Σχολή Θετικών Επιστημών & Τεχνολογίας

Πληροφορική

Προστασία και Ασφάλεια ΣυστημάτωνΥπολογιστών (ΠΛΗ-35)
2η Γραπτή Εργασία 2021-22

Καταγραφή συμβάντων και αξιοποίησή τους για την εντοπισμό ψηφιακών πειστηρίων για κυβερνοεπιθέσεις

Καραγκούνης Λεωνίδας Χρήστος ΑΜ: 114163
Τμήμα: ΗΛΕ-42, ΣΕΠ Μαυρίδης Ιωάννης

Πίνακας Περιεχομένων

Πίνακας Εικόνων

1. Εισαγωγή

Η αδυναμία παρακολούθησης, απόκρισης και διάγνωσης παραβιάσεων στο συνεχώς αυξανόμενο αριθμό μεμονωμένων συσκευών και δικτύων που προστίθενται στα σημερινά Πληροφοριακά Συστήματα (Information Systems) αποτελεί σημαντικό πρόβλημα ασφάλειας. Από έρευνα έχει παρατηρηθεί ότι το 80% μιας επίθεσης δαπανάται σε πλευρική κίνηση (lateral movement) κατά την οποία ο επιτιθέμενος προσπαθεί να επιτύχει κλιμάκωση προνομίων (privilege escalation) απαριθμώντας το σύστημα (system enumeration) (Smokescreen, 2020). Η συλλογή και ανάλυση αρχείων καταγραφής (logs) είναι μια σημαντική μέθοδος για τον εντοπισμό εισβολέων σε ένα δίκτυο.

Η παρούσα εργασία αποτελεί μια σύντομη μελέτη σε θέματα ψηφιακής εγκληματολογίας και ανταπόκρισης περιστατικών (Digital Forensics and Incident Response - DFIR), το σύστημα καταγραφής των Windows, το εργαλείο Sysmon και πως αρχεία καταγραφής μπορούν να αξιοποιηθούν για τον εντοπισμό ιχνών που μπορεί να έχει αφήσει πίσω του ένας εισβολέας κατά τη διάρκεια μιας κυβερνοεπίθεσης δίνοντας ως παράδειγμα την ανάλυση ενός αρχείου καταγραφής μιας επίθεσης. Τέλος αναγράφονται τα συμπεράσματα που εξήχθησαν κατα την εκπόνηση της εργασίας.

2. Υπόβαθρο

2.1 Ψηφιακή εγκληματολογία

Η ψηφιακή εγκληματολογία είναι κλάδος της εγκληματολογικής επιστήμης που χρησιμοποιεί επιστημονικές μεθόδους για τη συλλογή, τεκμηρίωση και παρουσίαση ψηφιακών αποδεικτικών στοιχείων με σκοπό τη χρήση τους στην εξιχνίαση εγκλημάτων (Hassan, 2019, pp.2–3). Αρχικά η ορολογία ήταν συνώνυμη με την εγκληματολογία υπολογιστών αλλά καθώς σήμερα μια επιθετική ενέργεια δεν περιορίζεται μόνο σε αυτούς, η ψηφιακή εγκληματολογία χωρίζεται σε πέντε κατηγορίες ανάλογα με την κατηγορία του μέσου:

- Εγκληματολογία υπολογιστών (computer forensics)
- Εγκληματολογία δικτύων (network forensics)
- Εγκληματολογία κινητής τηλεφωνίας (mobile forensics)
- Εγκληματολογία ανάλυσης δεδομένων (data analysis forensics)
- Εγκληματολογία βάσεων δεδομένων (database forensics)

Καθώς η διεξαγωγή μιας έρευνας είναι συνήθως μια αρκετά πολύπλοκη διαδικασία, ακολουθείται ένα μοντέλο διαδικασιών για την ομαλή εξέλιξή της, το οποίο προβλέπει τέσσερα στάδια:

1. Συλλογή πειστηρίων (Collection).
2. Εξέταση συλλεχθέντων πειστηρίων (Examination).
3. Αξιολόγηση των αποτελεσμάτων της εξέτασης και συσχέτιση τους με την υπόθεση (Analysis).
4. Παρουσίαση της εργασίας για νομική χρήση (Reporting).

2.2 Ανταπόκριση Περιστατικών

Ας ξεκινήσουμε εξηγώντας δύο βασικές έννοιες: συμβάν (event) και περιστατικό (incident). Συμβάν είναι κάθε παρατηρίσιμο γεγονός σε ένα σύστημα ή δίκτυο ανεξαρτήτου συνεπειών. Περιστατικό είναι η παραβίαση ή η άμεση απειλή παραβίασης των πολιτικών ασφάλειας υπολογιστών, των πολιτικών ορθής χρήσης ή των τυποποιημένων πρακτικών ασφάλειας (Cichonski et al., 2012).

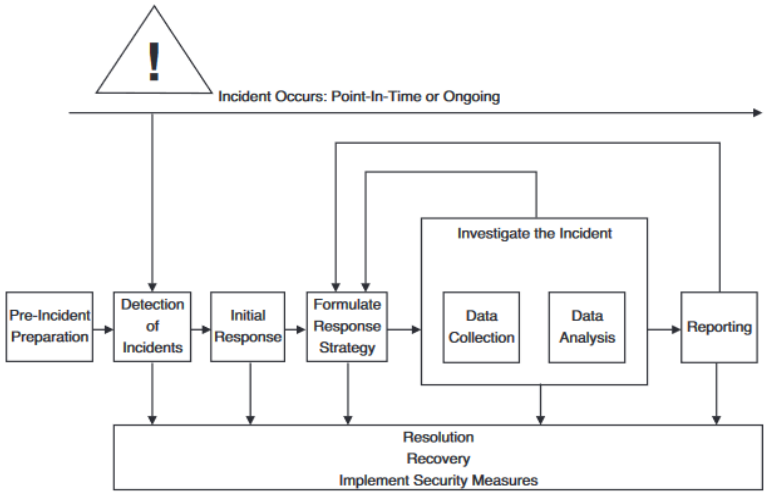
Σε έναν οργανισμό δημιουργούνται έως και εκατομμύρια συμβάντα κάθε μέρα. Όταν ένα συμβάν μετατραπεί σε περιστατικό[1], ο οργανισμός πρέπει να αντιδράσει έγκαιρα και αποτελεσματικά χρησιμοποιώντας ένα συστηματικό και καλά οργανωμένο πλάνο βασισμένο σε μεθόδους Ψηφιακής Εγκληματολογίας για την αντιμετώπισή του. Ανάλογα με την προτεραιότητα με την οποία αντιμετωπίζονται τα περιστατικά συνήθως ταξινομούνται με βάση τον επείγοντα χαρακτήρα (urgency) και τον αντίκτυπο (impact) που έχουν (Εικόνα 1). Ο επείγων χαρακτήρας καθορίζεται από τον τύπο της επίθεσης, ενώ ο αντίκτυπος καθορίζεται από το επηρεαζόμενο σύστημα και τις συνέπειες που έχει στις λειτουργίες του οργανισμού.

Impact / Urgency	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

Εικόνα 1. Ταξινόμηση περιστατικών

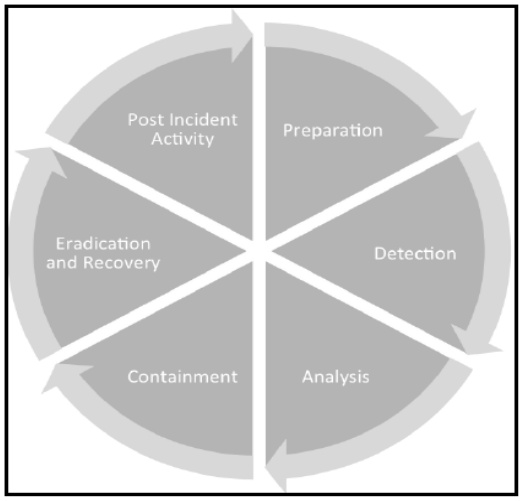
Έτσι λοιπόν η Ανταπόκριση Περιστατικών ορίζεται ως η διαδικασία (Εικόνα 2) με την οποία ένας οργανισμός διαχειρίζεται μια κυβερνοεπίθεση, συμπεριλαμβανομένου του τρόπου με τον οποίο διαχειρίζεται τις συνέπειές της. Για την έγκαιρη και αποτελεσματική αντιμετώπιση ενός περιστατικού η διαδικασία περατώνεται από την Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας Υπολογιστών (Computer Security Incident Response Team, CSIRT), η οποία αποτελείται από ειδικούς ασφαλείας με νομική και τεχνική εκπαίδευση (Freiling and Schwittay, 2007; Lord, 2015).

[1] Το τι αποτελεί περιστατικό μπορεί να διαφέρει και ο ορισμός του περιλαμβάνεται στο σχέδιο αντιμετώπισης περιστατικών που έχει κάθε οργανισμός.



Εικόνα 2 Διαδικασία Αντιμετώπισης Περιστατικών (Freiling and Schwittay, 2007)

Η διαδικασία αντιμετώπισης περιστατικών χωρίζεται σε έξι διακριτές φάσεις (Εικόνα 3) (Johansen, 2017, pp. 7-10):



Εικόνα 3. Αντιμετώπιση Περιστατικών Φάσεις (Johansen, 2017, p.7)

- **Προετοιμασία (Preparation)**. Περιλαμβάνει διαθέσιμους πόρους και σχέδια για την αντιμετώπιση περιστατικού, συμπεριλαμβανομένης διεξαγωγής ασκήσεων εξοικείωσης του προσωπικού με τη διαδικασία.
- **Ανίχνευση (Detection)**. Παρατήρηση συνόλου συμβάντων που ενδεχομένως υποδεικνύει κακόβουλη δραστηριότητα.

- **Ανάλυση (Analysis)**. Συλλογή πειστηρίων και ανάλυση τους με σκοπό τον προσδιορισμό της αιτίας του περιστατικού και την ανασύνθεση των ενεργειών των επιτιθέμενων.
- **Περιορισμός (Containment)**. Περιορισμός επιτιθέμενων στα εκτεθειμένα συστήματα και αποτροπή πρόσβασής τους σε περισσότερα συστήματα του οργανισμού.
- **Εξολόθρευση και ανάκτηση (Eradication and recovery)**. Αφαίρεση επιτιθέμενων από τα συστήματα του οργανισμού, καθαρισμός εγκατεστημένου κακόβουλου λογισμικού, επαναφορά δεδομένων, επιδιόρθωση βλαβών και ευπαθειών που εκμεταλλεύτηκαν οι επιτιθέμενοι και επαναφορά συστημάτων σε λειτουργία.
- **Δραστηριότητα μετά το περιστατικό (Post-incident activity)**. Διεξάγεται ενημέρωση αρμόδιων φορέων του οργανισμού για το περιστατικό και τις ενέργειες που διεξήχθησαν για την αντιμετώπισή του και συντάσσεται λεπτομερή γραπτή αναφορά. Το συγκεκριμένο βήμα είναι ίσως από τα πιο σημαντικά της διαδικασίας καθώς η συλλογή των πληροφοριών και η καταγραφή της αντιμετώπισης δίνει στον οργανισμό την δυνατότητα να είναι πιο αποτελεσματικός σε μελλοντικές παρόμοιες επιθέσεις.

3. Περιγραφή λύσεων

3.1 Σύστημα καταγραφής των Windows (Windows event logging)

3.1.1 Λειτουργία

Το σύστημα καταγραφής των Windows είναι μια λεπτομερή καταγραφή σημαντικών συμβάντων συστήματος, ασφάλειας και εφαρμογών. Κάθε φορά που δημιουργούνται συμβάντα, αποθηκεύονται από το λειτουργικό σύστημα σε ένα αρχείο καταγραφής ώστε να χρησιμοποιηθούν από τους διαχειριστές του συστήματος για τη διάγνωση προβλημάτων. Τα αρχεία καταγραφής χωρίζονται σε αρκετές κατηγορίες ανάλογα με το είδος του συμβάντος. Παρακάτω αναφέρονται τα τρία βασικά είδη (Mavridis, 2016, pp.45–46) :

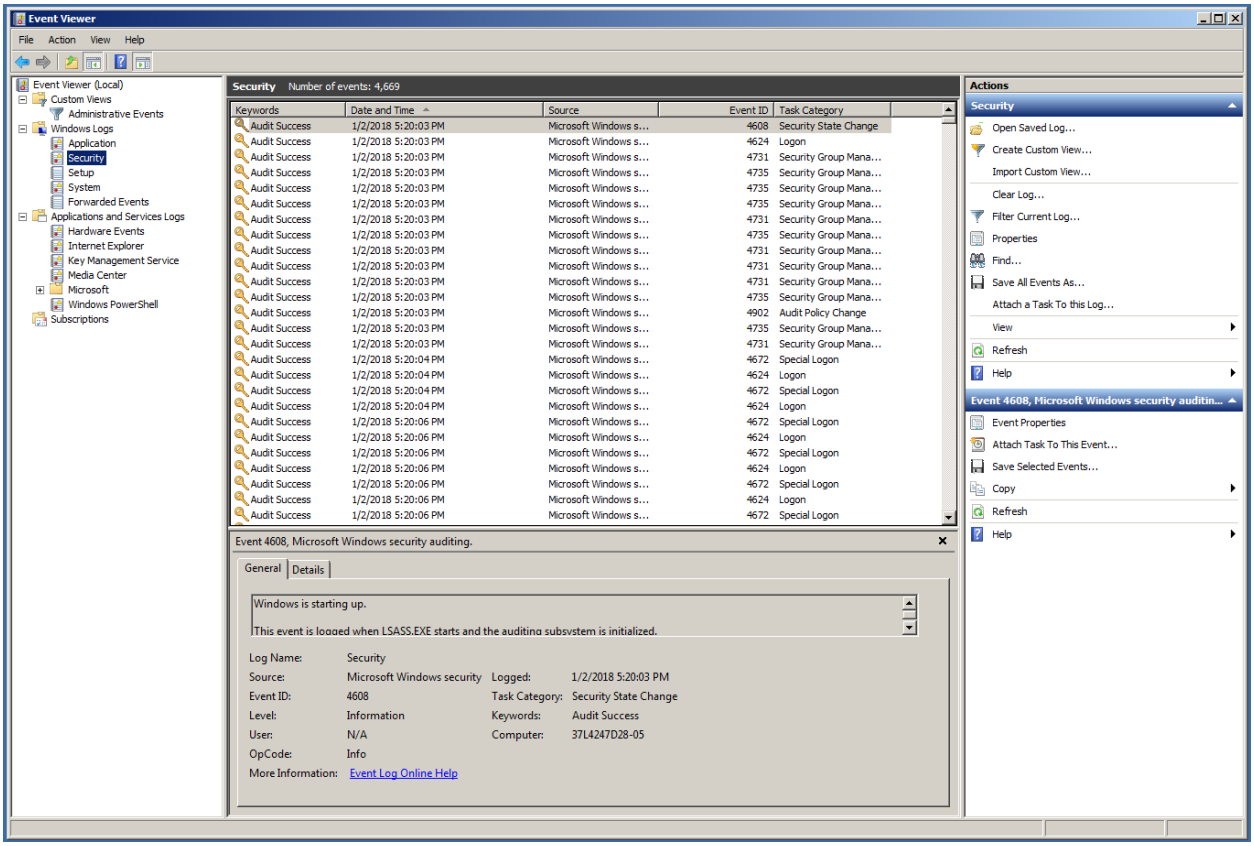
- **Αρχείο καταγραφής εφαρμογής (Application Log)**: Καταγραφή συμβάντων λειτουργίας εγκατεστημένων εφαρμογών. Το περιεχόμενο του καθορίζεται από το δημιουργό της κάθε εφαρμογής.
- **Αρχείο καταγραφής συστήματος (System Log)**: Καταγραφή συμβάντων λειτουργικού συστήματος. Περιέχει πληροφορίες όπως αστοχίες οδηγών συσκευών, αποτυχία εκκίνησης μιας μονάδας δίσκου κ.λπ. Τα συμβάντα προς καταγραφή είναι προκαθορισμένα για αυτή την κατηγορία.
- **Αρχείο καταγραφής ασφάλειας (Security Log)**: Καταγραφή συμβάντων που αφορούν την προστασία του συστήματος. Περιέχει πληροφορίες όπως συμβάντα αυθεντικοποίησης, μεταβολές αρχείων, χρήση πόρων του συστήματος κ.λπ. Η επιλογή συμβάντων προς καταγραφή καθορίζεται από τον διαχειριστή του συστήματος.

3.1.2 Διαχειριστικά εργαλεία

Το λειτουργικό σύστημα των Windows προσφέρει εργαλεία για την εμφάνιση των αρχείων καταγραφής ώστε να εντοπίσουμε και να διαγνώσουμε ζητούμενα προβλήματα, αλλά και για να ρυθμίσουμε την πολιτική ελέγχου (audit policy) καθώς προεπιλεγμένα πολλές συνθήκες ασφάλειας δεν καταγράφονται. Τα εργαλεία αυτά είναι το Event Viewer και τα Group Policy Management Editor – Local Security Policy αντίστοιχα.

Event Viewer

Το Event Viewer είναι ένα εργαλείο διαχείρισης που μας επιτρέπει να προβάλουμε πληροφορίες για αρχεία συμβάντων του συστήματός μας (Solarwinds Loggly, 2016). Τα συμβάντα παρατίθενται με χρονολογική σειρά και ανά κατηγορία (Εικόνα 4), ενώ επίσης διαθέτουν αναγνωριστικό (Event ID) με κωδικό που παραπέμπει στην κατηγορία του συγκεκριμένου συμβάντος. Για παράδειγμα ο κωδικός 4624 παραπέμπει σε συμβάν σύνδεσης ή αποσύνδεσης χρήστη.



Εικόνα 4. Event Viewer

Κάθε συμβάν διαθέτει ένα κλιμακούμενο επίπεδο σοβαρότητας:

- Πληροφορία (Information). Επιτυχείς ενέργειες εφαρμογών, υπηρεσιών κ.λπ.
- Προειδοποίηση (Warning). Ενημέρωση για συμβάν που μπορεί να αποτελεί πρόβλημα.
- Σφάλμα (Error). Ενημέρωση για πρόβλημα που μπορεί να προκαλέσει δυσλειτουργίες στο σύστημα.

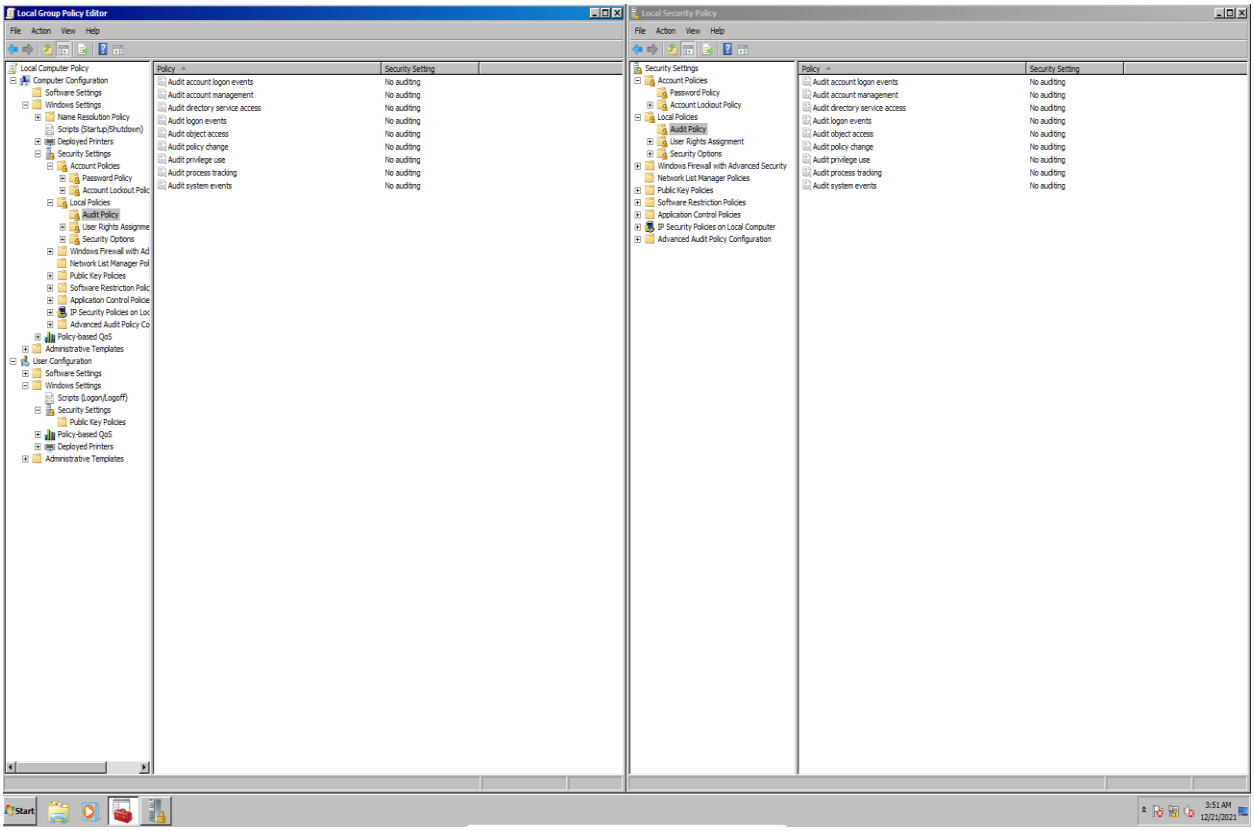
- Κρίσιμο (Critical). Ενημέρωση για σοβαρά προβλήματα που χρήζουν άμεσης αντιμετώπισης.

Επίσης συγκεκριμένα για τα συμβάντα καταγραφής ασφαλείας έχουμε τις ακόλουθες κατηγορίες:

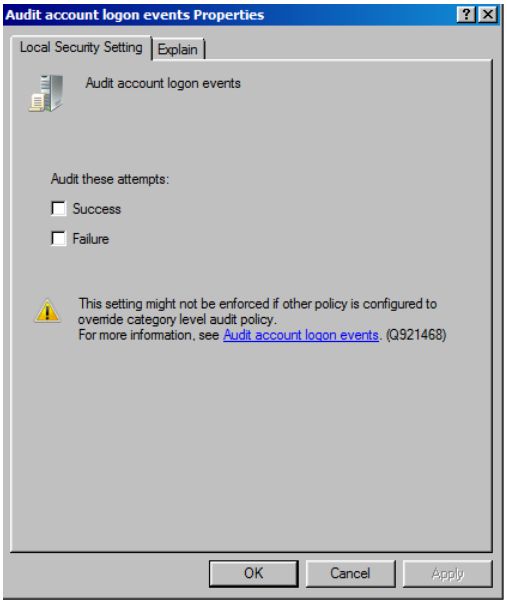
- Έλεγχος Επιτυχίας (Audit Success). Καταγράφει ένα επιτυχημένο συμβάν που ελέγχεται για λόγους ασφαλείας π.χ επιτυχής σύνδεση χρήστη στο σύστημα.
- Έλεγχος Αποτυχίας (Audit Failure) Καταγράφει ένα ανεπιτυχές συμβάν που ελέγχεται για λόγους ασφαλείας π.χ ανεπιτυχής σύνδεση χρήστη στο σύστημα.

Group Policy Management Editor – Local Security Policy

Τα δύο εργαλεία είναι υπεύθυνα για την διαχείριση ρυθμίσεων πολιτικής ελέγχου σε επίπεδο τομέα και σε τοπικό επίπεδο αντίστοιχα (Mavridis, 2016, pp.46-47; Smith, 2019) . Στην Εικόνα 5 βλέπουμε τα δύο εργαλεία παράλληλα, ενω στην Εικόνα 6 βλέπουμε ένα παράθυρο για ρύθμιση της σχετικής πολιτικής σε μια εικονική μηχανή λειτουργικού συστήματος Windows7.



Εικόνα 5. Group Policy Management Editor - Local Security Policy



Εικόνα 6. Ρύθμιση πολιτικής απορρήτου

3.2 Εργαλείο Microsoft System Monitor (Sysmon)

3.2.1 Λειτουργία και ρύθμιση

Το Sysmon είναι εργαλείο της «σουίτας» Sysinternals των Windows. Μετά την εγκατάστασή του στο σύστημα, παραμένει ενεργό σε καθε επανεκκίνησή του με στόχο την λεπτομερή παρακολούθηση και καταγραφή δραστηριοτήτων όπως δημιουργίες και αλλαγές διεργασιών (processes), συνδέσεις δικτύου, τροποποιήσεις αρχείων και δραστηριότητες μητρώου. Οι πληροφορίες συλλέγονται χρησιμοποιώντας τη Συλλογή Συμβάντων των Windows (Windows Event Collector) ή από κάποιο περιβάλλον SIEM με τη χρήση πράκτορα (agent) και με την ανάλυσή τους μπορούμε να κατανοήσουμε τον τρόπο που λειτουργούν διάφοροι παράγοντες απειλής του συστήματός μας. Για την ευκολία αναγνώρισης τα καταγεγραμμένα συμβάντα ανάλογα με το είδος τους διαθέτουν αριθμητικό αναγνωριστικό από το 1 μέχρι το 26, με ξέχωρη την κατηγορία αριθμού 255 η οποία αναφέρει σφάλματα λειτουργίας του Sysmon (Russinovich and Garnier, 2019).

Καθώς τα συμβάντα σε ένα σύστημα είναι υπερβολικά σε αριθμό και στην πλειοψηφία αδιάφορα ως προς τον τομέα της ασφάλειας πρέπει να ρυθμίσουμε ποια από αυτά θα συμπεριλάβουμε και με τι είδους πληροφορίες. Προεπιλεγμένα το Sysmon εγκαθίσταται με ένα αρχείο ρυθμίσεων

config.xml[2]. Τροποποιώντας ή αντικαθιστώντας[3] το, με ένα δικό μας (Εικόνα 7) και ενημερώνοντας το Sysmon για της αλλαγές (Εικόνα 8) μπορούμε να επιτύχουμε καλύτερη καταγραφή πληροφοριών συμβάντων που μας ενδιαφέρουν (Hasan, 2020).

```
<Sysmon schemaversion="4.22">
<HashAlgorithms>md5,sha256,IMPHASH</HashAlgorithms>
<RuleGroup name="" groupRelation="or">
    <RegistryEvent onmatch="include">
        <TargetObject name="T160, RunKey"
condition="contains">CurrentVersion\Run</TargetObject>
    </RegistryEvent>
</RuleGroup>
<RuleGroup name="" groupRelation="or">
   <FileCreateTime onmatch="include">
   <Image name="T1099" condition="begin with">C:\Users</Image>
   <TargetFilename name="T1099" condition="end
with">.exe</TargetFilename>
 </FileCreateTime>
 </RuleGroup>
</Sysmon>
```

Εικόνα 7. Παράδειγμα Sysmon config.xml (Hasan, 2020)

```
Sysmon64.exe -c config.xml
```

Εικόνα 8. Ενημέρωση ρυθμίσεων Sysmon (Hasan, 2020)

3.2.2 Αξιοποίηση πληροφοριών

Κάθε αρχείο καταγραφής περιλαμβάνει πληθώρα πληροφοριών αλλά κάποιες από αυτές μπορούν να αποδειχθούν ανεκτίμητες στην ανάλυση μιας επίθεσης:

- Κατακερματισμο (hash) SHA1, SHA256, IMPHASH και κυρίως MD5 για αναγνώριση κακόβουλων αρχείων μέσω εργαλείων όπως virustotal, analyzer κ.λπ.
- Αλλαγές και πληροφορίες διεργασιών. Ενδιαφέρον έχουν συνήθως δημιουργίες διεργασιών μέσω της γραμμής εντολών, γονικές διεργασίες και αναγνωριστικά.
- Συνδέσεις δικτύου. Πληροφορίες για διευθύνσεις IP, θύρες (ports), ονόματα συστημάτων κ.λπ.

[2] Οι προεπιλεγμένες ρυμίσεις καλύπτουν κατακερματισμούς SHA1, ενώ δεν καταγράφονται συνδέσεις δικτύου.
[3] Το αρχείο ρυθμίσεων της SwiftSecurity (2019) θεωρείται από τα καλύτερα στον τομέα καθώς περιλαμβάνει κατηγοριοποίηση με τεχνικές του MITRE ATT&CK.

- Φόρτωση αρχείων DLL για έγχυση (injection) κώδικα.
- Αναφορά λέξεων κλειδιά όπως whoami, quser, ping κ.λπ.

Στην Εικόνα 9 παρουσιάζουμε πίνακα με όλες τις κατηγορίες συμβάντων και ενδεικτικές επιθετικές ενέργειες ανά κατηγορία.

Κατηγορίες συμβάντων Sysmon και πιθανές επιθετικές ενέργειες			
ID	**Ελληνικός Όρος**	**Αγγλικός Όρος**	**Πιθανή επιθετική ενέργεια**
1	Δημιουργία διεργασίας	Process creation	Πιθανή δημιουργία διεργασιών απο την κονσόλα εντολών για διαφόρους σκοπούς, π.χ WMI
2	Αλλαγή χρόνου δημιουργίας αρχείου	A process changed a file creation time	Αλλαγή timestamps για κάλυψη ιχνών και αποφυγή εντοπισμού
3	Σύνδεση δικτύου	Network connection	Σύνδεση επιτιθέμενου, καταγράφεται η IP, καθώς και πιθανές θύρες σύνδεσης π.χ στην θύρα 22 με πρωτόκολλο SSH
4	Αλλαγή κατάστασης υπηρεσίας Sysmon	Sysmon service state changed	Αλλαγή παραμέτρων Sysmon για αποφυγή ανίχνευσης
5	Τερματισμός διεργασίας	Process terminated	Μπορούμε να αποφανθούμε αν ο επιτιθέμενος έχει εκπληρώσει το στόχο του ή όχι συνδέοντας τους χρόνους δημιουργίας και τερματισμού
6	Φόρτωση προγράμματος οδήγησης	Driver loaded	Επιθέσεις που εκμεταλλεύονται ένα ευάλωτο πρόγραμμα οδήγησης σε ένα σύστημα
7	Φόρτωση εικόνας	Image loaded	Πιθανή φόρτωση αρχείων DLL
8	Δημιουργία απομακρυσμένου νήματος	CreateRemoteThread	Έγχυση κώδικα σε τρέχουσα διεργασία. Το Sysmon περιλαμβάνει πληροφορίες νήματος, όπως η θέση μνήμης, την ενότητα έναρξης και την συνάρτηση που καλείται
9	Ακατέργαστη Πρόσβαση ανάγνωσης	RawAccessRead	Απομάκρυνση δεδομένων αρχείων κλειδωμένα για ανάγνωση
10	Πρόσβαση διεργασίας	ProcessAccess	Χρήση HKTL για κλοπή από την μνήμη διαπιστευτηρίων με σκοπό τη χρήση σε επιθέσεις Pass-the-Hash
11	Δημιουργία αρχείου	FileCreate	Δημιουργία αρχείων από κακόβουλο λογισμικό σε φακέλους αυτόματης έναρξης κατά την διάρκεια της διείσδυσης
12	Γεγονός μητρώου (δημιουργία και διαγραφή αντικειμένων)	RegistryEvent (Object create and delete)	Αλλαγές μητρώου απο κακόβουλο λογισμικό
13	Συμβάν μητρώου (Ορισμός τιμών)	RegistryEvent (Value Set)	
14	Συμβάν μητρώου (Μετονομασία κλειδιού και τιμής)	RegistryEvent (Key and Value Rename)	
15	Δημιουργία αρχείου κατακερματισμού ροής	FileCreateStreamHash	Ρίψη εκτελέσιμων αρχείων η ρυθμίσεων διαμόρφωσης μέσω λήψεων από προγράμμα περιήγησης
16	Αλλαγή διαμόρφωσης υπηρεσίας	ServiceConFigurationChange	Αλλαγές στις ρυθμίσεις παραμέτρων του Sysmon
17	Συμβάν σωλήνα (Δημιουργία σωλήνα)	PipeEvent (Pipe Created)	Χρήση γνωστών ονομάτων σωλήνων απο κακόβουλο λογισμικό
18	Συμβάν σωλήνα (Σύνδεση σωλήνα)	PipeEvent (Pipe Connected)	
19	Συμβάν Wmi (Εντοπίστηκε δραστηριότητα φίλτρου συμβάντων Wmi)	WmiEvent (WmiEventFilter activity detected)	Χρήση WMI από κακόβουλο λογισμικά όπως για παράδειγμα είδαμε στην επίθεση της Γραπτής Εργασίας 1
20	Συμβάν Wmi (Εντοπίστηκε δραστηριότητα καταναλωτή συμβάντος Wmi)	WmiEvent (WmiEventConsumer activity detected)	
21	Συμβάν Wmi (Εντοπίστηκε δραστηριότητα καταναλωτή προς φίλτρο)	WmiEvent (WmiEventConsumerToFilter activity detected)	
22	Συμβάν DNS (Ερώτημα DNS)	DNSEvent (DNS query)	Επιθέσεις DNS, π.χ DaS, DDaS, DNS hijacking, DNS tunneling κ.λπ
23	Διαγραφή Αρχείου (Αρχειοθέτηση διαγραφής αρχείου	FileDelete (File Delete archived)	Διαγραφή κακόβουλου λογισμικού μετά απο μια επίθεση για αποφυγή ανίχνευσης
24	Αλλαγή πρόχειρου (Νέο περιεχόμενο στο πρόχειρο)	ClipboardChange (New content in the clipboard)	Χρήση πρόχειρου για την ανταγραφή και επικόλληση μακροεκλών εντολών
25	Αλλαγή διεργασίας (Αλλαγή εικόνας διεργασίας)	ProcessTampering (Process image change)	Process Hollowing, Process Herpaderping
26	Ανίχνευση συμβάντος διαγραφής αρχείου (Καταγραφή διαγραφής αρχείου)	FileDeleteDetected (File Delete logged)	Διαγραφή κακόβουλου λογισμικού μετά απο μια επίθεση για αποφυγή ανίχνευσης
255	Σφάλμα	Error	Σφάλμα λειτουργίας Sysmon

Εικόνα 9. Κατηγορίες συμβάντων Sysmon και ενδεικτικές επιθετικές ενέργειες[4]

[4] https://github.com/KaragkounisL/PLH35/blob/main/GE2/Images/Εικόνα 09. Κατηγορίες συμβάντων Sysmon και ενδεικτικές επιθετικές ενέργειες.PNG

3.3 Ανάλυση Επίθεσης

Για την ανάλυση του αρχείου θα χρησιμοποιήσουμε το εργαλείο SysmonView (Shalabi, 2018). Αρχικά ακολουθούμε την διαδικασία[5] που αναφέρεται στην ενδεικτική βιβλιογραφία για την μετατροπή του δοθέντος evtx αρχείου σε xml με χρήση της εντολής που φαίνεται στην Εικόνα 10 (Aneja, 2017). Εισάγοντας το xml αρχείο στο SysmonView βλέπουμε το περιβάλλον της Εικόνα 11. Σαν αρχή παρατηρούμε την αναγραφή των αρχείων BootstrapDLL.dll, Keefarce.exe και Keepass.exe. Το Keepass είναι λογισμικό αποθήκευσης ψηφιακών διαπιστευτηρίων, ενώ το Keefarce είναι εργαλείο εξαγωγής δεδομένων που είναι αποθηκευμένα στη βάση δεδομένων του Keepass με την λειτουργία του να βασίζεται στην έγχυση DLL για την εκτέλεση κώδικα (DoI, 2015).

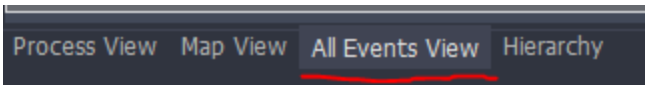
```
┌──(leo㉿kali)-[~/…/plh35/GE2/python-evtx/scripts]
└─$ python3 evtx_dump.py ~/Downloads/plh35/GE2/GE2.evtx > ~/Downloads/GE2.xml
```

Εικόνα 10. Εντολή μετατροπής αρχείου .evtx σε .xml

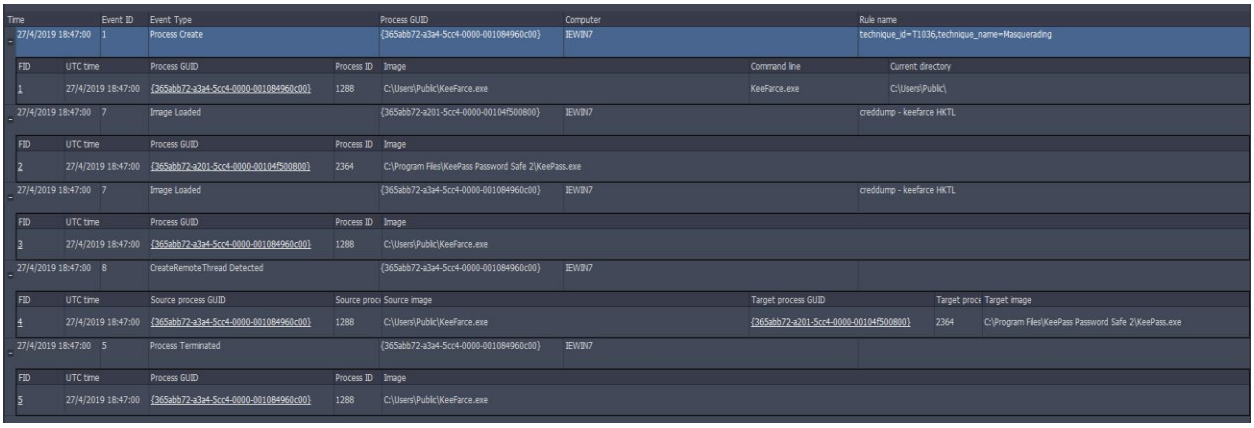
Εικόνα 11. SysmonView Αρχική

Κάνοντας πλοήγηση στον πίνακα προβολής στο κάτω αριστερά μέρος (Εικόνα 12) βλέπουμε λίστα όλων των συμβάντων του αρχείου με πληροφορίες όπως τύπο συμβάντος (Event ID - Event Type), χρόνο εκτέλεσης, παγκοσμίως μοναδικό αναγνωριστικό (GUID) κ.λπ. (Εικόνα 13).

[5] https://study.eap.gr/mod/forum/discuss.php?d=236846#p566111



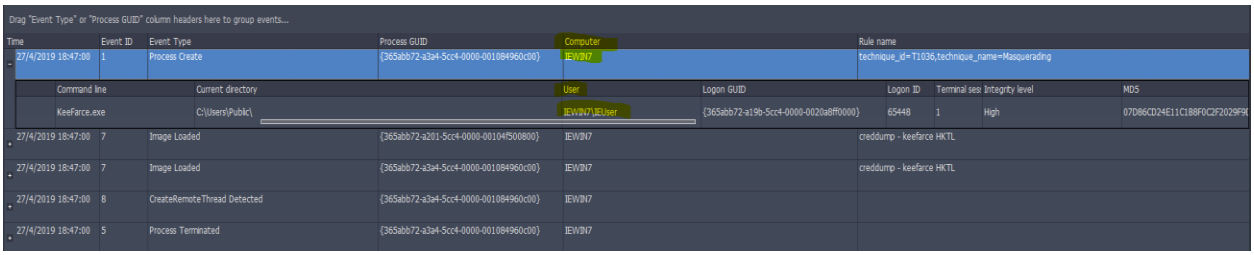
Εικόνα 12. All Events View Θέση



Εικόνα 13. All Events View Πληροφορίες

3.3.1 Πληροφορίες Συστήματος

Όπως βλέπουμε στην Εικόνα 14 αναγράφεται το όνομα συστήματος (hostname) IEWin7 στην στήλη «Computer» και το όνομα του χρήστη (username) IEUser στην στήλη «User».



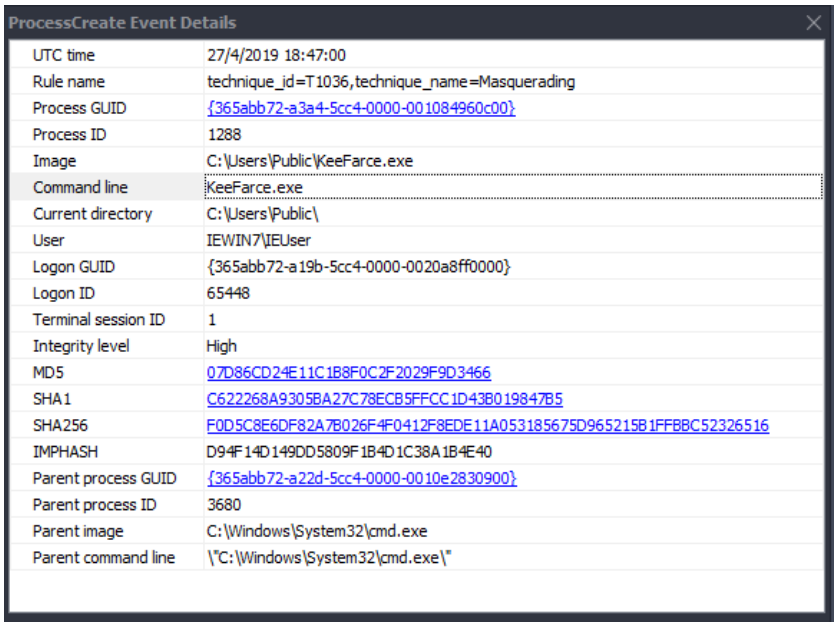
Εικόνα 14. Πληροφορίες συστήματος - χρήστη

Τα παραπάνω αποτελούν προεπιλεγμένες ονομασίες εικονικής μηχανής λειτουργικού συστήματος Windows7 που προσφέρει η Microsoft.

3.3.2 Ενέργειες επιτιθέμενου

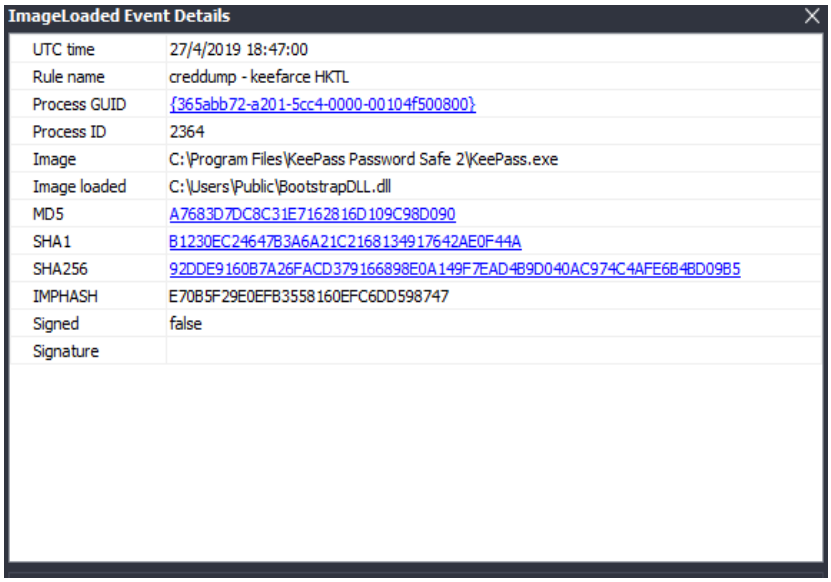
Είναι σημαντικό να αναφέρουμε ότι η εκτέλεση του προγράμματος Keefarce χρειάζεται δικαιώματα διαχειριστή και την ύπαρξη των αρχείων BootstrapDLL.dll, KeefarceDLL.dll και Microsoft.Diagnostic.Runtime.dll στον ίδιο φάκελο που εκτελείται το Keefarce. Ακολουθεί σύντομη περιγραφή και παράθεση εικόνων λεπτομερειών των γεγονότων της επίθεσης με χρονική σειρά, όπως αυτά φαίνονται στην Εικόνα 13:

1. Event ID-1: Δημιουργία διεργασίας Keefarce.exe από την γραμμή εντολών cmd.exe (Εικόνα 15).



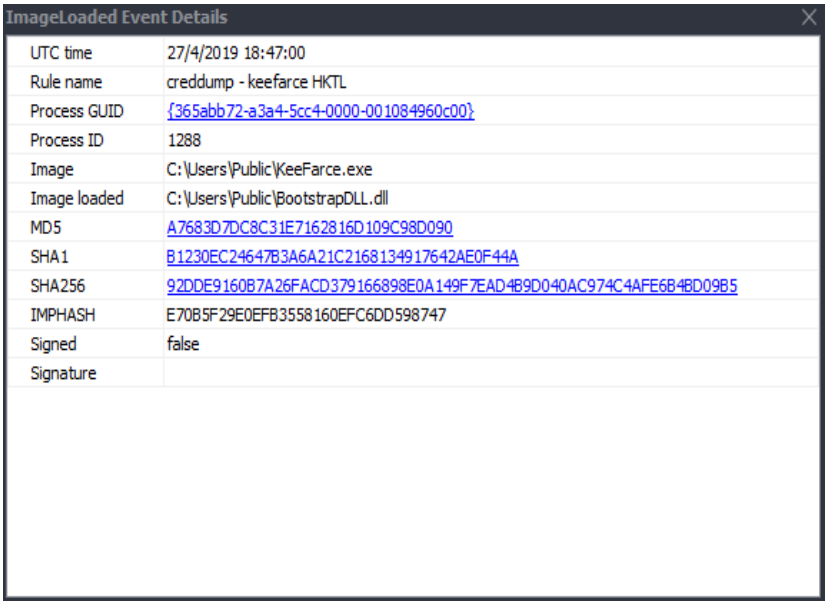
Εικόνα 15. Event FID1

2. Event ID-7: Φόρτωση εικόνας BootstrapDLL.dll στην διεργασία Keepass.exe (Εικόνα 16).



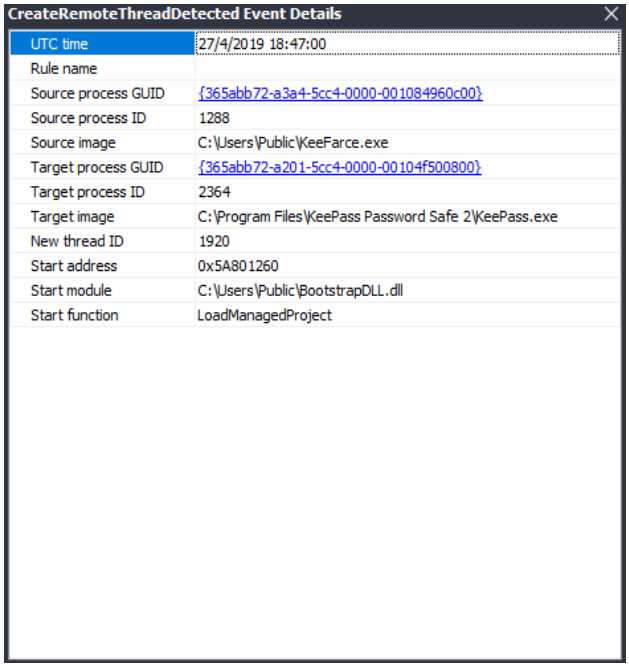
Εικόνα 16. Event FID2

3. Event ID-7: Φόρτωση εικόνας BootstrapDLL.dll στην διεργασία Keefarce.exe (Εικόνα 17).



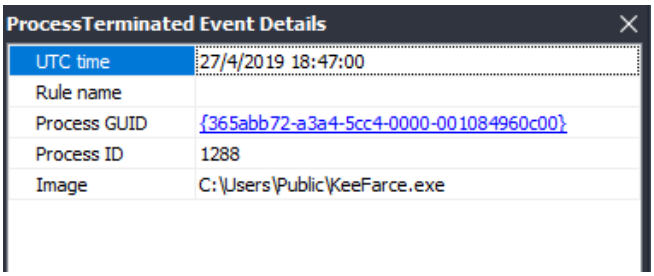
Εικόνα 17. Event FID3

4. Event ID-8: Δημιουργία απομακρυσμένου νήματος στη θέση μνήμης που τρέχει η διεργασία Keepass για την εγχυση του KeefarceDLL.dll με κλήση της αντίστοιχης συνάρτησης του BootstrapDLL.dll (Εικόνα 18).



Εικόνα 18. Event FID4

5. Event ID-5: Η διεργασία Keefarce.exe τερματίζει (Εικόνα 19).



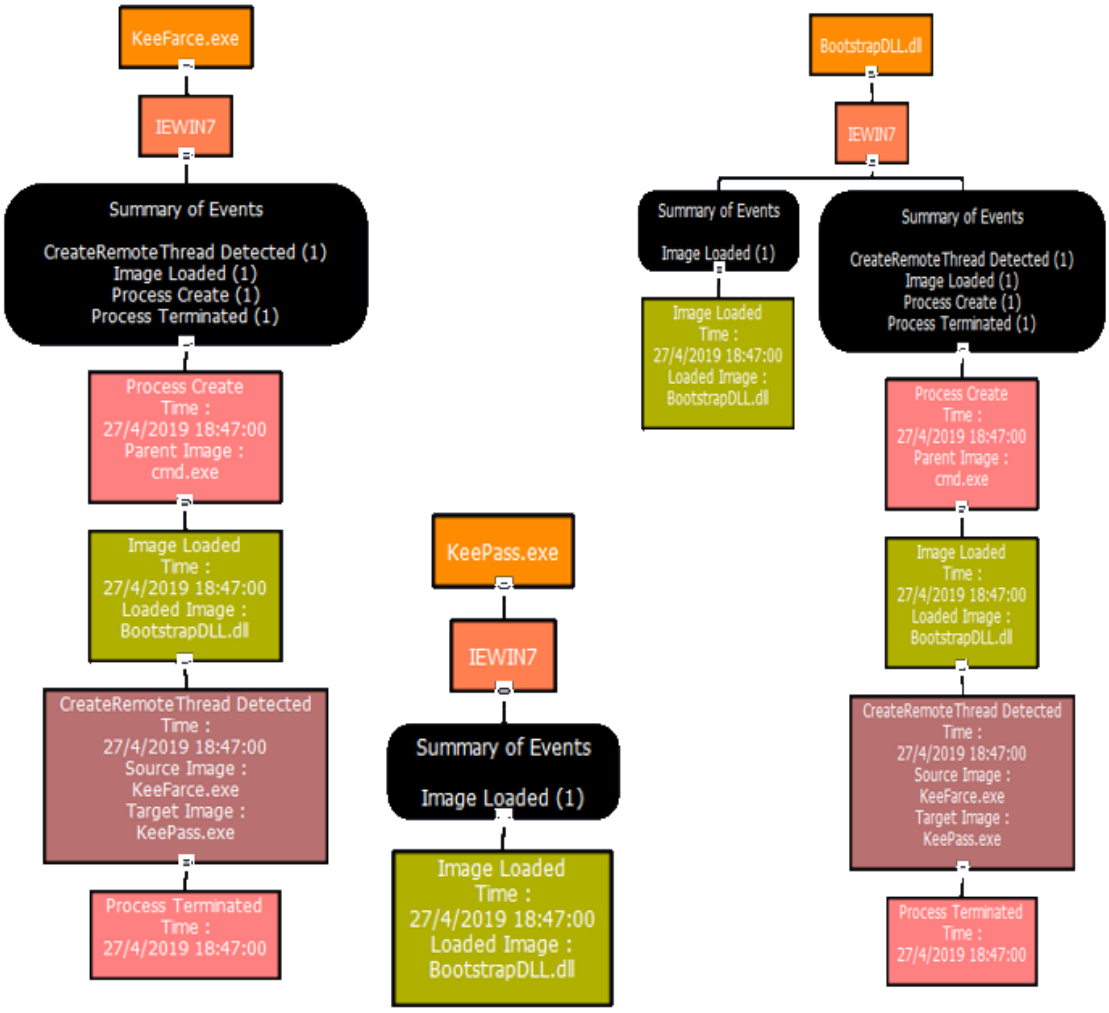
Εικόνα 19. Event FID5

Έχοντας μελετήσει τον κώδικα του προγράμματος Keefarce (DoI, 2015), παραθέτουμε πίνακα (Εικόνα 20) με σημαντικές εντολές και επιμέρους σχόλια καθώς και τα διαγράμματα γεγονότων (Εικόνα 21).

Καραγκούνης Λεωνίδας Χρήστος ΕΑΠ ΠΛΗ35 ΓΕ2 Ιαν-22		
Σύντομη επεξήγηση και σχολιασμός σημαντικών εντολών κώδικα προγράμματος Keefarce		
Event FID	**Εντολές Κώδικα**	**Σχόλια**
1		Έναρξη Keefarce.exe μέσω της γραμμής εντολών C:\Windows\System32\cmd.exe
2 + 3	char DllName [MAX_PATH] GetCurrentDirectoryA(MAX_PATH, DllName) wchar_t DllNameW[MAX_PATH] GetCurrentDirectory(MAX_PATH, DllNameW) wcscat_s(DllNameW, L"\\KeeFarceDLL.dll") strcat_s(DllName, "\\BootstrapDLL.dll")	Για τα αρχεία BootstrapDLL.dll και KeeFarceDLL.dll η πλήρης διαδρομή (κατάλογος + όνομα αρχείου) αποθηκεύονται στις μεταβλητές DllName και DllNameW αντίστοιχα
	Pid = GetProcessIdByName("KeePass.exe")	Βρίσκει το ID της διεργασίας Keepass.exe και το αποθηκεύει στην μεταβλητή Pid
	InjectAndRunThenUnload(Pid, DllName, "LoadManagedProject", DllNameW)	Το BootstrapDLL.dll φορτώνεται στη διεργασία Keepass **(Event FID 2)** χρησιμοποιώντας VirtualAllocEx()/CreateRemoteThread() για τον εξαναγκασμό της κλήσης LoadLibraryA(). Έπειτα καλείται η συνάρτηση LoadManagedProject και φορτώνεται το .NET CLR και γίνεται η αποφόρτωση του KeefarceDLL.dll **(Event FID 3)**.
4	**ExecuteInDefaultAppDomain**(managedDllLocation, L"KeeFarceDLL.KeeFarce", L"EntryPoint", L"Argument",&result);	Καλείται η συνάρτηση EntryPoint. Το KeefarceDLL.dll φορτώνει το Microsoft.Diagnostics.Runtime.dll, προσκολλάται στην τρέχουσα διεργασία Keepass και διατρέχει το σωρό μνήμης για αντικείμενα DocumentManagerEx. Έπειτα αποθηκεύονται όλες οι πληροφορίες και παράμετροι για το αντικείμενο και τέλος καλείται η μέθοδος εξαγωγής με τα στοιχεία (ονόματα χρήστη, κωδικοί πρόσβασης, σημειώσεις και urls) να αποθηκεύονται σε μορφή καθαρού κειμένου στο αρχείο με διαδρομή %%APPDATA%%/keepass_export.csv
5		Τερματισμός Keefarce.exe

Εικόνα 20. Πίνακας επεξήγησης κώδικα Keefarce[6]

[6] https://github.com/KaragkounisL/PLH35/blob/main/GE2/Images/Εικόνα 20. Πίνακας επεξήγησης κώδικα Keefarce.PNG



Εικόνα 21. Δέντρα γεγονότων

Έχοντας μια πλήρη εικόνα της επίθεσης μπορούμε να συνδέσουμε τα γεγονότα με τα στάδια επίθεσης του μοντέλου Cyber Kill Chain (CKC) όπως φαίνεται στην Εικόνα 22. Παραλείπονται τα πρώτα βήματα καθώς όπως έχει αναφερθεί ο επιτιθέμενος χρειάζεται δικαιώματα διαχειριστή στο σύστημα, επομένως κάνουμε την παραδοχή πως έχει ήδη κάνει τα απαραίτητα βήματα για την πρόσβαση και κλιμάκωση προνομίων στο σύστημα ή εξαπάτησε χρήστη με δικαιώματα διαχειριστή να εκτελέσει το πρόγραμμα με χρήση τεχνικών κοινωνικής μηχανικής (social engineering).

Βήμα CKC	Βήμα Επίθεσης
Exploitation	Έναρξη Keefarce.exe μέσω της γραμμής εντολών C:\Windows\System32\cmd.exe
Installation	Φόρτωση του BootstrapDLL.dll στην διεργασία Keepass.exe και αποφόρτωση του KeefarceDLL.dll
Command and Control	Η συνάρτηση Entrypoint του KeefarceDLL.dll εκτελείται και γίνεται καταμέτρηση του σωρού της μνήμης για την εύρεση των αντικειμένων της βάσης δεδομένων Keepass. Αποθήκευση εξαχθέντων δεδομένων σε αρχείο csv
Actions on Objectives	Ανάκτηση διαπιστευτηρίων από το αρχείο csv στον φάκελο %AppData%. Πιθανή χρήση τους για πρόσβαση σε υλικό δικτύωσης, υποδομές εκτός τομέα, υποκλοπή προσωπικών δεδομένων κ.λπ.

Εικόνα 22. Συσχετισμός βημάτων επίθεσης και CKC

3.3.3 Τελικός στόχος

Όπως αναφέρθηκε λειτουργία του Keefarce είναι να εξάγει τους κωδικούς πρόσβασης από τη βάση δεδομένων με την έγχυση ενός κώδικα βιβλιοθήκης δυναμικής σύνδεσης. Τα δεδομένα, με μορφή καθαρού κειμένου. εξάγονται σε ένα εξωτερικό αρχείο csv το οποίο αποθηκεύεται προεπιλεγμένα στο φάκελο %AppData%. Τα εξαγόμενα δεδομένα περιλαμβάνουν ονόματα χρηστών, κωδικούς πρόσβασης, σημειώσεις και διευθύνσεις URL και μπορούν να εξαχθούν εύκολα από τον επιτιθέμενο χρήστη με σκοπό την πρόσβαση σε υλικό δικτύωσης, υποδομές εκτός τομέα, πρόσβαση σε προσωπικούς λογαριασμούς και υπηρεσίες κ.λπ.

4. Συμπεράσματα

Στην παρούσα εργασία μελετήθηκε το σύστημα καταγραφής των Windows, το εργαλείο Sysmon αλλά και ο ρόλος της Ψηφιακής Εγκληματολογίας και της διαδικασίας Αντιμετώπισης Περιστατικών για την διαχείριση κρίσιμων γεγονότων. Παρατηρήσαμε επίσης την σημαντικότητα των αρχείων καταγραφής μελετώντας ένα αρχείο συμβάντος, πως θα μπορούσε να αξιοποιηθεί για την κατανόηση της επίθεσης και την χρήση των πειστηρίων για την αποτροπή μελλοντικών παρόμοιων επιθέσεων. Καθώς είναι σχεδόν αδύνατο να αποτραπεί η διείσδυση στα σημερινά Πληροφοριακά Συστήματα, η χρήση των αρχείων καταγραφής είναι ανεκτίμητη για την ανάλυση περιστατικών με σκοπό την πρόληψη εξάπλωσης και την μείωση προκληθέντων ζημιών στο σύστημα, αλλά και στην αναθεώρηση μέτρων ασφαλείας για την έγκαιρη ανίχνευση και άμεση ανταπόκριση σε μελλοντικά περιστατικά.

Βιβλιογραφία

Aneja, A. (2017). *Parsing Windows event log files (.evtx) using Python*. [online] Alisha Aneja. Available at: https://www.alishaaneja.com/evtx/ [Accessed 1 Jan. 2022].

Carpenter, T. (2011). *Microsoft Windows Server Administration Essentials*. Indianapolis, Ind.: Wiley, pp.220–241.

Casey, E. (2013). *Handbook of Digital Forensics and Investigation*. Amsterdam: Academic Press, pp.21–61, 240–243.

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. *Computer Security Incident Handling Guide*, [online] 2. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [Accessed 30 Dec. 2021].

CQURE Experts (2017). *Building A Perfect Sysmon Configuration File*. [online] CQURE Academy. Available at: https://cqureacademy.com/blog/hacks/sysmon-configuration-file [Accessed 19 Dec. 2021].

Crowdstrike (2021). *What is Digital Forensics and Incident Response (DFIR) | CrowdStrike*. [online] crowdstrike.com. Available at: https://www.crowdstrike.com/cybersecurity-101/digital-forensics-and-incident-response-dfir/ [Accessed 24 Dec. 2021].

Dimitriadis, A., Ivezic, N., Kulvatunyou, B. and Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, [online] 5(2590-0056), p.100015. Available at: https://www.sciencedirect.com/science/article/pii/S2590005619300153?via%3Dihub [Accessed 20 Dec. 2021].

DoI (2015). *KeeFarce*. [online] GitHub. Available at: https://github.com/denandz/KeeFarce [Accessed 14 Dec. 2021].

Drysdale, J. (2021). *A Sysmon Event ID Breakdown - Now with Event ID 25!!* [online] Black Hills Information Security. Available at: https://www.blackhillsinfosec.com/a-sysmon-event-id-breakdown/ [Accessed 17 Dec. 2021].

Freiling, F.C. and Schwittay, B. (2007). *A Common Process Model for Incident Response and Computer Forensics*. [online] CiteSeer. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.210.1659 [Accessed 3 Jan. 2022].

Green, A. (2020). *Sysmon Threat Analysis Guide*. [online] Inside Out Security. Available at: https://www.varonis.com/blog/sysmon-threat-detection-guide/ [Accessed 19 Dec. 2021].

Hasan, S. (2020). *Sysmon: How To Setup, Configure, and Analyze the System Monitor's Events*. [online] Medium. Available at: https://syedhasan010.medium.com/sysmon-how-to-setup-configure-and-analyze-the-system-monitors-events-930e9add78d [Accessed 16 Dec. 2021].

Hassan, N.A. (2019). *Digital forensics basics : a practical guide using Windows OS*. Berkeley, California: Apress, New York, Ny, pp.2–33.

Johansen, G. (2017). *Digital forensics and incident response : a practical guide to deploying digital forensic techniques in response to cyber security incidents*. Birmingham, Uk: Packt Publishing Ltd, pp.6–26, 31–53.

Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006). *SP 800-86. Guide to Integrating Forensic Techniques into Incident Response*. [online] Gaithersburg, MD, USA: National Institute of Standards & Technology, pp.15–60. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf [Accessed 21 Dec. 2021].

Lockheed Martin (2019). *Cyber Kill Chain®*. [online] Lockheed Martin. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Accessed 16 Dec. 2021].

Lord, N. (2015). *What is Incident Response?* [online] Digital Guardian. Available at: https://digitalguardian.com/blog/what-incident-response [Accessed 3 Jan. 2022].

Luttgens, J.T., Pepe, M. and Mandia, K. (2014). *Incident Response & Computer Forensics.* New York: Mcgraw-Hill Education, pp.27–71, 346–358.

Mavridis, I. (2015). *Information Security on the Internet*. [online] *Kallipos.gr*, Athens: Hellenic Academic Libraries Link, pp.236–252. Available at: https://repository.kallipos.gr/handle/11419/1024 [Accessed 13 Dec. 2021].

Mavridis, I. (2016). *Information and Security Systems Laboratory*. [online] *Kallipos.gr*, Athens: Hellenic Academic Libraries Link, pp.44–55. Available at: https://repository.kallipos.gr/handle/11419/525 [Accessed 9 Jan. 2022].

Mavroeidis, V. and Jøsang, A. (2018). Data-Driven Threat Hunting Using Sysmon. *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy - ICCSP 2018*. [online] Available at: https://arxiv.org/pdf/2103.15194.pdf [Accessed 2 Jan. 2022].

Michael Hale Ligh, Case, A., Levy, J. and Walters, A. (2014). *The art of memory forensics : detecting malware and threats in Windows, Linux, and Mac memory*. Indianapolis, In: Wiley, pp.265–280.

Robinson, M.K. (2015). *Digital forensics workbook*. North Charleston, South Carolina: Createspace, Printed In Lexington, Ky, pp.158–159.

Russinovich, M. and Garnier, T. (2019). *Sysmon - Windows Sysinternals*. [online] Microsoft.com. Available at: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon [Accessed 19 Dec. 2021].

Shalabi, N. (2018). *Sysmon Tools*. [online] GitHub. Available at: https://github.com/nshalabi/SysmonTools [Accessed 12 Dec. 2021].

Smith, R. (2019). *Group Policy Management*. [online] https://blog.netwrix.com/. Available at: https://blog.netwrix.com/2019/04/18/group-policy-management/ [Accessed 21 Dec. 2021].

Smokescreen (2020). *Top Lateral Movement Techniques – The Red Team Edition*. [online] Smokescreen.io. Available at: https://www.smokescreen.io/assets/uploads/2020/08/GUIDE-Smokescreen-Top-Lateral-Movement-Techniques-Red-Team-Edition.pdf [Accessed 12 Dec. 2021].

Solarwinds Loggly (2016). *Ultimate Guide to Logging*. [online] Loggly.com. Available at: https://www.loggly.com/ultimate-guide/windows-logging-basics/ [Accessed 18 Dec. 2021].

SwiftOnSecurity (2019). *sysmon-config | A Sysmon configuration file for everybody to fork*. [online] GitHub. Available at: https://github.com/SwiftOnSecurity/sysmon-config [Accessed 5 Jan. 2022].

Veca, M. (2015). *Extracting Windows event logs using memory forensics*. [MSc] Available at: https://scholarworks.uno.edu/td/2119/ [Accessed 14 Dec. 2021].