitation Framework το οποίο διαθέτει περιορισμένο αριθμό ενσωματωμένων ενοτήτων για την εκμετάλλευση απομακρυσμένων διακομιστών SMB, JBoss και Jenkins.
- Flame: Ένα εκλεπτυσμένο εργαλείο που έχει χρησιμοποιηθεί για τη συλλογή πληροφοριών από τουλάχιστον το 2010 και έχει την δυνατότητα να χρησιμοποιήσει το MS10-061 για να εκμεταλλευτεί την ευπάθεια του λογισμικού εκτύπωσης σε ένα απομακρυσμένο σύστημα με κοινόχρηστο εκτυπωτή έχοντας ως σκοπό να μετακινηθεί πλευρικά εντός ενός δικτύου.
- NotPetya: Ένα κακόβουλο λογισμικό που πρωτοξεκίνησε σε μια παγκόσμια επίθεση η οποία ξεκίνησε στις 27 Ιουνίου 2017 και έχει την δυνατότητα να χρησιμοποιήσει δύο εκμεταλλεύσεις σε SMBv1, EternalBlue και EternalRomance, για να εξαπλωθεί σε άλλα απομακρυσμένα συστήματα εντός του ίδιου δικτύου.
- PoshC2: Ένα Framework ανοιχτού κώδικα απομακρυσμένης διαχείρισης και Post Exploitation το οποίο περιέχει ένα Module για την εκμετάλλευση του SMB μέσω του EternalBlue.
- Ομάδα απειλών-3390: Μια κινεζική ομάδα απειλών που έχει χρησιμοποιήσει εκτενώς στρατηγικούς συμβιβασμούς στο Web για να στοχεύσει τα θύματα και η οποία εκμεταλλεύτηκε το MS17-101 για να μετακινηθεί πλευρικά σε άλλα συστήματα του δικτύου.
- WannaCry: Ένα ransomware που πρωτοεμφανίστηκε σε μια παγκόσμια επίθεση τον Μάιο του 2017, η οποία επηρέασε περισσότερες από 150 χώρες και χρησιμοποιεί ένα exploit του SMBv1 για να εξαπλωθεί σε άλλα απομακρυσμένα συστήματα ενός δικτύου.

Για την αντιμετώπιση και τη μείωση αυτών των μεθόδων επιθέσεων προτείνεται η εφαρμογή των διαδικασιών που αναφέρονται και περιγράφονται παρακάτω στο ***Πίνακα 3***.

Απομόνωση Εφαρμογής και Sandboxing	Καταστήστε δύσκολο για τους επιτιθέμενους να προωθήσουν τη λειτουργία τους μέσω της εκμετάλλευσης ανεξερεύνητων ή αδιατάρακτων τρωτών σημείων χρησιμοποιώντας sandboxing. Άλλοι τύποι virtualization και microsegmentation εφαρμογών μπορεί επίσης να μετριάσουν την επίδραση ορισμένων μεθόδων εκμετάλλευσης. Οι κίνδυνοι ωστόσο των πρόσθετων εκμεταλλεύσεων και αδυναμιών στα συστήματα αυτά μπορεί να εξακολουθούν να υπάρχουν.
Απενεργοποίηση ή	Ελαχιστοποίηση των διαθέσιμων υπηρεσιών μόνο σε εκείνες

κατάργηση δυνατότητας ή προγράμματος	που είναι απαραίτητες.
Τμηματοποίηση δικτύου	Ορθή τμηματοποίηση των δικτύων σε διάφορους τομείς και συστήματα κατάλληλα για τη μείωση της πρόσβασης σε κρίσιμα συστήματα και υπηρεσίες με ελεγχόμενες μεθόδους.
Αποκτήστε προστασία	Χρήση εφαρμογών ασφαλείας που αναζητούν συμπεριφορά που χρησιμοποιείται κατά την εκμετάλλευση, όπως το Windows Defender Exploit Guard (WDEG) και το Enhanced Mitigation Experience Toolkit (EMET) μπορούν να χρησιμοποιηθούν για να μετριάσουν κάποια συμπεριφορά εκμετάλλευσης. Επιπλέον επιθυμητό είναι να ελέγχεται η ροή του ελέγχου ακεραιότητας, όπου αυτό αποτελεί έναν άλλο τρόπο για να εντοπιστεί και να σταματήσει μία εκμετάλλευση λογισμικού από την εμφάνισή της. Πολλές από αυτές τις προστασίες εξαρτώνται από την αρχιτεκτονική και την εφαρμογή που έχουν στο κάθε στόχο και για λόγους συμβατότητας μπορεί να μην λειτουργούν για όλο το φάσμα των λογισμικών και των υπηρεσιών.
Διαχείριση προνομιούχων λογαριασμών	Ελαχιστοποιήστε τα δικαιώματα και την πρόσβαση για τους λογαριασμούς των υπηρεσιών έτσι ως ώστε να περιορίσετε τις επιπτώσεις της εκμετάλλευσης.
Threat Intelligence Program	Αναπτύξτε μια ισχυρή ικανότητα πληροφοριών σχετικά με απειλές στον κυβερνοχώρο για να καθορίσετε ποιοι τύποι και σε ποια επίπεδα απειλής μπορούν να χρησιμοποιούν τα Exploits και 0-days επιθέσεις έναντι συγκεκριμένων οργανισμών.
Ενημέρωση λογισμικού	Ενημερώστε τακτικά το λογισμικό χρησιμοποιώντας τη διαχείριση των ενημερώσεων κώδικα για εσωτερικά σημεία και διακομιστές της επιχείρησης.
Σάρωση για ευπάθειες	Να γίνεται τακτικά έλεγχος όσο αναφορά στις διαθέσιμες υπηρεσίες του εσωτερικού δικτύου για τον εντοπισμό νέων και ενδεχομένως ευάλωτων υπηρεσιών.

Πίνακας 3

Η ανίχνευση των τεχνικών και των εργαλείων που χρησιμοποιούνται από τους επιτιθέμενους για την εκμετάλλευση απομακρυσμένων υπηρεσιών μπορεί να είναι δύσκολη, ανάλογα με τα διαθέσιμα εργαλεία. Τα προγράμματα και οι εφαρμογές εκμετάλλευσης λογισμικού ενδέχεται να μην είναι πάντοτε επιτυχημένα ή μπορεί να προκαλέσουν την ασταθή διεργασία ή τη συντριβή της εκμεταλλευόμενης διαδικασίας [1].

Επίσης, μπορούμε να αναζητούμε για συμπεριφορά στα τερματικά συστήματα η οποία μπορεί να υποδηλώνει επιτυχή συμβιβασμό, όπως είναι η μη φυσιολογική συμπεριφορά των διαδικασιών. Αυτό θα μπορούσε να περιλαμβάνει τα ύποπτα αρχεία που έχουν εγγραφεί στο δίσκο, τα αποδεικτικά στοιχεία της διαδικασίας έγχυσης για απόπειρες

απόκρυψης εκτέλεσης, τα αποδεικτικά στοιχεία της ανακάλυψης-εξερεύνησης ή άλλης ασυνήθιστης κυκλοφορίας εντός του δικτύου που μπορεί να υποδεικνύουν πρόσθετα εργαλεία που μεταφέρονται στο σύστημα.

4.4 Εσωτερικό Spearphishing

Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τη μέθοδο του εσωτερικού Spearphishing για να αποκτήσουν πρόσβαση σε πρόσθετες πληροφορίες ή να εκμεταλλευτούν άλλους χρήστες μέσα στον ίδιο τον οργανισμό, αφού έχουν ήδη αποκτήσει πρόσβαση σε λογαριασμούς ή συστήματα εντός του οργανισμού. Το εσωτερικό Spearphishing είναι μια μέθοδος επίθεσης πολλαπλών σταδίων, όπου ένας λογαριασμός ηλεκτρονικού ταχυδρομείου γίνεται accessed είτε ελέγχοντας τη συσκευή του χρήστη με προηγουμένως εγκατεστημένο κακόβουλο λογισμικό, είτε διακυβεύοντας τα διαπιστευτήρια του λογαριασμού του χρήστη. Οι επιτιθέμενοι προσπαθούν να επωφεληθούν μέσω κάποιου αξιόπιστου εσωτερικού λογαριασμού του οργανισμού για να αυξήσουν την πιθανότητα να εξαπατήσουν τον στόχο στο να την πατήσει στην απόπειρα του phishing.

Οι επιτιθέμενοι μπορούν επίσης να εκμεταλλευτούν το Spearphishing Attachment ή το Spearphishing Link ως μέρος της επίθεσης εσωτερικού Spearphishing για να παραδώσουν κάποιο Payload ή να ανακατευθύνουν τον στόχο τους σε έναν εξωτερικό ιστότοπο για να καταγράψουν τα διαπιστευτήρια του χρήστη. Αυτό μπορεί να επιτευχθεί μέσω κάποιου Input Capture ενσωματωμένο σε ιστότοπο που μιμείται κάποια διεπαφή σύνδεσης σε ηλεκτρονικό ταχυδρομείο.

Χαρακτηριστικά και αξιοσημείωτα είναι τα περιστατικά όπου έχει χρησιμοποιηθεί η τεχνική του εσωτερικού Spearphishing. Αναφορικά, η εκστρατεία Eye Pyramid χρησιμοποιούσε χαρακτηριστικά E-mails ηλεκτρονικού "ψαρέματος" (phishing) με κακόβουλα συνημμένα για πλευρική μετακίνηση μεταξύ των θυμάτων, καταφέρνοντάς να κάνει Compromised με αυτό τον τρόπο σχεδόν 18.000 λογαριασμούς ηλεκτρονικού ταχυδρομείου. Επιπλέον, ένα ακόμη χαρακτηριστικό παράδειγμα τέτοιου είδους επίθεσης είναι ο Σύριος Ηλεκτρονικός Στρατός (SEA) ο οποίος παραβίασε λογαριασμούς email της Financial Times (FT) για να κλέψει πρόσθετα διαπιστευτήρια λογαριασμών. Μόλις η FT έμαθε για την επίθεση αυτή και άρχισε να προειδοποιεί τους υπαλλήλους της για την απειλή, η SEA έστειλε μηνύματα ηλεκτρονικού "ψαρέματος" που μιμούνταν το τμήμα IT της Financial Times και μπόρεσε με αυτό τον τρόπο να γίνουν Compromised ακόμη περισσότερους χρήστες.

Όσο αναφορά στην αντιμετώπιση και τη μείωση του κινδύνου και των επιθέσεων με τέτοιες τεχνικές είναι σημαντικό να αναφερθεί και να τονιστεί το γεγονός πως δεν μπορεί εύκολα να μετριαστεί με προληπτικούς ελέγχους, διότι ο κίνδυνος σε τέτοιες περιπτώσεις βασίζεται στην κατάχρηση των χαρακτηριστικών του συστήματος.

Ωστόσο, τα συστήματα ανίχνευσης εισβολής (IDS) των δικτύων και οι Gateways κάθε ηλεκτρονικού ταχυδρομείου συνήθως δεν σαρώνουν τα εσωτερικά μηνύματα ηλεκτρονικού ταχυδρομείου, αλλά ένας οργανισμός μπορεί να εκμεταλλευτεί κάποια λύση που βασίζεται στον περιοδικό έλεγχο. Η συγκεκριμένη λύση αποστέλλει ένα αντίγραφο μηνυμάτων ηλεκτρονικού ταχυδρομείου σε μια υπηρεσία ασφαλείας για την ανάλυση

αυτών χωρίς κάποια απευθείας σύνδεση μαζί της ή ενσωματώνει ολοκληρωμένες λύσεις για υπηρεσίες ασφάλειας χρησιμοποιώντας on-premise εγκαταστάσεις ή κάποιο API με σκοπό να βοηθήσουν στην ανίχνευση των εσωτερικών επιθέσεων κατά της προσβολής των λογαριασμών των χρηστών.

4.5 Logon Scripts

Τα Windows επιτρέπουν τη δημιουργία Scripts σύνδεσης κάθε φορά που ένας συγκεκριμένος χρήστης ή κάποια ομάδα χρηστών προσπαθεί να συνδεθεί σε ένα σύστημα. Τα Scripts αυτά μπορούν να χρησιμοποιηθούν για την εκτέλεση Management λειτουργιών, οι οποίες μπορεί συχνά να εκτελούν άλλα προγράμματα ή να στέλνουν πληροφορίες σε κάποιο εσωτερικό Server καταγραφής.

Αν οι επιτιθέμενοι μπορούν να έχουν πρόσβαση με κάποιο τρόπο σε αυτά τα Scripts, ενδέχεται να εισαγάγουν πρόσθετο κώδικα σε κάποιο από τα Scripts με σκοπό να εκτελέσουν τα εργαλεία τους όταν συνδεθεί κάποιος χρήστης. Αυτός ο κώδικας μπορεί να τους επιτρέψει να διατηρήσουν μόνιμα την πρόσβαση τους σε κάποιο σύστημα, αν πρόκειται για κάποιο τοπικό Script ή να μετακινηθούν πλευρικά σε ένα δίκτυο, αν το Script αυτό είναι αποθηκευμένο σε κεντρικό Server και έχει προωθηθεί σε αρκετά συστήματα του δικτύου. Ανάλογα με τη διαμόρφωση της πρόσβασης στα Logon Scripts, ενδέχεται να απαιτούνται τοπικά διαπιστευτήρια είτε ένας λογαριασμός διαχειριστή.

Παρακάτω παραθέτουμε ορισμένες ενδεικτικά από τις μεθόδους και των εργαλεία που έχουν χρησιμοποιηθεί για τέτοιους είδους επιθέσεις.

APT28	Ένα APT28 Trojan loader προσθέτει το KEY **HKCU\Environment\UserInitMprLogonScript** στη Registry με σκοπό να διατηρήσει την πρόσβασή του.
Ομάδα Cobalt	Η ομάδα Cobalt πρόσθεσε ως Module την διατήρηση της πρόσβασης, καταγράφοντας το όνομα του αρχείου για το κακόβουλο πρόγραμμα του επόμενου σταδίου κάτω από το **UserInitMprLogonScript**.
JHUHUGIT	Το JHUHUGIT έχει καταχωρήσει ένα Shell Script των Windows κάτω από το KEY της Registry **HKCU\Environment\UserInitMprLogonScript** για να καθορίσει την διατήρηση της πρόσβασης.
Zebrocy	Το Zebrocy επιτυγχάνει την διατήρηση της πρόσβασης μέσω της προσθήκης ενός KEY στη Registry με ένα Logon Script.

Για την αντιμετώπιση και τη μείωση αυτών των μεθόδων και των τεχνικών επιθέσεων προτείνεται ο περιορισμός των δικαιωμάτων στα αρχείων και στους καταλόγους του συστήματος. Πιο συγκεκριμένα μπορείτε να περιορίστε την πρόσβαση της εγγραφής στα Logon Scripts σε συγκεκριμένους διαχειριστές.

Όσο αναφορά στον εντοπισμό και στην ανίχνευση αυτών των τεχνικών επιθέσεων μπορείτε να παρακολουθείτε τα Logon Scripts για τυχόν ασυνήθιστη πρόσβαση από μη φυσιολογικούς χρήστες ή σε μη φυσιολογικές ώρες. Επιπλέον μπορείτε να αναζητείτε αρχεία που έχουν προστεθεί ή τροποποιηθεί από ασυνήθιστους λογαριασμούς εκτός των συνήθων Management διαδικασιών και καθηκόντων.

4.6 Pass the Hash

Η διαπεράση του Hash γνωστή ως **Pass the Hash** (PtH) είναι μια μέθοδος ελέγχου ταυτότητας του χρήστη χωρίς να υπάρχει πρόσβαση στον κωδικό πρόσβασης του σαφούς κειμένου του χρήστη. Αυτή η μέθοδος παρακάμπτει τα τυπικά βήματα ελέγχου ταυτότητας του χρήστη που απαιτούν συνήθως έναν κωδικό πρόσβασης σαφούς κειμένου, αλλά κινείται απευθείας στο τμήμα του ελέγχου της ταυτότητας όπου χρησιμοποιείται το Hash του κωδικού πρόσβασης του χρήστη. Σε αυτήν την τεχνική, οι έγκυροι Hashed κωδικοί πρόσβασης για τον ανάλογο χρησιμοποιούμενο λογαριασμό συλλαμβάνονται από τους επιτιθέμενους χρησιμοποιώντας μια τεχνική πρόσβασης γνωστή ως **Credentials Access**. Τα Hashes που έχουν καταγραφεί και συλλεχθεί από τους επιτιθέμενους χρησιμοποιούνται έπειτα μαζί με την μέθοδο του **Pass the Hash** (PtH) για τον έλεγχο ταυτότητας του συγκεκριμένου χρήστη. Μετά την αυθεντικοποίηση, το **Pass the Hash** (PtH) μπορεί να χρησιμοποιηθεί για την εκτέλεση ενεργειών σε τοπικά ή απομακρυσμένα συστήματα.

Τα Windows 7 και όλα τα νεότερα από αυτά λειτουργικά συστήματα με το KB2871997 απαιτούν έγκυρα Domain διαπιστευτήρια χρήστη ή RID 500 Hashes διαχειριστή.

Αξιοσημείωτο είναι το γεγονός του ότι είναι αρκετές οι περιπτώσεις και τα εργαλεία όπου κάνουν χρήση της μεθόδου **Pass the Hash** για την εκτέλεση επιθέσεων εσωτερικής μετακίνησης. Ενδεικτικά παρακάτω αναφέρονται ορισμένα παραδείγματα:

- APT1: Το Group APT1 είναι γνωστό ότι έχει χρησιμοποιήσει την τεχνική Pass the Hash.
- APT28: Το Group APT28 χρησιμοποίησε το Hash για πλευρική κίνηση.
- APT32: Το Group APT32 επίσης χρησιμοποίησε το Hash για πλευρική κίνηση.
- Cobalt Strike: Το Cobalt Strike μπορεί να εκτελέσει την μέθοδο Pass the Hash.
- Empire: Το Empire μπορεί να εκτελέσει επιθέσεις κάνοντας χρήση Pass the Hash.
- HOPLIGHT: Το **`HOPLIGHT`** έχει παρατηρηθεί να φορτώνει αρκετά APIs που σχετίζονται με την μέθοδο του Pass the Hash.
- Mimikatz: Το Module **`SEKURLSA: :Pth`** του Mimikatz μπορεί να μιμηθεί έναν χρήστη, με το Hash του κωδικού πρόσβασής του μονάχα, για να εκτελέσει αυθαίρετα εντολές.
- Night Dragon: Το Night Dragon χρησιμοποίησε εργαλεία Pass the Hash για να αποκτήσει ονόματα χρηστών και κωδικούς πρόσβασης.
- Pass-The-Hash Toolkit: Διάφορα Sets εργαλείων Pass-The-Hash μπορούν να εκτελέσουν την διαπέραση του Hash.
- PoshC2: Το PoshC2 διαθέτει έναν αριθμό από Modules τα οποία μοχλεύουν την μέθοδο του Pass the Hash για να επιτύχουν πλευρική κίνηση.
- Soft Cell: Το Soft Cell χρησιμοποίησε dumped Hashes για την αυθεντικοποίηση του σε άλλα συστήματα μέσω της τεχνικής Pass the Hash.

Για την αντιμετώπιση και τη μείωση αυτής της τεχνικής επιθέσεων προτείνεται η εφαρμογή και η τήρηση ορισμένων από τις διαδικασίες που περιγράφονται παρακάτω:

Πολιτικές κωδικού πρόσβασης	Βεβαιωθείτε ότι οι ενσωματωμένοι και οι δημιουργημένοι λογαριασμοί του τοπικού διαχειριστή έχουν πολύπλοκους και μοναδικούς κωδικούς πρόσβασης.
Διαχείριση των λογαριασμών με προνόμια	Περιορίστε την επικάλυψη των διαπιστευτηρίων σε όλα τα συστήματα, για να αποτρέψετε τη ζημιά των Compromised Credentials και να μειώσετε την ικανότητα του κάθε επιτιθέμενου όσο αναφορά στην πλευρική μετακίνηση μεταξύ συστημάτων.
Ενημέρωση λογισμικού	Εφαρμόστε το Patch KB2871997 στα συστήματα με Windows 7 καθώς και σε όλα τα συστήματα με νεότερα λειτουργικά, για να περιορίσετε την προεπιλεγμένη πρόσβαση λογαριασμών στην ομάδα των τοπικών διαχειριστών.
Έλεγχος λογαριασμού χρήστη	Ενεργοποιήστε Pass the Hash μετριασμούς για να εφαρμόσετε περιορισμούς UAC σε τοπικούς λογαριασμούς κατά την σύνδεση στο δίκτυο. Το συνδεδεμένο Registry Key βρίσκεται: **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy** μέσω του GPO: Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Εφαρμόστε περιορισμούς UAC σε τοπικούς λογαριασμούς στις συνδέσεις δικτύου.
Διαχείριση λογαριασμών χρηστών	Μην επιτρέπετε σε έναν χρήστη Domain να είναι στην ομάδα των τοπικών διαχειριστών σε πολλά συστήματα.

Όσο αναφορά στον εντοπισμό και στην ανίχνευση αυτής της τεχνικής επιθέσεων προτείνεται να ελέγχετε όλα τα Events για χρήση διαπιστευτηρίων και Logon και στη συνέχεια να κάνατε Review αυτών για το αν υπάρχουν τυχόν αποκλίσεις. Οι ασυνήθιστες απομακρυσμένες συνδέσεις που σχετίζονται με άλλη ύποπτη δραστηριότητα (όπως η εγγραφή και εκτέλεση δυαδικών αρχείων) ενδέχεται να υποδηλώνουν κακόβουλη δραστηριότητα. Επιπλέον, οι NTLM LogonType 3 Authentications που δεν συσχετίζονται με κάποια σύνδεση σε Domain και είναι ανώνυμες συνδέσεις είναι ύποπτες.

4.7 Pass the Ticket

Το Pass the Ticket (PtT) είναι μια μέθοδος ελέγχου ταυτότητας σε ένα σύστημα που χρησιμοποιεί Kerberos tickets για την αυθεντικοποίηση των χρηστών του, χωρίς να έχει πρόσβαση στον κωδικό πρόσβασης ενός λογαριασμού. Ο έλεγχος ταυτότητας Kerberos μπορεί να χρησιμοποιηθεί ως το πρώτο βήμα για πλευρική μετακίνηση σε ένα απομακρυσμένο σύστημα.

Σε αυτήν την τεχνική, τα έγκυρα tickets Kerberos για τους έγκυρους λογαριασμούς συλλαμβάνονται από τους επιτιθέμενους με την τεχνική του Credential Dumping. Μπορούν να συλληφθούν tickets υπηρεσίας χρήστη ή tickets χορήγησης ticket (TGT), ανάλογα με το επίπεδο της πρόσβασης. Ένα ticket υπηρεσίας χρήστη επιτρέπει την πρόσβαση σε έναν συγκεκριμένο πόρο, ενώ ένα TGT μπορεί να χρησιμοποιηθεί για να

ζητήσει tickets υπηρεσιών από την Υπηρεσία έκδοσης των Tickets (TGS) για πρόσβαση σε οποιονδήποτε πόρο έχει δικαιώματα πρόσβασης ο χρήστης.

Τα Silver Tickets μπορούν να ληφθούν για υπηρεσίες που χρησιμοποιούν μηχανισμό ελέγχου ταυτότητας Kerberos και χρησιμοποιούνται για τη δημιουργία εισιτηρίων που εξασφαλίζουν την πρόσβαση σε κάποιο συγκεκριμένο πόρο ενός συστήματος και στο σύστημα που φιλοξενεί τον πόρο αυτό (π.χ. SharePoint).

Τα Golden Tickets μπορούν να αποκτηθούν για το Domain χρησιμοποιώντας τον λογαριασμό Key Distribution Service KRBTGT λογαριασμού NTLM hash, όπου ενεργοποιεί την δημιουργία TGTs για οποιοδήποτε λογαριασμό στην υπηρεσία του Active Directory.

Ενδεικτικά παρακάτω αναφέρονται ορισμένα παραδείγματα περιπτώσεων χρήσης και εργαλείων όπου κάνουν χρήση της μεθόδου **Pass the Ticket** για την εκτέλεση επιθέσεων εσωτερικής μετακίνησης:

- APT29: Το APT29 χρησιμοποίησε εισβολές Kerberos για πλευρική κίνηση.
- APT32: Το APT32 απέκτησε επιτυχώς απομακρυσμένη πρόσβαση με τη χρήση του εισιτηρίου.
- BRONZE BUTLER: Το BRONZE BUTLER δημιούργησε πλαστά εισιτήρια εισιτηρίων εισιτηρίων (TGT) Kerberos και Ticketing Service Service (TGS) για τη διατήρηση διοικητικής πρόσβασης.
- Empire: Το Empire μπορεί να αξιοποιήσει την εφαρμογή του Mimikatz για να αποκτήσει και να χρησιμοποιήσει Silver και Golden εισιτήρια.
- Ke3chang: Το Ke3chang χρησιμοποίησε το Mimikatz για να δημιουργήσει Golden Tickets Kerberos.
- Mimikatz: Τα Modules του Mimikatz **`LSADUMP::DCSync`**, **`KERBEROS::Golden`** και **`KERBEROS::PTT`** εφαρμόζουν τα τρία βήματα που απαιτούνται για την εξαγωγή του hash λογαριασμό KRBTGT και τη δημιουργία / χρήση εισιτήρια Kerberos.
- SeaDuke: Ορισμένα δείγματα SeaDuke έχουν ένα Module το οποίο χρησιμοποιεί την τεχνική του Pass the Ticket με Kerberos για τον έλεγχο ταυτότητας.

Για την αντιμετώπιση και τη μείωση αυτής της τεχνικής επιθέσεων προτείνεται η εφαρμογή και η τήρηση ορισμένων από τις διαδικασίες που περιγράφονται παρακάτω:

Διαμόρφωση της υπηρεσίας του Active Directory	Για να περιορίσετε την επίπτωση ενός δημιουργημένου Golden Ticket επαναφέρετε δύο φορές τον ενσωματωμένο κωδικό πρόσβασης του λογαριασμού KRBTGT, γεγονός που θα ακυρώσει τυχόν υπάρχοντα Golden Tickets που έχουν δημιουργηθεί με το KRBTGT Hash και άλλα εισερχόμενα Kerberos Tickets από αυτό.
Πολιτικές κωδικού πρόσβασης	Βεβαιωθείτε ότι οι λογαριασμοί των τοπικών διαχειριστών έχουν σύνθετους και μοναδικούς κωδικούς πρόσβασης.
Διαχείριση των λογαριασμών με προνόμια	Περιορίστε τα δικαιώματα του λογαριασμού του domain Διαχειριστή σε domain controllers και σε περιορισμένους Servers. Αναθέστε και άλλες λειτουργίες διαχειριστή για να διαχωρίσετε τους λογαριασμούς.

Διαχείριση λογαριασμών χρηστών	Μην επιτρέπετε σε έναν χρήστη να είναι τοπικός διαχειριστής για πολλά συστήματα.

Για την ανίχνευση και τον εντοπισμό της τεχνικής του Pass the Ticket όπου χρησιμοποιούν οι επιτιθέμενοι προτείνεται να ελέγχετε όλα τα Events που αφορούν χρήση του Kerberos Authentication καθώς και τα Events που αφορούν χρήση διαπιστευτηρίων. Έπειτα να αξιολογείτε αν υπάρχουν αποκλίσεις σε αυτά. Τα ασυνήθιστα απομακρυσμένα Events ελέγχου ταυτότητας που σχετίζονται με άλλη ύποπτη δραστηριότητα (όπως η εγγραφή και εκτέλεση δυαδικών αρχείων) μπορεί να υποδηλώνουν κακόβουλη δραστηριότητα. Το Αναγνωριστικό συμβάντος (Event ID) **4769** δημιουργείται στον Domain Controller όταν χρησιμοποιείται ένα Golden Ticket μετά την επαναφορά του κωδικού πρόσβασης KRBTGT δύο φορές, όπως αναφέρεται και στην προηγούμενη ενότητα παραπάνω. Ο κωδικός κατάστασης **0x1F** υποδεικνύει ότι η ενέργεια απέτυχε λόγω του "Έλεγχος ακεραιότητας του αποκρυπτογραφημένου πεδίου απέτυχε" και αυτό υποδεικνύει την κατάχρηση ενός μη έγκυρου Golden Ticket [1].

4.8 Πρωτόκολλο Remote Desktop

Το Remote Desktop είναι μια κοινή λειτουργία στα λειτουργικά συστήματα. Επιτρέπει σε έναν χρήστη να συνδεθεί μέσω μιας διαδραστικής συνεδρίας με ένα γραφικό περιβάλλον χρήστη 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.

Οι επιτιθέμενοι μπορούν να συνδεθούν σε ένα απομακρυσμένο σύστημα μέσω του RDP / RDS για να επεκτείνουν την πρόσβαση τους εάν η υπηρεσία είναι ενεργοποιημένη και επιτρέπει πρόσβαση σε λογαριασμούς με γνωστά διαπιστευτήρια. Οι επιτιθέμενοι πιθανότατα θα χρησιμοποιήσουν τεχνικές πρόσβασης πιστοποίησης για να αποκτήσουν τα διαπιστευτήρια που θα χρησιμοποιήσουν με το RDP. Οι επιτιθέμενοι μπορούν επίσης να χρησιμοποιήσουν το RDP σε συνδυασμό με τα χαρακτηριστικά της τεχνικής προσβασιμότητας για να επιτύχουν διατήρηση της πρόσβασής τους.

Οι επιτιθέμενοι μπορούν επίσης να εκτελούν hijacking της συνεδρίας RDP, η οποία συνεπάγεται την κλοπή της απομακρυσμένης περιόδου λειτουργίας ενός νόμιμου χρήστη. Συνήθως, ένας χρήστης ειδοποιείται όταν κάποιος άλλος προσπαθεί να κλέψει την συνεδρία του και του το εμφανίζει μέσω μια ερώτησης στην οθόνη του. Με δικαιώματα συστήματος και με χρήση υπηρεσιών της τερματικής κονσόλας (Terminal Services Console) **c:\windows\system32\tscon.exe [session number to be stolen]**, ένας επιτιθέμενος μπορεί να πειραματιστεί σε μια συνεδρία χωρίς να χρειαστεί πιστοποιήσεις ή υποδείξεις προς το χρήστη. Αυτό μπορεί να γίνει απομακρυσμένα ή τοπικά με ενεργές ή και με αποσυνδεδεμένες συνεδρίες. Μπορεί επίσης να οδηγήσει σε απομακρυσμένη ανακάλυψη του συστήματος και σε εξέλιξη των προνομίων, κλέβοντας μια συνεδρία μέσω ενός λογαριασμού Domain διαχειριστή ή ένα λογαριασμό με υψηλότερα προνόμια. Όλα αυτά

μπορούν να γίνουν με τη χρήση εγγενών-ενσωματωμένων εντολών των Windows, αλλά έχουν επίσης προστεθεί και ως χαρακτηριστικό στο εργαλείο RedSnarf όπου το χρησιμοποιούν οι ομάδες που επιτίθονται σε δίκτυα υπολογιστών με σκοπό να τα ελέγξουν και να τα διασφαλίσουν καλυτέρα.

Αξιοσημείωτος είναι ο αριθμός των περιπτώσεων όπου έχει εκμεταλλευτεί η λειτουργία αυτή των Windows σε συνδυασμό με την εφαρμογή σχετικών τεχνικών και εργαλείων για την εκτέλεση επιθέσεων εσωτερικής μετακίνησης. Ενδεικτικά παρακάτω αναφέρονται ορισμένα παραδείγματα [1]:

APT1 & Axiom	Η ομάδες APT1 και Axiom είναι γνωστό ότι έχουν χρησιμοποιήσει το RDP κατά τη διάρκεια των κακόβουλων εργασιών τους.
APT39 & APT41	Οι ομάδες APT39 και APT41 έχουν παρατηρηθεί να χρησιμοποιούν το RDP για να επιτύχουν πλευρική μετακίνηση και διατήρηση πρόσβασης.
Carbanak	Το Carbanak ενεργοποιεί και επιτρέπει την υπηρεσία της απομακρυσμένης επιφάνειας εργασίας (RDP).
Cobalt Group & Dragonfly	Η ομάδα του Cobalt και το Dragonfly 2.0 χρησιμοποίησαν το πρωτόκολλο του RDP για να πραγματοποιήσουν πλευρική κίνηση.
Cobalt Strike	Το Cobalt Strike μπορεί να ξεκινήσει έναν εξυπηρετητή RDP σύνδεσης ο οποίος βασίζεται σε VNC σύνδεση και να κάνει tunnel τη σύνδεση αυτή μέσω του ήδη καθιερωμένου C2 καναλιού.
DarkComet	Το DarkComet μπορεί να ανοίξει μια ενεργή οθόνη στο μηχάνημα του θύματος και να πάρει τον έλεγχο του ποντικιού και του πληκτρολογίου.
FIN10	Το FIN10 χρησιμοποίησε το πρωτόκολλο RDP για να μετακινηθεί πλευρικά σε συστήματα εντός του περιβάλλοντος του θύματος.
FIN6	Το FIN6 χρησιμοποίησε το πρωτόκολλο RDP για να μετακινηθεί πλευρικά σε δίκτυα του θύματος.
FIN8	Το FIN8 χρησιμοποίησε το πρωτόκολλο RDP για να πραγματοποιήσει πλευρική κίνηση.
jRAT	Το jRAT μπορεί να υποστηρίξει τον έλεγχο του πρωτοκόλλου RDP.
Koadic	Το Koadic μπορεί να ενεργοποιήσει την υπηρεσία της απομακρυσμένης επιφάνειας εργασίας στο μηχάνημα του θύματος.
Lazarus Group	Το κακόβουλο λογισμικό της ομάδας Lazarus SierraCharlie χρησιμοποιεί το πρωτόκολλο RDP για την διάδοση του.
Leviathan	Το Leviathan έχει στοχεύσει τα διαπιστευτήρια της υπηρεσίας του RDP και τα χρησιμοποίησε για να περάσει από το περιβάλλον του θύματος.
menuPass	Το menuPass έχει χρησιμοποιήσει συνδέσεις RDP για να μετακινηθεί εσωτερικά στο δίκτυο του θύματος.
njRAT	Το njRAT διαθέτει ένα Module για την εκτέλεση απομακρυσμένης

	επιφάνειας εργασίας (RDP).
OilRig	Το OilRig έχει χρησιμοποιήσει το πρωτόκολλο του RDP για να επιτύχει πλευρική κίνηση. Η ομάδα του OilRig χρησιμοποίησε επίσης εργαλεία tunneling για να καταφέρει να κάνει tunnel το RDP μέσα στο περιβάλλον.
Patchwork	Το Patchwork επιχείρησε να χρησιμοποιήσει το πρωτόκολλο του RDP για να κινηθεί πλευρικά.
Pupy	Το εργαλείο Pupy μπορεί να ενεργοποιήσει / απενεργοποιήσει συνδέσεις RDP και να ξεκινήσει μια συνεδρία απομακρυσμένης επιφάνειας εργασίας (RDP) χρησιμοποιώντας έναν browser web socket client.
QuasarRAT	Το QuasarRAT διαθέτει ένα Module για την εκτέλεση απομακρυσμένης επιφάνειας εργασίας (RDP).
Revenge RAT	Το Revenge RAT διαθέτει ένα plugin για την απόκτηση πρόσβασης μέσω του RDP.
ServHelper	Το κακόβουλο λογισμικό ServHelper διαθέτει εντολές για την προσθήκη ενός χρήστη απομακρυσμένης επιφάνειας εργασίας (RDP) και για την αποστολή RDP κίνησης στον επιτιθέμενο μέσω ενός Reverse SSH tunnel.
Stolen Pencil	Το Group απειλών Stolen Pencil χρησιμοποίησε την υπηρεσία του RDP για άμεση απομακρυσμένη πρόσβαση τύπου point-and-click.
TEMP.Veles	Το TEMP.Veles χρησιμοποίησε την λειτουργία RDP καθ’ όλη τη διάρκεια μιας λειτουργίας του.
WannaCry	Το WannaCry απαριθμεί τις τρέχουσες συνεδρίες απομακρυσμένης επιφάνειας εργασίας (RDP) και προσπαθεί να εκτελέσει το κακόβουλο λογισμικό του σε κάθε σύνοδο.
zwShell	Το zwShell χρησιμοποίησε το RDP για πλευρική μετακίνηση.
ZxShell	Το ZxShell έχει λειτουργικότητα απομακρυσμένης επιφάνειας εργασίας (RDP).

Για την αντιμετώπιση και τη μείωση της τεχνικής επιθέσεων μέσω της υπηρεσίας του RDP προτείνεται η εφαρμογή και η τήρηση των διαδικασιών που περιγράφονται παρακάτω:

Έλεγχος	Ελέγχετε τακτικά την ιδιότητα κάθε μέλους της ομάδας των χρηστών Remote Desktop. Καταργήστε τους λογαριασμούς και τις ομάδες που δεν χρησιμοποιούνται από τις ομάδες χρηστών της υπηρεσίας RDP.
Απενεργοποίηση ή κατάργηση δυνατότητας ή προγράμματος	Απενεργοποιήστε την υπηρεσία RDP εάν δεν είναι απαραίτητη.
Περιορίστε την	Χρησιμοποιήστε Gateways απομακρυσμένης επιφάνειας εργασίας

πρόσβαση στους πόρους μέσω δικτύου	(RDP).
Έλεγχος ταυτότητας πολλαπλών παραγόντων	Χρησιμοποιήστε έλεγχο ταυτότητας πολλαπλών παραγόντων για απομακρυσμένες συνδέσεις.
Τμηματοποίηση δικτύου	Μην αφήνετε την υπηρεσία του RDP να είναι προσβάσιμη από το Διαδίκτυο. Ενεργοποιήστε κατάλληλους κανόνες στο τείχος προστασίας σας για να αποκλείσετε την κίνηση της υπηρεσίας RDP μεταξύ των δικτυακών ζωνών ασφάλειας εντός του δικτύου σας.
Ρύθμιση λειτουργικού συστήματος	Αλλάξτε τα GPOs για να ορίσετε συντομότερες σε χρονικό όριο συνεδρίες και το μέγιστο χρονικό διάστημα που μπορεί να είναι ενεργή οποιαδήποτε μεμονωμένη συνεδρία. Αλλάξτε τα Group Policy Objects (GPOs) για να καθορίσετε το μέγιστο χρονικό διάστημα κατά το οποίο μια αποσυνδεδεμένη συνεδρία παραμένει ενεργή στον Host εξυπηρετητή των συνεδρίων RDP.
Διαχείριση των λογαριασμών με προνόμια	Εξετάστε την περίπτωση να αφαιρέσετε την τοπική ομάδα των Administrators από τη λίστα των ομάδων που επιτρέπεται να συνδεθούν μέσω της υπηρεσίας του RDP.
Διαχείριση των λογαριασμών των χρηστών	Περιορίστε τα δικαιώματα των απομακρυσμένων χρηστών εάν τους είναι απαραίτητη η απομακρυσμένη πρόσβαση.

Για την ανίχνευση και τον εντοπισμό των επιθέσεων μέσω της τεχνικής που χρησιμοποιούν οι επιτιθέμενοι κάνοντας χρήση της υπηρεσίας του RDP προτείνεται να επιτρέπεται μονάχα η νόμιμη χρήση του RDP, ανάλογα με το περιβάλλον του δικτύου και τον τρόπο χρήσης της υπηρεσίας. Άλλοι παράγοντες, όπως τα πρότυπα πρόσβασης και η δραστηριότητα που συμβαίνει μετά από μια απομακρυσμένη σύνδεση, ενδέχεται να υποδηλώνουν ύποπτη ή κακόβουλη συμπεριφορά με τη λειτουργία του RDP. Παρακολουθήστε επίσης τους λογαριασμούς των χρηστών που έχουν συνδεθεί σε συστήματα που κανονικά δεν τους επιτρέπεται να έχουν πρόσβαση ή έχουν συνδεθεί σε πολλά διαφορετικά συστήματα σε σχετικά σύντομο χρονικό διάστημα.

Τέλος, ρυθμίστε την παρακολούθηση του Process για χρήση του **`tscon.exe`** και την παρακολούθηση της δημιουργίας της υπηρεσίας που χρησιμοποιεί το **`cmd.exe /k`** ή το **`cmd.exe /c`** στα arguments του για να αποτρέψετε την αεροπειρατεία μιας συνεδρίας RDP.

4.9 Απομακρυσμένη αντιγραφή αρχείου

Αρχεία μπορούν να αντιγραφούν από το ένα σύστημα στο άλλο για να οργανώσουν τα εργαλεία των επιτιθέμενων ή άλλα αρχεία κατά τη διάρκεια μιας ενέργειας. Αρχεία μπορούν επίσης να αντιγραφούν από ένα εξωτερικό ελεγχόμενο από τους επιτιθέμενους σύστημα μέσω Command και να παρθεί ο έλεγχος του καναλιού για να φέρουν εργαλεία στο δίκτυο του στόχου ή μέσω εναλλακτικών πρωτοκόλλων με άλλα εργαλεία όπως το FTP. Τα αρχεία μπορούν επίσης να αντιγραφούν σε Mac και σε Linux συστήματα με εγγενή εργαλεία όπως scp, rsync και sftp.

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

Οι περιπτώσεις αυτές όπου έχει χρησιμοποιηθεί η τεχνική της απομακρυσμένης αντιγραφής αρχείου από επιτιθέμενους κατά την διάρκεια εκτέλεσης κάποιας επίθεσής τους είναι πάρα πολλές. Ενδεικτικά παρακάτω αναφέρονται ορισμένα πολύ γνωστά παραδείγματα [1]:

Agent Tesla	Ο Agent Tesla μπορεί να κατεβάσει πρόσθετα αρχεία για εκτέλεση στο μηχάνημα του θύματος.
Agent.btz	Ο Agent.btz προσπαθεί να πραγματοποιήσει λήψη κρυπτογραφημένων δυαδικών αρχείων από συγκεκριμένο domain.
APT18	Το APT18 μπορεί να φορτώσει ένα αρχείο στο μηχάνημα του θύματος.
APT28	Το APT28 έκανε Download πρόσθετα αρχεία, μεταξύ άλλων χρησιμοποιώντας ένα downloader πρώτου σταδίου για να επικοινωνήσει με το διακομιστή C2 και να αποκτήσει έτσι το εμφύτευμα του δεύτερου σταδίου.
APT38	Το APT38 χρησιμοποίησε ένα backdoor, το NESTEGG, το οποίο έχει τη δυνατότητα λήψης και φόρτωσης αρχείων προς και από το μηχάνημα του θύματος.
Astaroth	Το Astaroth έκανε χρήση certutil και BITSAdmin για να κατεβάσει επιπλέον κακόβουλο λογισμικό.
AuditCred	Το AuditCred μπορεί να κατεβάσει αρχεία και πρόσθετο κακόβουλο λογισμικό.
Azorult	Το Azorult μπορεί να κατεβάσει και να εκτελέσει πρόσθετα αρχεία. Το Azorult έχει επίσης κατεβάσει στο παρελθόν ένα φορτίο ransomware που ονομάζεται Hermes.
BabyShark	Το BabyShark έχει κατεβάσει πρόσθετα αρχεία από το C2.
BADNEWS	Το BADNEWS έχει τη δυνατότητα λήψης πρόσθετων αρχείων μέσω καναλιών C2, συμπεριλαμβανομένης μιας καινούριας έκδοσης του.

BadPatch	Το BadPatch μπορεί να κατεβάσει και να εκτελέσει ή να ενημερώσει κακόβουλο λογισμικό.
Bankshot	Το Bankshot ανεβάζει αρχεία και δευτερεύοντα ωφέλιμα φορτία(payloads) στο μηχάνημα του θύματος.
BISCUIT	Το BISCUIT διαθέτει εντολή για να κατεβάσει ένα αρχείο από το διακομιστή C2.
Bisonal	Το Bisonal έχει τη δυνατότητα να κατεβάσει αρχεία για εκτέλεση στο μηχάνημα του θύματος.
BITSAdmin	Το BITSAdmin μπορεί να χρησιμοποιηθεί για δημιουργία εργασιών BITS και να κάνει UPLOAD ή DOWNLOAD αρχεία.
Briba	Το Briba κατεβάζει αρχεία σε μολυσμένους κεντρικούς υπολογιστές.
BRONZE BUTLER	Το BRONZE BUTLER χρησιμοποίησε διάφορα εργαλεία για τη λήψη αρχείων, συμπεριλαμβανομένου του DGet (ένα παρόμοιο εργαλείο με το wget).
Calisto	Το Calisto έχει τη δυνατότητα να κάνει Upload και Download αρχεία στο και από το μηχάνημα του θύματος.
Daserf	Το Daserf μπορεί να κάνει λήψη απομακρυσμένων αρχείων.
Denis	Το Denis(Windows backdoor και Trojan) διαθέτει στο σύστημα πρόσθετα backdoors και εργαλεία hacking.
Dragonfly 2.0	Το Dragonfly 2.0 αντιγράφει και εγκαθιστά εργαλεία που λειτουργούν μία φορά στο περιβάλλον του θύματος.
Linfo	Το Linfo δημιουργεί ένα backdoor μέσω του οποίου οι απομακρυσμένοι εισβολείς μπορούν να κατεβάζουν αρχεία σε συμβιβασμένους οικοδεσπότες.
LOWBALL	Το LOWBALL χρησιμοποιεί το API του Dropbox για να ζητήσει δύο αρχεία, ένα εκ των οποίων είναι το ίδιο αρχείο με εκείνο που έγινε dropped από το κακόβουλο συνημμένο του ηλεκτρονικού ταχυδρομείου. Αυτό πιθανότατα επρόκειτο να είναι ένας μηχανισμός για την ενημέρωση του compromised host με μια νέα έκδοση του κακόβουλου λογισμικού LOWBALL.
Mivast	Το Mivast έχει τη δυνατότητα λήψης και εκτέλεσης αρχείων .exe.
More_eggs	Το JavaScript Backdoor More_eggs μπορεί να κατεβάσει και να εκκινήσει επιπλέον ωφέλιμα φορτία(Payloads).
NanHaiShu	Το NanHaiShu μπορεί να κατεβάσει πρόσθετα αρχεία από διευθύνσεις URL.
NOKKI	Το NOKKI έχει κατεβάσει ένα απομακρυσμένο Module για εκτέλεση.
Remsec	Το Remsec(Modular Backdoor)περιέχει έναν loader δικτύου για να λαμβάνει εκτελέσιμα Modules από απομακρυσμένους εισβολείς και να τα εκτελεί στο τοπικό θύμα. Μπορεί επίσης να κάνει Upload αλλά

	και να κατεβάσει αρχεία μέσω HTTP και HTTPS.
SQLRat	Το Malware SQLRat μπορεί να πραγματοποιήσει απευθείας σύνδεση σε μια βάση δεδομένων SQL της Microsoft που ελέγχεται από τους επιτιθέμενους, να ανακτήσει ένα στοιχείο από τον πίνακα bindata και στη συνέχεια να γράψει και να εκτελέσει το αρχείο στο δίσκο.
TrickBot	Το TrickBot κατεβάζει αρκετά πρόσθετα αρχεία και τα αποθηκεύει στη μηχανή του θύματος.
TURNEDUP	Το TURNEDUP έχει τη δυνατότητα λήψης πρόσθετων αρχείων.

Για την αντιμετώπιση και τη μείωση των επιθέσεων που πραγματοποιούνται μέσω της τεχνικής της απομακρυσμένης αντιγραφής αρχείων προτείνεται η χρήση συστημάτων αποτροπής εισβολών στην περίμετρο του δικτύου σας. Τα συστήματα ανίχνευσης και αποτροπής εισβολών δικτύου που χρησιμοποιούν υπογραφές δικτύου για τον εντοπισμό της επισκεψιμότητας για συγκεκριμένο κακόβουλο λογισμικό ή για ασυνήθιστη μεταφορά δεδομένων με γνωστά εργαλεία και πρωτόκολλα, όπως το FTP, μπορούν να χρησιμοποιηθούν για να μετριάσουν τη δραστηριότητα αυτή σε επίπεδο δικτύου. Οι υπογραφές αναφέρονται συχνά σε μοναδικούς δείκτες μέσα στα πρωτόκολλα και μπορεί να βασίζονται στην συγκεκριμένη τεχνική συσκότισης που χρησιμοποιείται από έναν συγκεκριμένο επιτιθέμενο ή εργαλείο και πιθανότατα να είναι διαφορετικές σε διάφορες οικογένειες και εκδόσεις malware. Οι επιτιθέμενοι είναι πιθανόν να αλλάξουν εργαλείο για τις υπογραφές C2 με την πάροδο του χρόνου ή να κατασκευάσουν πρωτόκολλα με τέτοιο τρόπο ώστε να αποφευχθεί η ανίχνευση τους από τα κοινά αμυντικά εργαλεία.

Για την ανίχνευση και τον εντοπισμό επιθέσεων μέσω της τεχνικής της απομακρυσμένης αντιγραφής αρχείων προτείνεται να παρακολουθείτε η δημιουργία των αρχείων και τα αρχεία που μεταφέρονται μέσα σε ένα δίκτυο μέσω του πρωτοκόλλου SMB. Επιπλέον τα ασυνήθιστα Processes με εξωτερικές συνδέσεις δικτύου που δημιουργούν αρχεία στο σύστημα ενδέχεται να είναι ύποπτα. Ακόμη ύποπτη μπορεί να είναι η χρήση βοηθητικών προγραμμάτων μεταφοράς αρχείων, όπως το FTP, που δεν συμβαίνει συχνά σε ένα σύστημα. Προτείνεται επίσης να γίνεται ανάλυση στα δεδομένα του δικτύου για τυχόν εύρεση ασυνήθιστων ροών δεδομένων (π.χ. ένας Client που στέλνει σημαντικά περισσότερα δεδομένα από αυτά που λαμβάνει από έναν διακομιστή). Τα Processes που χρησιμοποιούν το δίκτυο και δεν έχουν κανονικά κάποια επικοινωνία μέσω δικτύου ή δεν έχουν ξαναεμφανιστεί ποτέ ξανά πρώτού γίνουν ύποπτα. Τέλος, προτείνεται να γίνεται ανάλυση στα περιεχόμενα των πακέτων του δικτύου για την ανίχνευση των επικοινωνιών που δεν ακολουθούν την αναμενόμενη συμπεριφορά πρωτοκόλλου για τη θύρα που χρησιμοποιείται.

4.10 Απομακρυσμένες Υπηρεσίες

Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει έγκυρους λογαριασμούς σε ένα σύστημα 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 στο συγκεκριμένο σύστημα.

Οι περιπτώσεις αυτές όπου έχει γίνει χρήση των απομακρυσμένων υπηρεσιών από επιτιθέμενους κατά την διάρκεια εκτέλεσης κάποιας επίθεσής τους είναι αρκετές και συχνά εμφανιζόμενες. Ενδεικτικά παρακάτω αναφέρονται ορισμένα παραδείγματα:

APT39	Το APT39 χρησιμοποίησε ασφαλές κέλυφος (SSH) για να μετακινηθεί πλευρικά μεταξύ των στόχων του.
Cobalt Strike	Το Cobalt Strike μπορεί να συνδεθεί με SSH σε μια απομακρυσμένη υπηρεσία.
Empire	Το Empire περιέχει Modules για την εκτέλεση εντολών μέσω SSH όπως και VNC injection μέσα στη μνήμη του μηχανήματος του στόχου.
GCMAN	Το GCMAN χρησιμοποιεί το Putty και το VNC για πλευρική κίνηση.
Leviathan	Το toolkit Leviathan χρησιμοποίησε ssh για εσωτερική αναγνώριση.
menuPass	Το group απειλών menuPass έχει χρησιμοποιήσει το Client Putty Secure Copy Client (PSCP) για τη μεταφορά δεδομένων.
OilRig	Το OilRig έχει χρησιμοποιήσει το Putty για πρόσβαση σε Compromised συστήματα.
Proton	Το Proton χρησιμοποιεί το VNC για να συνδεθεί σε συστήματα.
TEMP.Veles	Το TEMP.Veles (Russia-based threat group) βασίστηκε σε κρυπτογραφημένα SSH-based tunnels για να μεταφέρει εργαλεία και για να εκτελέσει απομακρυσμένα εντολές / προγράμματα.
ZxShell	Το ZxShell υποστηρίζει λειτουργικότητα για συνεδρίες VNC.

Για την αντιμετώπιση και τη μείωση των επιθέσεων που πραγματοποιούνται μέσω της τεχνικής χρήσης των απομακρυσμένων υπηρεσιών από τους επιτιθέμενους προτείνεται να γίνεται έλεγχος της ταυτότητας των χρηστών με τη μέθοδο των πολλαπλών παραγόντων(Multi-factor Authentication), δηλαδή να χρησιμοποιείτε έλεγχο ταυτότητας πολλαπλών παραγόντων στις συνδέσεις των απομακρυσμένων υπηρεσιών όπου είναι δυνατόν αυτό βέβαια.

Επιπλέον προτείνεται η ορθή διαχείριση των λογαριασμών των χρηστών, δηλαδή να περιορίστε τους λογαριασμούς που ενδέχεται να χρησιμοποιούν απομακρυσμένες υπηρεσίες. Προτείνεται να περιορίστε τα δικαιώματα για τους λογαριασμούς εκείνους όπου διατρέχουν μεγαλύτερο κίνδυνο στο να γίνουν Compromised. Για παράδειγμα, ρυθμίστε ορθά το SSH, ώστε οι χρήστες που συνδέονται μέσω αυτής της υπηρεσίας να μπορούν να εκτελούν μόνο συγκεκριμένα προγράμματα.

Για την ανίχνευση και τον εντοπισμό των επιθέσεων που πραγματοποιούνται μέσω της τεχνικής χρήσης των απομακρυσμένων υπηρεσιών από τους επιτιθέμενους μπορείτε να ελέγχετε τη χρήση της δραστηριότητας σύνδεσης που σχετίζεται με απομακρυσμένες υπηρεσίες με ασυνήθιστη συμπεριφορά ή άλλη κακόβουλη ή ύποπτη δραστηριότητα. Οι επιτιθέμενοι θα πρέπει πιθανόν να μάθουν για ένα περιβάλλον και τις σχέσεις μεταξύ των συστημάτων μέσω των τεχνικών του Discovery πριν από την προσπάθεια τους για εσωτερική μετακίνηση(Lateral Movement).

4.11 Αναπαραγωγή μέσω αφαιρούμενων μέσων

Οι επιτιθέμενοι μπορούν να μετακινούνται από συστήματα σε συστήματα, πιθανώς και σε δίκτυα από τα οποία έχουν αποσυνδεθεί, αντιγράφοντας κακόβουλα προγράμματα σε αφαιρούμενα μέσα και εκμεταλλευόμενοι τις δυνατότητες του Autorun όταν τα μέσα αυτά εισάγονται σε ένα σύστημα και να εκτελούνται αυτόματα. Στην περίπτωση της πλευρικής κίνησης, αυτό μπορεί να συμβεί με τροποποίηση των εκτελέσιμων αρχείων που είναι αποθηκευμένα σε αφαιρούμενα μέσα ή με κάποια αντιγραφή ενός κακόβουλου λογισμικού και μετονομασία αυτού για να μοιάζει με ένα νόμιμο αρχείο και για να εξαπατήσουν τους χρήστες να το εκτελέσουν σε κάποιο ξεχωριστό σύστημα. Στην περίπτωση της αρχικής πρόσβασης, αυτό μπορεί να συμβεί με το χειροκίνητο χειρισμό των αφαιρούμενων μέσων, την τροποποίηση των συστημάτων που χρησιμοποιήθηκαν για την αρχική διαμόρφωση του μέσου ή την τροποποίηση του ίδιου του υλικολογισμικού των αφαιρούμενων μέσων.

Οι περιπτώσεις όπου έχει γίνει χρήση αφαιρούμενων μέσων από επιτιθέμενους κατά την διάρκεια εκτέλεσης κάποιας επίθεσής τους για την επίτευξη εσωτερικής μετακίνησης μέσα σε ένα δίκτυο με Windows Domain είναι αρκετές και συχνά εμφανιζόμενες. Ενδεικτικά παρακάτω αναφέρονται ορισμένα παραδείγματα [1]:

Agent.btz	Το worm Agent.btz πέφτει πάνω σε αφαιρούμενες συσκευές πολυμέσων και δημιουργεί ένα αρχείο autorun.inf με μια εντολή για την εκτέλεση αυτού του κακόβουλου αρχείου. Όταν η συσκευή εισάγεται σε κάποιο άλλο σύστημα, ανοίγει το autorun.inf και φορτώνει το κακόβουλο πρόγραμμα.
APT28	Το APT28 χρησιμοποιεί ένα εργαλείο για να μολύνει τις συσκευές USB που είναι συνδεδεμένες σε ένα σύστημα και να μεταδοθεί έτσι και σε άλλους υπολογιστές στους οποίους έχει εισαχθεί η μολυσμένη αυτή συσκευή USB.
CHOPSTICK	Μέρος της λειτουργίας του APT28 περιλάμβανε τη χρήση των Modules του CHOPSTICK για την αντιγραφή του ίδιου και σε άλλα συστήματα όπως και τη χρήση αρχείων γραμμένων σε USB sticks για μεταφορά δεδομένων και για την εκτέλεση εντολών κίνησης.
Darkhotel	Ο μολυντικός παράγοντας που διαθέτει το Darkhotel τροποποιεί τα εκτελέσιμα αρχεία που είναι αποθηκευμένα σε αφαιρούμενα μέσα ως μια μέθοδο διάδοσης του και σε άλλους υπολογιστές.
DustySky	Το Malware DustySky ψάχνει για αφαιρούμενα μέσα σε ένα σύστημα και δημιουργεί διπλότυπα του σε αυτά.
Flame	Το toolkit Flame περιέχει Modules για να μολύνει τα USB Sticks και να εξαπλωθεί έτσι πλευρικά και σε άλλα συστήματα Windows, καθώς το USB Stick είναι συνδεδεμένο στο μηχάνημα και χρησιμοποιώντας τη λειτουργία του Autorun.
H1N1	Το H1N1 έχει λειτουργικότητα η οποία του επιτρέπει την αντιγραφή του σε αφαιρούμενα μέσα.
njRAT	Το njRAT μπορεί να ρυθμιστεί ώστε να εξαπλώνεται μέσω αφαιρούμενων

	μονάδων δίσκου.
SHIPSHAPE	Το APT30 μπορεί να έχει χρησιμοποιήσει το κακόβουλο λογισμικό SHIPSHAPE για να μετακινηθεί σε δίκτυα με κενά αέρος. Το SHIPSHAPE στοχεύει σε αφαιρούμενες μονάδες δίσκου για να εξαπλωθεί και σε άλλα συστήματα τροποποιώντας τη μονάδα δίσκου για να χρησιμοποιήσει το Autorun για να εκτελέσει ή αποκρύπτοντας τα νόμιμα αρχεία εγγράφων και αντιγράφοντας ένα εκτελέσιμο αρχείο στο φάκελο με το ίδιο όνομα με το νόμιμο έγγραφο.
Unknown Logger	Το Unknown Logger είναι ικανό να εξαπλωθεί σε συσκευές USB.
Ursnif	Το Ursnif έχει αντιγράψει και έχει μολύνει μετακινούμενους δίσκους για την διάδοση του.
USBStealer	Το USBStealer πέφτει πάνω σε αφαιρούμενα μέσα και στηρίζεται στο Autorun για να εκτελέσει το κακόβουλο αρχείο όταν ένας χρήστης ανοίξει το αφαιρούμενο μέσο σε κάποιο άλλο σύστημα.

Για την αντιμετώπιση και τη μείωση των επιθέσεων που πραγματοποιούνται από τους επιτιθέμενους μέσω της τεχνικής χρήσης των αφαιρούμενων μέσων προτείνεται να απενεργοποιήσετε το Autorun αν δεν είναι απαραίτητο όπως και να απενεργοποιήσετε ή περιορίσετε τα αφαιρούμενα μέσα σε επίπεδο πολιτικής οργανισμού, εάν δεν απαιτείται φυσικά για επιχειρησιακές λειτουργίες. Επιπλέον προτείνεται να περιορίσετε την χρήση των συσκευών USB και των αφαιρούμενων μέσων εντός ενός δικτύου.

Για την ανίχνευση και τον εντοπισμό των επιθέσεων που πραγματοποιούνται από τους επιτιθέμενους μέσω της τεχνικής χρήσης των αφαιρούμενων μέσων μπορείτε να παρακολουθείτε την πρόσβαση των αρχείων που βρίσκονται στα αφαιρούμενα μέσα. Εντοπίστε διεργασίες που εκτελούνται από αφαιρούμενα μέσα μετά την τοποθέτησή τους ή όταν ξεκινούν από έναν χρήστη. Εάν διαπιστωθεί η χρήση ενός εργαλείου απομακρυσμένης πρόσβασης για να μετακινηθεί πλευρικά ο επιτιθέμενος με αυτόν τον τρόπο, 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 του συστήματος και του δικτύου.

4.12 Κοινόχρηστο Webroot

Οι επιτιθέμενοι μπορούν να προσθέσουν κακόβουλο περιεχόμενο σε έναν ιστότοπο που είναι προσβάσιμος από το διαδίκτυο μέσω ενός ανοιχτού δικτυακού κοινόχρηστου αρχείου το οποίο περιέχει το webroot του ιστότοπου ή τον κατάλογο του περιεχομένου του ιστότοπου και στη συνέχεια αφού περιηγείστε σε αυτό το περιεχόμενο με κάποιο πρόγραμμα περιήγησης στο Web να αναγκάσει έτσι τον διακομιστή να εκτελέσει το κακόβουλο περιεχόμενο.

Το κακόβουλο περιεχόμενο συνήθως εκτελείται κάτω από το πλαίσιο και τα δικαιώματα της λειτουργίας 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 πλευρική μετακίνηση στο σύστημα που εκτελεί το διακομιστή Web.

Για παράδειγμα, ένας διακομιστής Web που εκτελεί PHP με ανοιχτό network share θα μπορούσε να επιτρέψει σε έναν επιτιθέμενο να φορτώσει ένα εργαλείο απομακρυσμένης πρόσβασης(RAT) και ένα Script PHP για να εκτελέσει το RAT(Remote Admin Tool) στο σύστημα που εκτελεί τον διακομιστή Web όταν επισκέπτεται μια συγκεκριμένη σελίδα.

Για την αντιμετώπιση και τη μείωση των επιθέσεων που πραγματοποιούνται με τον συγκεκριμένο τρόπο-τεχνική προτείνεται να εφαρμόζετε ορισμένες από τις παρακάτω μεθόδους [1]:

Περιορίστε την πρόσβαση στους πόρους μέσω δικτύου	Αποκλείστε την απομακρυσμένη πρόσβαση σε καταλόγους του webroot ή σε άλλους καταλόγους που χρησιμοποιούνται για την προβολή περιεχομένου του ιστού.
Τμηματοποίηση δικτύου	Δίκτυα που επιτρέπουν την ανοιχτή ανάπτυξη και δοκιμή περιεχομένου Web όπως επίσης επιτρέπουν στους χρήστες να δημιουργήσουν τους δικούς τους διακομιστές Ιστού στο επιχειρηματικό δίκτυο μπορεί να είναι ιδιαίτερα ευάλωτα εάν τα συστήματα και οι διακομιστές Web δεν είναι σωστά ασφαλισμένοι για να περιορίσουν τη μη εξουσιοδοτημένη πρόσβαση στο κοινόχρηστο δίκτυο καθώς και για να καθορίσουν σωστή απομόνωση του δικτύου.
Διαχείριση προνομιούχων λογαριασμών	Τα δίκτυα που επιτρέπουν την ανοιχτή ανάπτυξη και δοκιμή περιεχομένου Web όπως επίσης επιτρέπουν στους χρήστες να δημιουργήσουν τους δικούς τους εξυπηρετητές ιστού στο επιχειρηματικό δίκτυο, ενδέχεται να είναι ιδιαίτερα ευάλωτοι εάν τα συστήματα και οι διακομιστές Web δεν είναι σωστά ασφαλισμένοι για να περιορίσουν τη χρήση ενός προνομιούχου λογαριασμού και την πρόσβαση στο κοινόχρηστο δίκτυο χωρίς τον έλεγχο ταυτότητας.
Περιορίστε τα δικαιώματα αρχείων και καταλόγων	Απενεργοποιήστε τα δικαιώματα της εκτέλεσης σε καταλόγους μέσα στο webroot. Βεβαιωθείτε ότι υπάρχουν κατάλληλες άδειες πρόσβασης σε καταλόγους που είναι προσβάσιμοι μέσω ενός διακομιστή Web.
Διαχείριση λογαριασμών χρηστών	Βεβαιωθείτε ότι τα δικαιώματα των processes του διακομιστή Web είναι μόνο αυτά που απαιτούνται με το να μην χρησιμοποιείτε ενσωματωμένους λογαριασμούς. Αντιθέτως μπορείτε να δημιουργήσετε συγκεκριμένους λογαριασμούς για να περιορίσετε την περιττή πρόσβαση ή τις επικαλύψεις των δικαιωμάτων σε πολλά συστήματα.

Για την ανίχνευση και τον εντοπισμό των επιθέσεων που πραγματοποιούνται με τον συγκεκριμένο τρόπο-τεχνική προτείνεται να χρησιμοποιείτε την παρακολούθηση αρχείων και processes για να εντοπίζετε πότε γράφονται αρχεία στον διακομιστή Web με μια διαδικασία που δεν είναι η κανονική διαδικασία που ορίζεται για το συγκεκριμένο

διακομιστή Web όπως επίσης και για να εντοπίζετε αρχεία που γράφονται εκτός των κανονικών περιόδων διαχείρισης.

Επιπλέον προτείνεται να χρησιμοποιείτε την παρακολούθηση των processes για τον εντοπισμό των κανονικών processes που εκτελούνται στον διακομιστή Web και για την ανίχνευση των processes που συνήθως δεν εκτελούνται.

4.13 Παραβίαση κοινόχρηστου περιεχομένου

Το περιεχόμενο που είναι αποθηκευμένο σε μονάδες δικτύου ή σε άλλες κοινόχρηστες τοποθεσίες ενδέχεται να παραβιαστεί προσθέτοντας οι επιτιθέμενοι κακόβουλα προγράμματα, Scripts ή εκμεταλλευόμενο κώδικα μέσα σε έγκυρα αρχεία. Μόλις ένας χρήστης ανοίξει το κοινόχρηστο περιεχόμενό του, το κακόβουλο τμήμα που εμπεριέχεται μέσα στο αρχείο αυτό μπορεί να εκτελεστεί για να εκτελέσει τον κώδικα του επιτιθέμενου σε ένα απομακρυσμένο σύστημα. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν το παραβιασμένο αυτό κοινόχρηστο περιεχόμενο για να μετακινηθούν πλευρικά σε ένα δίκτυο με Windows Domain.

Το pivot κοινόχρηστου καταλόγου είναι μια παραλλαγή αυτής της τεχνικής όπου χρησιμοποιεί αρκετές άλλες τεχνικές για τη διάδοση κακόβουλου λογισμικού όταν οι χρήστες έχουν πρόσβαση σε ένα κοινόχρηστο κατάλογο μέσω δικτύου. Η τεχνική αυτή χρησιμοποιεί την τροποποίηση συντομεύσεων των καταλόγων μέσω των αρχείων .LNK που χρησιμοποιούν το Masquerading(Τεχνική Μασκαρέματος) για να μοιάζουν με τους πραγματικούς καταλόγους, οι οποίοι είναι κρυμμένοι μέσω κρυφών αρχείων και καταλόγων. Οι κακόβουλοι .LNK-based κατάλογοι διαθέτουν μια ενσωματωμένη εντολή η οποία εκτελεί το κρυφό αρχείο κακόβουλου λογισμικού μέσα στον κατάλογο και, στη συνέχεια, ανοίγει τον πραγματικό κατάλογο που θέλετε, έτσι ώστε να εμφανίζεται η αναμενόμενη ενέργεια στον χρήστη. Όταν η συγκεκριμένη τεχνική χρησιμοποιείται με τους συχνά χρησιμοποιούμενους δικτυακούς καταλόγους, μπορεί να έχει ως αποτέλεσμα συχνές παραβιάσεις και ευρεία πρόσβαση σε συστήματα και ενδεχομένως σε νέους και υψηλότερα προνομιούχους λογαριασμούς.

Οι επιτιθέμενοι μπορούν επίσης να θέσουν σε κίνδυνο τους κοινόχρηστους καταλόγους του δικτύου μέσω δυαδικών μολύνσεων, προσαρτώντας ή προσθέτοντας τον κώδικα τους στο υγιή δυαδικό ενός κοινόχρηστου καταλόγου του δικτύου. Το κακόβουλο λογισμικό μπορεί να τροποποιήσει το πραγματικό σημείο εισόδου (OEP) του υγιούς δυαδικού κώδικα για να βεβαιωθεί ότι εκτελείται πριν από τον νόμιμο κώδικα. Η μόλυνση αυτή θα μπορούσε να συνεχίσει να εξαπλώνεται μέσω του πρόσφατα μολυσμένου αρχείου όταν εκτελείται από ένα απομακρυσμένο σύστημα. Αυτές οι μολύνσεις μπορούν να στοχεύσουν τόσο σε δυαδικές όσο και σε μη δυαδικές μορφές που τελειώνουν με επεκτάσεις συμπεριλαμβανομένων, αλλά και χωρίς περιορισμό, των .EXE, .DLL, .SCR, .BAT και / ή .VBS.

Οι περιπτώσεις αυτές όπου έχει γίνει χρήση της τεχνικής παραβίασης κοινόχρηστου περιεχομένου από επιτιθέμενους κατά την διάρκεια εκτέλεσης κάποιας επίθεσής τους με σκοπό την επίτευξη εσωτερικής μετακίνησης μέσα σε ένα δίκτυο με Windows Domain είναι αρκετές και συχνά εμφανιζόμενες. Ενδεικτικά παρακάτω αναφέρονται ορισμένα παραδείγματα:

Darkhotel	Το Darkhotel χρησιμοποίησε έναν ιό που διαδίδεται μολύνοντας εκτελέσιμα που είναι αποθηκευμένα σε κοινόχρηστους δίσκους.
H1N1	Το H1N1 έχει λειτουργίες για την αντιγραφή του ίδιου σε δικτυακά κοινόχρηστα μέρη.
Miner-C	Το malware Miner-C αντιγράφει τον εαυτό της στον Public φάκελο των συσκευών NAS (Network Attached Storage) και προσβάλλει τα νέα θύματα που ανοίγουν το αρχείο.
Ursnif	Το Ursnif έχει αντιγράψει τον εαυτό του και έχει μολύνει αρχεία σε δικτυακούς δίσκους για την διάδοση του.

Για την αντιμετώπιση και τη μείωση των επιθέσεων που πραγματοποιούνται μέσω της τεχνικής παραβίασης κοινόχρηστου περιεχομένου από τους επιτιθέμενους προτείνεται να γίνεται εφαρμογή των παρακάτω μεθόδων [1]:

Πρόληψη εκτέλεσης	Προσδιορίστε το δυνητικά κακόβουλο λογισμικό που μπορεί να χρησιμοποιηθεί για να παραβιάσει περιεχόμενο ή να προκύψει από αυτό και να ελέγχετε ή / και να αποκλείσετε τα άγνωστα προγράμματα, χρησιμοποιώντας εργαλεία με δυνατότητα whitelisting, όπως AppLocker ή Πολιτικές Περιορισμού Λογισμικού, όπου χρειάζεται.
Προστασία από Exploit	Χρησιμοποιήστε βοηθητικά προγράμματα που ανιχνεύουν ή μετριάζουν κοινά χαρακτηριστικά που χρησιμοποιούνται στην εκμετάλλευση(Exploitation), όπως το Microsoft Enhanced Mitigation Experience Toolkit (EMET).
Περιορίστε τα δικαιώματα των αρχείων και των καταλόγων	Προστατεύστε τους κοινόχρηστους φακέλους ελαχιστοποιώντας τους χρήστες που έχουν πρόσβαση εγγραφής.

Για την ανίχνευση και τον εντοπισμό των επιθέσεων που πραγματοποιούνται με τον συγκεκριμένο τρόπο-τεχνική προτείνεται να χρησιμοποιείτε Οι διαδικασίες που γράφουν ή αντικαθιστούν πολλά αρχεία σε έναν κοινόχρηστο κατάλογο δικτύου ενδέχεται να είναι ύποπτοι. Παρακολουθήστε διαδικασίες που εκτελούνται από αφαιρούμενα μέσα για κακόβουλη ή μη φυσιολογική δραστηριότητα, όπως συνδέσεις δικτύου λόγω εντολών και ελέγχου και πιθανές τεχνικές ανίχνευσης δικτύου.

Συχνά σάρωση καταλόγων κοινόχρηστου δικτύου για κακόβουλα αρχεία, κρυφά αρχεία, αρχεία .LNK και άλλους τύπους αρχείων που ενδέχεται να μην είναι τυπικοί υπάρχουν σε καταλόγους που χρησιμοποιούνται για την κοινή χρήση συγκεκριμένων τύπων περιεχομένου.

4.14 Λογισμικό τρίτων κατασκευαστών

Οι εφαρμογές τρίτων κατασκευαστών και τα συστήματα ανάπτυξης λογισμικού ενδέχεται να χρησιμοποιούνται εντός του δικτυακού περιβάλλοντος 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 και κώδικα.

Οι επιτιθέμενοι μπορούν να αποκτήσουν πρόσβαση και να χρησιμοποιήσουν third-party συστήματα που είναι εγκατεστημένα σε ένα επιχειρηματικό δίκτυο, όπως συστήματα διαχείρισης, παρακολούθησης και ανάπτυξης εφαρμογών, καθώς και third-party gateways όπως και jump Serves που χρησιμοποιούνται για τη διαχείριση άλλων συστημάτων. Η πρόσβαση σε ένα third-party σύστημα ανάπτυξης λογισμικού σε όλο το φάσμα του δίκτυο ή ολόκληρου του οργανισμού μπορεί να επιτρέψει σε έναν αντίπαλο να έχει απομακρυσμένη εκτέλεση κώδικα σε όλα τα συστήματα που είναι συνδεδεμένα σε ένα τέτοιο σύστημα. Η πρόσβαση μπορεί να χρησιμοποιηθεί για την πλευρική μετάβαση σε άλλα συστήματα, για τη συγκέντρωση πληροφοριών ή για την πρόκληση ενός συγκεκριμένου αποτελέσματος, όπως το άδειασμα των σκληρών δίσκων σε όλα τα τελικά σημεία.

Τα δικαιώματα που απαιτούνται για αυτήν τη δράση ποικίλλουν ανάλογα με τη διαμόρφωση του συστήματος. Τα τοπικά διαπιστευτήρια μπορεί να είναι επαρκή για την άμεση πρόσβαση σε αυτό το third-party σύστημα ή ενδέχεται να απαιτούνται και διαπιστευτήρια συγκεκριμένου Domain. Ωστόσο, το σύστημα ενδέχεται να απαιτήσει την σύνδεση ενός λογαριασμού διαχειριστή ή για να γίνει η επίτευξη του σκοπού του.

Οι περιπτώσεις κατά τις οποίες έχει χρησιμοποιηθεί η τεχνική χρήσης λογισμικού τρίτων κατασκευαστών κατά την διάρκεια εκτέλεσης κάποιας επίθεσής με σκοπό την επίτευξη εσωτερικής μετακίνησης μέσα σε ένα δίκτυο με Windows Domain είναι αρκετές και συχνά εμφανιζόμενες. Ενδεικτικά παρακάτω αναφέρονται δύο αντίστοιχα παραδείγματα χρήσης.

Group απειλών - 1314	Το Group απειλών 1314 χρησιμοποίησε την πλατφόρμα διαχείρισης Altiris στο τελικό σημείο του θύματος, για την επίτευξη πλευρικής κίνησης.
Wiper	Φημολογείται ότι ένα σύστημα διαχείρισης patch για ένα προϊόν προστασίας από ιούς που είναι εγκατεστημένο συνήθως μεταξύ των στοχοθετημένων εταιρειών χρησιμοποιήθηκε για τη διανομή του κακόβουλου λογισμικού Wiper.

Για την αντιμετώπιση και τη μείωση των επιθέσεων που πραγματοποιούνται μέσω της τεχνικής χρήσης λογισμικού τρίτων κατασκευαστών από τους επιτιθέμενους προτείνεται να γίνεται εφαρμογή των παρακάτω μεθόδων [1]:

Διαμόρφωση υπηρεσίας Active Directory	Εξασφαλίστε τη σωστή απομόνωση των συστημάτων καθώς και την πρόσβαση στα κρίσιμα συστήματα του δικτύου σας μέσω της χρήσης του Group Policy.
Έλεγχος ταυτότητας πολλαπλών παραγόντων	Εξασφαλίστε τη σωστή απομόνωση των συστημάτων και της πρόσβασης για τα κρίσιμα συστήματα του δικτύου σας μέσω της χρήσης ελέγχου ταυτότητας πολλαπλών παραγόντων.
Τμηματοποίηση δικτύου	Εξασφαλίστε τη σωστή απομόνωση για τα κρίσιμα συστήματα του δικτύου σας μέσω της χρήσης τείχους προστασίας(Firewalls).

Πολιτικές κωδικού πρόσβασης	Βεβαιωθείτε ότι τα διαπιστευτήρια των λογαριασμών που μπορούν να χρησιμοποιηθούν για την πρόσβαση σε συστήματα ανάπτυξης λογισμικού είναι μοναδικά και δεν χρησιμοποιούνται σε όλο το εταιρικό δίκτυο.
Διαχείριση λογαριασμών με προνόμια	Αποκτήστε πρόσβαση σε συστήματα ανάπτυξης εφαρμογών μόνο σε περιορισμένο αριθμό εξουσιοδοτημένων διαχειριστών.
Απομακρυσμένη αποθήκευση δεδομένων	Εάν το σύστημα ανάπτυξης εφαρμογών μπορεί να ρυθμιστεί ώστε να αναπτύξει μόνο υπογεγραμμένα δυαδικά αρχεία, βεβαιωθείτε ότι τα αξιόπιστα υπογεγραμμένα πιστοποιητικά δεν βρίσκονται μαζί με το σύστημα ανάπτυξης εφαρμογών και αντίθετα βρίσκονται σε ένα άλλο σύστημα στο οποίο δεν είναι δυνατή η απομακρυσμένη πρόσβαση ή σε ποια απομακρυσμένη πρόσβαση είναι σφιχτά ελεγχόμενα.
Ενημέρωση λογισμικού	Να γίνεται τακτικά η εγκατάσταση των Patches και των ενημερωμένων εκδόσεων στα συστήματα ανάπτυξης εφαρμογών και λογισμικού για να αποτρέψετε την πιθανή απομακρυσμένη πρόσβαση μέσω της εκμετάλλευσης με σκοπό την εξέλιξη και την επαύξηση προνομίων .
Διαχείριση λογαριασμών χρηστών	Βεβαιωθείτε ότι όλοι οι λογαριασμοί που χρησιμοποιούνται από τρίτους παρόχους για την πρόσβαση σε third-party συστήματα δεν χρησιμοποιούνται σε όλο το δίκτυο σας ή δεν χρησιμοποιούνται από άλλους τρίτους παρόχους στο ίδιο περιβάλλον. Βεβαιωθείτε ότι υπάρχουν τακτικές αναθεωρήσεις των λογαριασμών που παρέχονται σε αυτά τα συστήματα για να εξακριβωθεί η συνεχιζόμενη επιχειρηματική ανάγκη και να διασφαλιστεί επίσης ότι υπάρχει διακυβέρνηση για να εντοπιστεί η αποδέσμευση της πρόσβασης που δεν απαιτείται πλέον. Τέλος εξασφαλίστε σωστή απομόνωση συστήματος και πρόσβασης για τα κρίσιμα συστήματα του δικτύου μέσω της χρήσης του διαχωρισμού των λογαριασμών με προνόμια.
Εκπαίδευση χρηστών	Καλό είναι να έχετε μια αυστηρή πολιτική έγκρισης για τη χρήση συστημάτων ανάπτυξης λογισμικού και εφαρμογών.

Οι μέθοδοι για την ανίχνευση των επιθέσεων που κάνουν χρήση λογισμικών τρίτων κατασκευαστών διαφέρουν ανάλογα με τον τύπο του λογισμικού ή του third-party συστήματος καθώς και τον τρόπο με τον οποίο χρησιμοποιείται συνήθως.

Η ίδια διαδικασία διερεύνησης μπορεί να εφαρμοστεί και εδώ όπως και σε άλλες δυνητικά κακόβουλες δραστηριότητες όπου ο φορέας διανομής είναι αρχικά άγνωστος αλλά η προκύπτουσα δραστηριότητα ακολουθεί ένα διακριτό πρότυπο. Αναλύστε τα δέντρα εκτέλεσης διεργασιών, τις ιστορικές δραστηριότητες από τις εφαρμογές τρίτων (όπως ποιες μορφές αρχείων γίνονται συνήθως pushed) και τις δραστηριότητες ή τα συμβάντα που προκύπτουν από το αρχείο / δυαδικό / Script που γίνεται pushed στα συστήματα σας.

Συχνά αυτές οι εφαρμογές τρίτων θα έχουν δικά τους Logs που μπορούν να συλλεχθούν και να συσχετιστούν με άλλα δεδομένα από το περιβάλλον. Βεβαιωθείτε ότι τα αρχεία

καταγραφής εφαρμογών τρίτου κατασκευαστή είναι ενσωματωμένα στο σύστημα καταγραφής του οργανισμού σας και ότι τα αρχεία καταγραφής ελέγχονται τακτικά.

Ελέγξτε επίσης τα αρχεία ανάπτυξης λογισμικού και αναζητήστε ύποπτη ή μη εξουσιοδοτημένη δραστηριότητα σε αυτά. Για παράδειγμα, ένα σύστημα που δεν χρησιμοποιείται συνήθως για να κάνει Push το λογισμικό του σε Clients και που ξαφνικά χρησιμοποιείται για μια τέτοια εργασία εκτός μιας γνωστής λειτουργίας διαχειριστή μπορεί να είναι ύποπτο.

Εκτελέστε την ανάπτυξη εφαρμογών σε συγκεκριμένα τακτά χρονικά διαστήματα, ώστε να ξεχωρίζει η δραστηριότητα παράνομης ανάπτυξης. Επιπλέον, παρακολουθήστε τη δραστηριότητα της διαδικασίας που δεν συσχετίζεται με το γνωστό καλό λογισμικό. Τέλος, παρακολουθήστε τη δραστηριότητα σύνδεσης λογαριασμού στο σύστημα ανάπτυξης εφαρμογών.

4.15 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 διοικητικών λειτουργιών. Για παράδειγμα δικτυακά Shares περιλαμβάνουν **C$**, **ADMIN$**, και **IPC$**.

Επιτιθέμενοι μπορούν να χρησιμοποιούν αυτή την τεχνική σε συνδυασμό με έγκυρους λογαριασμούς του συστήματος σε επίπεδο διαχειριστή για να αποκτήσουν απομακρυσμένη πρόσβαση σε ένα δικτυωμένο σύστημα μέσω server message block (SMB) και να αλληλοεπιδρούν κατά αυτό τον τρόπο με συστήματα που χρησιμοποιούν απομακρυσμένα procedure calls (RPCs), μεταφορές αρχείων, και εκτέλεση μεταμορφωμένων δυαδικών αρχείων μέσω απομακρυσμένης εκτέλεσης.

Για παράδειγμα τεχνικές εκτέλεσης που βασίζονται σε αυθεντικοποιημένες συνεδρίες μέσω **SMB/RPC** μπορεί να είναι κάποιο Scheduled Task, μια εκτέλεση ενός Service καθώς και ορισμένα από τα μέσα διαχείρισης των Windows . Οι επιτιθέμενοι μπορούν επίσης να χρησιμοποιήσουν hashes του NTLM για να αποκτήσουν πρόσβαση σε administrator shares σε συστήματα με Pass the Hash και με ορισμένα επίπεδα διαμόρφωσης και επιδιορθώσεων.

Το βοηθητικό πρόγραμμα **Net** των Windows μπορεί να χρησιμοποιηθεί για να συνδεθεί σε Windows Admin Shares σε απομακρυσμένα συστήματα χρησιμοποιώντας **net use** εντολές με έγκυρα διαπιστευτήρια.

Οι περιπτώσεις κατά τις οποίες έχει χρησιμοποιηθεί η τεχνική χρήσης του Windows Admin Shares κατά την διάρκεια εκτέλεσης κάποιας επίθεσής με σκοπό την επίτευξη εσωτερικής μετακίνησης μέσα σε ένα δίκτυο με Windows Domain είναι αρκετές και συχνά εμφανιζόμενες. Ενδεικτικά παρακάτω αναφέρονται ορισμένα παραδείγματα χρήσης των Windows Admin Shares [1].

APT3	Το APT3 θα αντιγράψει τα αρχεία πάνω στα Windows Admin Shares (όπως το ADMIN $) ως μέρος της πλευρικής κίνησης.
APT32	Το APT32 χρησιμοποίησε το **Net** για να χρησιμοποιήσει κρυφά

	δικτυακά Windows Shares με σκοπό να αντιγράψει τα εργαλεία του σε απομακρυσμένα μηχανήματα για εκτέλεση.
BlackEnergy	Το BlackEnergy είχε εκτελέσει ένα plug-in σε κάποιο θύμα για να εξαπλωθεί μέσω του τοπικού δικτύου χρησιμοποιώντας το **PsExec** και την πρόσβαση σε admin shares.
Cobalt Strike	Το Cobalt Strike μπορεί να χρησιμοποιήσει Windows admin shares (C $ και ADMIN $) για να επιτύχει πλευρική κίνηση.
Deep Panda	Το Deep Panda χρησιμοποιεί το **Net.exe** για να συνδεθεί σε Shares του δικτύου χρησιμοποιώντας **net use** εντολές με compromised διαπιστευτήρια.
Duqu	Οι επιτιθέμενοι μπορούν να δώσουν εντολή στο Malware Duqu για να διαδοθεί πλευρικά αντιγράφοντας τον εαυτό του στα Shares που έχει απαριθμήσει και για αυτά που έχει λάβει έγκυρα διαπιστευτήρια (μέσω keylogging ή άλλων μέσων). Στη συνέχεια, ο απομακρυσμένος Host εφόσον είναι μολυσμένος με την χρήση των Compromised διαπιστευτηρίων γίνεται ο προγραμματισμός ενός Task σε απομακρυσμένα συστήματα για να εκτελούν το συγκεκριμένο κακόβουλο πρόγραμμα.
Emotet	Το Emotet εκμεταλλεύεται το Share **Admin$** για πλευρική μετακίνηση όταν ο κωδικός πρόσβασης του τοπικού διαχειριστή έχει γίνει δεχθεί brute force επίθεση.
FIN8	Το FIN8 προσπάθησε να χαρτογραφήσει τα **C$** σε απαριθμημένους Hosts για να ελέγξει το πεδίο των Current διαπιστευτηρίων τους.
Ke3chang	Το Group απειλών Ke3chang είναι γνωστό ότι αντιγράφει αρχεία στα network shares άλλων υπολογιστών για να κινηθεί πλευρικά.
Kwampirs	Το Backdoor Kwampirs αντιγράφει τον εαυτό του μέσω των network shares του δικτύου για να μετακινηθεί πλευρικά σε ένα δίκτυο με Windows Domain.
Lazarus Group	Το κακόβουλο λογισμικό της ομάδας Lazarus SierraAlfa έχει πρόσβαση στο share **ADMIN$** μέσω του SMB για να πραγματοποιήσει πλευρική μετακίνηση.
Net	Η πλευρική μετακίνηση μπορεί να γίνει με το **Net** μέσω **net use** εντολών για την επίτευξη σύνδεσης σε απομακρυσμένα συστήματα.
Net Crawler	Το Net Crawler χρησιμοποιεί Windows admin shares για να δημιουργήσει επικυρωμένες συνεδρίες σε απομακρυσμένα συστήματα μέσω SMB ως μέρος πλευρικής κίνησης.
NotPetya	Το NotPetya μπορεί να χρησιμοποιήσει το **PsExec**, το οποίο αλληλοεπιδρά με το share **ADMIN$** για να εκτελέσει εντολές σε απομακρυσμένα συστήματα.
Olympic	Το Olympic Destroyer χρησιμοποιεί το PsExec για να αλληλοεπιδράσει με το share **ADMIN$** για να εκτελέσει εντολές σε απομακρυσμένα

Destroyer	συστήματα.
Orangeworm	Το Orangeworm έχει αντιγράψει το backdoor του μέσω ανοιχτών network shares, συμπεριλαμβανομένων των **ADMIN$**, **C$WINDOWS**, **D$WINDOWS** και **E$WINDOWS**.
PsExec	Το **PsExec** , ένα εργαλείο που έχει χρησιμοποιηθεί από επιτιθέμενους, γράφει προγράμματα στο **ADMIN$** shares του δικτύου για την εκτέλεση εντολών σε απομακρυσμένα συστήματα.
Regin	Η πλατφόρμα κακόβουλου λογισμικού Regin μπορεί να χρησιμοποιήσει Windows admin shares για να μετακινηθεί πλευρικά.
Shamoon	Το Shamoon αποκτά πρόσβαση σε network shares, ενεργοποιεί την κοινή χρήση στη συσκευής του στόχου, αντιγράφει ένα εκτελέσιμο ωφέλιμο φορτίο στο σύστημα του στόχου και χρησιμοποιεί ένα Scheduled Task για την εκτέλεση του κακόβουλου λογισμικού.
Threat Group-1314	Το Group απειών-1314 χαρτογράφησε δίσκους δικτύου χρησιμοποιώντας **net use**.
Turla	Το Turla χρησιμοποίησε **net use** εντολές για να συνδεθεί με πλευρικά συστήματα μέσα σε ένα δίκτυο.
zwShell	Το zwShell έχει αντιγραφεί μέσω δικτυακών shares για να μετακινηθεί πλευρικά.

Για την αντιμετώπιση και τη μείωση των επιθέσεων που πραγματοποιούνται μέσω της τεχνικής χρήσης των Windows Admin Shares από τους επιτιθέμενους προτείνεται να γίνεται εφαρμογή των παρακάτω μεθόδων:

Πολιτικές κωδικού πρόσβασης	Μην επαναχρησιμοποιείτε τους κωδικούς πρόσβασης του λογαριασμού του τοπικού διαχειριστή σε όλα τα συστήματα. Εξασφαλίστε την πολυπλοκότητα και τη μοναδικότητα του κωδικών πρόσβασης, ώστε να μην μπορούν να διασπαστούν ή να μαντεφτούν.
Διαχείριση λογαριασμών με προνόμια	Καταργήστε την απομακρυσμένη χρήση των διαπιστευτηρίων του τοπικού διαχειριστή για να συνδεθείτε σε συστήματα. Μην επιτρέπετε στους λογαριασμούς των χρηστών του Domain να είναι στην ομάδα των τοπικών διαχειριστών σε πολλαπλά συστήματα.

Όσο αναφορά στην ανίχνευση των επιθέσεων που κάνουν χρήση των Windows Admin Shares μπορείτε να βεβαιωθείτε ότι είναι ενεργοποιημένη και συλλέγεται κεντρικά η σωστή καταγραφή των λογαριασμών που χρησιμοποιούνται για την είσοδο σε συστήματα του δικτύου.

Η καταγραφή των Windows είναι σε θέση να συλλέξει την επιτυχία ή αντίθετα την αποτυχία σύνδεσης για λογαριασμούς που μπορούν να χρησιμοποιηθούν από τους επιτιθέμενους για να μετακινηθούν πλευρικά και αυτά τα Logs μπορούν να συλλεχθούν χρησιμοποιώντας εργαλεία όπως το Windows Event Forwarding.

Επιπλέον προτείνεται να γίνεται παρακολούθηση των Events για κάθε απομακρυσμένη σύνδεση και σχετικής δραστηριότητας SMB για μεταφορά αρχείων καθώς και για κάθε εκτέλεση κάποιας απομακρυσμένης διαδικασίας. Παρακολουθήστε τις ενέργειες των

απομακρυσμένων χρηστών που συνδέονται με administrative shares. Τέλος παρακολουθήστε τη χρήση εργαλείων και εντολών που χρησιμοποιούνται για σύνδεση σε απομακρυσμένα κοινόχρηστα στοιχεία, όπως το **Net**, τη διεπαφή γραμμής εντολών και τις τεχνικές Discovery που θα μπορούσαν να χρησιμοποιηθούν για την εύρεση εξ αποστάσεως προσβάσιμων συστημάτων.

4.16 Εργαλείο Windows Remote Management

Η απομακρυσμένη διαχείριση των Windows (WinRM) ακούει στο όνομα μιας υπηρεσίας των Windows και ενός πρωτοκόλλου που επιτρέπει σε ένα χρήστη να αλληλοεπιδρά με ένα απομακρυσμένο σύστημα (π.χ. μπορείτε να εκτελέστε ένα εκτελέσιμο αρχείο, έχετε τη δυνατότητα να τροποποιήστε το μητρώο του συστήματος καθώς και να τροποποιήσετε τις υπηρεσίες του συστήματος). Μπορεί να καλείται η λειτουργία αυτή με την εντολή **winrm** ή κάνοντας χρήση οποιουδήποτε άλλου αριθμού προγραμμάτων όπως το PowerShell.

Ενδεικτικά αναφέρονται παρακάτω ορισμένες από τις περιπτώσεις κατά τις οποίες έχει χρησιμοποιηθεί η τεχνική χρήσης της απομακρυσμένης διαχείρισης των Windows (WinRM) κατά την διάρκεια εκτέλεσης κάποιας επίθεσης με σκοπό την επίτευξη εσωτερικής μετακίνησης μέσα σε ένα δίκτυο με Windows Domain.

Cobalt Strike	Το Cobalt Strike μπορεί να χρησιμοποιήσει το **WinRM** για να εκτελέσει ένα ωφέλιμο φορτίο(payload) σε ένα απομακρυσμένο μηχάνημα.
Group Απειλών - 3390	Το Group Απειλών 3390 χρησιμοποίησε το **WinRM** για να ενεργοποιήσει την απομακρυσμένη εκτέλεση.

Για την αντιμετώπιση και τη μείωση των επιθέσεων που πραγματοποιούνται μέσω της τεχνικής χρήσης της υπηρεσίας των Windows **WinRM** από τους επιτιθέμενους προτείνεται η εφαρμογή των παρακάτω μεθόδων [1]:

Απενεργοποίηση ή κατάργηση δυνατοτήτων ή προγραμμάτων	Απενεργοποιήστε την υπηρεσία **WinRM**.
Τμηματοποίηση δικτύου	Εάν η υπηρεσία είναι απαραίτητη, κλειδώστε τους κρίσιμους θύλακες με μια ξεχωριστή υποδομή για το **WinRM** και ακολουθήστε τις βέλτιστες πρακτικές για το **WinRM** κάνοντας χρήση τείχους προστασίας για να περιορίσετε την πρόσβαση του **WinRM** και για να επιτρέψετε την επικοινωνία μόνο προς ή από συγκεκριμένες συσκευές.
Διαχείριση λογαριασμών με προνόμια	Εάν η υπηρεσία είναι απαραίτητη, κλειδώστε τους κρίσιμους θύλακες με ξεχωριστούς λογαριασμούς και δικαιώματα αποκλειστικά για την υπηρεσία του **WinRM**.

Όσο αναφορά στην ανίχνευση των επιθέσεων που κάνουν χρήση της υπηρεσίας **WinRM** προτείνεται να παρακολουθείτε τη χρήση του **WinRM** μέσα σε ένα περιβάλλον παρακολουθώντας την εκτέλεση της υπηρεσίας. Αν δεν χρησιμοποιείται κανονικά ή είναι απενεργοποιημένη η συγκεκριμένη υπηρεσία, τότε αυτό μπορεί να αποτελεί ένδειξη

ύποπτης συμπεριφοράς. Επιπλέον προτείνεται να παρακολουθείτε τα processes που δημιουργήθηκαν και τις ενέργειες που έγιναν από την υπηρεσία **WinRM** ή από ένα Script που επικαλείται το **WinRM** για να το συσχετίσετε με άλλα σχετικά γεγονότα.

5 Ανίχνευση και τρόποι προστασίας κατά της εσωτερικής μετακίνησης

Σε αυτή την ενότητα 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. Είναι αρκετά σημαντικό να υπολογιστεί ότι μία επίθεση με επαρκή χρόνο και ορισμένες πηγές θα είναι τελικά επιτυχής. Είναι επίσης σημαντικό να σημειωθεί ότι οι παραβιάσεις πρέπει να εντοπίζονται όσο το δυνατόν συντομότερα και να εφαρμόζονται εσωτερικοί έλεγχοι ασφαλείας για τη μείωση των ζημιών που προκαλούνται από έναν επιτιθέμενο μετά την παραβίαση. Δίκτυα με ισχυρή προστασία των συνόρων τους, αλλά καμία εσωτερική ασφάλεια δίνει στους επιτιθέμενους τη δυνατότητα να διασχίσουν το δίκτυο μόλις αποκτήσουν αρχική πρόσβαση σε αυτό. Οι πιθανότητες επίτευξης των στόχων τους μπορούν να αυξηθούν σε τέτοιο βαθμό που να είναι σε θέση να διατηρήσουν μια μόνιμη θέση στο δίκτυο. Δείτε παρακάτω ορισμένες τακτικές για την ανίχνευση της εσωτερικής μετακίνησης ενός επιτιθέμενου σε ένα δίκτυο με windows domain [6].

- **Αναγνώριση**

Πολλοί επιτιθέμενοι χρησιμοποιούν κάποιο RAT (εργαλείο 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.

- **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.

- **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. Οι τακτικές κοινωνικής μηχανικής όπως οι επιθέσεις 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 λίστα 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.

- **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.

Παρακάτω δείτε ορισμένες τεχνικές και τρόπους που μπορούν να εφαρμοστούν με σκοπό να κερδίσουν χρόνο οι αμυνόμενοι και να διευκολυνθούν στην διαδικασία ανίχνευσης απόπειρας εσωτερικής μετακίνησης ενός επιτιθέμενου.

5.1 Ανάπτυξη ορθών πρακτικών επαλήθευσης ταυτότητας

Ο έλεγχος ταυτότητας πρέπει να είναι εύκολος για τον χρήστη, αλλά και ταυτόχρονα να δυσκολεύει τον επιτιθέμενο να αποκτήσει πρόσβαση. Για παράδειγμα, δεν πρέπει να γίνεται χρήση των ίδιων κωδικών πρόσβασης σε διαφορετικά συστήματα και εξέταση της χρήσης των διαχειριστικών κωδικών πρόσβασης εντός του δίκτυο. Με αυτό τον τρόπο θα περιοριστεί ο αριθμός των χρηστών που αποθηκεύουν διαπιστευτήρια σε απλό κείμενο. Οι περιορισμοί σύνδεσης (όπως αποκλεισμός κωδικού πρόσβασης και περιορισμός χρήσης) μειώνουν τις πιθανότητες ενός εισβολέα που διατηρεί πρόσβαση 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 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 χρήση εναλλακτικών τεχνικών μεθόδων ελέγχου ταυτότητας, όπως βιομετρικά στοιχεία, συνδέσεις εισόδου μιας χρήσης και έξυπνες κάρτες. Συνοψίζοντας προτείνεται να ακολουθείτε τις οδηγίες του κωδικού πρόσβασης που δόθηκαν παραπάνω και μην επαναχρησιμοποιήσετε κωδικούς πρόσβασης για διαφορετικά συστήματα [6].

- 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 για λογαριασμούς υψηλού κινδύνου.
- Όπου είναι δυνατόν, χρησιμοποιήστε εναλλακτικές μεθόδους ελέγχου ταυτότητας με κωδικούς πρόσβασης.

5.2 Προστασία κωδικών πρόσβασης

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 σε ένα σύστημα. 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 ίδια τη συσκευή. Οι συσκευές που υποστηρίζουν αποθήκευση διαπιστευτηρίων μέσω υλικού 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 [6]:

- Δεν πρέπει να γίνεται αποθήκευση κωδικών πρόσβασης σε απλό κείμενο καθώς και να διασφαλίζεται ότι τα hashes των κωδικών πρόσβασης αποθηκεύονται σε προστατευμένες περιοχές.
- Προτείνεται να γίνεται χρήση συσκευών με συγκεκριμένο αποθηκευτικό χώρο αποθήκευσης διαπιστευτηρίων υλικού, όπου είναι δυνατόν. Χρησιμοποιήστε τα

διαπιστευτήρια εργασίας μόνο σε συσκευές και υπηρεσίες που έχουν εγκριθεί για χρήση από την εργασία σας.

5.3 Προστασία των λογαριασμών με υψηλά προνόμια

Οι λογαριασμοί διαχείρισης σε τοπικό αλλά και σε επίπεδο τομέα - με πρόσβαση στα περισσότερα συστήματα και δεδομένα - είναι πολύ ισχυρά εργαλεία σε ένα δίκτυο. Η χρήση τους θα πρέπει να ελέγχεται αυστηρά και να κλειδώνεται με κατάλληλους μεθόδους. Οι διαχειριστές πρέπει να χρησιμοποιούν ξεχωριστούς λογαριασμούς. ένα για την καθημερινή επιχειρησιακή χρήση (όπως απλή 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 μόλυνσης μια 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 επαυξημένα δικαιώματα.

Συνοψίζοντας:

- Θα πρέπει να γίνεται χρήση ξεχωριστών συσκευών για κανονικούς λογαριασμούς και για λογαριασμούς διαχειριστών, αν αυτό είναι δυνατόν.
- Οι διαχειριστές θα πρέπει να χρησιμοποιούν έναν κανονικό λογαριασμό για κανονικές δραστηριότητες χρήστη και έναν ξεχωριστό λογαριασμό διαχειριστή μόνο για τις δραστηριότητες που απαιτούν δικαιώματα διαχειριστή.

5.4 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 αυτοί οι λογαριασμοί έχουν πρόσβαση μόνο σε συγκεκριμένες δυνατότητες που απαιτούν υψηλά προνόμια, και όχι σε όλες. Λογαριασμοί με πλήρη δικαιώματα σε ένα δίκτυο (όπως ένας διαχειριστής τομέα ή λογαριασμός διαχειριστή σύννεφου) δεν πρέπει κανονικά να χρησιμοποιούνται. Ενώ απαιτούνται για ορισμένες μόνο ενέργειες (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. Συνοψίζοντας:

- Προτείνεται η χρήση ενός μοντέλου κλιμάκωσης για διαχειριστικούς λογαριασμούς, ώστε να μην έχουν καμία περιττή πρόσβαση ή προνόμια.
- Προτείνεται χρήση λογαριασμών με πλήρη δικαιώματα σε μια επιχείρηση όταν είναι απολύτως απαραίτητο και να γίνεται εξέταση της χρήσης των δικαιωμάτων τους με βάση το χρόνο για να περιορίζεται περαιτέρω η χρήση τους.
- Να γίνεται αξιολόγηση των συσκευών, των υπηρεσιών και των χρηστών υψηλού κινδύνου για να ελαχιστοποιήσετε τις προσβάσεις τους.

5.5 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 οι συσκευές που είναι σε ζεύγη θα ενημερώνονται σε διαφορετικές χρονικές στιγμές για να διατηρηθεί ο πλεονασμός. Τα τερματικά των χρηστών σε ένα δίκτυο πρέπει να ρυθμιστούν με ασφάλεια. Εάν είναι δυνατόν, οι εφαρμογές θα πρέπει να κατατεθούν σε 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. Η λίστα των εγκεκριμένων συνδέσεων θα πρέπει να αναθεωρείται τακτικά για να καταργούνται όσες δεν χρειάζονται πλέον. Πρέπει επίσης 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 [6].

Συνοψίζοντας:

- Προτείνεται η εφαρμογή των ενημερώσεων λογισμικού σε όλες τις συσκευές μόλις κυκλοφορήσουν και χρήση αυτοματοποιημένων ενημερώσεων όπου είναι δυνατόν.
- Προτείνεται να γίνεται εφαρμογή χρήσης συγκειμένων μόνο εφαρμογών όπως και να γίνεται ενεργοποίηση των τοπικών τειχών προστασίας στους κεντρικούς υπολογιστές.
- Προτείνεται η χρήση ασφαλούς μηχανισμού εκκίνησης, αν είναι διαθέσιμος.

5.6 Διαχωρισμός δικτύου

Ο διαχωρισμός του δικτύου περιλαμβάνει τη διάσπαση ενός δικτύου σε διάφορα τμήματα του. Αυτό αυξάνει σημαντικά τη δυσκολία ενός εισβολέα να επιτύχει το στόχο του στο μέσα στο δίκτυο, καθώς το σημείο εισόδου του ενδέχεται να μην έχει καμία επικοινωνία με το σύστημα του στόχου του. 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 επιτρέπεται στους χρήστες να έχουν πρόσβαση σε ένα μονάχα 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. Συνοψίζοντας προτείνεται να εφαρμόζεται διαχωρισμός μέσα σε ένα δίκτυο, να γίνεται ομαδοποίηση και απομόνωση των κρίσιμων δικτυακών

συστημάτων καθώς και να επιτυγχάνεται εφαρμογή κατάλληλων ελέγχων ασφαλείας δικτύου.

5.7 Παρακολούθηση δικτύου

Είναι πολύ σημαντικό να γίνεται παρακολούθηση του δικτύου για τυχόν γεγονότα ασφαλείας που μπορεί να είναι ύποπτα. Καθώς ανακαλύπτονται συνεχώς νέες ευπάθειες, ορισμένοι επιτιθέμενοι θα αποκτήσουν τελικά πρόσβαση, ανεξάρτητα από το πόσο καλά προστατεύεται το δίκτυό. Μόλις αυτό συμβεί, η παρακολούθηση του δικτύου είναι ο μόνος τρόπος για να εντοπιστεί μια παραβίαση και, στη συνέχεια, να παρθούν αντίμετρα. Η βάση της παρακολούθησης είναι η καταγραφή και η αποθήκευση αυτών των αρχείων καταγραφής. 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 δίκτυο και να προειδοποιήσει τους υπεύθυνους διαχείρισης του δικτύου. Θα πρέπει επίσης 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 κίνησης και χρήσης. Οι επιτιθέμενοι συνήθως προσπαθούν να συνδυαστούν με τη συνήθη κυκλοφορία του 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 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. Συνοψίζοντας:

- Προτείνεται η ενεργοποίηση των λειτουργιών καταγραφής και ελέγχου στα συστήματά και η χρήση αυτών για να ανιχνεύεται ασυνήθιστη δραστηριότητα.
- Να γίνεται έλεγχος και καταγραφή όλων των συσκευών που μπορούν να συνδεθούν στο δίκτυό και κατανόηση των στοιχείων υψηλής αξίας.
- Χρειάζεται να υπάρχει καλή κατανόηση και εξοικείωση με το δίκτυο για το πώς χρησιμοποιείται συνήθως.

5.8 Εξέταση χρήσης honeypots

Τα honeypots είναι συστήματα ή εφαρμογές ή αρχεία που δημιουργούνται με σκοπό να απορροφούν την επίθεση. Η υλοποίηση των honeypots, που έχουν εγκατασταθεί εσωτερικά σε ένα δίκτυο ως στόχος για πραγματικά συστήματα, μπορούν να αποτελέσουν πολύτιμα εργαλεία για την ανίχνευση μιας εισβολής μέσα σε ένα δίξτυο. 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 νόμιμοι 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. Για παράδειγμα, θα μπορούσαν να αξιοποιηθούν και να χρησιμοποιηθούν ως πλατφόρμα για την απορρόφηση επιθέσεων σε νόμιμα συστήματα μέσα σε ένα στο δίκτυο κατά την τελική μετακίνηση. Για τους λόγους αυτούς, τα honeypots θα πρέπει να χρησιμοποιούνται μόνο αν έχει γίνει αξιολόγηση στον αντίκτυπο της λανθασμένης εφαρμογής. Να σημειωθεί εδώ ότι η χρήση ενός honeypot μέσα στο δίκτυο, προϋποθέτει ότι υπάρχει η εξειδίκευση και η τεχνογνωσία για να επιτευχθεί ορθά και η κατανόηση των κινδύνων που συνεπάγεται αυτό.

6 Κυνήγι απειλών εσωτερικής μετακίνησης μέσω παρακολούθησης συγκεκριμένων εργαλείων

Είναι σπάνιο για τους επιτιθέμενους ενώ έχουν αποκτήσει αρχική πρόσβαση σε ένα δίκτυο να κατευθύνονται κατευθείαν σε ένα μόνο σύστημα για να πάρουν αυτό που χρειάζονται. Οι επιτιθέμενοι δεν θα χτυπήσουν μόνο ένα σημείο στο δίκτυο το οποίο θα περιέχει όλα τα δεδομένα που προσπαθούν να τα κλέψουν. Συνήθως μετακινούνται εσωτερικά από σύστημα σε σύστημα για να συγκεντρώσουν τις πληροφορίες που χρειάζονται. Για να μετακινούνται ελεύθερα χωρίς να προσελκύουν μεγάλη προσοχή, οι επιτιθέμενοι συχνά χρησιμοποιούν αξιόπιστο λογισμικό που μπορεί φαίνεται φυσιολογικό σε ένα περιβάλλον. Ένα από τα αγαπημένα εργαλεία των επιτιθέμενων είναι το PsExec, το οποίο χρησιμοποιούταν από πολλούς διαχειριστές πληροφορικής παλιότερα. Στη συγκεκριμένη 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) όπως και άλλα παρόμοια εργαλεία για να μετακινηθούν εσωτερικά μεταξύ των τερματικών στο δίκτυό.

6.1 PsExec

Το PsExec είναι ένα βοηθητικό πρόγραμμα διαχείρισης συστήματος της σουίτας Sysinternals που μπορεί να εκτελέσει προγράμματα σε απομακρυσμένους υπολογιστές Windows. Το εργαλείο είναι ένα ελαφρύ, αυτόνομο βοηθητικό πρόγραμμα που μπορεί να παρέχει διαδραστική πρόσβαση στα προγράμματα που εκτελούνται εξ’ αποστάσεως. Παρόμοια λειτουργικότητα είναι διαθέσιμη χρησιμοποιώντας πράγματα όπως το PowerShell Remoting σε νεότερες εκδόσεις των Windows, ωστόσο η ευελιξία και η ευκολία χρήσης του PsExec το καθιστούν αγαπημένο για τους εισβολείς. Τα κοινά πακέτα εκμετάλλευσης όπως Cobalt Strike και Metasploit παρέχουν το καθένα δυνατότητες τύπου PsExec. Υπάρχει επίσης ένας αριθμός παραγόντων απειλών που είναι γνωστό ότι χρησιμοποιούν είτε την επίσημη έκδοση του εργαλείου, η οποία είναι υπογεγραμμένη από τη Microsoft, είτε μια προσαρμοσμένη παραλλαγή. Οι επιτιθέμενοι χρησιμοποιούν συχνά το Sysinternals PsExec για να εκτελέσουν πλευρική κίνηση. Ας υποθέσουμε ότι ένας

εισβολέας έχει θέση σε ένα περιβάλλον και έχει επίσης παραβιάσει διαπιστευτήρια με δικαιώματα τοπικού διαχειριστή συστήματος σε έναν κεντρικό υπολογιστή. Ο εισβολέας μπορεί να εκτελέσει το PsExec στον παραβιασμένο κεντρικό υπολογιστή και να εκτελέσει εντολές απομακρυσμένα σε έναν άλλο κεντρικό υπολογιστή [5].

Το τυπικό μοτίβο δραστηριότητας PsExec έχει ως εξής:

(1) Πραγματοποιήστε έλεγχο ταυτότητας στον κεντρικό υπολογιστή προορισμού μέσω SMB χρησιμοποιώντας είτε την τρέχουσα περίοδο σύνδεσης είτε τα παρεχόμενα διαπιστευτήρια.

(2) Αντιγράψτε το εκτελέσιμο αρχείο υπηρεσίας PSEXECSVC.EXE στη διαδρομή <target_host>admin$system32.

(3) Συνδεθείτε με τη διαχείριση ελέγχου υπηρεσιών στον κεντρικό υπολογιστή προορισμού για εγκατάσταση και εκκίνηση του PSEXESVC.

(4) Διευκολύνετε την είσοδο/έξοδο μέσω του ονομαζόμενου σωλήνα .pipepsexesvc.

(5) (Μετά την ολοκλήρωση) Απεγκαταστήστε την υπηρεσία και διαγράψτε το εκτελέσιμο αρχείο υπηρεσίας.

Οι περισσότεροι δείκτες της δραστηριότητας του PSExec είναι διαθέσιμοι από εργαλεία τηλεμετρίας που βασίζονται σε κεντρικό υπολογιστή. Σε αυτήν την περίπτωση, τα αναγνωριστικά συμβάντων θα ληφθούν από τα αρχεία καταγραφής συστήματος/ασφάλειας Sysmon και Windows, αλλά υπάρχουν ανάλογα διαθέσιμα σε άλλες δημοφιλείς λύσεις παρακολούθησης. Η εκτέλεση του PsExec περιλαμβάνει πάντα τη δημιουργία απομακρυσμένης υπηρεσίας. Τα Windows για αυτήν τη δραστηριότητα έχουν το Event Code: ***7045*** και το προεπιλεγμένο όνομά της είναι PSEXESVC. Το αντίστοιχο συμβάν δημιουργίας της υπηρεσίας που δημιουργήθηκε από το παράδειγμα χρήσης.

Επιπλέον, για την εκτέλεση του PsExec, οι χρήστες πρέπει να αποδεχτούν την Άδεια Χρήσης του. Αυτό δημιουργεί μια αλλαγή μητρώου στον κεντρικό υπολογιστή προέλευσης. (Πολλά περιβάλλοντα ενδέχεται να μην καταγράφουν όλες τις αλλαγές μητρώου, αλλά αυτό μπορεί να είναι χρήσιμος δείκτης κατά τη διερεύνηση.) Το κλειδί μητρώου είναι: HKEY_CURRENT_USERsoftwaresysinternalspsexeceulaaccepted.

Ακόμη, ο προεπιλεγμένος σωλήνας με το όνομα PsExec που χρησιμοποιείται για την επικοινωνία είναι .pipepsexesvc. Η MENASEC Applied Security Research έχει επίσης σημειώσει ότι οι σωλήνες με μοναδική ονομασία δημιουργούνται στον κεντρικό υπολογιστή-στόχο για κάθε χρήση. Αυτοί οι σωλήνες ονομάζονται σύμφωνα με τη μορφή <psexecsvc_name>-<machine_name>-<5_random_digits>-<stdin|stdout|stderr>4. Το συμβάν ασφάλειας των Windows Event Code: ***5145*** καταγράφεται όταν γίνεται πρόσβαση σε αυτούς τους αγωγούς.

Η βασική ανίχνευση της δραστηριότητας PsExec μπορεί να επιτευχθεί με παρακολούθηση για δημιουργία απομακρυσμένης υπηρεσίας χρησιμοποιώντας το γνωστό όνομα «PSEXESVC»: ***EventCode==7045 AND (“Service Name” CONTAINS “PSEXESVC”)***

Εάν είναι διαθέσιμη η τηλεμετρία, η βέλτιστη λύση είναι η παρακολούθηση των σωλήνων με μοναδική ονομασία που δημιουργούνται ως μέρος της διαδικασίας 4:

EventCode==5145 AND ("Relative Target Name" CONTAINS ("*-stdin" OR "*-stdout" OR "*-stderr"))

Επιπλέον, οι αλλαγές στο κλειδί μητρώου EULA θα μπορούσαν να είναι μια χρήσιμη προσθήκη σε οποιοδήποτε από τα παραπάνω: ***EventCode==13 AND ("TargetObject" CONTAINS "*softwaresysinternalspsexeceulaaccepted")***. Τέλος, το όνομά του σωλήνα ***psexec*** προστέθηκε στο ειδικά διαμορφωμένο αρχείο διαμόρφωσης του sysmon με σκοπό την έγκαιρη ανίχνευση του.

Η σωστή ένταξη στη λίστα επιτρεπόμενων και η βασική γραμμή είναι ζωτικής σημασίας για τον εντοπισμό ανώμαλης και δυνητικά κακόβουλης δραστηριότητας. Το Sysinternals PsExec είναι ένα νόμιμο βοηθητικό πρόγραμμα διαχείρισης συστημάτων και μπορεί να χρησιμοποιηθεί ως τέτοιο καθημερινά σε ένα περιβάλλον. Ορισμένες νόμιμες λύσεις παρακολούθησης, σαρωτές ευπάθειας ή συστήματα διαχείρισης περιουσιακών στοιχείων ενδέχεται επίσης να εμφανίζουν αυτό το μοτίβο δραστηριότητας. Η γνώση των λιστών επιτρεπόμενων και του βασικού προφίλ σας μπορεί να βοηθήσει στη διάκριση μεταξύ κοινής καλοήθους δραστηριότητας και δυνητικά κακόβουλης συμπεριφοράς [5].

6.2 RemCom

Το RemCom είναι ένα βοηθητικό πρόγραμμα ανοιχτού κώδικα, με δυνατότητα αναδιανομής που παρέχει λειτουργίες απομακρυσμένης διαχείρισης. Έχει πετύχει ένα επίπεδο φήμης αφού οι επιτιθέμενοι το χρησιμοποίησαν για να κινηθούν πλευρικά στην επίθεσή τους στην Εθνική Επιτροπή των Δημοκρατικών το 2016. Ωστόσο, περιλαμβάνεται και σε πολλά νόμιμα πακέτα λογισμικού. Από προεπιλογή, το RemCom στέλνει RemComSvc.exe σε έναν απομακρυσμένο υπολογιστή, ο οποίος στη συνέχεια χρησιμοποιεί τον επώνυμο σωλήνα \\.\pipe\remcom_comunication(ορθογραφικά λάθη και όλα) στη θέση του ονομασμένου σωλήνα του PsExec. Επιπλέον, το εσωτερικό όνομα της διεργασίας έχει τιμή από το remcom. Το όνομά του σωλήνα προστέθηκε στο ειδικά διαμορφωμένο αρχείο διαμόρφωσης του sysmon με σκοπό την έγκαιρη ανίχνευση του [5].

6.3 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, το 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 συνήθως paexec. Το όνομά του έχει επίσης προστεθεί στο ειδικά διαμορφωμένο αρχείο διαμόρφωσης του sysmon με σκοπό την έγκαιρη ανίχνευση του [5].

7 Μεθοδολογία επιτιθέμενου

Τα κύρια στάδια της πλευρικής κίνησης είναι τρία. Η αναγνώριση, η συλλογή διαπιστευτηρίων/προνομίων και η απόκτηση πρόσβασης σε άλλους υπολογιστές του δικτύου. Στις παρακάτω ενότητες θα βρείτε μια μικρή περιγραφή για το καθένα από αυτά ξεχωριστά.

7.1 Αναγνώριση

Κατά τη διάρκεια της αναγνώρισης, ο εισβολέας παρατηρεί, εξερευνά και χαρτογραφεί το δίκτυο, τους χρήστες και τις συσκευές του. Αυτός ο χάρτης επιτρέπει στον εισβολέα να κατανοήσει τις συμβάσεις ονομασίας κεντρικού υπολογιστή και τις ιεραρχίες δικτύου, να αναγνωρίσει λειτουργικά συστήματα, να εντοπίσει πιθανά ωφέλιμα φορτία και να αποκτήσει νοημοσύνη για να κάνει ενημερωμένες κινήσεις. Οι φορείς απειλών αναπτύσσουν μια ποικιλία εργαλείων για να μάθουν πού βρίσκονται στο δίκτυο, σε τι μπορούν να έχουν πρόσβαση και ποια τείχη προστασίας ή άλλα αποτρεπτικά μέσα υπάρχουν. Ένας εισβολέας μπορεί να αξιοποιήσει πολλά εξωτερικά προσαρμοσμένα εργαλεία και εργαλεία ανοιχτού κώδικα για σάρωση θυρών, συνδέσεις διακομιστή μεσολάβησης και άλλες τεχνικές, αλλά η χρήση ενσωματωμένων Windows ή εργαλείων υποστήριξης προσφέρει το πλεονέκτημα ότι είναι πιο δύσκολο να εντοπιστεί [8].

Εδώ είναι μερικά από τα ενσωματωμένα εργαλεία που μπορούν να χρησιμοποιηθούν κατά την αναγνώριση [12]:

- Το Netstat εμφανίζει τις τρέχουσες συνδέσεις δικτύου του μηχανήματος. Αυτό μπορεί να χρησιμοποιηθεί για τον εντοπισμό κρίσιμων περιουσιακών στοιχείων ή για την απόκτηση γνώσεων σχετικά με το δίκτυο.
- Το IPConfig/IFConfig παρέχει πρόσβαση στις πληροφορίες διαμόρφωσης δικτύου και τοποθεσίας.
- Η προσωρινή μνήμη ARP δίνει πληροφορίες σχετικά με τη διεύθυνση IP στη φυσική διεύθυνση. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για τη στόχευση μεμονωμένων μηχανημάτων εντός του δικτύου.
- Ο πίνακας Local Routing εμφανίζει τις τρέχουσες διαδρομές επικοινωνίας για τον συνδεδεμένο κεντρικό υπολογιστή.
- Το PowerShell , μια ισχυρή γραμμή εντολών και εργαλείο δέσμης ενεργειών, επιτρέπει τη γρήγορη αναγνώριση συστημάτων δικτύου στα οποία ο τρέχων χρήστης έχει πρόσβαση τοπικού διαχειριστή.

Μόλις ο εισβολέας εντοπίσει κρίσιμες περιοχές για πρόσβαση, το επόμενο βήμα είναι η συλλογή διαπιστευτηρίων σύνδεσης που θα του επιτρέψουν την είσοδο [8].

7.2 Συλλογή διαπιστευτηρίων και κλιμάκωση προνομίων

Για να μετακινηθεί σε ένα δίκτυο, ένας εισβολέας χρειάζεται έγκυρα διαπιστευτήρια σύνδεσης. Ο όρος που χρησιμοποιείται για την παράνομη απόκτηση διαπιστευτηρίων ονομάζεται «ντάμπινγκ διαπιστευτηρίων». Ένας τρόπος για να αποκτήσετε αυτά τα διαπιστευτήρια είναι να εξαπατήσετε τους χρήστες να τα μοιραστούν χρησιμοποιώντας τακτικές κοινωνικής μηχανικής, όπως το typosquatting και οι επιθέσεις phishing. Άλλες κοινές τεχνικές για την κλοπή διαπιστευτηρίων περιλαμβάνουν [12]:

- Το Pass the Hash είναι μια μέθοδος ελέγχου ταυτότητας χωρίς πρόσβαση στον κωδικό πρόσβασης του χρήστη. Αυτή η τεχνική παρακάμπτει τα τυπικά βήματα ελέγχου ταυτότητας καταγράφοντας έγκυρους κατακερματισμούς κωδικών πρόσβασης που αφού πιστοποιηθούν επιτρέπουν στον εισβολέα να εκτελεί ενέργειες σε τοπικά ή απομακρυσμένα συστήματα.
- Το Pass the Ticket είναι ένας τρόπος ελέγχου ταυτότητας χρησιμοποιώντας εισιτήρια Kerberos. Ένας εισβολέας που έχει παραβιάσει έναν ελεγκτή τομέα μπορεί να δημιουργήσει ένα "χρυσό εισιτήριο" της Kerberos εκτός σύνδεσης που παραμένει έγκυρο επ' αόριστον και μπορεί να χρησιμοποιηθεί για την μίμηση οποιουδήποτε λογαριασμού, ακόμη και μετά από επαναφορά κωδικού πρόσβασης.
- Εργαλεία όπως το Mimikatz χρησιμοποιούνται για την κλοπή αποθηκευμένων κωδικών πρόσβασης απλού κειμένου ή πιστοποιητικών ελέγχου ταυτότητας από τη μνήμη ενός παραβιασμένου μηχανήματος. Στη συνέχεια, μπορούν να χρησιμοποιηθούν για έλεγχο ταυτότητας σε άλλα μηχανήματα.
- Εργαλεία καταγραφής πλήκτρων που επιτρέπουν στον εισβολέα να συλλαμβάνει τους κωδικούς πρόσβασης απευθείας όταν ένας ανυποψίαστος χρήστης τους εισάγει μέσω του πληκτρολογίου.

7.3 Απόκτηση Πρόσβασης

Η διαδικασία εκτέλεσης εσωτερικής αναγνώρισης και, στη συνέχεια, παράκαμψης των ελέγχων ασφαλείας για την παραβίαση διαδοχικών κεντρικών υπολογιστών μπορεί να επαναληφθεί έως ότου βρεθούν και εξαχθούν τα δεδομένα ενός στόχου. Και, καθώς οι κυβερνοεπιθέσεις γίνονται πιο εξελιγμένες, συχνά περιέχουν ένα έντονο ανθρώπινο στοιχείο. Αυτό ισχύει ιδιαίτερα για τις πλευρικές κινήσεις, όταν ένας οργανισμός μπορεί να βρεθεί αντιμέτωπος με κινήσεις και αντίστροφες κινήσεις από έναν αντίπαλο. Ωστόσο, η ανθρώπινη συμπεριφορά μπορεί να ανιχνευθεί - και να αναχαιτιστεί - από μια ισχυρή λύση ασφαλείας [12].

8 Χρήση Εργαλείων και Προσομοίωση επίτευξης Εσωτερικής Μετακίνησης

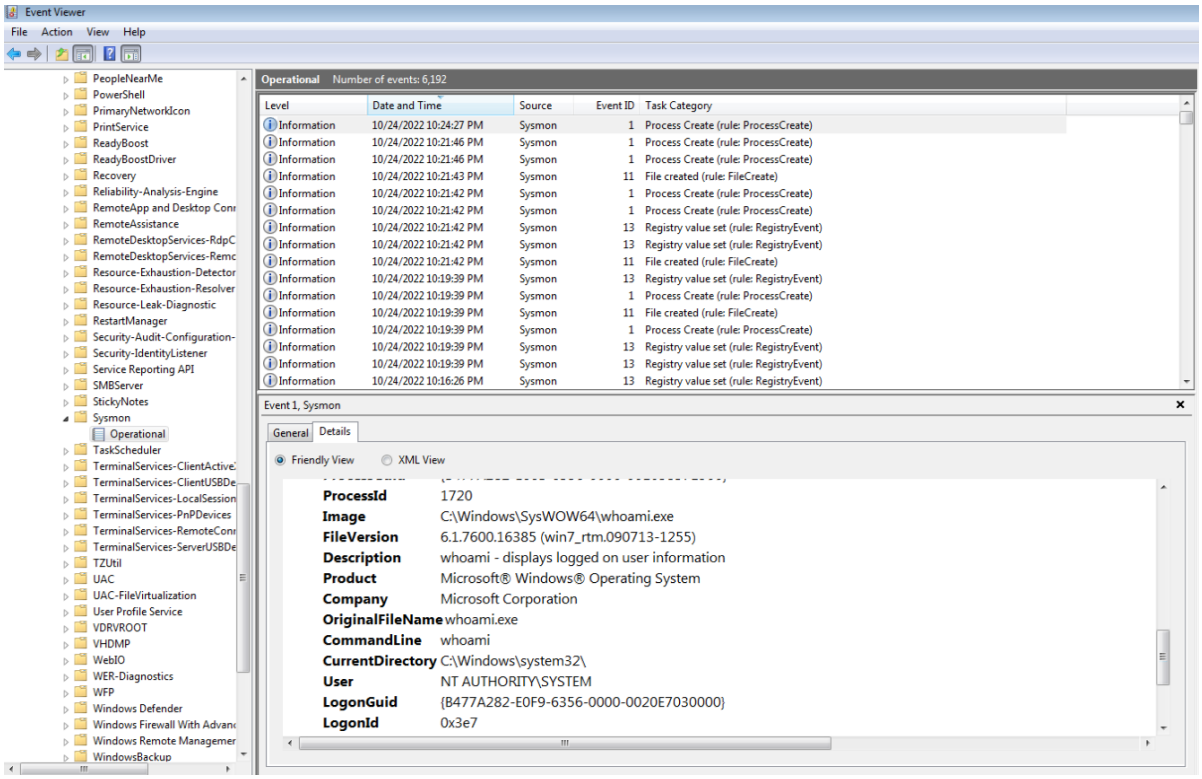
Στην ενότητα αυτή παρουσιάζονται και προσομοιώνονται ορισμένα από τα εργαλεία και τις τακτικές που χρησιμοποιούν οι επιτιθέμενοι προκειμένου να βοηθηθούν οι αμυνόμενοι ενός δικτύου να κατανοήσουν και στη συνέχεια να ενημερώσουν τις δραστηριότητες τους ως προς το κυνήγι απειλών εντός του δίκτυού τους. Οι σύγχρονοι εισβολείς χρησιμοποιούν συχνά επιθέσεις από την πλευρά του πελάτη για να επιτύχουν ένα αρχικό βήμα μέσα σε ένα δίκτυο, αλλά μόλις επιτευχθεί αυτό το βήμα, χρησιμοποιούν συχνά υπάρχοντα ενσωματωμένα εργαλεία και λογαριασμούς για να μετακινηθούν εσωτερικά ή να περιστραφούν σε όλο το δίκτυο των αμυνόμενων. Με την κατανόηση της μεθοδολογίας των επιτιθέμενων καθώς και των στοιχείων που αφήνουν πίσω τους αυτές οι επιθέσεις, οι αμυνόμενοι θα είναι πιο κατάλληλα προετοιμασμένοι για να αναζητήσουν δραστηριότητα επιτιθέμενου και να αναγνωρίσουν αποδεικτικά στοιχεία τέτοιων επιθέσεων όταν συναντηθούν. Αυτή η ενότητα όπως θα δείτε χωρίζεται σε κατηγορίες βάσει μεθοδολογιών και εργαλείων των επιτιθέμενων. Σε καθεμία από αυτές τις κατηγορίες, περιγράφονται μέθοδοι που χρησιμοποιούνται από επιτιθέμενους καθώς και επισημαίνονται δείκτες που μπορούν να χρησιμοποιηθούν για τον εντοπισμό αντίστοιχης τέτοιας δραστηριότητας σε οποιοδήποτε δίκτυο Windows Domain.

8.1 WMI

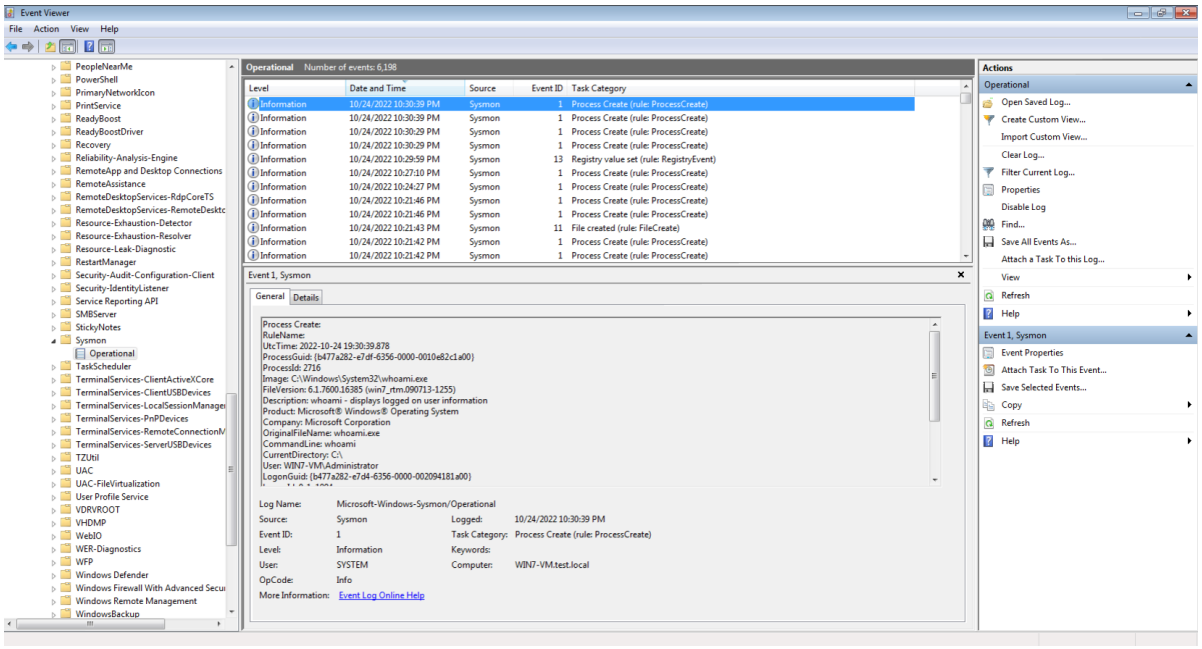
Για άλλη μια φορά να τονίσουμε ότι η χρήση του WMIC απαιτεί την πραγματοποίηση επικυρωμένης πρόσβασης στο σύστημα προορισμού, οπότε χρησιμοποιώντας συμβάντα ελέγχου και συμβάντα σύνδεσης για τον εντοπισμό ασυνήθιστης πρόσβασης στο σύστημα είναι ένας χρήσιμος δείκτης για τον εντοπισμό ύποπτης δραστηριότητας 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 προσαρμοστούν κατάλληλα στο περιβάλλον σας. Μπορείτε να βρείτε το έργο του Matt στο GitHub στη διεύθυνση: https://github.com/mattifestation. Ωστόσο παρακάτω θα δείτε ένα απλό παράδειγμα χρήσης του wmiexec.exe της σουίτας impacket από το σύστημα ενός κακόβουλου χρήστη καθώς και τη καταγραφή των συμβάντων στο σύστημα του αμυνόμενου. Μέσω τέτοιων και άλλων παρόμοιων περιπτώσεων μπορεί να εντοπιστεί εσωτερική μετακίνηση εντός ενός δικτύου Domain (Βλ. ***Εικόνα 17, 18, 19***) [13].

```
┌──(root💀kali)-[~/Downloads/impacket/examples]
└─# wmiexec.py  WIN7-VM/administrator@172.16.10.111
Impacket v0.9.25.dev1+20211027.123255.1dad8f7f - Copyright 2021 SecureAuth Corporation

Password:
[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
win7-vm\administrator

C:\>sS
```

Εικόνα 17 – Εκτέλεση του wmiexec με δυνατότητα εκτέλεσης εντολών σε απομακρυσμένο μηχάνημα Windows 7 του domain κάνοντας χρήση διαπιστευτηρίων τοπικού διαχειριστή



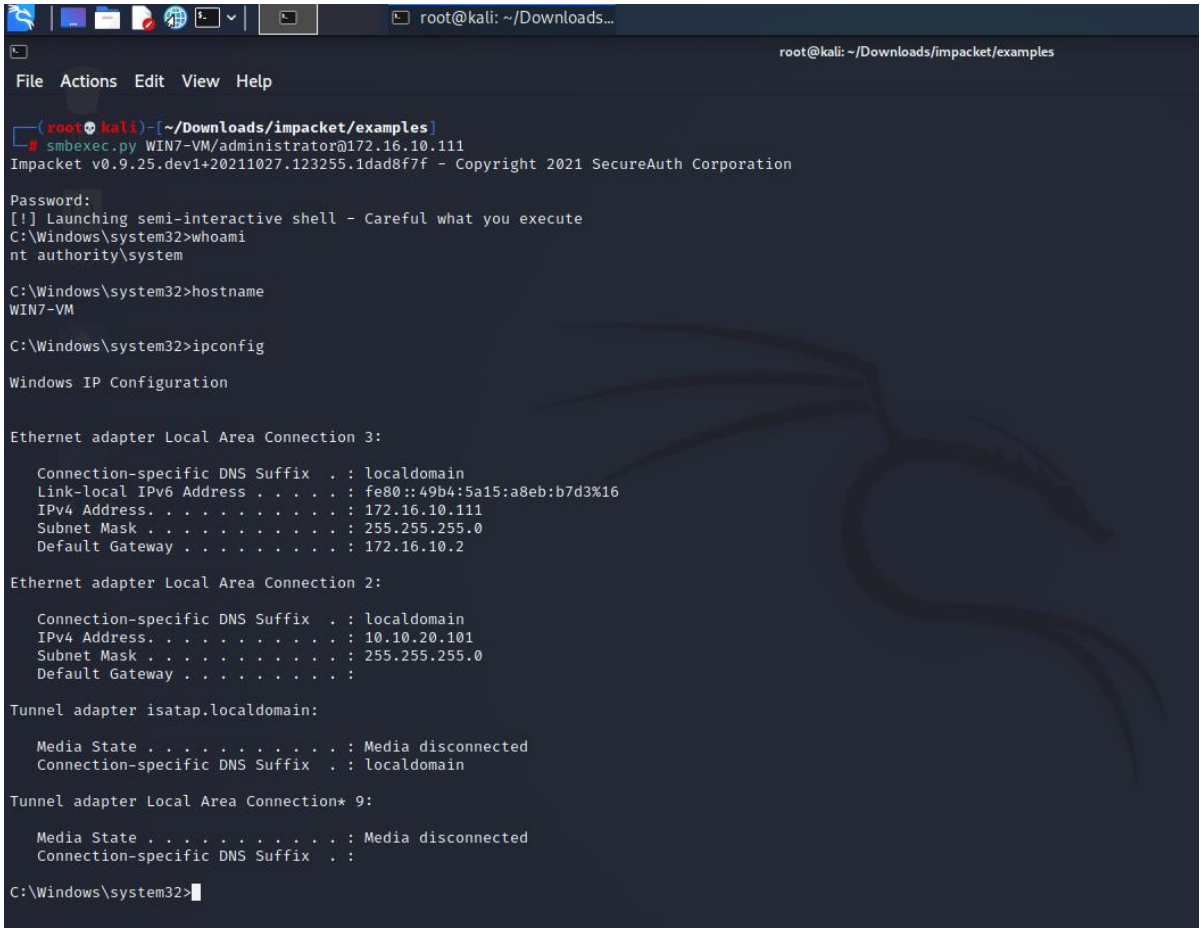
Εικόνα 18 – Καταγραφή απομακρυσμένων εντολών που έτρεξε ο επιτιθέμενος στο μηχάνημα του θύματος μέσω του sysmon



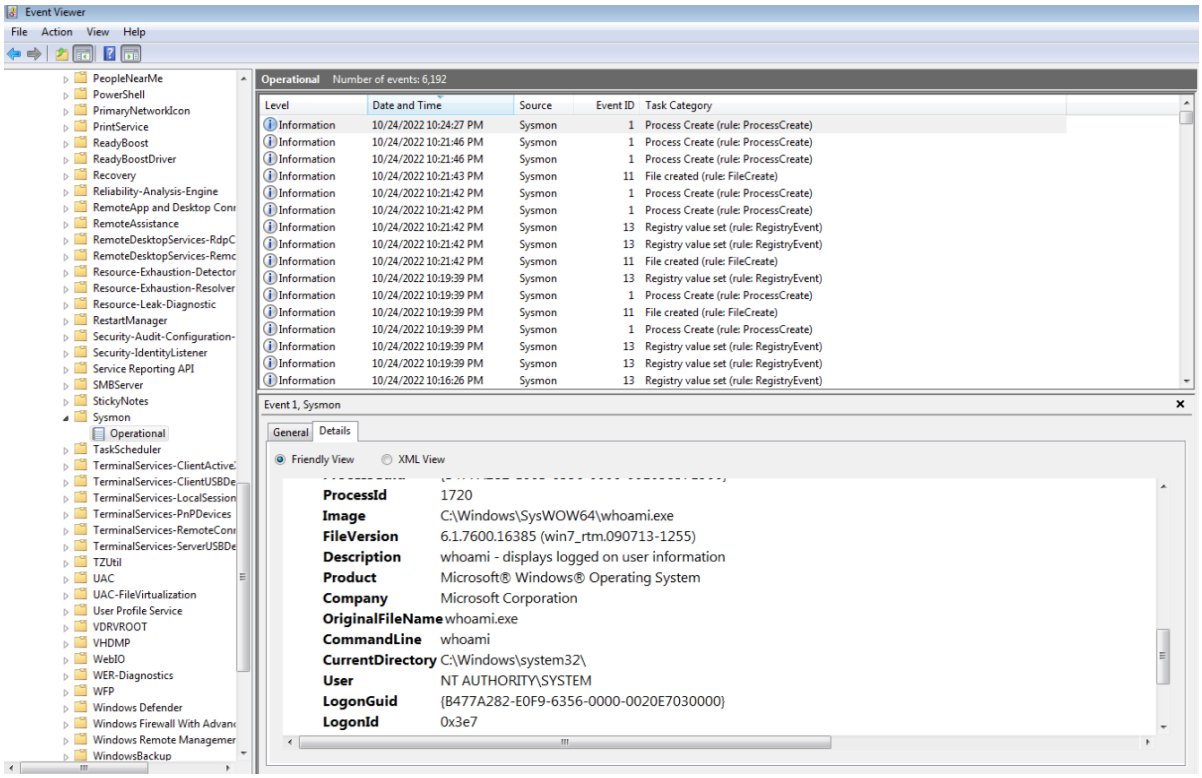
Εικόνα 19 – Καταγραφή απομακρυσμένων εντολών που έτρεξε ο επιτιθέμενος στο μηχάνημα του θύματος μέσω του sysmon

8.2 SMBExec

Η μέθοδος χρήσης του εργαλείου "**`smbexec.py`**" εκμεταλλεύεται τη προεγκατεστημένη λειτουργικότητα των Windows SMB για την εκτέλεση αυθαίρετων εντολών σε ένα απομακρυσμένο σύστημα. Κάνοντας χρήση του συγκεκριμένου εργαλείου δεν απαιτείται να φορτωθεί τίποτα στο απομακρυσμένο σύστημα και επομένως αυτό το καθιστά κάπως λιγότερο θορυβώδης. Σημειώστε ότι η επικοινωνία γίνεται μόνο μέσω της θύρας **`tcp/445`**. Ακολουθεί ένα παράδειγμα χρήσης του **`smbexec.py`** της σουίτας Impacket με τοπικό διαχειριστή συστήματος και κωδικό πρόσβασης απλού κειμένου (Βλ. ***Εικόνα 20, 21***).



Εικόνα 20 – Απομακρυσμένη εκτέλεση εντολών σε μηχάνημα Windows 7 του domain κάνοντας χρήση διαπιστευτηρίων τοπικού διαχειριστή



Εικόνα 21 – Καταγραφή απομακρυσμένων εντολών που έτρεξε ο επιτιθέμενος στο μηχάνημα του θύματος μέσω του sysmon

8.3 Mimikatz (Pass-the-hash)

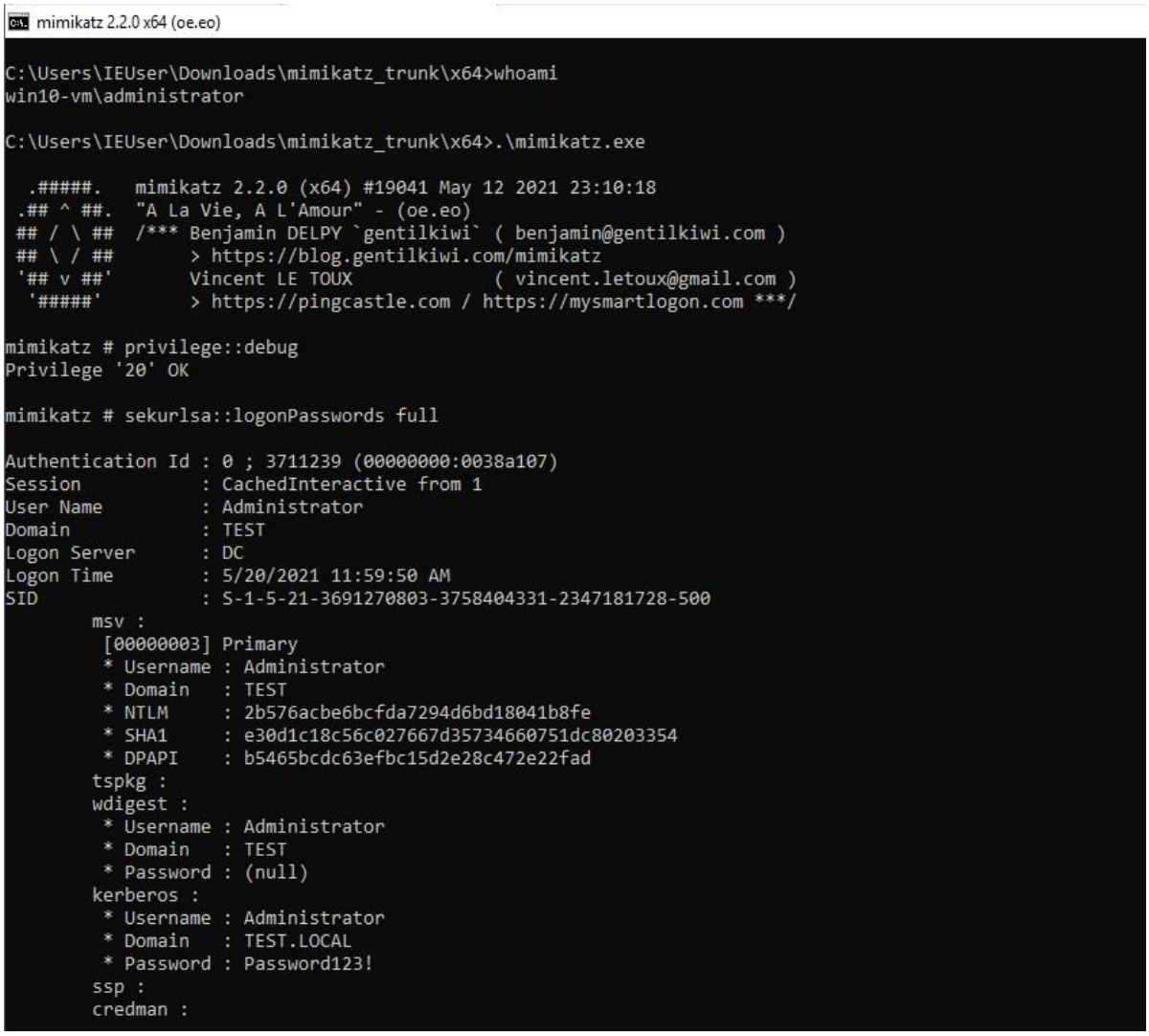
Οι εισβολείς επιδιώκουν συνήθως την ανάκτηση των διαπιστευτηρίων που είναι αποθηκευμένα σε κοινές τοποθεσίες, όπως η διεργασία υποσυστήματος τοπικής αρχής ασφαλείας (LSASS) όπου χρησιμοποιούνται για τον έλεγχο ταυτότητας χρηστών, συνδέσεων και δικαιωμάτων σε συστήματα Windows. Η συγκεκριμένη διεργασία των Windows διατηρεί στη μνήμη τα διαπιστευτήρια (κωδικοποιημένοι κωδικοί πρόσβασης / εισιτήρια) ώστε για τη μεμονωμένη σύνδεση να μην είναι απαραίτητο οι χρήστες να επαναλαμβάνουν τον έλεγχο της ταυτότητας τους συνεχώς.

Εάν οι εισβολείς είναι τυχεροί, θέτουν σε κίνδυνο ένα σύστημα όπου έχουν παραμείνει στη μνήμη του προηγούμενες συνδέσεις από έναν διαχειριστή. Αυτά τα διαπιστευτήρια σύνδεσης μπορούν να ανακτηθούν με το Mimikatz ή παρόμοια εργαλεία ανίχνευσης μνήμης και συγκεκριμένα της διεργασίας LSASS.

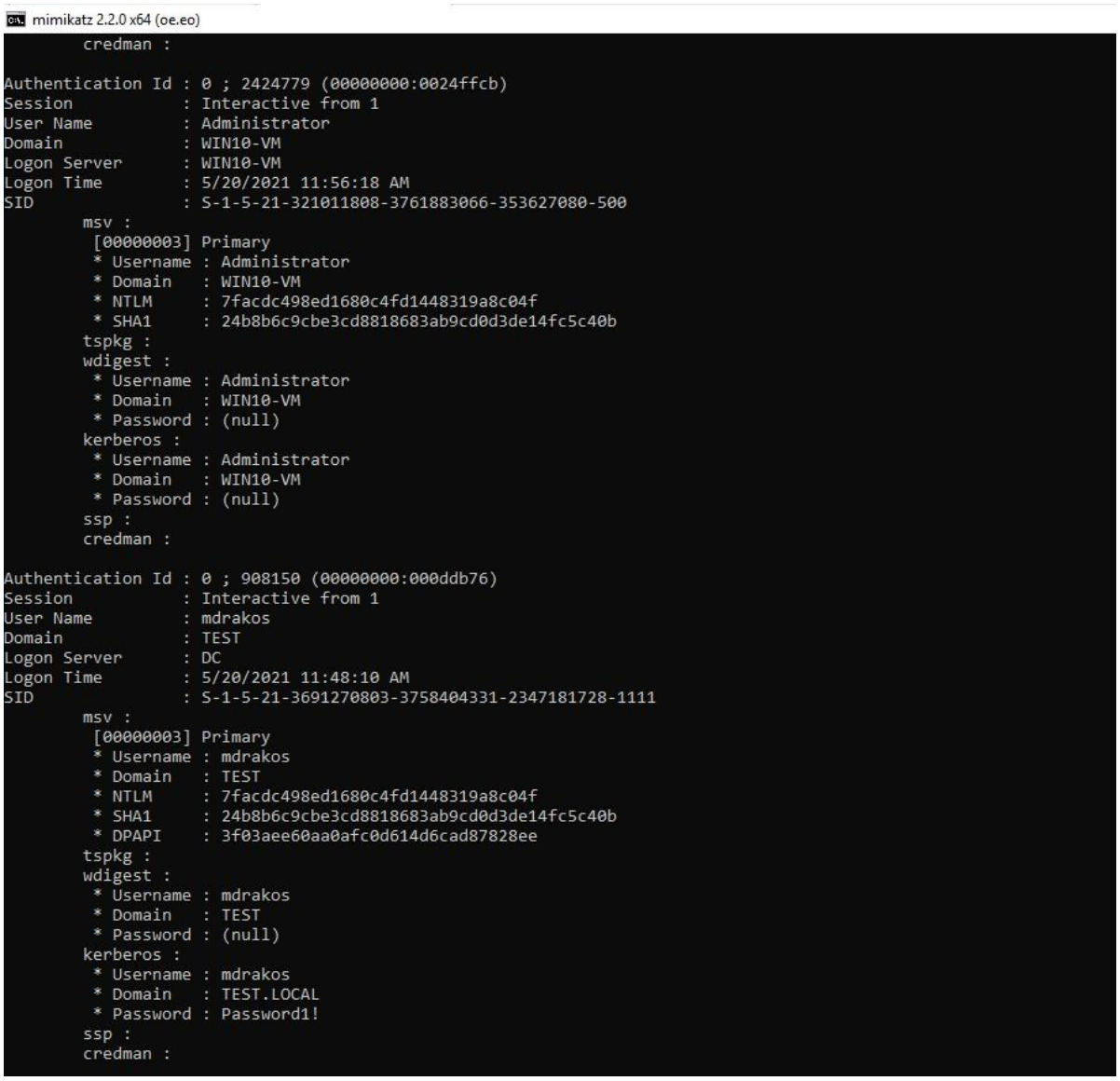
Το Mimikatz είναι ένα εργαλείο το οποίο μπορεί να φανερώσει σε έναν επιτιθέμενο τα διαπιστευτήρια που είναι αποθηκευμένα συνήθως στον περιηγητή καθώς και στο σύστημα του εκάστοτε θύματος. Όταν αποκαλυφθούν τα διαπιστευτήρια του διαχειριστή του τομέα, ο επιτιθέμενος είναι συνήθως μια γραμμή εντολών μακριά από το να πάρει και τον έλεγχο του τομέα. Το Mimikatz όπως και άλλα παρόμοια εργαλεία επιτρέπουν στους παράγοντες απειλής να βρουν και να εξαγάγουν διαπιστευτήρια πιστοποίησης, όπως κατακερματισμούς NTLM και πληροφορίες εισιτηρίων Kerberos από τη μνήμη του πυρήνα ενός τρέχοντος υπολογιστή που χρησιμοποιείται από τη διεργασία LSASS. Το παρακάτω

παράδειγμα δείχνει την ανάκτηση διαπιστευτηρίων χρησιμοποιώντας το Mimikatz από ένα Windows 10 λειτουργικό σύστημα το οποίο ανήκει στο Windows Domain: `test.local`.

Έστω ότι έχουμε αποκτήσει πρόσβαση τοπικού διαχειριστή στο συγκεκριμένο Windows μηχάνημα και τρέχουμε το Mimikatz. Ξεκινάμε με την εντολή: **`privilege::debug`** η οποία θα εκχωρήσει στον τρέχοντα λογαριασμό τα δικαιώματα για διαδικασίες εντοπισμού σφαλμάτων και αμέσως μετά τρέχουμε την εντολή: **`sekurlsa::logonPasswords full`** για να μας εμφανιστεί η λίστα των ενεργών περιόδων σύνδεσης όλων των χρηστών στο εκάστοτε σύστημα (Βλ. ***Εικόνα 22, 23***).



Εικόνα 22 – Προβολή των διαπιστευτηρίων διαχειριστή τομέα μέσω του Mimikatz



Εικόνα 23 – Προβολή των διαπιστευτηρίων χρήστη τομέα μέσω του Mimikatz

Όπως μπορείτε να διακρίνετε μέσω των δύο παραπάνω εικόνων ο επιτιθέμενος έχει πλέον στη διάθεσή του τα διαπιστευτήρια του διαχειριστή του τομέα υπό τη μορφή απλού κειμένου και αυτομάτως του είναι πολύ εύκολο πλέον να μετακινηθεί πλευρικά σε οποιοδήποτε σύστημα του τομέα με επαυξημένα δικαιώματα και προνόμια καθώς επίσης να πάρει τον έλεγχο του κεντρικού συστήματος όλου του τομέα (Domain Controller).

8.4 psexec

Το psexec είναι ένα εργαλείο διαχείρισης που αξιοποιεί το SMB για να εκτελεί εξ' αποστάσεως εντολές σε άλλα συστήματα. Αν και δεν είναι εγγενές εκτελέσιμο αρχείο των Windows, παρέχεται από τη σουίτα της Sysinternals, η οποία ανήκει στη Microsoft. Ως αποτέλεσμα αυτού, πολλοί διαχειριστές το χρησιμοποιούν στο περιβάλλον τους, οπότε η εύρεση του σε ένα δίκτυο μπορεί να μην αποτελεί απαραίτητα ένα ασυνήθιστο συμβάν. Η

εντολή επιτρέπει την απομακρυσμένη εκτέλεση προγραμμάτων μέσω κρυπτογραφημένης σύνδεσης δικτύου, όταν παρέχονται τα απαραίτητα διαπιστευτήρια. Εάν το εκτελέσιμο προς εκτέλεση δεν υπάρχει ήδη στο σύστημα προορισμού, μπορεί να αντιγραφεί από το εργαλείο psexec στον στόχο και στη συνέχεια να εκτελεστεί. Το εργαλείο psexec εκτελείται στη γραμμή εντολών των Windows με την ακόλουθη σύνταξη:

psexec \\ [targetIP] [-d] [-e] [-u user] [-p password] [εντολή]

Όπου το **targetIP** είναι το απομακρυσμένο σύστημα και η εντολή είναι οποιαδήποτε εκτελέσιμη στο σύστημα. Μια κοινή τεχνική είναι να χρησιμοποιήσετε το cmd.exe ως απομακρυσμένη εντολή για να παραχωρήσετε ένα απομακρυσμένο κέλυφος στον εισβολέα. Ο διακόπτης **-c** μπορεί να προστεθεί για να αντιγράψει το εκτελέσιμο στον στόχο πρώτα εάν το επιθυμητό εκτελέσιμο δεν είναι ήδη στο στόχο ή δεν βρίσκεται σε μια θέση που βρίσκεται στη διαδρομή συστήματος στο στόχο. Ο διακόπτης **-d** χρησιμοποιείται για την εκτέλεση της καθορισμένης εντολής με μη διαδραστικό τρόπο και αποσυνδέεται χωρίς να περιμένει να ολοκληρωθεί η διαδικασία που δημιουργήθηκε. Ο διακόπτης **-e** μπορεί προαιρετικά να χρησιμοποιηθεί για την απενεργοποίηση της δημιουργίας προφίλ χρήστη στο απομακρυσμένο σύστημα. Ο διακόπτης **-s** μπορεί να χρησιμοποιηθεί για την εκτέλεση της απομακρυσμένης διαδικασίας στο πλαίσιο του λογαριασμού συστήματος. Όταν χρησιμοποιείται για νόμιμες εργασίες διαχείρισης συστήματος, σημειώστε ότι η χρήση του διακόπτη **-u** προκαλεί στο απομακρυσμένο σύστημα να αντιμετωπίζει τη σύνδεση ως διαδραστική, με αποτέλεσμα την προσωρινή αποθήκευση των διαπιστευτηρίων σύνδεσης στη μνήμη RAM. Εάν το απομακρυσμένο σύστημα έχει ήδη παραβιαστεί, αυτό μπορεί να εκθέσει τα διαπιστευτήρια σε έναν εισβολέα. Η ομάδα του Metasploit έχει προσθέσει επίσης μια έκδοση του psexec ως ενότητα εκμετάλλευσης στο Metasploit Framework. Το εργαλείο psexec απαιτεί έγκυρη πιστοποίηση για την πρόσβαση στο απομακρυσμένο σύστημα, αλλά μπορεί να αποδεχτεί είτε έναν κωδικό πρόσβασης καθαρού κειμένου είτε μια αναπαράσταση κατακερματισμού κωδικού πρόσβασης για να διευκολύνει τις επιθέσεις του τύπου pass-the-hash. Η έλλειψη έγκυρης πιστοποίησης θα οδηγήσει αυτή την ενότητα εκμετάλλευσης στην προσπάθεια σύνδεσης ως επισκέπτης στο εκάστοτε σύστημα [13].

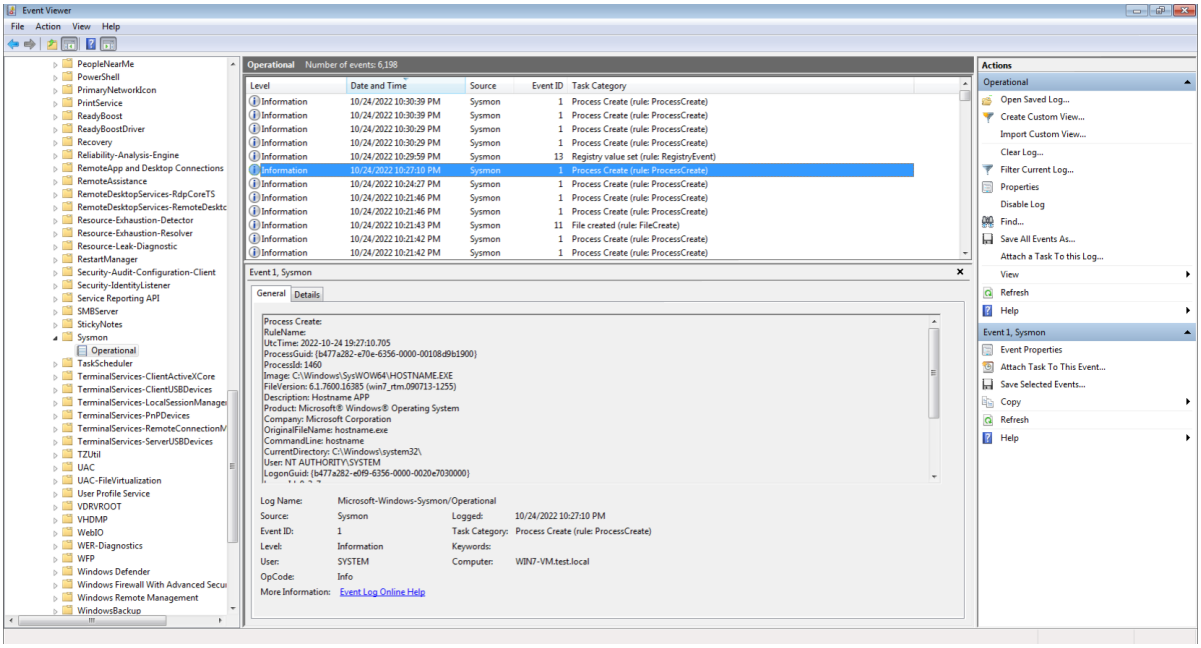
Όσο αναφορά στον εντοπισμό της κακόβουλης χρήσης του εργαλείου psexec, η μονάδα εκμετάλλευσης psexec του Metasploit Framework χρησιμοποιεί έγκυρα διαπιστευτήρια διαχειριστή για να αντιγράψει ένα εκτελέσιμο αρχείο στο σύστημα προορισμού, να δημιουργήσει μια υπηρεσία για να φορτώσει το επιθυμητό ωφέλιμο φορτίο, να διαγράψει την υπηρεσία που δημιούργησε και στη συνέχεια να διαγράψει το μεταφορτωμένο εκτελέσιμο. Από προεπιλογή, τόσο στο εκτελέσιμο αρχείο όσο και στην υπηρεσία δίνεται μια τυχαία σειρά χαρακτήρων ως όνομα. Ωστόσο, τα αυθαίρετα ονόματα μπορούν να καθοριστούν από τον επιτιθέμενο. Η δημιουργία της υπηρεσίας δημιουργεί ένα Αναγνωριστικό συμβάντος: **7045** στο αρχείο καταγραφής συμβάντων του συστήματος, συμπληρωμένο με το όνομα της δημιουργούμενης υπηρεσίας (πεδίο: Όνομα υπηρεσίας) και το εκτελέσιμο που χρησιμοποιήθηκε για τη δημιουργία του (πεδίο: Όνομα αρχείου υπηρεσίας). Το εκτελέσιμο μπορεί να φορτωθεί με ένα τυχαίο ή ρητά παρεχόμενο όνομα ή το Όνομα αρχείου υπηρεσίας μπορεί να εκτελείται με PowerShell με μια μακρά, κωδικοποιημένη με Base64 εντολή. Εάν είναι ενεργοποιημένο, το αναγνωριστικό

συμβάντος **4697** θα καταγραφεί επίσης στο αρχείο καταγραφής συμβάντων ασφαλείας του συστήματος, καταγράφοντας την υπηρεσία που είναι εγκατεστημένη στο σύστημα. Από προεπιλογή, η έκδοση της Sysinternals του psexec θα εγκατασταθεί επίσης ως υπηρεσία με το όνομα υπηρεσίας: **PSEXESVC** και το σχετικό εκτελέσιμο: **psexesvc.exe** γραμμένο στο δίσκο του εκάστοτε συστήματος, καθιστώντας εύκολο τον εντοπισμό του στο αρχείο καταγραφής συμβάντων συστήματος με το αναγνωριστικό: **7045** (και πιθανώς συμβάντος με αναγνωριστικό: **4697** στο αρχείο καταγραφής συμβάντων ασφαλείας, εάν είναι ενεργοποιημένο όπως περιγράφεται παραπάνω). Ωστόσο, το όνομα της υπηρεσίας και το σχετικό εκτελέσιμο σύστημα μπορούν να αλλάξουν σε οποιοδήποτε αυθαίρετο όνομα χρησιμοποιώντας το διακόπτη **-r** όταν εκτελείται το psexec. Σε αντίθεση με την έκδοση του Metasploit, η έκδοση της Sysinternals του psexec δεν διαγράφει αυτόματα την υπηρεσία μετά την ολοκλήρωση. Από προεπιλογή, η έκδοση του psexec από τη σουίτα της Sysinternals θα προκαλέσει επίσης τη δημιουργία προφίλ χρήστη στο απομακρυσμένο σύστημα, εάν δεν υπάρχει ήδη για το σχετικά διαπιστευτήρια χρήστη. Αυτό μπορεί να αποφευχθεί εάν ο επιτιθέμενος χρησιμοποιεί το διακόπτη **-e** κατά την έναρξη της σύνδεσης, αλλά επειδή ο επιτιθέμενος μπορεί να παραλείψει αυτόν τον διακόπτη, ο έλεγχος για την παρουσία ασυνήθιστων προφίλ χρήστη μπορεί να είναι ένας χρήσιμος δείκτης μη εξουσιοδοτημένης δραστηριότητας. Όταν τελειώσει η περίοδος λειτουργίας, ενδέχεται να δείτε ένα συμβάν με αναγνωριστικό: **7036** στο αρχείο καταγραφής συμβάντων του συστήματος που δείχνει την υπηρεσία **PSEXESVC** να εισέρχεται σε κατάσταση διακοπής. Στο σύστημα που ξεκινά τη σύνδεση, όταν χρησιμοποιείται ο διακόπτης **-u**, καταγράφεται ένα συμβάν με το αναγνωριστικό **4648**, που δείχνει τον λογαριασμό που ξεκινά τη χρήση των διαπιστευτηρίων στην ενότητα Θέμα, τα διαπιστευτήρια που παρέχονται με το διακόπτη **-u** στο λογαριασμό των οποίων τα διαπιστευτήρια χρησιμοποιήθηκαν και το απομακρυσμένο σύστημα που στοχεύει στην ενότητα "Διακομιστής προορισμού". Εάν χρησιμοποιήθηκε η έκδοση της Sysinternals του psexec, ενδέχεται να βρείτε ενδείξεις ότι χρησιμοποιείται στο μητρώο. Εκτός από τα τυπικά εγκληματολογικά αντικείμενα που δείχνουν την εκτέλεση του προγράμματος, αυτό το βοηθητικό πρόγραμμα γράφει επίσης σε ένα κλειδί μητρώου στην τοποθεσία: **NTUSER.DAT\Software\Sysinternals\PsExec** όπου ορίζει την τιμή **EulaAccepted** σε 1. Αυτό το κλειδί ονομάζεται PsExec ακόμη και αν ο εισβολέας ονόμασε το εργαλείο κάτι άλλο σε μια προσπάθεια απόκρυψης της εκτέλεσης του [13].

Δεδομένου ότι χρησιμοποιούνται έγκυρα διαπιστευτήρια, τα συμβάντα σύνδεσης λογαριασμού και σύνδεσης που αναφέρθηκαν και παραπάνω ισχύουν επίσης για αυτόν τον φορέα επίθεσης. Εάν ο επιτιθέμενος χρησιμοποιεί τα διαπιστευτήρια του συνδεδεμένου χρήστη, τα Windows θα καταγράψουν την πρόσβαση στο απομακρυσμένο σύστημα με το αναγνωριστικό συμβάντος: **4624**, τύπος: **3** (Σύνδεση δικτύου). Ωστόσο, εάν ο επιτιθέμενος παρέχει υπό της μορφή καθαρού κειμένου διαφορετικά διαπιστευτήρια στο psexec κάνοντας χρήση του διακόπτη **-u**, τα Windows το αντιμετωπίζουν ως διαδραστική σύνδεση (αναγνωριστικό συμβάντος: **4624**, τύπος: **2**) στο απομακρυσμένο σύστημα και επίσης καταγράφεται ένα συμβάν με αναγνωριστικό: **4648** που δείχνει τη διαδικασία **PSEXESVC.exe** χρησιμοποιώντας καθαρού κειμένου διαπιστευτήρια για τον χρήστη που καθορίζεται στο διακόπτη **-u**. Παρακάτω θα δείτε να εκτελείται ένα απλό παράδειγμα χρήσης του **psexec.exe** μέσω της σουίτας impacket από το σύστημα ενός

κακόβουλου χρήστη σε έναν απομακρυσμένο στόχο του Windows Domain. Επιπλέον θα δείτε τη καταγραφή των συμβάντων ασφαλείας στο σύστημα του αμυνόμενου μέσω του sysmon. Μέσω αυτού αλλά και αρκετών άλλων παρόμοιων περιπτώσεων μπορεί να εντοπιστεί η εσωτερική μετακίνηση εντός ενός δικτύου με Windows Domain (Βλ. ***Εικόνα 24, 25***).

Εικόνα 24 – Απομακρυσμένη απόκτηση cmd για εκτέλεση εντολών σε μηχάνημα Windows 7 του domain κάνοντας χρήση διαπιστευτηρίων τοπικού διαχειριστή



Εικόνα 25 – Καταγραφή απομακρυσμένων εντολών που έτρεξε ο επιτιθέμενος στο σύστημα του θύματος μέσω του sysmon

9 Αποτελέσματα, Συμπεράσματα και Μελλοντικές Επεκτάσεις

Ο στόχος της συγκεκριμένης διπλωματικής διατριβής ήταν να ολοκληρωθεί μία ορθή ρύθμιση του εργαλείου Sysmon μέσω της παραμετροποίησης του από ένα αρχείο τύπου .xml, το οποίο ευθύνεται για τη λειτουργία του Sysmon, ώστε σε συνεργασία του με το αρχείο καταγραφής των Windows να επιτυγχάνεται ένα σωστό φιλτράρισμα των συμβάντων. Στην αναφορά της διπλωματικής αυτής εργασίας παρουσιάστηκαν οι πλέον γνωστές τεχνικές και τρόποι που χρησιμοποιούν οι επιτιθέμενοι για να μετακινηθούν εσωτερικά σε ένα δίκτυο καθώς και τρόποι με τους οποίους μπορούμε να ανιχνεύσουμε και να περιορίσουμε ή να αποκλείσουμε την προσπάθεια εσωτερικής μετακίνησης από την πλευρά ενός αμυνόμενου. Τα συμβάντα με τα οποία ασχοληθήκαμε και επικεντρωθήκαμε αφορούν στην ανίχνευση της εσωτερικής μετακίνησης ενός επιτιθέμενου μέσα σε ένα δίκτυο με Windows Domain. Είδαμε και αναλύσαμε το πώς μπορούμε να ανιχνεύσουμε και στη συνέχεια να περιορίσουμε ή και να αποκλείσουμε την προσπάθεια για εσωτερική μετακίνηση μέσα σε ένα δίκτυο με Windows Domain τόσο από την πλευρά ενός επιτιθέμενου όσο και από την πλευρά ενός αμυνόμενου. Όπως παρατηρήθηκε τόσο το εργαλείο Sysmon όσο και το εργαλείο καταγραφής συμβάντων των Windows διαθέτουν πολλές επιλογές παραμετροποίησης σαν μονάδες. Σε αυτή την έρευνα καταφέραμε να συνδυάσουμε τις επιλογές αυτών των δύο εργαλείων ώστε να επιτύχουμε το τελικό σκοπό μας σε ένα αρκετά ικανοποιητικό βαθμό και να έχουμε μία αρκετά καλή αναφορά από πλευράς ασφάλειας σχετικά με το τι πρέπει κανείς να προσέχει και ελέγχει σε ένα λειτουργικό σύστημα Windows που δέχεται μία επίθεση εσωτερικής μετακίνησης. Κατά τη σύνταξη της αναφοράς χρειάστηκε να δοκιμάσουμε να κάνουμε επιθέσεις και να εκμεταλλευτούμε ευπάθειες συστημάτων Windows κάνοντας χρήση μιας ομάδας εργαλείων χειραγώγησης ενός λειτουργικού συστήματος. Τα εργαλεία όπως και οι ομάδες των εργαλείων που χρησιμοποιήθηκαν αφορούν και είναι ικανά να επιφέρουν επαύξηση δικαιωμάτων, εκτέλεση απομακρυσμένων εντολών, συλλογή πληροφοριών-διαπιστευτηρίων και έλεγχο σε ένα απομακρυσμένο σύστημα. Στο τέλος της αναφοράς παρουσιάστηκε το σύνολο των συμβάντων που καταγράψαμε ανάλογα με το εργαλείο που τα ενεργοποίησε κάθε φορά και παραδόθηκε ένα ειδικά κατάλληλο αρχείο διαμόρφωσης του Sysmon με σκοπό στον εντοπισμό επιθέσεων εσωτερικής μετακίνησης.

9.1 Πιθανές μελλοντικές επεκτάσεις

Σαν συνέχεια της διπλωματικής αυτής θα μπορούσε να αποτελέσει η δημιουργία ενός GUI(Γραφικό Περιβάλλον) μέσω του οποίου 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 οποίο θα θέλαμε να ερευνήσουμε.

10 Βιβλιογραφικές Πηγές

[1] MITRE | ATT&CK *Matrices->Windows Matrix->Lateral Movement*
https://attack.mitre.org/matrices/enterprise/windows/

[2] Microsoft | Sysinternals. *Sysmon v13.20 By Mark Russinovich and Thomas Garnier*
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

[3] CQURE ACADEMY *Sysmon: How to set up, update and use?*
https://cqureacademy.com/blog/server-monitoring/sysmon

[4] Applied Incident Response *Windows Event Log Analysis*
https://secureservercdn.net/160.153.138.53/x27.24e.myftpupload.com/download/Windows-Event-Log-Analyst-Reference.pdf?time=1622104504

[5] redcanary.com *threat-hunting-psexec-lateral-movement/*
https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/

[6] CERT-EU *Ανίχνευση εσωτερικής μετακίνησης σε συστήματα Windows*
https://cert.europa.eu/static/WhitePapers/CERT-EU_SWP_17-002_Lateral_Movements.pdf

[7] JPCERT-CC *Tracking Windows Events Logs for Detection of Lateral Movement*
https://www.jpcert.or.jp/english/pub/sr/DetectingLateralMovementThroughTrackingEventLogs_version2.pdf

[8] Applied Incident Response *Ανάλυση εσωτερικής μετακίνησης*
https://secureservercdn.net/160.153.138.53/x27.24e.myftpupload.com/download/Lateral-Movement-Analyst-Reference.pdf?time=1622104504

[9] Ελληνικά Ακαδημαϊκά Συγγράμματα και Βοηθήματα *Καταγραφή και Επίβλεψη Ενεργειών Χρήστη*
https://repository.kallipos.gr/bitstream/11419/529/1/05_chapter_04.pdf

[10] SwiftOnSecurity / sysmon-config *Αρχείο Παραμετροποίησης του Sysmon*
https://github.com/SwiftOnSecurity/sysmon-config

[11] CQURE Academy *Building a Perfect Sysmon Configuration File*
https://cqureacademy.com/blog/hacks/sysmon-configuration-file

[12] Crowdstrike *Cybersecurity 101 › Lateral Movement*
https://www.crowdstrike.com/cybersecurity-101/lateral-movement/

[13] pentestlab *lateral-movement*
https://pentestlab.blog/2021/10/20/lateral-movement-webclient/

Παράρτημα [10]

```
<!--
  sysmon-config | A Sysmon configuration focused on default high-quality
event tracing and easy customization by the community
  Source version: 74 | Date: 2021-07-08
  Source project: https://github.com/SwiftOnSecurity/sysmon-config
  Source 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 13 or higher (due to changes in syntax and bug-
fixes)
      https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

  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 is 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 technicians armed only with Event Viewer. Its purpose
is to democratize system monitoring for all organizations.

  NOTE: Sysmon is NOT a whitelist solution or HIDS correlation engine, it
is a computer change logging tool.
      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: By default this monitors DNS, which is extremely noisy. If you are
starting out on your monitoring journey, just remove that section.
      You can remove DNS events from Event Viewer screen by applying a
'Filter Current View' for event IDs of: -22
      Additionally, if you want to monitor DNS, you should deploy client-
side adblocking to reduce lookups. See the DNS section for info.

  NOTE: This configuration is designed for PER-MACHINE installs of Chrome
and OneDrive. That moves their binaries out of user-controlled folders.
      Otherwise, attackers could imitate these common applications, and
bypass your logging. Below are silent upgrades you can do, no user impact:
      - https://docs.microsoft.com/en-us/onedrive/per-machine-installation
      - https://cloud.google.com/chrome-enterprise/browser/download/
```

```
      - As of 2021-02-16 there is no machine-level version of Microsoft
Teams. The one provided copies itself to the user profile.

  NOTE: Sysmon is not hardened against an attacker with admin rights.
Additionally, this configuration offers an attacker, willing
      to study it, limited ways to evade some of the logging. If you are
in a very high-threat environment, you should consider a broader,
      log-most approach. However, in the vast majority of cases, an
attacker will bumble through multiple behavioral traps which
      this configuration monitors, especially in the first minutes.

  NOTE: If you encounter unexplainable event inclusion/exclusion, you may
have a second Sysmon instance installed under a different exe filename.
      To clear this, try downloading the latest version and uninstalling
with -u force. If it hangs, kill the processes and run it again to
cleanup.

  TECHNICAL:
  - Run sysmon.exe -? for a briefing on Sysmon configuration.
  - Sysmon XML cannot use the AMPERSAND sign. Replace it with this: &amp;
  - Sysmon 8+ can track which rule caused an event to be logged through
the "RuleName" field.
  - 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" and "LoginGuid" are not random, they contain some
embedded information.
https://gist.github.com/mattifestation/0102042160c9a60b2b847378c0ef70b4

  FILTERING: Filter conditions available for use are: is,is
not,contains,contains any,contains all,excludes,excludes any,excludes
all,begin with,end with,less than,more than,image
  - The "image" filter is usable on any field. Same as "is" but can either
match entire string, or only the text after last "\". Credit:
@mattifestation

-->

<Sysmon schemaversion="4.50">
      <!--SYSMON META CONFIG-->
      <HashAlgorithms>md5,sha256,IMPHASH</HashAlgorithms> <!-- Both MD5
and SHA256 are the industry-standard algorithms. Remove IMPHASH if you do
not use DLL import fingerprinting. -->
      <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. -->
      <!-- <ArchiveDirectory> -->

      <EventFiltering>

      <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
            <!--COMMENT:      All processes launched will be logged,
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 AppLocker/WindowsDeviceGuard for whitelisting support. -->

            <!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion,
Description, Product, Company, CommandLine, CurrentDirectory, User,
LogonGuid, LogonId, TerminalSessionId, IntegrityLevel, Hashes,
ParentProcessGuid, ParentProcessId, ParentImage, ParentCommandLine,
RuleName-->
      <RuleGroup name="" groupRelation="or">
            <ProcessCreate onmatch="exclude">
                  <!--SECTION: Microsoft Windows-->
                  <CommandLine condition="begin with">
"C:\Windows\system32\wermgr.exe" "-queuereporting_svc" </CommandLine> <!--
Windows:Windows error reporting/telemetry-->
                  <CommandLine condition="begin
with">C:\Windows\system32\DllHost.exe /Processid</CommandLine> <!--
Windows-->
                  <CommandLine condition="begin
with">C:\Windows\system32\wbem\wmiprvse.exe -Embedding</CommandLine> <!--
Windows: WMI provider host-->
                  <CommandLine condition="begin
with">C:\Windows\system32\wbem\wmiprvse.exe -secured -
Embedding</CommandLine> <!--Windows: WMI provider host-->
                  <CommandLine
condition="is">C:\Windows\system32\wermgr.exe -upload</CommandLine> <!--
Windows:Windows error reporting/telemetry-->
                  <CommandLine
condition="is">C:\Windows\system32\SearchIndexer.exe
/Embedding</CommandLine> <!--Windows: Search Indexer-->
                  <CommandLine
condition="is">C:\windows\system32\wermgr.exe -
queuereporting</CommandLine> <!--Windows:Windows error
reporting/telemetry-->
```

```
                    <CommandLine
condition="is">\??\C:\Windows\system32\autochk.exe *</CommandLine> <!--
Microsoft:Bootup: Auto Check Utility-->
                    <CommandLine
condition="is">\SystemRoot\System32\smss.exe</CommandLine> <!--
Microsoft:Bootup: Windows Session Manager-->
                    <CommandLine
condition="is">C:\Windows\System32\RuntimeBroker.exe -
Embedding</CommandLine> <!--Windows:Apps permissions [
https://fossbytes.com/runtime-broker-process-windows-10/ ] -->
                    <Image condition="is">C:\Program Files (x86)\Common
Files\microsoft shared\ink\TabTip32.exe</Image> <!--Windows: Touch
Keyboard and Handwriting Panel Helper-->
                    <Image
condition="is">C:\Windows\System32\TokenBrokerCookies.exe</Image> <!--
Windows: SSO sign-in assistant for MicrosoftOnline.com-->
                    <Image
condition="is">C:\Windows\System32\plasrv.exe</Image> <!--Windows:
Performance Logs and Alerts DCOM Server-->
                    <Image
condition="is">C:\Windows\System32\wifitask.exe</Image> <!--Windows:
Wireless Background Task-->
                    <Image
condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--
Windows: Customer Experience Improvement-->
                    <Image
condition="is">C:\Windows\system32\PrintIsolationHost.exe</Image> <!--
Windows: Printing-->
                    <Image
condition="is">C:\Windows\system32\SppExtComObj.Exe</Image> <!--Windows:
KMS activation-->
                    <Image
condition="is">C:\Windows\system32\audiodg.exe</Image> <!--Windows:
Launched constantly-->
                    <Image
condition="is">C:\Windows\system32\conhost.exe</Image> <!--Windows:
Command line interface host process-->
                    <Image
condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Windows:
Network file syncing-->
                    <Image
condition="is">C:\Windows\system32\musNotification.exe</Image> <!--
Windows: Update pop-ups-->
                    <Image
condition="is">C:\Windows\system32\musNotificationUx.exe</Image> <!--
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> <!--Windows: Volume
control-->
                    <Image
condition="is">C:\Windows\system32\sppsvc.exe</Image> <!--Windows:
Software Protection Service-->
                    <Image
condition="is">C:\Windows\system32\wbem\WmiApSrv.exe</Image> <!--Windows:
```

```
WMI performance adapter host process-->
                    <IntegrityLevel
condition="is">AppContainer</IntegrityLevel> <!--Windows: Don't care about
sandboxed processes right now. Will need to revisit this decision.-->
                    <ParentCommandLine condition="begin
with">%%SystemRoot%%\system32\csrss.exe
ObjectDirectory=\Windows</ParentCommandLine> <!--Windows:CommandShell:
Triggered when programs use the command shell, but doesn't provide
attribution for what caused it-->
                    <ParentCommandLine
condition="is">C:\windows\system32\wermgr.exe -
queuereporting</ParentCommandLine> <!--Windows:Windows error
reporting/telemetry-->
                    <CommandLine
condition="is">C:\WINDOWS\system32\devicecensus.exe UserCxt</CommandLine>
                    <CommandLine
condition="is">C:\Windows\System32\usocoreworker.exe -
Embedding</CommandLine>
                    <ParentImage
condition="is">C:\Windows\system32\SearchIndexer.exe</ParentImage> <!--
Windows:Search: Launches many uninteresting sub-processes-->
                    <!--SECTION: Windows:svchost-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k appmodel -s
StateRepository</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k appmodel -p -s
camsvc</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k appmodel</CommandLine>
<!--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>
<!--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 -p -s
BthAvctpSvc</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> <!--Windows: Network
services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localServiceAndNoImpersonation -p</CommandLine> <!--Windows: Network
services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localServiceNetworkRestricted -s Dhcp</CommandLine> <!--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 -s BTAGService</CommandLine>
                    <CommandLine
condition="is">C:\Windows\System32\svchost.exe -k
LocalSystemNetworkRestricted -p -s NcbService</CommandLine> <!--
Win10:1903:Network Connection Broker-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localServiceNetworkRestricted</CommandLine> <!--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
localServiceAndNoImpersonation -p -s SSDPSRV</CommandLine> <!--
Windows:SSDP [
https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol ] -->
                    <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 -p -s NgcSvc</CommandLine> <!--
Microsoft:Passport-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localServiceNetworkRestricted -p -s NgcCtnrSvc</CommandLine> <!--
Microsoft:Passport Container-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localServiceAndNoImpersonation -s SCardSvr</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -s
wuauserv</CommandLine>
                    <CommandLine
condition="is">C:\Windows\System32\svchost.exe -k netsvcs -p -s
SessionEnv</CommandLine> <!--Windows:Remote desktop configuration-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -s WdiSystemHost</CommandLine> <!--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> <!--
Windows: Diagnostic System Host [ http://www.blackviper.com/windows-
services/diagnostic-system-host/ ] -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted</CommandLine> <!--Windows-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -s
wlidsvc</CommandLine> <!--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> <!--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> <!--Windows:Network: BitLocker Drive Encryption-->
                    <CommandLine
condition="is">C:\Windows\System32\svchost.exe -k netsvcs -p -s
BDESVC</CommandLine> <!--Microsoft:Win10:1903:Network: BitLocker Drive
Encryption-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -s
BITS</CommandLine> <!--Windows:Network: Background Intelligent File
Transfer (BITS) -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
BITS</CommandLine> <!--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 -p -s
Appinfo</CommandLine>
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
Gpsvc</CommandLine> <!--Windows:Network: Group Policy -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
ProfSvc</CommandLine> <!--Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
SENS</CommandLine> <!--Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
SessionEnv</CommandLine> <!--Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
Themes</CommandLine> <!--Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
Winmgmt</CommandLine> <!--Windows: Windows Management Instrumentation
(WMI) -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k netsvcs</CommandLine>
<!--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> <!--Windows:Network: DNS caching, other uses -->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k networkService -s
LanmanWorkstation</CommandLine> <!--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> <!--Windows:Network: Network Location Awareness-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k networkService -s
TermService</CommandLine> <!--Windows:Network: Terminal Services (RDP)-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
networkService</CommandLine> <!--Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k networkService -
p</CommandLine> <!--Windows: Network services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
networkServiceNetworkRestricted</CommandLine> <!--Windows: Network
services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k rPCSS</CommandLine> <!--
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> <!--Windows 10-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k utcsvc</CommandLine> <!-
-Windows Services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
wbioSvcGroup</CommandLine> <!--Windows Services-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k
werSvcGroup</CommandLine> <!--Windows: ErrorReporting-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k wusvcs -p -s
WaaSMedicSvc</CommandLine> <!--Windows: Update Medic Service [
https://www.thewindowsclub.com/windows-update-medic-service ] -->
                    <CommandLine
condition="is">C:\Windows\System32\svchost.exe -k wsappx -p -s
ClipSVC</CommandLine> <!--Windows:Apps: Client License Service-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k wsappx -p -s
AppXSvc</CommandLine> <!--Windows:Apps: AppX Deployment Service-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k wsappx -s
ClipSVC</CommandLine> <!--Windows:Apps: Client License Service-->
                    <CommandLine
condition="is">C:\Windows\system32\svchost.exe -k wsappx</CommandLine> <!-
-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> <!--Windows: Network services: Spawns
```

```
Consent.exe-->
                    <ParentCommandLine
condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted</ParentCommandLine> <!--Windows-->
                    <CommandLine
condition="is">C:\Windows\system32\deviceenroller.exe /c
/AutoEnrollMDM</CommandLine> <!--Windows: AzureAD device enrollment agent-
->
                    <!--SECTION: Microsoft:Edge-->
                    <CommandLine condition="begin with">"C:\Program Files
(x86)\Microsoft\Edge Dev\Application\msedge.exe" --type=</CommandLine>
                    <!--SECTION: Microsoft:dotNet-->
                    <CommandLine condition="begin
with">C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe</CommandLine>
<!--Microsoft:DotNet-->
                    <CommandLine condition="begin
with">C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\Ngen.exe</CommandLin
e> <!--Microsoft:DotNet-->
                    <CommandLine condition="begin
with">C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe</CommandL
ine> <!--Microsoft:DotNet-->
                    <CommandLine condition="begin
with">C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\ngentask.exe</Comman
dLine> <!--Microsoft:DotNet-->
                    <Image
condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.ex
e</Image> <!--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\PresentationF
ontCache.exe</Image> <!--Windows: Font cache service-->
                    <ParentCommandLine condition="begin
with">C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngentask.exe</Parent
CommandLine>
                    <ParentImage
condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.ex
e</ParentImage> <!--Microsoft:DotNet-->
                    <ParentImage
condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngentask.ex
e</ParentImage> <!--Microsoft:DotNet-->
                    <ParentImage
condition="is">C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe<
/ParentImage> <!--Microsoft:DotNet-->
                    <ParentImage
condition="is">C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe<
/ParentImage> <!--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\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="is">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: Windows: Media player-->
                  <Image condition="is">C:\Program Files\Windows Media
Player\wmpnscfg.exe</Image> <!--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-->
            </ProcessCreate>
      </RuleGroup>

      <!--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-->
      <RuleGroup name="" groupRelation="or">
            <FileCreateTime onmatch="include">
                  <Image name="T1099" condition="begin
with">C:\Users</Image> <!--Look for timestomping in user area, usually
nothing should be doing that here-->
                  <TargetFilename name="T1099" condition="end
with">.exe</TargetFilename> <!--Look for backdated executables anywhere-->
                  <Image name="T1099" condition="begin
with">\Device\HarddiskVolumeShadowCopy</Image> <!--Nothing should be
written here | Credit: @SBousseaden [
https://twitter.com/SBousseaden/status/1133030955407630336 ] -->
            </FileCreateTime>
      </RuleGroup>

      <RuleGroup name="" groupRelation="or">
            <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-->
                <TargetFilename
condition="contains">\NVIDIA\NvBackend\ApplicationOntology\</TargetFilenam
e> <!--NVIDIA GeForce Experience Application Ontology, 1000's of events in
user profile-->
          </FileCreateTime>
     </RuleGroup>

     <!--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-->
     <RuleGroup name="" groupRelation="or">
          <NetworkConnect onmatch="include">
                <!--Suspicious sources for network-connecting binaries--
>
                <Image name="Usermode" condition="begin
with">C:\Users</Image> <!--Tools downloaded by users can use other
processes for networking, but this is a very valuable indicator.-->
                <Image name="Caution" condition="begin
with">C:\Recycle</Image> <!--Nothing should operate from the RecycleBin
locations.-->
                <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-->
                    <Image name="Caution" condition="begin with">\</Image>
<!--Devices and VSC shouldn't be executing changes | Credit: @SBousseaden
@ionstorm @neu5ron @PerchedSystems [
https://twitter.com/SwiftOnSecurity/status/1133167323991486464 ] -->
                    <Image name="Caution" condition="begin
with">C:\perflogs</Image> <!-- Credit @blu3_team [ https://blu3-
team.blogspot.com/2019/05/netconn-from-suspicious-directories.html ] -->
                    <Image name="Caution" condition="begin
with">C:\intel</Image> <!-- Credit @blu3_team [ https://blu3-
team.blogspot.com/2019/05/netconn-from-suspicious-directories.html ] -->
                    <Image name="Caution" condition="begin
with">C:\Windows\fonts</Image> <!-- Credit @blu3_team [ https://blu3-
team.blogspot.com/2019/05/netconn-from-suspicious-directories.html ] -->
                    <Image name="Caution" condition="begin
with">C:\Windows\system32\config</Image> <!-- Credit @blu3_team [
https://blu3-team.blogspot.com/2019/05/netconn-from-suspicious-
directories.html ] -->
                    <!--Suspicious Windows tools-->
                    <Image condition="image">at.exe</Image> <!--Windows:
Remote task scheduling, removed in Win10 | Credit @ion-storm -->
                    <Image condition="image">certutil.exe</Image> <!--
Windows: Certificate tool can contact outbound | Credit @ion-storm @FVT [
https://twitter.com/FVT/status/834433734602530817 ] -->
                    <Image condition="image">cmd.exe</Image> <!--Windows:
Remote command prompt-->
                    <Image condition="image">cmstp.exe</Image> <!--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> <!--
WindowsScriptingHost: | Credit @Cyb3rOps [
https://gist.github.com/Neo23x0/a4b4af9481e01e749409 ] -->
                    <Image condition="image">driverquery.exe</Image> <!--
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> <!--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> <!--Windows: --
>
                    <Image condition="image">msbuild.exe</Image> <!--
Windows: [ https://www.hybrid-
```

```
analysis.com/sample/a314f6106633fba4b70f9d6ddbee452e8f8f44a72117749c21243d
c93c7ed3ac?environmentId=100 ] -->
                    <Image condition="image">mshta.exe</Image> <!--Windows:
HTML application executes scripts without IE protections | Credit @ion-
storm [ https://en.wikipedia.org/wiki/HTML_Application ] -->
                    <Image condition="image">msiexec.exe</Image> <!--
Windows: Can install from http:// paths | Credit @vector-sec -->
                    <Image condition="image">nbtstat.exe</Image> <!--
Windows: NetBIOS statistics, attackers use to enumerate local network -->
                    <Image condition="image">net.exe</Image> <!--Windows:
Note - May not detect anything, net.exe is a front-end to lower APIs |
Credit @ion-storm -->
                    <Image condition="image">net1.exe</Image> <!--Windows:
Launched by "net.exe", but it may not detect connections either -->
                    <Image condition="image">notepad.exe</Image> <!--
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> <!--
Windows: Retrieve data over DNS -->
                    <Image condition="image">powershell.exe</Image> <!--
Windows: PowerShell interface-->
                    <Image condition="image">powershell_ise.exe</Image> <!--
Windows: PowerShell interface-->
                    <Image condition="image">qprocess.exe</Image> <!--
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> <!--
Windows: Query remote sessions | Credit @ion-storm -->
                    <Image condition="image">qwinsta.exe</Image> <!--
Windows: Remotely query login sessions on a server or workstation | Credit
@ion-storm -->
                    <Image condition="image">reg.exe</Image> <!--Windows:
Remote Registry editing ability | Credit @ion-storm -->
                    <Image condition="image">regsvcs.exe</Image> <!--
Windows: [ https://www.hybrid-
analysis.com/sample/3f94d7080e6c5b8f59eeecc3d44f7e817b31562caeba21d02ad705
a0bfc63d67?environmentId=100 ] -->
                    <Image condition="image">regsvr32.exe</Image> <!--
Windows: [ https://subt0x10.blogspot.com/2016/04/bypass-application-
whitelisting-script.html ] -->
                    <Image condition="image">rundll32.exe</Image> <!--
Windows: [ https://blog.cobaltstrike.com/2016/07/22/why-is-rundll32-exe-
connecting-to-the-internet/ ] -->
                    <Image condition="image">rwinsta.exe</Image> <!--
Windows: Disconnect remote sessions | Credit @ion-storm -->
                    <Image condition="image">sc.exe</Image> <!--Windows:
Remotely change Windows service settings | Credit @ion-storm -->
                    <Image condition="image">schtasks.exe</Image> <!--
Windows: Command-line interface to local and remote tasks -->
                    <Image condition="image">taskkill.exe</Image> <!--
Windows: Kill processes, has remote ability -->
                    <Image condition="image">tasklist.exe</Image> <!--
Windows: List processes, has remote ability -->
                    <Image condition="image">wmic.exe</Image> <!--
WindowsManagementInstrumentation: Credit @Cyb3rOps [
https://gist.github.com/Neo23x0/a4b4af9481e01e749409 ] -->
```

```
                    <Image condition="image">wscript.exe</Image> <!--
WindowsScriptingHost: | Credit @arekfurt -->
                    <!--Live of the Land Binaries and scripts (LOLBAS) -->
                    <Image condition="image">bitsadmin.exe</Image> <!--
Windows: Background Intelligent Transfer Service - Can download from URLs
-->
                    <Image condition="image">esentutl.exe</Image> <!--
Windows: Database utilities for the ESE - Can fetch from UNC paths -->
                    <Image condition="image">expand.exe</Image> <!--
Windows: Expands one or more compressed files - Can fetch from UNC paths -
->
                    <Image condition="image">extrac32.exe</Image> <!--
Windows: Uncompress .cab files - Can fetch from UNC paths -->
                    <Image condition="image">findstr.exe</Image> <!--
Windows: Search for strings - Can fetch from UNC paths -->
                    <Image condition="image">GfxDownloadWrapper.exe</Image>
<!-- Intel Graphics Control Panel: Remote file download -->
                    <Image condition="image">ieexec.exe</Image> <!--
Windows: Microsoft .NET Framework application - Download and execute from
URLs -->
                    <Image condition="image">makecab.exe</Image> <!--
Windows: Packages existing files into a .cab - Can fetch from UNC paths --
>
                    <Image condition="image">replace.exe</Image> <!--
Windows: Used to replace file with another file - Can fetch from UNC paths
-->
                    <Image condition="image">Excel.exe</Image> <!-- Windows
Office: Excel - Can download from URLs -->
                    <Image condition="image">Powerpnt.exe</Image> <!--
Windows Office: PowerPoint - Can download from URLs -->
                    <Image condition="image">Winword.exe</Image> <!--
Windows Office: Word - Can download from URLs -->
                    <Image condition="image">squirrel.exe</Image> <!--
Windows: Update the Nuget/Squirrel packages. Part of Teams. - Can download
from URLs -->
                    <!--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/800bf028a23440134fc834efc5c1e02cc70f05b2e800bbc285d7c9
2a4b126b1c?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 name="SSH"
condition="is">22</DestinationPort> <!--SSH protocol, monitor admin
connections-->
                  <DestinationPort name="Telnet"
condition="is">23</DestinationPort> <!--Telnet protocol, monitor admin
connections, insecure-->
                  <DestinationPort name="SMTP"
condition="is">25</DestinationPort> <!--SMTP mail protocol port, insecure,
used by threats-->
                  <DestinationPort name="IMAP"
condition="is">143</DestinationPort> <!--IMAP mail protocol port,
insecure, used by threats-->
                  <DestinationPort name="RDP"
condition="is">3389</DestinationPort> <!--Windows:RDP: Monitor admin
connections-->
                  <DestinationPort name="VNC"
condition="is">5800</DestinationPort> <!--VNC protocol: Monitor admin
connections, often insecure, using hard-coded admin password-->
                  <DestinationPort name="VNC"
condition="is">5900</DestinationPort> <!--VNC protocol Monitor admin
connections, often insecure, using hard-coded admin password-->
                  <DestinationPort name="Alert,Metasploit"
condition="is">4444</DestinationPort>
                  <!--Ports: Proxy-->
                  <DestinationPort name="Proxy"
condition="is">1080</DestinationPort> <!--Socks proxy port | Credit @ion-
storm-->
                  <DestinationPort name="Proxy"
condition="is">3128</DestinationPort> <!--Socks proxy port | Credit @ion-
storm-->
                  <DestinationPort name="Proxy"
condition="is">8080</DestinationPort> <!--Socks proxy port | Credit @ion-
storm-->
                  <!--Ports: Tor-->
                  <DestinationPort name="Tor"
condition="is">1723</DestinationPort> <!--Tor protocol [
https://attack.mitre.org/wiki/Technique/T1090 ] | Credit @ion-storm-->
                  <DestinationPort name="Tor"
condition="is">9001</DestinationPort> <!--Tor protocol [
http://www.computerworlduk.com/tutorial/security/tor-enterprise-2016-
blocking-malware-darknet-use-rogue-nodes-3633907/ ] -->
                  <DestinationPort name="Tor"
condition="is">9030</DestinationPort> <!--Tor protocol [
http://www.computerworlduk.com/tutorial/security/tor-enterprise-2016-
blocking-malware-darknet-use-rogue-nodes-3633907/ ] -->
            </NetworkConnect>
      </RuleGroup>

      <RuleGroup name="" groupRelation="or">
            <NetworkConnect onmatch="exclude">
                  <!--SECTION: Microsoft-->
```

```
                  <Image condition="begin
with">C:\ProgramData\Microsoft\Windows Defender\Platform\</Image>
                  <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-->
                  <!--OCSP known addresses-->
                  <DestinationIp condition="is">23.4.43.27</DestinationIp>
<!--Digicert [ https://otx.alienvault.com/indicator/ip/23.4.43.27 ] -->
                  <DestinationIp
condition="is">72.21.91.29</DestinationIp> <!--Digicert [
https://otx.alienvault.com/indicator/ip/72.21.91.29 ] -->
                  <!--Section: Loopback Addresses-->
                  <DestinationIp condition="is">127.0.0.1</DestinationIp>
<!--Credit @ITProPaul-->
                  <DestinationIp condition="begin
with">fe80:0:0:0</DestinationIp> <!--Credit @ITProPaul-->
            </NetworkConnect>
      </RuleGroup>

      <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE 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-->
      <RuleGroup name="" groupRelation="or">
            <ProcessTerminate onmatch="include">
                  <Image condition="begin with">C:\Users</Image> <!--
Process terminations by user binaries-->
                  <Image condition="begin with">\</Image> <!--Devices and
VSC shouldn't be executing changes | Credit: @SBousseaden @ionstorm
@neu5ron @PerchedSystems [
https://twitter.com/SwiftOnSecurity/status/1133167323991486464 ] -->
            </ProcessTerminate>
      </RuleGroup>

      <RuleGroup name="" groupRelation="or">
            <ProcessTerminate onmatch="exclude">
            </ProcessTerminate>
      </RuleGroup>

      <!--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-->
      <RuleGroup name="" groupRelation="or">
            <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>
      </RuleGroup>

      <!--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-->
      <RuleGroup name="" groupRelation="or">
            <ImageLoad onmatch="include">
                  <!--NOTE: Using "include" with no rules means nothing in
this section will be logged-->
            </ImageLoad>
      </RuleGroup>

      <!--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-->
      <RuleGroup name="" groupRelation="or">
            <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="is">C:\Program Files
(x86)\Google\Chrome\Application\chrome.exe</TargetImage>
            </CreateRemoteThread>
      </RuleGroup>

      <!--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-->
      <RuleGroup name="" groupRelation="or">
            <RawAccessRead onmatch="include">
                  <!--NOTE: Using "include" with no rules means nothing in
this section will be logged-->
            </RawAccessRead>
      </RuleGroup>

      <!--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-->
      <RuleGroup name="" groupRelation="or">
            <ProcessAccess onmatch="include">
                  <!--NOTE: Using "include" with no rules means nothing in
this section will be logged-->
            </ProcessAccess>
      </RuleGroup>

      <!--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-->
      <RuleGroup name="" groupRelation="or">
            <FileCreate onmatch="include">
                  <TargetFilename name="T1023" condition="contains">\Start
Menu</TargetFilename> <!--Windows: Startup links and shortcut modification
[ https://attack.mitre.org/wiki/Technique/T1023 ] -->
                  <TargetFilename name="T1165"
condition="contains">\Startup\</TargetFilename> <!--Microsoft:Changes to
user's auto-launched files and shortcuts-->
                  <TargetFilename name="OutlookAttachment"
condition="contains">\Content.Outlook\</TargetFilename> <!--
Microsoft:Outlook: attachments-->
                  <TargetFilename name="Downloads"
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 name="T1176" condition="end
with">.crx</TargetFilename> <!--Chrome extension-->
                  <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 name="DLL" condition="end
with">.dll</TargetFilename> <!--Microsoft:Office:Word: Macro-->
                  <TargetFilename name="EXE" condition="end
with">.exe</TargetFilename> <!--Executable-->
                  <TargetFilename name="ProcessHostingdotNETCode"
condition="end with">.exe.log</TargetFilename> <!-- [
https://github.com/bitsadmin/nopowershell ] | Credit: @SBousseaden [
https://twitter.com/SBousseaden/status/1137493597769687040 ]  -->
                  <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">.job</TargetFilename> <!--Scheduled task-->
                    <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">.sct</TargetFilename> <!--Scripting | Credit @bartblaze -->
                    <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">.wsc</TargetFilename> <!--Scripting | Credit @bartblaze -->
                    <TargetFilename condition="end
with">.wsf</TargetFilename> <!--Scripting | Credit @bartblaze -->
                    <TargetFilename condition="end
with">.xlsm</TargetFilename> <!--Microsoft:Office:Word: Macro-->
                    <TargetFilename condition="end
with">.ocx</TargetFilename> <!--Microsoft:ActiveX-->
                    <TargetFilename condition="end
with">proj</TargetFilename><!--Microsoft:MSBuild:Script: [
https://twitter.com/subTee/status/885919612969394177 ] -->
                    <TargetFilename condition="end
with">.sln</TargetFilename><!--Microsoft:MSBuild:Script: [
https://twitter.com/subTee/status/885919612969394177 ] -->
                    <TargetFilename condition="end
with">.xls</TargetFilename><!--Microsoft [
https://medium.com/@threathuntingteam/msxsl-exe-and-wmic-exe-a-way-to-
proxy-code-execution-8d524f642b75 ] -->
                    <TargetFilename name="DefaultUserModified"
condition="begin with">C:\Users\Default</TargetFilename> <!--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 name="T1037,T1484" 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 name="T1037,T1484" 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 name="T1053" condition="begin
with">C:\Windows\Tasks\</TargetFilename> <!--Microsoft:ScheduledTasks [
https://attack.mitre.org/wiki/Technique/T1053 ] -->
                    <TargetFilename name="T1053" condition="begin
with">C:\Windows\system32\Tasks</TargetFilename> <!--
Microsoft:ScheduledTasks [ https://attack.mitre.org/wiki/Technique/T1053 ]
-->
                    <TargetFilename name="T1053" condition="begin
with">C:\Windows\SysWOW64\Tasks</TargetFilename> <!--
Microsoft:ScheduledTasks [ https://attack.mitre.org/wiki/Technique/T1053 ]
-->
                    <Image condition="begin
with">\Device\HarddiskVolumeShadowCopy</Image> <!--Nothing should be
executing from VSC | Credit: @SBousseaden [
https://twitter.com/SBousseaden/status/1133030955407630336 ] -->
                    <!--Windows application compatibility-->
                    <TargetFilename condition="begin
with">C:\Windows\AppPatch\Custom</TargetFilename> <!--Windows: Application
compatibility shims [ https://www.fireeye.com/blog/threat-
research/2017/05/fin7-shim-databases-persistence.html ] -->
                    <TargetFilename
condition="contains">VirtualStore</TargetFilename> <!--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">.rtf</TargetFilename> <!--RTF files often 0day malware vectors when
opened by Office-->
            </FileCreate>
```

```
      </RuleGroup>

      <RuleGroup name="" groupRelation="or">
            <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:Click2Run-->
                  <Image condition="is">C:\Program Files\Common
Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe</Image> <!--
Microsoft:Office Click2Run-->
                  <!--SECTION: Windows-->
                  <Image
condition="is">C:\Windows\system32\smss.exe</Image> <!-- Windows: Session
Manager SubSystem: Creates swapfile.sys,pagefile.sys,hiberfile.sys-->
                  <Image
condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--
Windows: Windows 10 app, creates tons of cache files-->
                  <Image
condition="is">\\?\C:\Windows\system32\wbem\WMIADAP.EXE</Image> <!--
Windows: WMI Performance updates-->
                  <Image
condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Windows:
Network file syncing-->
                  <TargetFilename condition="begin
with">C:\Windows\system32\DriverStore\Temp\</TargetFilename> <!-- Windows:
Temp files by DrvInst.exe-->
                  <TargetFilename condition="begin
with">C:\Windows\system32\wbem\Performance\</TargetFilename> <!-- Windows:
Created in wbem by WMIADAP.exe-->
                  <TargetFilename condition="begin
with">C:\Windows\Installer\</TargetFilename> <!--Windows:Installer: Ignore
MSI installer files caching-->
                  <!--SECTION: Windows:Updates-->
                  <TargetFilename condition="begin
with">C:\$WINDOWS.~BT\Sources\</TargetFilename> <!-- Windows: Feature
updates containing lots of .exe and .sys-->
                  <Image condition="begin
with">C:\Windows\winsxs\amd64_microsoft-windows</Image> <!-- Windows:
Windows update-->
            </FileCreate>
      </RuleGroup>

      <!--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.
                                                    Sysmon's wildcard
monitoring along with highly-tuned generic strings cuts the rulesets down
immensely, compared to doing this in other tools.
                                                    For example, most COM
hijacking in CLSID's across the registry is covered by a single rule
monitoring a InProcServer32 wildcard-->

            <!--DATA: EventType, UtcTime, ProcessGuid, ProcessId, Image,
TargetObject, Details (can't filter on), NewName (can't filter on)-->
      <RuleGroup name="" groupRelation="or">
            <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 ] -->
                        <!--ADDITIONAL REFERENCE: [
https://web.archive.org/web/20200116001643/http://scholarworks.rit.edu/cgi
/viewcontent.cgi?article=1533&context=theses | Understanding malware
autostart techniques - Matthew Gottlieb ] -->
                  <TargetObject name="T1060,RunKey"
condition="contains">CurrentVersion\Run</TargetObject> <!--Windows:
Wildcard for Run keys, including RunOnce, RunOnceEx, RunServices,
RunServicesOnce [Also covers terminal server] -->
                  <TargetObject name="T1060,RunPolicy"
condition="contains">Policies\Explorer\Run</TargetObject> <!--Windows:
Alternate runs keys | Credit @ion-storm-->
```

```
                    <TargetObject name="T1484" condition="contains">Group
Policy\Scripts</TargetObject> <!--Windows: Group policy scripts-->
                    <TargetObject name="T1484"
condition="contains">Windows\System\Scripts</TargetObject> <!--Windows:
Wildcard for Logon, Loggoff, Shutdown-->
                    <TargetObject name="T1060"
condition="contains">CurrentVersion\Windows\Load</TargetObject> <!--
Windows: [ https://msdn.microsoft.com/en-us/library/jj874148.aspx ] -->
                    <TargetObject name="T1060"
condition="contains">CurrentVersion\Windows\Run</TargetObject> <!--
Windows: [ https://msdn.microsoft.com/en-us/library/jj874148.aspx ] -->
                    <TargetObject name="T1060"
condition="contains">CurrentVersion\Winlogon\Shell</TargetObject> <!--
Windows: [ https://msdn.microsoft.com/en-
us/library/ms838576(v=winembedded.5).aspx ] -->
                    <TargetObject name="T1060"
condition="contains">CurrentVersion\Winlogon\System</TargetObject> <!--
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> <!--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> <!--Windows: [
https://technet.microsoft.com/en-us/library/ee851671.aspx ] -->
                    <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\Userinit</TargetObject> <!--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> <!--Windows: Legacy driver
loading | Credit @ion-storm -->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\BootExecute</TargetObject> <!--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> <!--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> <!--Windows:
Legacy logon script environment variable [
http://www.hexacorn.com/blog/2014/11/14/beyond-good-ol-run-key-part-18/ ]
-->
                    <TargetObject name="T1112,ChangeStartupFolderPath"
condition="end with">user shell folders\startup</TargetObject> <!--Monitor
changes to Startup folder location for monitoring evasion | Credit
```

```
@SBousseaden-->
                    <!--Services-->
                    <TargetObject name="T1031,T1050" condition="end
with">\ServiceDll</TargetObject> <!--Windows: Points to a service's DLL [
https://blog.cylance.com/windows-registry-persistence-part-1-introduction-
attack-phases-and-windows-services ] -->
                    <TargetObject name="T1031,T1050" condition="end
with">\ServiceManifest</TargetObject> <!--Windows: Manifest pointing to
service's DLL [
https://www.geoffchappell.com/studies/windows/win32/services/svchost/index
.htm ] -->
                    <TargetObject name="T1031,T1050" condition="end
with">\ImagePath</TargetObject> <!--Windows: Points to a service's EXE [
https://attack.mitre.org/wiki/Technique/T1050 ] -->
                    <TargetObject name="T1031,T1050" condition="end
with">\Start</TargetObject> <!--Windows: Services start mode changes
(Disabled, Automatically, Manual)-->
                    <!--RDP-->
                    <TargetObject name="RDP port change" condition="end
with">Control\Terminal Server\WinStations\RDP-
Tcp\PortNumber</TargetObject> <!--Windows: RDP port change under Control [
https://blog.menasec.net/2019/02/of-rdp-hijacking-part1-remote-
desktop.html ]-->
                    <TargetObject name="RDP port change" condition="end
with">Control\Terminal Server\fSingleSessionPerUser</TargetObject> <!--
Windows: Allow same user to have mutliple RDP sessions, to hide from admin
being impersonated-->
                    <TargetObject name="ModifyRemoteDesktopState"
condition="end with">fDenyTSConnections</TargetObject> <!--Windows:
Attacker turning on RDP-->
                    <TargetObject condition="end
with">LastLoggedOnUser</TargetObject> <!--Windows: Changing last-logged in
user-->
                    <TargetObject name="ModifyRemoteDesktopPort"
condition="end with">RDP-tcp\PortNumber</TargetObject> <!--Windows:
Changing RDP port to evade IDS-->
                    <TargetObject condition="end
with">Services\PortProxy\v4tov4</TargetObject> <!--Windows: Changing RDP
port to evade IDS-->
                    <!--CLSID launch commands and Default File Association
changes-->
                    <TargetObject name="T1042"
condition="contains">\command\</TargetObject> <!--Windows: Sensitive sub-
key under file associations and CLSID that map to launch command-->
                    <TargetObject name="T1122"
condition="contains">\ddeexec\</TargetObject> <!--Windows: Sensitive sub-
key under file associations and CLSID that map to launch command-->
                    <TargetObject name="T1122"
condition="contains">{86C86720-42A0-1069-A2E8-08002B30309D}</TargetObject>
<!--Windows: Tooltip handler-->
                    <TargetObject name="T1042"
condition="contains">exefile</TargetObject> <!--Windows Executable
handler, to log any changes not already monitored-->
                    <!--Windows COM-->
                    <TargetObject name="T1122" condition="end
with">\InprocServer32\(Default)</TargetObject> <!--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 used by malware--
>
                  <TargetObject name="T1158" condition="end
with">\Hidden</TargetObject> <!--Windows:Explorer: Some types of malware
try to hide their hidden system files from the user, good signal event -->
                  <TargetObject name="T1158" condition="end
with">\ShowSuperHidden</TargetObject> <!--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 name="T1158" condition="end
with">\HideFileExt</TargetObject> <!--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> <!--Windows:Explorer: [
http://www.silentrunners.org/launchpoints.html ] -->
                  <TargetObject
condition="contains">Classes\AllFilesystemObjects\</TargetObject> <!--
Windows:Explorer: [ http://www.silentrunners.org/launchpoints.html ] -->
                  <TargetObject
condition="contains">Classes\Directory\</TargetObject> <!--
Windows:Explorer: [ https://stackoverflow.com/questions/1323663/windows-
shell-context-menu-option ] -->
                  <TargetObject
condition="contains">Classes\Drive\</TargetObject> <!--Windows:Explorer: [
https://stackoverflow.com/questions/1323663/windows-shell-context-menu-
option ] -->
                  <TargetObject
condition="contains">Classes\Folder\</TargetObject> <!--Windows:Explorer:
ContextMenuHandlers, DragDropHandlers, CopyHookHandlers, [
https://stackoverflow.com/questions/1323663/windows-shell-context-menu-
option ] -->
                  <TargetObject
condition="contains">Classes\PROTOCOLS\</TargetObject> <!--
Windows:Explorer: Protocol handlers-->
                  <TargetObject
condition="contains">ContextMenuHandlers\</TargetObject> <!--Windows: [
http://oalabs.openanalysis.net/2015/06/04/malware-persistence-
hkey_current_user-shell-extension-handlers/ ] -->
                  <TargetObject
condition="contains">CurrentVersion\Shell</TargetObject> <!--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\ShellExecute
Hooks</TargetObject> <!--Windows: ShellExecuteHooks-->
                  <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\ShellService
ObjectDelayLoad</TargetObject> <!--Windows: ShellExecuteHooks-->
                  <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\ShellIconOve
```

```
rlayIdentifiers</TargetObject> <!--Windows: ShellExecuteHooks-->
                    <!--AppPaths hijacking-->
                    <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\App
Paths\</TargetObject> <!--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> <!--Windows:RDP:
Note other Terminal Server run keys are handled by another wildcard
already-->
                    <!--Group Policy integrity-->
                    <TargetObject name="T1484" condition="begin
with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\GPExtensions\</TargetObject> <!--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> <!--
Windows: Wildcard, includes Winsock and Winsock2-->
                    <TargetObject condition="end
with">\ProxyServer</TargetObject> <!--Windows: System and user proxy
server-->
                    <!--Credential providers-->
                    <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\Creden
tial Provider</TargetObject> <!--Wildcard, includes Credential Providers
and Credential Provider Filters-->
                    <TargetObject name="T1101" 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</TargetObjec
t> <!--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> <!--Windows: Netsh
helper DLL [ https://attack.mitre.org/wiki/Technique/T1128 ] -->
                    <TargetObject
condition="contains">Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ProxyEnable</TargetObject> <!--Windows: Malware often disables a
web proxy for 2nd stage downloads -->
                    <!--Networking-->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order\</Target
Object> <!--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> <!--Windows: |
Credit @ion-storm -->
```

```
                    <TargetObject name="T1089" condition="end
with">\EnableFirewall</TargetObject> <!--Windows: Monitor for firewall
disablement, all firewall profiles [
https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject name="T1089" condition="end
with">\DoNotAllowExceptions</TargetObject> <!--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\Firew
allPolicy\StandardProfile\AuthorizedApplications\List</TargetObject> <!--
Windows Firewall authorized applications for all networks| Credit @ion-
storm -->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Firew
allPolicy\DomainProfile\AuthorizedApplications\List</TargetObject> <!--
Windows Firewall authorized applications for domain networks -->
                    <!--DLLs that get injected into every process at launch-
->
                    <TargetObject name="T1103" condition="begin
with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows\Appinit_Dlls\</TargetObject> <!--Windows:
Feature disabled by default [
https://attack.mitre.org/wiki/Technique/T1103 ] -->
                    <TargetObject name="T1103" condition="begin
with">HKLM\Software\Wow6432Node\Microsoft\Windows
NT\CurrentVersion\Windows\Appinit_Dlls\</TargetObject> <!--Windows:
Feature disabled by default [
https://attack.mitre.org/wiki/Technique/T1103 ] -->
                    <TargetObject condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\AppCertDlls\</TargetObject> <!--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 name="T1137"
condition="contains">Microsoft\Office\Outlook\Addins\</TargetObject> <!--
Microsoft:Office: Outlook add-ins, access to sensitive data and often
cause issues-->
                    <TargetObject name="T1137" 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
name="Context,ProtectedModeExitOrMacrosUsed"
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/ ] -->
                    <TargetObject name="Context,ContactedDomain"
condition="end with">\EnableBHO</TargetObject> <!--Microsoft:Office:
Contacted domains stored here
'HKEY_CURRENT_USER\<SID>\SOFTWARE\Microsoft\Office\16.0\Common\Internet\Se
rver Cache\<domain>\EnableBHO' -->
                    <!--IE-->
                    <TargetObject name="T1176" condition="contains">Internet
```

```
Explorer\Toolbar\</TargetObject> <!--Microsoft:InternetExplorer: Machine
and user [ Example: https://www.exterminate-it.com/malpedia/remove-
mywebsearch ] -->
                    <TargetObject name="T1176" condition="contains">Internet
Explorer\Extensions\</TargetObject> <!--Microsoft:InternetExplorer:
Machine and user [ Example: https://www.exterminate-
it.com/malpedia/remove-mywebsearch ] -->
                    <TargetObject name="T1176" 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="begin
with">HKLM\Software\Classes\CLSID\{AB8902B4-09CA-4BB6-B78D-
A8F59079A8D5}\</TargetObject> <!--Windows: Thumbnail cache autostart [
http://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-
levels-up-with-new-autostart-mechanism/ ] -->
                    <TargetObject condition="begin
with">HKLM\Software\Classes\WOW6432Node\CLSID\{AB8902B4-09CA-4BB6-B78D-
A8F59079A8D5}\</TargetObject> <!--Windows: Thumbnail cache autostart [
http://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-
levels-up-with-new-autostart-mechanism/ ] -->
                    <TargetObject condition="begin
with">HKLM\Software\Classes\CLSID\{083863F1-70DE-11d0-BD40-
00A0C911CE86}\</TargetObject> <!--Windows: DirectX instances-->
                    <TargetObject condition="begin
with">HKLM\Software\Classes\WOW6432Node\CLSID\{083863F1-70DE-11d0-BD40-
00A0C911CE86}\</TargetObject> <!--Windows: DirectX instances-->
                    <!--Install/Run 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> <!--Windows: Source folder for certain
program and component installations-->
                    <TargetObject name="Alert,Sysinternals Tool Used"
condition="end with">\EulaAccepted</TargetObject> <!--Sysinternals tool
launched. Lots of useful abilities for attackers -->
                    <!--Antivirus tampering-->
```

```
                    <TargetObject name="T1089,Tamper-Defender"
condition="end with">\DisableAntiSpyware</TargetObject> <!--
Windows:Defender: State modified via registry-->
                    <TargetObject name="T1089,Tamper-Defender"
condition="end with">\DisableAntiVirus</TargetObject> <!--
Windows:Defender: State modified via registry-->
                    <TargetObject name="T1089,Tamper-Defender"
condition="end with">\SpynetReporting</TargetObject> <!--Windows:Defender:
State modified via registry-->
                    <TargetObject name="T1089,Tamper-Defender"
condition="end with">DisableRealtimeMonitoring</TargetObject> <!--
Windows:Defender: State modified via registry-->
                    <TargetObject name="T1089,Tamper-Defender"
condition="end with">\SubmitSamplesConsent</TargetObject> <!--
Windows:Defender: State modified via registry-->
                    <TargetObject name="T1562,Tamper-Defender"
condition="begin with">HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\Exclusions\</TargetObject> <!--Windows:Defender: Exclusions in
policy key-->
                    <!--Windows UAC tampering-->
                    <TargetObject name="T1088" condition="end
with">HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Enabl
eLUA</TargetObject> <!--Detect: UAC Tampering | Credit @ion-storm -->
                    <TargetObject name="T1088" condition="end
with">HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Local
AccountTokenFilterPolicy</TargetObject> <!--Detect: UAC Tampering | Credit
@ion-storm -->
                    <!--Microsoft Security Center tampering | Credit @ion-
storm -->
                    <TargetObject name="T1089,Tamper-SecCenter"
condition="end with">HKLM\Software\Microsoft\Security
Center\</TargetObject> <!-- [
https://attack.mitre.org/wiki/Technique/T1089 ] -->
                    <TargetObject name="T1089,Tamper-SecCenter"
condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\HideSCAH
ealth</TargetObject> <!--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 name="T1138,AppCompatShim"
condition="begin with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Custom</TargetObject> <!--Windows:
AppCompat [ https://www.fireeye.com/blog/threat-research/2017/05/fin7-
shim-databases-persistence.html ] -->
                    <TargetObject name="T1138,AppCompatShim"
condition="begin with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\InstalledSDB</TargetObject> <!--Windows:
AppCompat [ https://attack.mitre.org/wiki/Technique/T1138 ] -->
                    <TargetObject
condition="contains">VirtualStore</TargetObject> <!--Windows: Registry
virtualization, something's wrong if it's in use [
https://msdn.microsoft.com/en-
us/library/windows/desktop/aa965884(v=vs.85).aspx ] -->
                    <!--Windows internals integrity monitoring-->
                    <TargetObject name="T1183,IFEO" condition="begin
with">HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File
```

```
Execution Options\</TargetObject> <!--Windows: Malware likes changing
IFEO, like adding Debugger to disable antivirus EXE-->
                    <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\WINEVT\</TargetObject
> <!--Windows: Event log system integrity and ACLs-->
                    <TargetObject name="Tamper-Safemode" condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\Safeboot\</TargetObject> <!--
Windows: Services approved to load in safe mode. Almost nothing should
ever modify this.-->
                    <TargetObject name="Tamper-Winlogon" condition="begin
with">HKLM\SYSTEM\CurrentControlSet\Control\Winlogon\</TargetObject> <!--
Windows: Providers notified by WinLogon-->
                    <TargetObject name="Context,DeviceConnectedOrUpdated"
condition="end with">\FriendlyName</TargetObject> <!--Windows: New devices
connected and remembered-->
                    <TargetObject name="Context,MsiInstallerStarted"
condition="is">HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\In
Progress\(Default)</TargetObject> <!--Windows: See when WindowsInstaller
is engaged, useful for timeline matching with other events-->
                    <TargetObject name="Tamper-Tracing" condition="begin
with">HKLM\Software\Microsoft\Tracing\RASAPI32</TargetObject> <!--Windows:
Malware sometimes disables tracing to obfuscate tracks-->
                    <TargetObject
name="Context,ProcessAccessedPrivateResource" condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\CapabilityAccessManag
er\ConsentStore\</TargetObject> <!-- Windows: Win10 tracks when and what
process uses webcam/microphone/location etc [
https://medium.com/@7a616368/can-you-track-processes-accessing-the-camera-
and-microphone-7e6885b37072 ] -->
                    <TargetObject condition="contains">\Keyboard
Layout\Preload</TargetObject> <!--Microsoft:Windows: Keyboard layout
loaded into user session [
https://renenyffenegger.ch/notes/Windows/registry/tree/HKEY_CURRENT_USER/K
eyboard-Layout/Preload/index ] | Credit @cyb3rops -->
                    <TargetObject condition="contains">\Keyboard
Layout\Substitutes</TargetObject> <!--Microsoft:Windows: Keyboard layout
loaded into user session [
https://renenyffenegger.ch/notes/Windows/registry/tree/HKEY_CURRENT_USER/K
eyboard-Layout/Preload/index ] | Credit @cyb3rops -->
                    <!--Windows inventory events-->
                    <TargetObject name="InvDB-Path" condition="end
with">\LowerCaseLongPath</TargetObject> <!-- [
https://binaryforay.blogspot.com/2017/10/amcache-still-rules-everything-
around.html ] -->
                    <TargetObject name="InvDB-Pub" condition="end
with">\Publisher</TargetObject> <!-- [
https://binaryforay.blogspot.com/2017/10/amcache-still-rules-everything-
around.html ] -->
                    <TargetObject name="InvDB-Ver" condition="end
with">\BinProductVersion</TargetObject> <!-- [
https://docs.microsoft.com/en-us/windows/privacy/basic-level-windows-
diagnostic-events-and-fields-1709 ] -->
                    <TargetObject name="InvDB-DriverVer" condition="end
with">\DriverVersion</TargetObject> <!-- [ https://df-
stream.com/2015/02/leveraging-devicecontainers-key/ ] -->
                    <TargetObject name="InvDB-DriverVer" condition="end
with">\DriverVerVersion</TargetObject> <!-- [ https://df-
```

```
stream.com/2015/02/leveraging-devicecontainers-key/ ] -->
                  <TargetObject name="InvDB-CompileTimeClaim"
condition="end with">\LinkDate</TargetObject> <!-- Compile time of EXE,
may not be reliable [ https://en.wikipedia.org/wiki/Link_time ] -->
                  <TargetObject name="InvDB"
condition="contains">Compatibility Assistant\Store\</TargetObject> <!--
Inventory -->
                  <!--Suspicious sources-->
                  <Image name="Suspicious,ImageBeginWithBackslash"
condition="end with">regedit.exe</Image> <!--Users and helpdesk staff
making system modifications -->
                  <Image name="Suspicious,ImageBeginWithBackslash"
condition="begin with">\</Image> <!--Devices and VSC shouldn't be
executing changes | Credit: @SBousseaden @ionstorm @neu5ron
@PerchedSystems [
https://twitter.com/SwiftOnSecurity/status/1133167323991486464 ] -->
            </RegistryEvent>
      </RuleGroup>

      <RuleGroup name="" groupRelation="or">
            <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.-->
            <!--NOTE:   A lot of noise can be removed by excluding
CreateKey events, which are largely innocuous-->
                  <TargetObject condition="contains">\{CAFEEFAC-
</TargetObject>
                  <EventType condition="is">CreateKey</EventType>
                  <TargetObject condition="begin
with">HKLM\COMPONENTS</TargetObject>
                  <!--Inventory noise-->
                  <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\AppModel\StateReposit
ory\Cache</TargetObject>
                  <!--Misc-->
                  <TargetObject condition="end
with">Toolbar\WebBrowser</TargetObject> <!--Microsoft:IE: Extraneous
activity-->
                  <TargetObject condition="end
with">Browser\ITBar7Height</TargetObject> <!--Microsoft:IE: Extraneous
activity, covers ShellBrowser and WebBrowser-->
                  <TargetObject condition="end
with">Browser\ITBar7Layout</TargetObject> <!--Microsoft:IE: Extraneous
activity-->
                  <TargetObject condition="end with">Internet
Explorer\Toolbar\Locked</TargetObject> <!--Windows:Explorer: Extraneous
activity-->
                  <TargetObject condition="end
with">Toolbar\WebBrowser\{47833539-D0C5-4125-9FA8-
0819E2EAAC93}</TargetObject> <!--Windows:Explorer: Extraneous activity-->
                  <TargetObject condition="end
with">}\PreviousPolicyAreas</TargetObject> <!--Windows: Remove noise from
\Winlogon\GPExtensions by svchost.exe-->
                  <TargetObject
condition="contains">\Control\WMI\Autologger\</TargetObject> <!--Windows:
Remove noise from monitoring "\Start"-->
```

```
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Services\UsoSvc\Start</TargetObject>
<!--Windows: Remove noise from monitoring "\Start"-->
                    <TargetObject condition="end
with">\Lsa\OfflineJoin\CurrentValue</TargetObject> <!--Windows: Sensitive
value during domain join-->
                    <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\</TargetObject> <!--Windows: Remove noise monitoring installations
run as system-->
                    <TargetObject
condition="contains">_Classes\AppX</TargetObject> <!--Windows: Remove
noise monitoring "Shell\open\command"--> <!--Win8+-->
                    <TargetObject condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\</T
argetObject> <!--Windows: SvcHost Noise-->
                    <!--Bootup Control noise-->
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\LsaPid</TargetObject> <!--
Windows:lsass.exe: Boot noise-->
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SspiCache</TargetObject>
<!--Windows:lsass.exe: Boot noise--> <!--Win8+-->
                    <TargetObject condition="end
with">HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Domains</TargetOb
ject> <!--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> <!--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> <!--Windows:
Remove noise from monitoring "\Start"-->
                    <TargetObject condition="end
with">\services\fhsvc\Start</TargetObject> <!--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> <!--Windows: Remove
noise from monitoring "\Start"-->
                    <TargetObject condition="end
with">\services\tunnel\Start</TargetObject> <!--Windows: Remove noise from
```

```
monitoring "\Start"-->
                    <TargetObject condition="end
with">\services\usoSvc\Start</TargetObject> <!--Windows: Remove noise from
monitoring "\Start"-->
                    <!--FileExts noise filtering-->
                    <TargetObject condition="end
with">\UserChoice\ProgId</TargetObject> <!--Windows: Remove noise from
monitoring "FileExts"--> <!--Win8+-->
                    <TargetObject condition="end
with">\UserChoice\Hash</TargetObject> <!--Windows: Remove noise from
monitoring "FileExts"--> <!--Win8+-->
                    <TargetObject condition="end
with">\OpenWithList\MRUList</TargetObject> <!--Windows: Remove noise from
monitoring "FileExts"-->
                    <TargetObject condition="contains">Shell
Extentions\Cached</TargetObject> <!--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</Targe
tObject> <!--Windows: Routinely set through Group Policy, not especially
important to log-->
                    <TargetObject condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup\0\PSScriptOrder</TargetObject> <!--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> <!--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> <!--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> <!--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> <!--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> <!--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> <!--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> <!--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> <!--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> <!--Windows:Group
Policy: Noise below the actual key while building-->
                  <TargetObject
condition="contains">\safer\codeidentifiers\0\HASHES\{</TargetObject> <!--
Windows: Software Restriction Policies. Can be used to disable security
tools, but very noisy to monitor if you use it-->
                  <!--SECTION: Office C2R-->
                  <TargetObject
condition="contains">VirtualStore\MACHINE\SOFTWARE\Microsoft\Office\ClickT
oRun\</TargetObject> <!--Microsoft: SearchProtocolHost writes to OfficeC2R
registry for Outlook, seemingly regarding mail indexing-->
                  <TargetObject condition="begin
with">HKLM\SOFTWARE\Microsoft\Office\ClickToRun\</TargetObject> <!--
Microsoft: Virtual registry for Office-->
                  <!--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-->
                  <!--WINEVT publishers noise-->
                  <TargetObject
condition="is">HKLM\Software\Microsoft\Windows\CurrentVersion\WINEVT\Publi
shers\{945a8954-c147-4acd-923f-40c45405a658}</TargetObject> <!--Windows
update-->
            </RegistryEvent>
      </RuleGroup>

      <!--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/a314f6106633fba4b70f9d6ddbee452e8f8f44a72117749c21243d
c93c7ed3ac?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">.doc</TargetFilename> <!--Office doc potentially with macro -->
                  <TargetFilename condition="end
with">.hta</TargetFilename> <!--Scripting-->
                  <TargetFilename condition="end
with">.jse</TargetFilename> <!--Registry File-->
                  <TargetFilename condition="end
with">.lnk</TargetFilename> <!--Shortcut file | Credit @ion-storm -->
                  <TargetFilename condition="end
with">.ppt</TargetFilename> <!--Office doc potentially with macros-->
                  <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">.sct</TargetFilename> <!--Scripting | Credit @bartblaze -->
                  <TargetFilename condition="end
with">.vb</TargetFilename> <!--VisualBasicScripting files-->
                  <TargetFilename condition="end
with">.vbe</TargetFilename> <!--VisualBasicScripting files-->
                  <TargetFilename condition="end
with">.vbs</TargetFilename> <!--VisualBasicScripting files-->
                  <TargetFilename condition="end
with">.wsc</TargetFilename> <!--Scripting | Credit @bartblaze -->
                  <TargetFilename condition="end
with">.wsf</TargetFilename> <!--Scripting | Credit @bartblaze -->
            </FileCreateStreamHash>

      <RuleGroup name="" groupRelation="or">
            <FileCreateStreamHash onmatch="exclude">
            </FileCreateStreamHash>
      </RuleGroup>

      <!--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-->
            <RuleGroup name="" groupRelation="or">
                  <PipeEvent onmatch="include">
                        <!-- Remote Command Execution Tools -->
                        <PipeName condition="contains
any">paexec;remcom;csexec</PipeName>
                        <!-- Password or Credential Dumpers -->
                        <PipeName condition="contains
any">\lsadump;\cachedump;\wceservicepipe</PipeName>
                        <!-- Malware -->
                        <PipeName condition="contains
any">\isapi_http;\isapi_dg;\isapi_dg2;\sdlrpc;\ahexec;\winsession;\lsassw;
\46a676ab7f179e511e30dd2dc41bd388;\9f81f59bc58452127884ce513865ed20;\e710f
28d59aa529d6792ca6ff0ca1b34;\rpchlp_3;\NamePipe_MoreWindows;\pcheap_reuse;
\gruntsvc;\583da945-62af-10e8-4902-
a8f205c72b2e;\bizkaz;\svcctl;\Posh;\jaccdpqnvbrrxlaf;\csexecsvc</PipeName>
                        <PipeName condition="contains
any">\atctl;\userpipe;\iehelper;\sdlrpc;\comnap</PipeName>
                        <!-- Cobalt Strike Pipe Names -->
                        <PipeName condition="contains all">MSSE-;-
server</PipeName>
                        <PipeName condition="begin
with">\postex_</PipeName>
                        <PipeName condition="begin
with">\postex_ssh_</PipeName>
                        <PipeName condition="begin
with">\status_</PipeName>
                        <PipeName condition="begin
with">\msagent_</PipeName>
                  </PipeEvent>
            </RuleGroup>

      <!--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-->
      <RuleGroup name="" groupRelation="or">
            <WmiEvent onmatch="exclude">
                  <!--NOTE: Using exclude with no rules means everything
will be logged-->
            </WmiEvent>
```

```
      </RuleGroup>

      <!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
            <!--EVENT 22: "Dns query"-->

            <!--NOTE:   Due to the volume of events that DNS queries
generate, some orgs may want to remove this section from their
configuration to reduce Sysmon log turnover. -->

            <!--COMMENT:      DNS logging is a very nuanced challenge in
monitoring due to event volume. Legitimate domains can be used to host
malware/C2, but lookup itself is not very informative.
                                    It's fine to exclude monitoring these
bulk low-value lookups, but at same time, you would not have a full log of
how malware communicated, potentially missing C2.
                                    This section of Sysmon configuration
will require your full judgement and knowledge of your org's priorities.
There is no correct answer.-->

            <!--OPERATIONS:   Chrome and Firefox prefetch DNS lookups, or
use alternate DNS lookup methods Sysmon won't capture. You need to turn
these off.
                                    Search for Group Policy for these
browsers to configure this.-->

            <!--OPERATIONS:   Most DNS traffic is web advertising. To
significantly reduce DNS queries and malware ads, enable client-side
advertising filtering via Group Policy. This is easy.
                        Internet Explorer:
https://decentsecurity.com/adblocking-for-internet-explorer-deployment/
                        Chrome: https://decentsecurity.com/ublock-for-
google-chrome-deployment/
                        Firefox: ToDo
                                    Also note, this configuration is
designed for United States computers. Your country's users will may need
customization to reduce noise.
                  -->

            <!--CONFIG: DNS poisoning is an issue during threat
investigations. Try to only exclude ROUTINE system-level queries you know
are strongly validated with HTTPS or code signing.-->
            <!--CONFIG: If you exclude microsoft.com, someone could
register malware-microsoft.com and it wouldn't be logged. Use "END WITH"
with leading . or "IS" operators.-->
            <!--CONFIG: Be very specific in exclusions. Threat actors use
legitimate services, too. Dont exclude all of AWS or Azure or Google or
CDNs!-->
            <!--CONFIG: Popularity data: [ http://s3-us-west-
1.amazonaws.com/umbrella-static/index.html ] [
https://better.fyi/trackers/alexa-top-500-news/ ] -->

            <!--CRITICAL:     Do NOT exclude "wpad" lookups. This is a
MitM vector routinely used by attackers. Disable WPAD or enforce client-
side DNSSEC for AD domain lookups.-->
            <!--CRITICAL:     Do NOT exclude IPv6 lookups.-->

            <!--DATA: RuleName, UtcTime, ProcessGuid, ProcessId,
```

```
QueryName, QueryType, QueryStatus, QueryResults (can't filter on)-->

            <!--BELOW: These domains should not be excluded at the top
level. Be specific if you want to reduce noise under them.-->
            <!-- Rejected: .cloudapp.net, customer content [
https://blogs.technet.microsoft.com/ptsblog/2012/06/18/security-
consideration-when-using-cloudapp-net-domain-as-production-environment-in-
windows-azure/ ] -->
            <!-- Rejected: .googleapis.com, customer content [
https://www.zdnet.com/article/this-business-email-scam-spreads-trojans-
through-google-cloud-storage/ ] -->
            <!-- Rejected: .cloudfront.net, customer content -->
            <!-- Rejected: .windows.net, customer content -->
            <!-- Rejected: *github.com, customer content, including open-
source malware components -->

      <RuleGroup name="" groupRelation="or">
            <DnsQuery onmatch="exclude">
                  <!--Network noise-->
                  <QueryName condition="end with">.arpa.</QueryName> <!--
Design decision to not log reverse DNS lookups. You will need to decide.--
>
                  <QueryName condition="end with">.arpa</QueryName> <!--
Design decision to not log reverse DNS lookups. You will need to decide.--
>
                  <QueryName condition="end
with">.msftncsi.com</QueryName> <!--Microsoft proxy detection | Microsoft
default exclusion-->
                  <QueryName condition="is">..localmachine</QueryName>
                  <QueryName condition="is">localhost</QueryName>
                  <!--Microsoft-->
                  <QueryName condition="end with">-
pushp.svc.ms</QueryName> <!--Microsoft: Doesn't appear to host customer
content or subdomains-->
                  <QueryName condition="end with">.b-
msedge.net</QueryName> <!--Microsoft: Doesn't appear to host customer
content or subdomains-->
                  <QueryName condition="end with">.bing.com</QueryName>
<!-- Microsoft | Microsoft default exclusion -->
                  <QueryName condition="end with">.hotmail.com</QueryName>
<!--Microsoft | Microsoft default exclusion-->
                  <QueryName condition="end with">.live.com</QueryName>
<!--Microsoft | Microsoft default exclusion-->
                  <QueryName condition="end with">.live.net</QueryName>
<!--Microsoft | Microsoft default exclusion-->
                  <QueryName condition="end with">.s-
microsoft.com</QueryName> <!--Microsoft-->
                  <QueryName condition="end
with">.microsoft.com</QueryName> <!--Microsoft | Microsoft default
exclusion-->
                  <QueryName condition="end
with">.microsoftonline.com</QueryName> <!--Microsoft | Microsoft default
exclusion-->
                  <QueryName condition="end
with">.microsoftstore.com</QueryName> <!--Microsoft | Microsoft default
exclusion-->
                  <QueryName condition="end with">.ms-
```

```
acdc.office.com</QueryName> <!--Microsoft: Doesn't appear to host customer
content or subdomains-->
                    <QueryName condition="end with">.msedge.net</QueryName>
<!--Microsoft: Doesn't appear to host customer content or subdomains-->
                    <QueryName condition="end with">.msn.com</QueryName> <!-
-Microsoft | Microsoft default exclusion-->
                    <QueryName condition="end with">.msocdn.com</QueryName>
<!--Microsoft-->
                    <QueryName condition="end with">.skype.com</QueryName>
<!--Microsoft | Microsoft default exclusion-->
                    <QueryName condition="end with">.skype.net</QueryName>
<!--Microsoft | Microsoft default exclusion-->
                    <QueryName condition="end with">.windows.com</QueryName>
<!--Microsoft-->
                    <QueryName condition="end
with">.windows.net.nsatc.net</QueryName> <!--Microsoft-->
                    <QueryName condition="end
with">.windowsupdate.com</QueryName> <!--Microsoft-->
                    <QueryName condition="end
with">.xboxlive.com</QueryName> <!--Microsoft-->
                    <QueryName condition="is">login.windows.net</QueryName>
<!--Microsoft-->
                    <Image condition="begin
with">C:\ProgramData\Microsoft\Windows Defender\Platform\</Image> <!--
Microsoft: https://docs.microsoft.com/en-us/windows/security/threat-
protection/microsoft-defender-atp/network-protection -->
                    <!--Microsoft:Office365/AzureAD-->
                    <QueryName condition="end
with">.activedirectory.windowsazure.com</QueryName> <!--Microsoft:
AzureAD-->
                    <QueryName condition="end
with">.aria.microsoft.com</QueryName> <!--Microsoft: OneDrive/SharePoint--
>
                    <QueryName condition="end with">.msauth.net</QueryName>
                    <QueryName condition="end
with">.msftauth.net</QueryName>
                    <QueryName condition="end with">.office.net</QueryName>
<!--Microsoft: Office-->
                    <QueryName condition="end
with">.opinsights.azure.com</QueryName> <!--Microsoft: AzureAD/InTune
client event monitoring-->
                    <QueryName condition="end
with">.res.office365.com</QueryName> <!--Microsoft: Office-->
                    <QueryName condition="is">acdc-
direct.office.com</QueryName> <!--Microsoft: Office-->
                    <QueryName condition="is">atm-fp-
direct.office.com</QueryName> <!--Microsoft: Office-->
                    <QueryName
condition="is">loki.delve.office.com</QueryName> <!--Microsoft: Office-->
                    <QueryName
condition="is">management.azure.com</QueryName> <!--Microsoft:
AzureAD/InTune-->
                    <QueryName
condition="is">messaging.office.com</QueryName> <!--Microsoft: Office-->
                    <QueryName
condition="is">outlook.office365.com</QueryName> <!--Microsoft: Protected
by HSTS-->
```

```
                    <QueryName condition="is">portal.azure.com</QueryName>
<!--Microsoft: AzureAD/InTune-->
                    <QueryName
condition="is">protection.outlook.com</QueryName> <!--Microsoft: Office-->
                    <QueryName
condition="is">substrate.office.com</QueryName> <!--Microsoft: Office-->
                    <QueryName condition="end
with">.measure.office.com</QueryName> <!--Microsoft: Office-->
                    <!--3rd-party applications-->
                    <QueryName condition="end with">.adobe.com</QueryName>
<!--Adobe-->
                    <QueryName condition="end with">.adobe.io</QueryName>
<!--Adobe-->
                    <QueryName condition="end with">.mozaws.net</QueryName>
<!--Mozilla-->
                    <QueryName condition="end with">.mozilla.com</QueryName>
<!--Mozilla-->
                    <QueryName condition="end with">.mozilla.net</QueryName>
<!--Mozilla-->
                    <QueryName condition="end with">.mozilla.org</QueryName>
<!--Mozilla-->
                    <QueryName condition="end with">.spotify.com</QueryName>
<!--Spotify-->
                    <QueryName condition="end
with">.spotify.map.fastly.net</QueryName> <!--Spotify-->
                    <QueryName condition="end with">.wbx2.com</QueryName>
<!--Webex-->
                    <QueryName condition="end with">.webex.com</QueryName>
<!--Webex-->
                    <QueryName
condition="is">clients1.google.com</QueryName> <!--Google-->
                    <QueryName
condition="is">clients2.google.com</QueryName> <!--Google-->
                    <QueryName
condition="is">clients3.google.com</QueryName> <!--Google-->
                    <QueryName
condition="is">clients4.google.com</QueryName> <!--Google-->
                    <QueryName
condition="is">clients5.google.com</QueryName> <!--Google-->
                    <QueryName
condition="is">clients6.google.com</QueryName> <!--Google-->
                    <QueryName
condition="is">safebrowsing.googleapis.com</QueryName> <!--Google-->
                    <!--Goodlist CDN-->
                    <QueryName condition="end with">.akadns.net</QueryName>
<!--AkamaiCDN, extensively used by Microsoft | Microsoft default
exclusion-->
                    <QueryName condition="end with">.netflix.com</QueryName>
                    <QueryName condition="end
with">aspnetcdn.com</QueryName> <!--Microsoft [
https://docs.microsoft.com/en-us/aspnet/ajax/cdn/overview ]-->
                    <QueryName
condition="is">ajax.googleapis.com</QueryName>
                    <QueryName
condition="is">cdnjs.cloudflare.com</QueryName> <!--Cloudflare: Hosts
popular javascript libraries-->
                    <QueryName
```

```
condition="is">fonts.googleapis.com</QueryName> <!--Google fonts-->
                    <QueryName condition="end with">.typekit.net</QueryName>
<!--Adobe fonts-->
                    <QueryName
condition="is">cdnjs.cloudflare.com</QueryName>
                    <QueryName condition="end
with">.stackassets.com</QueryName> <!--Stack Overflow-->
                    <QueryName condition="end
with">.steamcontent.com</QueryName>
                    <QueryName condition="is">play.google.com</QueryName>
                    <QueryName condition="is">content-
autofill.googleapis.com</QueryName>
                    <!--Web resources-->
                    <QueryName condition="end with">.disqus.com</QueryName>
<!--Microsoft default exclusion-->
                    <QueryName condition="end
with">.fontawesome.com</QueryName>
                    <QueryName condition="is">disqus.com</QueryName> <!--
Microsoft default exclusion-->
                    <!--Ads-->
                    <QueryName condition="end with">.1rx.io</QueryName> <!--
Ads-->
                    <QueryName condition="end with">.2mdn.net</QueryName>
<!--Ads: Google | Microsoft default exclusion-->
                    <QueryName condition="end with">.3lift.com</QueryName>
<!--Ads-->
                    <QueryName condition="end
with">.adadvisor.net</QueryName> <!--Ads: Neustar [
https://better.fyi/trackers/adadvisor.net/ ] -->
                    <QueryName condition="end with">.adap.tv</QueryName> <!-
-Ads:AOL | Microsoft default exclusion [
https://www.crunchbase.com/organization/adap-tv ] -->
                    <QueryName condition="end with">.addthis.com</QueryName>
<!--Ads:Oracle | Microsoft default exclusion [
https://en.wikipedia.org/wiki/AddThis ] -->
                    <QueryName condition="end with">.adform.net</QueryName>
<!--Ads-->
                    <QueryName condition="end with">.adnxs.com</QueryName>
<!--Ads: AppNexus | Microsoft default exclusion-->
                    <QueryName condition="end with">.adroll.com</QueryName>
<!--Ads-->
                    <QueryName condition="end with">.adrta.com</QueryName>
<!--Ads-->
                    <QueryName condition="end
with">.adsafeprotected.com</QueryName> <!--Ads-->
                    <QueryName condition="end with">.adsrvr.org</QueryName>
<!--Ads-->
                    <QueryName condition="end
with">.adsymptotic.com</QueryName> <!--Ads-->
                    <QueryName condition="end
with">.advertising.com</QueryName> <!--Ads | Microsoft default exclusion--
>
                    <QueryName condition="end with">.agkn.com</QueryName>
<!--Ads | [ https://www.home.neustar/privacy ] -->
                    <QueryName condition="end with">.amazon-
adsystem.com</QueryName> <!--Ads-->
                    <QueryName condition="end with">.amazon-
```

```
adsystem.com</QueryName> <!--Ads-->
                    <QueryName condition="end
with">.analytics.yahoo.com</QueryName> <!--Ads:Yahoo-->
                    <QueryName condition="end with">.aol.com</QueryName> <!-
-Ads | Microsoft default exclusion -->
                    <QueryName condition="end with">.betrad.com</QueryName>
<!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end
with">.bidswitch.net</QueryName> <!--Ads-->
                    <QueryName condition="end
with">.casalemedia.com</QueryName> <!--Ads | Microsoft default exclusion--
>
                    <QueryName condition="end
with">.chartbeat.net</QueryName> <!--Ads | Microsoft default exclusion [
https://better.fyi/trackers/chartbeat.com/ ]-->
                    <QueryName condition="end with">.cnn.com</QueryName> <!-
- Microsoft default exclusion-->
                    <QueryName condition="end
with">.convertro.com</QueryName> <!--Ads:Verizon-->
                    <QueryName condition="end with">.criteo.com</QueryName>
<!--Ads [ https://better.fyi/trackers/criteo.com/ ] -->
                    <QueryName condition="end with">.criteo.net</QueryName>
<!--Ads [ https://better.fyi/trackers/criteo.com/ ] -->
                    <QueryName condition="end
with">.crwdcntrl.net</QueryName> <!--Ads: Lotame [
https://better.fyi/trackers/crwdcntrl.net/ ] -->
                    <QueryName condition="end with">.demdex.net</QueryName>
<!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end with">.domdex.com</QueryName>
                    <QueryName condition="end with">.dotomi.com</QueryName>
<!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end
with">.doubleclick.net</QueryName> <!--Ads:Conversant | Microsoft default
exclusion [ https://www.crunchbase.com/organization/dotomi ] -->
                    <QueryName condition="end
with">.doubleverify.com</QueryName> <!--Ads: Google-->
                    <QueryName condition="end with">.emxdgt.com</QueryName>
<!--Ads: EMX-->
                    <QueryName condition="end
with">.everesttech.net</QueryName> <!--Ads | [
https://better.fyi/trackers/everesttech.net/ ] -->
                    <QueryName condition="end
with">.exelator.com</QueryName> <!--Ads:Nielson Marketing Cloud-->
                    <QueryName condition="end with">.google-
analytics.com</QueryName> <!--Ads:Google | Microsoft default exclusion-->
                    <QueryName condition="end
with">.googleadservices.com</QueryName> <!--Google-->
                    <QueryName condition="end
with">.googlesyndication.com</QueryName> <!--Ads:Google, sometimes called
during malicious ads, but not directly responsible | Microsoft default
exclusion [ https://www.hackread.com/wp-
content/uploads/2018/06/Bitdefender-Whitepaper-Zacinlo.pdf ]-->
                    <QueryName condition="end
with">.googletagmanager.com</QueryName> <!--Google-->
                    <QueryName condition="end
with">.googlevideo.com</QueryName> <!--Google | Microsoft default
exclusion-->
```

```
                    <QueryName condition="end with">.gstatic.com</QueryName>
<!--Google | Microsoft default exclusion-->
                    <QueryName condition="end with">.gvt1.com</QueryName>
<!--Google-->
                    <QueryName condition="end with">.gvt2.com</QueryName>
<!--Google-->
                    <QueryName condition="end with">.ib-ibi.com</QueryName>
<!--Ads: Offerpath [ https://better.fyi/trackers/ib-ibi.com/ ] -->
                    <QueryName condition="end with">.jivox.com</QueryName>
<!--Ads-->
                    <QueryName condition="end with">.krxd.net</QueryName>
<!--Ads-->
                    <QueryName condition="end with">.lijit.com</QueryName>
<!--Ads-->
                    <QueryName condition="end with">.mathtag.com</QueryName>
<!--Microsoft default exclusion-->
                    <QueryName condition="end with">.moatads.com</QueryName>
<!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end
with">.moatpixel.com</QueryName> <!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end with">.mookie1.com</QueryName>
<!--Ads-->
                    <QueryName condition="end
with">.myvisualiq.net</QueryName> <!--Ads-->
                    <QueryName condition="end with">.netmng.com</QueryName>
<!--Ads-->
                    <QueryName condition="end with">.nexac.com</QueryName>
<!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end with">.openx.net</QueryName>
<!--Ads-->
                    <QueryName condition="end
with">.optimizely.com</QueryName> <!--Ads-->
                    <QueryName condition="end
with">.outbrain.com</QueryName> <!--Ads-->
                    <QueryName condition="end with">.pardot.com</QueryName>
<!--Ads-->
                    <QueryName condition="end with">.phx.gbl</QueryName> <!-
-Ads | Microsoft default exclusion-->
                    <QueryName condition="end
with">.pinterest.com</QueryName> <!--Pinerest-->
                    <QueryName condition="end
with">.pubmatic.com</QueryName> <!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end
with">.quantcount.com</QueryName>
                    <QueryName condition="end
with">.quantserve.com</QueryName>
                    <QueryName condition="end with">.revsci.net</QueryName>
<!--Ads:Omniture | Microsoft default exclusion-->
                    <QueryName condition="end with">.rfihub.net</QueryName>
<!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end with">.rlcdn.com</QueryName>
<!--Ads: Rapleaf [ https://better.fyi/trackers/rlcdn.com/ ] -->
                    <QueryName condition="end
with">.rubiconproject.com</QueryName> <!--Ads: Rubicon Project | Microsoft
default exclusion [ https://better.fyi/trackers/rubiconproject.com/ ] -->
                    <QueryName condition="end with">.scdn.co</QueryName> <!-
-Spotify-->
```

```
                    <QueryName condition="end
with">.scorecardresearch.com</QueryName> <!--Ads: Comscore | Microsoft
default exclusion-->
                    <QueryName condition="end with">.serving-
sys.com</QueryName> <!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end
with">.sharethrough.com</QueryName> <!--Ads-->
                    <QueryName condition="end with">.simpli.fi</QueryName>
                    <QueryName condition="end
with">.sitescout.com</QueryName> <!--Ads-->
                    <QueryName condition="end
with">.smartadserver.com</QueryName> <!--Ads-->
                    <QueryName condition="end with">.snapads.com</QueryName>
<!--Ads-->
                    <QueryName condition="end
with">.spotxchange.com</QueryName> <!--Ads-->
                    <QueryName condition="end with">.taboola.com</QueryName>
<!--Ads:Taboola-->
                    <QueryName condition="end
with">.taboola.map.fastly.net</QueryName> <!--Ads:Taboola-->
                    <QueryName condition="end with">.tapad.com</QueryName>
                    <QueryName condition="end with">.tidaltv.com</QueryName>
<!--Ads: Videology [ https://better.fyi/trackers/tidaltv.com/ ] -->
                    <QueryName condition="end
with">.trafficmanager.net</QueryName> <!--Ads | Microsoft default
exclusion-->
                    <QueryName condition="end
with">.tremorhub.com</QueryName> <!--Ads-->
                    <QueryName condition="end
with">.tribalfusion.com</QueryName> <!--Ads: Exponential [
https://better.fyi/trackers/tribalfusion.com/ ] -->
                    <QueryName condition="end with">.turn.com</QueryName>
<!--Ads | Microsoft default exclusion [
https://better.fyi/trackers/turn.com/ ] -->
                    <QueryName condition="end with">.twimg.com</QueryName>
<!--Ads | Microsoft default exclusion-->
                    <QueryName condition="end with">.tynt.com</QueryName>
<!--Ads-->
                    <QueryName condition="end with">.w55c.net</QueryName>
<!--Ads:dataxu-->
                    <QueryName condition="end with">.ytimg.com</QueryName>
<!--Google-->
                    <QueryName condition="end with">.zorosrv.com</QueryName>
<!--Ads:Taboola-->
                    <QueryName condition="is">1rx.io</QueryName> <!--Ads-->
                    <QueryName
condition="is">adservice.google.com</QueryName> <!--Google-->
                    <QueryName condition="is">ampcid.google.com</QueryName>
<!--Google-->
                    <QueryName
condition="is">clientservices.googleapis.com</QueryName> <!--Google-->
                    <QueryName
condition="is">googleadapis.l.google.com</QueryName> <!--Google-->
                    <QueryName
condition="is">imasdk.googleapis.com</QueryName> <!--Google [
https://developers.google.com/interactive-media-ads/docs/sdks/html5/ ] -->
                    <QueryName condition="is">l.google.com</QueryName> <!--
```

```
Google-->
                    <QueryName condition="is">ml314.com</QueryName> <!--Ads-
->
                    <QueryName condition="is">mtalk.google.com</QueryName>
<!--Google-->
                    <QueryName
condition="is">update.googleapis.com</QueryName> <!--Google-->
                    <QueryName
condition="is">www.googletagservices.com</QueryName> <!--Google-->
                    <!--SocialNet-->
                    <QueryName condition="end with">.pscp.tv</QueryName> <!-
-Twitter:Periscope-->
                    <!--OSCP/CRL Common-->
                    <QueryName condition="end
with">.amazontrust.com</QueryName>
                    <QueryName condition="end
with">.digicert.com</QueryName>
                    <QueryName condition="end
with">.globalsign.com</QueryName>
                    <QueryName condition="end
with">.globalsign.net</QueryName>
                    <QueryName condition="end with">.intel.com</QueryName>
                    <QueryName condition="end with">.symcb.com</QueryName>
<!--Digicert-->
                    <QueryName condition="end with">.symcd.com</QueryName>
<!--Digicert-->
                    <QueryName condition="end with">.thawte.com</QueryName>
                    <QueryName condition="end
with">.usertrust.com</QueryName>
                    <QueryName condition="end
with">.verisign.com</QueryName>
                    <QueryName condition="end
with">ocsp.identrust.com</QueryName>
                    <QueryName condition="end with">pki.goog</QueryName>
                    <QueryName condition="is">msocsp.com</QueryName> <!--
Microsoft:OCSP-->
                    <QueryName condition="is">ocsp.comodoca.com</QueryName>
                    <QueryName condition="is">ocsp.entrust.net</QueryName>
                    <QueryName condition="is">ocsp.godaddy.com</QueryName>
                    <QueryName condition="is">ocsp.int-
x3.letsencrypt.org</QueryName>
                    <QueryName condition="is">ocsp.msocsp.com</QueryName>
<!--Microsoft:OCSP-->
                    <QueryName condition="end with">pki.goog</QueryName>
                    <QueryName condition="is">ocsp.godaddy.com</QueryName>
                    <QueryName condition="end
with">amazontrust.com</QueryName>
                    <QueryName condition="is">ocsp.sectigo.com</QueryName>
                    <QueryName condition="is">pki-
goog.l.google.com</QueryName>
                    <QueryName condition="end
with">.usertrust.com</QueryName>
                    <QueryName condition="is">ocsp.comodoca.com</QueryName>
                    <QueryName condition="is">ocsp.verisign.com</QueryName>
                    <QueryName condition="is">ocsp.entrust.net</QueryName>
                    <QueryName condition="end
with">ocsp.identrust.com</QueryName>
```

```
                  <QueryName
condition="is">status.rapidssl.com</QueryName>
                  <QueryName condition="is">status.thawte.com</QueryName>
                  <QueryName condition="is">ocsp.int-
x3.letsencrypt.org</QueryName>
            </DnsQuery>
      </RuleGroup>

      <!--SYSMON EVENT ID 23 : FILE DELETE [FileDelete]-->
            <!--EVENT 22: "File Delete"-->
            <!--COMMENT:      Sandbox usage. When a program signals to
Windows a file should be deleted or wiped, Sysmon may be able to capture
it.
                  [
https://isc.sans.edu/forums/diary/Sysmon+and+File+Deletion/26084/ ]
            -->

            <!--DATA: RuleName, UtcTime, ProcessGuid, ProcessId, User,
Image, TargetFilename, Hashes, IsExecutable, Archived -->

      <!--
      <RuleGroup name="" groupRelation="or">
            <ClipboardChange onmatch="include">
            </ClipboardChange>
      </RuleGroup>
      -->

      <!--SYSMON EVENT ID 24 : CLIPBOARD EVENT MONITORING
[ClipboardChange]-->
            <!--EVENT 24: "Clipboard changed"-->
            <!--COMMENT:      Sandbox usage.  Sysmon can capture the
contents of clipboard events.
                  An  example of what could be a production usage on
restricted desktops is provided below, but it is commented-out. -->

            <!--DATA: EventType, UtcTime, ProcessGuid, ProcessId, Image,
Session, ClientInfo, Hashes, Archived -->

      <!--
      <RuleGroup name="" groupRelation="or">
            <ClipboardChange onmatch="include">
                  <Image condition="end with">wscript.exe</Image>
                  <Image condition="end with">cscript.exe</Image>
                  <Image condition="end with">powershell.exe</Image>
                  <Image condition="end with">rdpclip.exe</Image>
            </ClipboardChange>
      </RuleGroup>
      -->

      <!--SYSMON EVENT ID 25 : PROCESS TAMPERING [ProcessTampering]-->
            <!--EVENT 25: "Process Tampering"-->
            <!--COMMENT:      This event is generated when a process image
is changed from an external source, such as a different process.
                  This may or may not provide value in your environment as
it requires tuning and a SIEM to correlate the ProcessGuids.
                  [ https://medium.com/falconforce/sysmon-13-process-
tampering-detection-820366138a6c ] -->
```

```
            <!--DATA: EventType, RuleName, UtcTime, ProcessGuid,
ProcessId, Image, Type -->

      <!--
      <RuleGroup name="" groupRelation="or">
            <ProcessTampering onmatch="exclude">
                  <Image condition="begin with">C:\Program Files
(x86)\Microsoft\Edge\Application\</Image>
            </ProcessTampering>
      </RuleGroup>
      -->

      <!--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>
```