ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Σύγκριση των Συστημάτων Ανίχνευσης Εισβολών Zeek και Suricata με χρήση κακόβουλης κίνησης δικτύου

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ίκοντας Εμμανουήλ

Επιβλέπων : Καθηγητής Καμπουράκης Γεώργιος

Μέλη εξεταστικής επιτροπής: Δρ. Μπαρμπάτσαλου Κωνσταντία
Καθηγήτρια Καρύδα Μαρία

Σάμος, Φεβρουάριος 2023

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η εκπόνηση της παρούσας διπλωματικής είναι αποτέλεσμα συλλογικής εργασίας και για το λόγο αυτό, θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν στην υλοποίησή της.

Αρχικά, θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στους επιβλέποντες αυτής της έρευνας, τον καθηγητή κο Καμπουράκη Γεώργιο και την διδακτορική ερευνήτρια κα Μπαρμπάτσαλου Κωνσταντία για την καλοσύνη τους και τις σχολαστικές συμβουλές τους καθ' όλη την διάρκεια συγγραφής αυτής της διπλωματικής εργασίας. Επιπρόσθετα, οι επιστημονικές τους γνώσεις, η επαγγελματική τους εμπειρία και οι πάντα ακριβείς παρατηρήσεις τους ήταν ανεκτίμητες και καθοριστικές στην εξέλιξη της έρευνας.

Θα ήθελα επίσης να ευχαριστήσω την κα Καρύδα Μαρία, μέλος της κριτικής επιτροπής, που μου έκανε την τιμή να κρίνει την δουλειά μου.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου για την αγάπη, την κατανόηση, την υπομονή και την στήριξή τους σε όλη την διάρκεια των σπουδών μου.

Ίκοντας Εμμανουήλ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Περιεχόμενα

Λίστα Εικόνων

Λίστα Πινάκων

Ακρωνύμια

NIDS	Network Intrusion Detection System
ΣΑΕ	Σύστημα Ανίχνευσης Εισβολών
CAGR	Compound Annual Growth Rate
IoT	Internet of Things
ENISA	European Union Agency For Cybersecurity
DDoS	Distributed Denial of Service
TTPs	Tactics Techniques Procedures
SIEM	Security Information and Event Management
MCDM	Multi-Criteria Decision-Making
NIST	National Institute of Standards and Technology
DPI	Deep Packet Inspection
IPC	Inter-Process Communication
SMB	Server Message Block
DCE	Distributed Computing Environment
RPC	Remote Procedure Call
RAT	Remote Access Tool
SAM	Security Account Manager
SAMR	Security Account Manager Remote Protocol
TGT	Ticket Granting Service
DC	Domain Controller
IoCs	Indicators of Compromise

Περίληψη

Το διαδίκτυο και οι συν αυτώ τεχνολογίες εξελίσσονται με ραγδαίο ρυθμό. Ο συνολικός αριθμός χρηστών του διαδικτύου εκτιμάται να φτάσει τα 5.3 δις μέχρι το 2023 – από 3.9 δις το 2018 – εμφανίζοντας σύνθετο ετήσιο ρυθμό ανάπτυξης (Compound Annual Growth Rate – CAGR) 6%. Με αναγωγή σε μέγεθος πληθυσμού, οι αριθμοί αυτοί αντιπροσωπεύουν το 66% και το 51% του παγκόσμιου πληθυσμού, αντίστοιχα. (Cisco, 2020, p. 5)

Σύμφωνα με στοιχεία από την *Cisco Talos Incident Response (Talos IR)*, το τρίτο τετράμηνο του 2022 τα εκπαιδευτικά ιδρύματα υπήρξαν ο υπ' αριθμόν ένα στόχος επιθέσεων (Huey, 2022), ενώ το τελευταίο τέταρτο την πρωτοκαθεδρία είχαν οι εταιρείες τηλεπικοινωνιών (Dontje, 2022).

Η παρούσα διπλωματική εργασία εντάσσεται στον τομέα της ασφάλειας των πληροφοριακών και επικοινωνιακών συστημάτων. Σκόπος της είναι η συγκριτική μελέτη δύο ευρέως διαδεδομένων συστημάτων ανίχνευσης εισβολών (Intrusion Detection Systems – IDS), εν ονόματι Zeek και Suricata, βασιζόμενοι στα αποτελέσματα που προέκυψαν κατά την αναπαραγωγή κακόβουλης δικτυακής κίνησης, υπό την μορφή pcap αρχείων.

Στόχος μας ήταν να συγκρίνουμε τα εν λόγω IDSs, μέσα από εξέταση και καταγραφή της συμπεριφοράς τους, με όσο το δυνατόν περισσότερες περιπτώσεις κακόβουλων λογισμικών, μελετώντας τα αρχεία καταγραφών για ενδείξεις παραβίασης (Indicators of Compromise – IoCs), ως συνεπακόλουθα της επίθεσης.

Λέξεις Κλειδιά: *Συστήματα Ανίχνευσης Εισβολών Δικτύου (ΣΑΕ), Zeek IDS, Suricata IDS, αρχεία καταγραφών, κακόβουλη κίνηση δικτύου, MITRE ATT&CK framework*

Abstract

Internet and related technologies are evolving at a rapid pace. The total number of internet users is estimated to reach 5.3 billion by 2023 – up from 3.9 billion in 2018 – showing a compound annual growth rate (CAGR) of 6%. Adjusted for population size, these numbers represent 66% and 51% of the world's population, respectively.

According to data from Cisco Talos Incident Response (Talos IR), in the third quarter of 2022, educational institutions were the number one target of attacks (Huey, 2022), whilst in the last quarter, priority was given to telecommunications companies (Dontje, 2022).

But how can we ensure the protection of the information that circulates in a network? How can we safeguard our data, the smooth and uninterrupted operation of our network and consequently the services offered?

This thesis joins the domain of information and communication systems security. Its purpose is the comparative study of two widespread Intrusion Detection Systems (IDS), namely Zeek and Suricata, based on the results obtained during the reproduction of malicious network traffic, in the form of pcap files.

Our goal was to compare the IDSs in question by examining and recording their behavior with as many cases of malicious software as possible, scrutinizing their log files for indicators of compromise (IoCs), as a consequence of the attack.

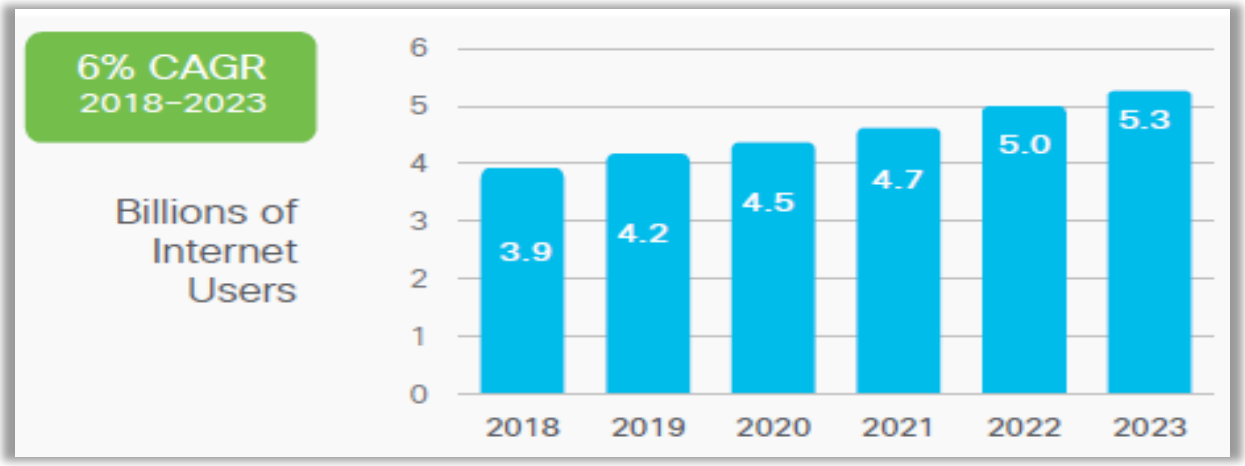
Keywords: *Network Intrusion Detection Systems (NIDS), Zeek IDS, Suricata IDS, log files, malware traffic, MITRE ATT&CK framework*

1

Εισαγωγή

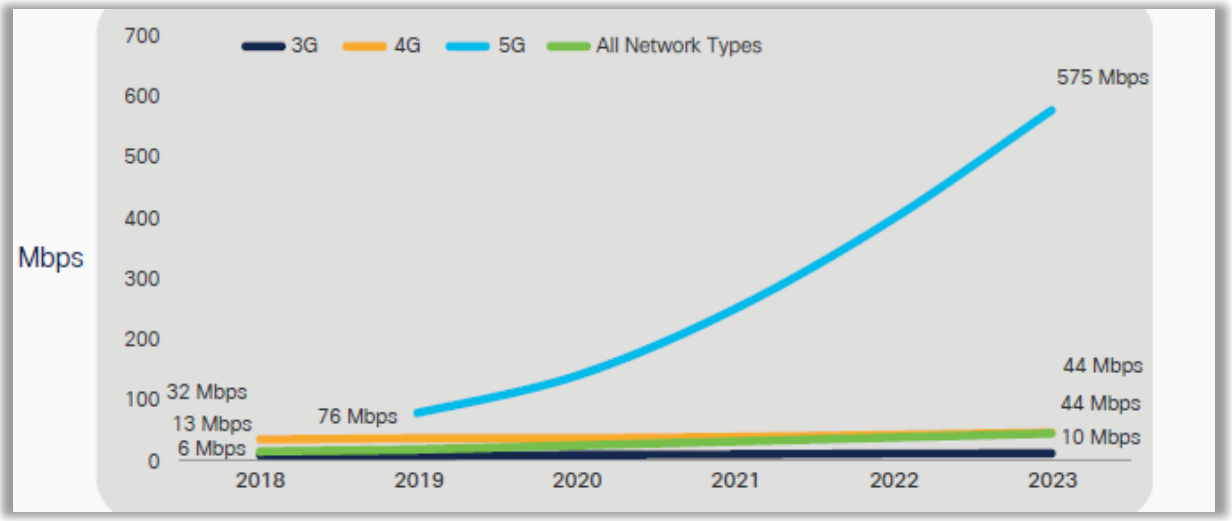
1.1 Η ανάπτυξη των δικτύων ως παράγοντας αύξησης της επιφάνειας επιθέσεων

Το διαδίκτυο και οι συν αυτώ τεχνολογίες εξελίσσονται με ραγδαίο ρυθμό. Ο συνολικός αριθμός χρηστών του διαδικτύου εκτιμάται να φτάσει τα 5.3 δις μέχρι το 2023 – από 3.9 δις το 2018 – εμφανίζοντας σύνθετο ετήσιο ρυθμό ανάπτυξης (Compound Annual Growth Rate – CAGR) 6%. Με αναγωγή σε μέγεθος πληθυσμού, οι αριθμοί αυτοί αντιπροσωπεύουν το 66% και το 51% του παγκόσμιου πληθυσμού, αντίστοιχα. (Cisco, 2020, p. 5)



Εικόνα 1. Η παγκόσμια ανάπτυξη των χρηστών του intenet. ***Πηγή: Cisco Annual Internet Report, 2018 – 2023***

Την ίδια στιγμή επιχειρήσεις και οργανισμοί ωθούνται να προσαρμοστούν στις επιταγές της εποχής. Ενισχύουν τα δίκτυά τους και διευρύνουν τις υπηρεσίες τους, ώστε να ανταποκριθούν στις αυξημένες απαιτήσεις τόσο για μεγαλύτερη ταχύτητα στην επικοινωνία, όσο και στην ποικιλομορφία των δεδομένων που διακινούνται. Την πεποίθηση αυτή έρχεται να επαληθεύσει η εκτίμηση πως μέχρι το 2023 η μέση ταχύτητα των δικτύων 5G, θα είναι 13 φορές υψηλότερη από εκείνη οποιουδήποτε άλλου τύπου δικτύων (Cisco, 2020, p. 18), όπως βλέπουμε και στο γράφημα της εικόνας 2.



Εικόνα 2. Μέση ταχύτητα κινητών δικτύων παγκοσμίως ανά τύπο δικτύου. ***Πηγή: Cisco Annual Internet Report, 2018 – 2023***

Φαίνεται πως στην μετά-COVID εποχή ο άξονας της ανθρώπινης δραστηριότητας έχει μετατοπιστεί προς το διαδίκτυο σε αξιοσημείωτο βαθμό. Τομείς όπως η εργασία, η εκπαίδευση, το ηλεκτρονικό εμπόριο, οι δημόσιες υπηρεσίες, διεισδύουν και αναπτύσσονται όλο και περισσότερο στον χώρο του διαδικτύου. Ωστόσο, δημοφιλείς υπηρεσίες και τεχνολογίες αιχμής, οι οποίες αποτελούν και κυρίαρχες «τάσεις» τα τελευταία χρόνια όπως, IoT (Internet of Things), τεχνητή νοημοσύνη, μηχανική μάθηση, μέσα κοινωνικής δικτύωσης, Big Data, αυξάνουν το ρίσκο (υπό την έννοια της έκθεσης σε πιθανή απειλή) για χρήστες, επιχειρήσεις και οργανισμούς (Cisco, 2020, p. 21). Κάτι τέτοιο δικαιολογείται από το γεγονός πως ταυτόχρονα υπάρχει αύξηση στον όγκο των δεδομένων που μεταδίδονται, στις ευπάθειες των υποδομών και των λογισμικών που χρησιμοποιούνται και στον βαθμό αλληλεπίδρασης του ανθρώπινου παράγοντα με τις υπηρεσίες και τις τεχνολογίες αυτές.

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (European Union Agency For Cybersecurity – ENISA) σε πρόσφατη αναφορά του με τίτλο *"ENISA THREAT LANDSCAPE 2022"* (ENISA, 2022, p. 102) αναφέρει μια *«ενδεικτική λίστα περιστατικών ασφάλειας» (Indicative List of Incidents)*, στην οποία μεταξύ άλλων γίνεται λόγος για:

- ιστοσελίδες της Γερουσίας, του Υπουργείου Άμυνας και του Εθνικού Ινστιτούτου Υγείας της Ιταλίας, οι οποίες τον Μάιο του 2022, έγιναν στόχος κατανεμημένης επίθεσης άρνησης υπηρεσιών (Distributed Denial of Service – DDOS), που σκοπό είχε να πλήξει χώρες του NATO.
- μια αναφορά, τον Σεπτέμβριο του 2021, στην οποία εμφανίζεται το σύστημα ενός νοσοκομείου στο Παρίσι να έχει γίνει στόχος επίθεσης παραβίασης δεδομένων, με αποτέλεσμα να διαρρεύσουν δεδομένα από τεστ COVID 1.4 εκατ. πολιτών.

Σύμφωνα με στοιχεία από την *Cisco Talos Incident Response (Talos IR)*, το τρίτο τετράμηνο του 2022 τα εκπαιδευτικά ιδρύματα υπήρξαν ο υπ' αριθμόν ένα στόχος επιθέσεων (Huey, 2022), ενώ το τελευταίο τέταρτο την πρωτοκαθεδρία είχαν οι εταιρείες τηλεπικοινωνιών (Dontje, 2022).

Πώς όμως μπορούμε να διασφαλίσουμε την προστασία της πληροφορίας που διακινείται σε ένα δίκτυο; Με ποιον τρόπο μπορούμε να διαφυλάξουμε τα δεδομένα μας, την ομαλή και

απρόσκοπτη λειτουργία του δικτύου μας και κατά συνέπεια τις προσφερόμενες από αυτό υπηρεσίες;

Όλα τα προαναφερθέντα συνηγορούν στα εξής:

i. Η παρακολούθηση (Monitoring) και ανάλυση της δικτυακής κίνησης (Network Traffic Analysis) αποκτά ιδιαίτερη βαρύτητα πλέον, εφόσον μπορεί να δράσει τόσο ως μέτρο πρόληψης, όσο και ως μέτρο ανίχνευσης. Παρακολουθώντας την δικτυακή κίνηση ο διαχειριστής πιθανόν να εντοπίσει ύποπτες δραστηριότητες ή συνδέσεις, τις οποίες θα μπορούσε να αποτρέψει πριν αυτές προκαλέσουν περαιτέρω ζημιά. Ωστόσο, ακόμα και στην περίπτωση που δεν δράσει προληπτικά και η επίθεση θεωρηθεί επιτυχής ως προς τον σκοπό της, μέσω της ανάλυσης της δικτυακής κίνησης ο υπεύθυνος ασφάλειας θα είναι σε θέση να συλλέξει στοιχεία για πιθανές μετέπειτα νομικές διαδικασίες για την απόδοση ευθυνών και ίσως το πιο σημαντικό, να εντοπίσει τις ευπάθειες που εκμεταλλεύτηκαν οι επιτιθέμενοι, και είχε ως αποτέλεσμα οι απειλές να μετατραπούν σε πραγματικά γεγονότα και κατ' επέκταση ζημιά για την επιχείρηση.

ii. Απαιτείται συνεχής αξιολόγηση των εργαλείων που χρησιμοποιούνται στην παραπάνω διαδικασία και ενδεχομένως η εξέταση του όρου της «αποτελεσματικότητάς» τους με διαφορετικούς τρόπους και κριτήρια, στοχεύοντας πάντα στην εξέλιξη και βελτιστοποίησή τους.

iii. Η μελέτη των εργαλείων και η ενημέρωση σε θέματα που άπτονται του χώρου της ασφάλειας των πληροφοριακών συστημάτων θα πρέπει να είναι διαρκής, ώστε να ανταπεξέλθουμε στην προσπάθεια για την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας που τα χαρακτηρίζουν.

Αυτές είναι και οι γενικές κατευθύνσεις της εργασίας μας.

1.2 Αντικείμενο διπλωματικής

Η παρούσα διπλωματική εργασία εντάσσεται στον τομέα της ασφάλειας των πληροφοριακών και επικοινωνιακών συστημάτων. Σκόπος της είναι η συγκριτική μελέτη δύο ευρέως διαδεδομένων συστημάτων ανίχνευσης εισβολών (Intrusion Detection Systems – IDS), εν ονόματι Zeek και Suricata, βασιζόμενοι στα αποτελέσματα που προέκυψαν κατά την αναπαραγωγή κακόβουλης δικτυακής κίνησης, υπό την μορφή pcap αρχείων.

Στόχος μας ήταν να συγκρίνουμε τα εν λόγω IDSs, μέσα από εξέταση και καταγραφή της συμπεριφοράς τους, με όσο το δυνατόν περισσότερες περιπτώσεις κακόβουλων λογισμικών, μελετώντας τα αρχεία καταγραφών για ενδείξεις παραβίασης (Indicators of Compromise – IoCs), ως συνεπακόλουθα της επίθεσης.

Η συγκριτική ανάλυση των ευρημάτων θα μας επιτρέψει αφενός να απεικονίσουμε συμπεράσματα σε επίπεδο σύγκρισης των δύο εργαλείων σε σχέση με την αποτελεσματικότητά τους, αφετέρου να δημιουργήσουμε ένα είδος συμβουλευτικού εργαλείου για κάθε ενδιαφερόμενο αναγνώστη.

1.3 Περιγραφή της μεθοδολογίας

Για την εκπόνηση της εργασίας μας πραγματοποιήσαμε σε πρώτο στάδιο μία βιβλιογραφική και διαδικτυακή έρευνα πάνω στο αντικείμενο, με λέξεις κλειδιά που αναφέρονται πιο πάνω. Σε δεύτερο στάδιο, με την βοήθεια εργαλείων προχωρήσαμε στην αναπαραγωγή κακόβουλης δικτυακής κίνησης (malware traffic), με σκοπό την συγκομιδή στοιχείων και την εξαγωγή συμπερασμάτων, με βάση τα καταγεγραμμένα αποτελέσματα που προέκυψαν από τα υπό σύγκριση συστήματα. Για τον λόγο αυτό, προχωρήσαμε σε διεξοδική μελέτη των παραγόμενων αρχείων καταγραφής (log files), για την ανεύρεση ενδείξεων παραβίασης (IoCs). Στην τρίτη φάση της μελέτης επικεντρωθήκαμε στις επιθέσεις και το κακόβουλο λογισμικό που αυτές περιείχαν. Έγινε προσπάθεια για συγκεντρωτική καταγραφή των τακτικών και τεχνικών (Tactics Techniques and Procedures[1] – TTPs) (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016), που τα συγκεκριμένα λογισμικά χρησιμοποιούν στον τρόπο λειτουργίας τους (modus operandi), σύμφωνα με τον πίνακα του MITRE ATT&CK. Στόχος μας ήταν να παρουσιάσουμε εκείνες τις τεχνικές που χρησιμοποιούνται περισσότερο (ή αλλιώς τις συνηθέστερες) στο συγκεκριμένο δείγμα. Μέρος της προσπάθεια αυτής ήταν η εκ νέου βιβλιογραφική και διαδικτυακή αναζήτηση βασισμένη αυτή την φορά στα κακόβουλα λογισμικά που περιέχονται στο δείγμα, έτσι ώστε να μελετηθεί ο τρόπος λειτουργίας τους. Περισσότερα για το δείγμα και τα κριτήρια επιλογής του αναφέρονται στην ενότητα 4.2. Θα πρέπει να σημειωθεί πως δεν προχωρήσαμε σε ανάκτηση του κακόβουλου λογισμικού και ανάλυσή του μέσω της διαδικασίας της αντίστροφης μηχανικής (reverse engineering), καθώς κάτι τέτοιο θα ήταν εκτός του εύρους της εργασίας.

1.4 Δομή

Η παρούσα εργασία διαρθρώνεται γύρω από πέντε διακριτά μέρη. Πιο συγκεκριμένα, μετά την εισαγωγή, στην ενότητα 2 έχουμε την παρουσίαση της σχετικής με το θέμα μας, βιβλιογραφίας που μελετήθηκε, ενώ στην ενότητα 3 εμφανίζονται οι απαραίτητοι ορισμοί για το θεωρητικό υπόβαθρο. Η ενότητα 4 αναφέρεται στην μεθοδολογία που ακολουθήθηκε. Εκεί γίνεται λόγος για την υποδομή, το δείγμα της εργασίας , ενώ ακολουθεί ενδεικτικά μία περίπτωση μελέτης. Στην ενότητα 5 παρουσιάζονται τα αποτελέσματα της σύγκρισης ως προς τα ευρήματα, καθώς επίσης και η ταξινόμηση των επιθέσεων με σκοπό την εξαγωγή χρήσιμων συμπερασμάτων, με τα οποία ολοκληρώνουμε την εργασία στην ενότητα 6.

1.5 Αναγνωστικό κοινό

Όπως πολύ εύστοχα αναφέρει η Cecil A. (Cecil, 2018), με την συνεχή ανάπτυξη των δικτύων των επιχειρήσεων, αυξάνεται και η υποχρέωση των διαχειριστών τους να είναι ενήμεροι και ικανοί να χειριστούν τους διαφορετικούς τύπους της κίνησης που διέρχεται από το δίκτυό τους. Με απώτερο σκοπό, περισσότερο την πρόληψη παρά την θεραπεία, οι διαχειριστές δικτύων πρέπει να παρακολουθούν την κυκλοφορία και την απόδοση του δικτύου και να είναι σε θέση να εγγυηθούν

[1] Tactics, Techniques and Procedures (TTP) https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures

πως δεν υφίστανται παραβιάσεις στην ασφάλεια. Επομένως, η εν λόγω εργασία απευθύνεται στο προσωπικό ασφαλείας και στους διαχειριστές δικτύων, στο προσωπικό τεχνικής υποστήριξης και στις ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών, οι οποίοι είναι υπεύθυνοι για την πρόληψη, την προετοιμασία ή την αντιμετώπιση περιστατικών κακόβουλου λογισμικού.

2

Μελέτη βιβλιογραφίας

Όπως αναφέραμε και στη ενότητα 1.3, μέρος της υλοποίησης της παρούσας διπλωματικής ήταν η βιβλιογραφική και διαδικτυακή έρευνα, η οποία σε πρώτη φάση είχε ως αντικείμενο πηγές σχετικές με σύγκριση ή αξιολόγηση εν γένει στον χώρο των IDSs. Σε δεύτερη φάση η αναζήτηση περιορίστηκε στα δύο IDSs που μας ενδιαφέρουν και αποτελούν το αντικείμενο μελέτης μας, ενώ στην τρίτη φάση η αναζήτηση επιπλέον περιελάμβανε πηγές σχετικές με κακόβουλη δικτυακή κίνηση (malware traffic) και το MITRE ATT&CK framework, περιορίζοντας ακόμα περισσότερο τον χώρο αναζήτησης. Τα αποτελέσματα της όλης διαδικασίας έδειξαν πως υπάρχουν διαφορετικές προσεγγίσεις όσον αφορά το θέμα της αξιολόγησης ενός IDS και αυτές παρουσιάζονται σε αυτή την ενότητα.

Στο μεγαλύτερο μέρος της υπάρχουσας βιβλιογραφίας, η σύγκριση ανάμεσα σε IDS πραγματοποιείται με γνώμονα την κατανάλωση πόρων του συστήματος και με σκοπό την μετέπειτα μείωσή της. Ουσιαστικά στην περίπτωση αυτή, η σύγκριση ή αξιολόγηση των IDSs βρίσκεται εγγύτερα σε επίπεδο εκτίμησης της απόδοσης του IDS, παρά της αποτελεσματικότητάς του, καθώς καταγράφονται και λαμβάνονται υπ' όψιν μετρικές όπως για παράδειγμα τα ποσοστά χρήσης μνήμης, επεξεργαστή και δικτύου.

Αυτό έκανε ο Albin E. (Albin, 2011), ο οποίος προχώρησε στην σύγκριση των Snort και Suricata και στην αξιολόγηση μεγεθών όπως ταχύτητα, απαιτήσεις μνήμης και ακρίβεια των μηχανών ανίχνευσης (detection engines) σε μία σειρά από πειράματα. Για την απαιτούμενη παρακολούθηση δικτυακής κίνησης χρησιμοποίησε το Education Research Network (ERN) του Naval Postgraduate School (NPS), καθώς επίσης και εργαλεία για την εκτέλεση μιας σειράς επιθέσεων όπως DDoS, πολλαπλές αποτυχημένες συνδέσεις (multiple failed logins) κ.ά.. Καταλήγει στο συμπέρασμα πως το Suricata είναι πιο ικανό να διαχειριστεί μεγαλύτερα φορτία δικτυακής κίνησης σε σχέση με το Snort, με παρόμοια ωστόσο ακρίβεια στα αποτελέσματα. Η εν λόγω εργασία δεν καλύπτει την περίπτωση του Zeek και σίγουρα υπολείπεται ως προς τις δοκιμές με πραγματική κακόβουλη κίνηση δικτύου.

Στο ίδιο μήκος κύματος και ο Hanninen M. (Hanninen, 2019), ο οποίος χρησιμοποιώντας ένα απλό δίκτυο από εικονικές μηχανές αξιολόγησε τρία IDSs (Snort, Suricata, Zeek) με γνώμονα τα ιδιαίτερα χαρακτηριστικά, την ποιότητα και την χρηστικότητα του καθενός και κριτήρια όπως μεταξύ άλλων, το πόσο καλά διατηρείται και υλοποιείται, πόσο εύκολα προσαρμόζεται και ρυθμίζεται και το πόσο καλά ανιχνεύει μία σειρά επιθέσεων (port scanning, password guessing, SQL injection). Ωστόσο, για τις επιθέσεις χρησιμοποιήθηκαν εργαλεία όπως το ARPSpooftool και

το Metasploit. Η εργασία ολοκληρώνεται εκφράζοντας την απορία αν τα συμπεράσματα που προέκυψαν ισχύουν και για πραγματική κίνηση δικτύου με πραγματικά περιστατικά.

Με ζωτικούς παράγοντες που επηρεάζουν και περιορίζουν την εφαρμογή των IDSs σε υψηλής ταχύτητας δίκτυα, ασχολήθηκαν οι Qinwen, Se-Young και Muhammad (Qinwen, Se-Young, Asghar, & Muhammad, 2020). Μελετώντας παράγοντες όπως ο βαθμός χρήσης του επεξεργαστή του συστήματος, η ταχύτητα επεξεργασίας των πακέτων, η ακρίβεια της ανίχνευσης και ο ρυθμός απώλειας πακέτων, στοχεύουν να δώσουν απάντηση στο ερώτημα αν είναι απαραίτητος ένας πολύ «ισχυρός» εξυπηρετητής (server) για την εγκατάσταση και την χρήση ενός IDS, το οποίο με την σειρά του θα μπορεί να διαχειριστεί αυτή την υψηλή ταχύτητα. Και αυτή την φορά τα συστήματα υπό σύγκριση είναι τα Snort και Suricata.

Ο ρυθμός απώλειας πακέτων, και τα ποσοστά χρήσης επεξεργαστή και μνήμης είναι το αντικείμενο μελέτης του Pihelgas M. (Pihelgas, 2012), στοχεύοντας σε μία συγκριτική αξιολόγηση τριών IDSs (Snort, Suricata, Zeek). Στην διαδικασία αυτή χρησιμοποιήθηκε τόσο «καθαρή», όσο και κακόβουλη κίνηση δικτύου, με την τελευταία να προκύπτει με χρήση του Metasploit. Τα IDSs εγκαταστάθηκαν σε διαφορετικά λειτουργικά συστήματα το καθένα και διενεργήθηκαν πειράματα αξιολόγησης πριν και μετά από σχετικές ρυθμίσεις που έγιναν σε αυτά, με σκοπό την βελτίωση της λειτουργίας τους. Άξια αναφοράς μεταξύ των αποτελεσμάτων είναι πως το Suricata λόγω της multi-threaded αρχιτεκτονικής του είχε καλή απόδοση, ενώ το Zeek αντιμετώπισε θέματα συμβατότητας και για τον λόγο αυτό δεν χρησιμοποιήθηκε σε πολλά από τα πειράματα.

Τα ίδια τρία IDSs θέλησε να συγκρίνει και ο Rodfoss J. (Rodfoss, 2011), αυτή την φορά όμως όλα εγκατεστημένα στο ίδιο σύστημα. Στην δική του περίπτωση, η σύγκριση εστιάζει στην διαδικασία εγκατάστασης και στην σύγκριση των ειδοποιήσεων (alerts) που αυτά παράγουν, καθώς τροφοδοτούνται τόσο από κακόβουλη (με χρήση Metasploit), όσο και από «καθαρή» δικτυακή κίνηση. Ιδιαίτερη έμφαση έδωσε και στον προσδιορισμό της ακρίβειας, θέλοντας να συγκρίνει τα Αληθώς-Αληθή (True-positive) και τα Ψευδώς-Αληθή (False-Positive) αποτελέσματα για κάθε ένα από τα IDSs.

Η σύγκριση των τριών open-source IDS (Snort, Suricata και Zeek) για την εφαρμογή τους σε δίκτυα μικρομεσαίων επιχειρήσεων (όπως άλλωστε συμβαίνει και στις προαναφερθείσες εργασίες), είναι το αντικείμενο έρευνας για τους Abdul W. et al (Abdul, Abdul, & Ammar, 2022). Η σύγκριση αυτή πραγματοποιείται επίσης με βάση τεχνικά χαρακτηριστικά (κατανάλωση πόρων, επεξεργασία πακέτων, ρυθμός απώλειας πακέτων, χωρητικότητα και καθυστέρηση). Στην περίπτωση αυτή, έγινε αναπαραγωγή φυσιολογικής, αλλά και κακόβουλης κίνησης δικτύου με την βοήθεια εργαλείων (Ostinato, IPERF3 and Pytbull), κάποια από τα οποία άλλωστε χρησιμοποίησαν και οι προηγούμενοι συγγραφείς.

Ο τομέας της μηχανικής μάθησης αποτελεί μία άλλη πτυχή της προσπάθειας για έρευνα, αξιολόγηση και βελτίωση των IDSs. Ο Μουζενίδης Π. (Μουζενίδης, 2022) στην εργασία του συνδέει το πρόβλημα της αποτυχίας των συστημάτων με την συνεχή μεταβολή των αρχιτεκτονικών τους και προτείνει την χρήση τεχνητής νοημοσύνης και ειδικότερα νευρωνικών δικτύων, για την υλοποίηση τριών αρχιτεκτονικών και την περαιτέρω αξιολόγησή τους με χρήση συνόλων δεδομένων. Την ίδια άποψη σχετικά με την διείσδυση της τεχνητής νοημοσύνης στα συστήματα ανίχνευσης συμμερίζεται και ο Παπαμαρτζιβάνος Δ. (Παπαμαρτζιβάνος, 2019).

Υποστηρίζει πως οι μέθοδοι μηχανικής μάθησης προσδίδουν ευελιξία στα συστήματα ανίχνευσης εισβολών και προτείνει τον σχεδιασμό και την υλοποίηση ενός αλγορίθμου ταξινόμησης (Dendron), βασισμένο σε γεννετικούς αλγόριθμους και δέντρα απόφασης. Σκοπός του είναι να ενισχυθούν οι μέθοδοι επαγωγής των κανόνων ανίχνευσης των IDSs. Οι Adabi M. et al (Adabi, Parman, & Aulia, 2022), σε μία ακόμα έρευνα στον τομέα των συστημάτων ανίχνευσης εισβολών με χρήση μηχανικής μάθησης, στοχεύουν στην ανάπτυξη ενός Security Information and Event Management (SIEM), μέρος του οποίου είναι το Zeek IDS. Επιθέσεις άρνησης παροχής υπηρεσιών (DDoS) χρησιμοποιήθηκαν για την δοκιμή και την αξιολόγηση των αντοχών του συστήματος. Οι μετρήσεις για την αξιολόγηση του συστήματος αφορούν την απόδοση ως προς την κατανάλωση πόρων (μνήμης και επεξεργαστή), για την εκάστοτε συνιστώσα. (IDS – Machine Learning – SIEM).

Οι Hashem A. et al (Hashem, et al., 2022) προχωρούν στην αξιολόγηση της αποτελεσματικότητας για μία σειρά από IDSs με την βοήθεια ενός ολοκληρωμένου fuzzy MCDM (Multi-Criteria Decision-Making) μοντέλου και οδηγούνται στο συμπέρασμα πως παρά το γεγονός ότι το Snort είναι μία ευρέως διαδεδομένη λύση στον χώρο των IDS, εντούτοις το Suricata εμφανίζει σημαντικά πλεονεκτήματα. Στην εργασία των Hafizul A., Ilir G. (Hafizul & Ilir, 2022) πραγματοποιείται δυναμική ανάλυση της ποικιλομορφίας που αφορά τα σύνολα των κανόνων των συστημάτων Snort και Suricata.

Οι Neha V. S. et al (Neha, Kavita, Gaurav, & Saurabh, 2021) διεξήγαγαν μία μελέτη για την απόδοση των Snort και Suricata, εκτελώντας μία σειρά από επιθέσεις με χρήση του εργαλείου Metasploit. Η συγκεκριμένη εργασία εξετάζει όχι μόνο μετρικές, όπως η απώλεια πακέτων και η κατανάλωση πόρων του συστήματος. Επεκτείνεται και στις ειδοποιήσεις (alerts) που προκύπτουν από τα δύο IDSs και διερευνά πως αυτές επηρεάζονται από αλλαγές στην αρχιτεκτονική του συστήματος, στο οποίο είναι εγκατεστημένα, καθώς και από την αύξηση του δικτυακού φορτίου. Το συμπέρασμα στο οποίο οδηγούνται είναι πως το Suricata υπερτερεί έναντι του Snort στον τομέα των alerts, όμως είναι αξιοσημείωτα πιο αργό.

Στο σημείο αυτό θα θέλαμε να αναφερθούμε σε μία εργασία η οποία παρουσιάζει ιδιαίτερο ενδιαφέρον (Μέμτσας, 2020). Ο συγγραφέας στην περίπτωση αυτή ασχολείται με την μελέτη των ιχνών που αφήνει η κακόβουλη δραστηριότητα σε ένα σύστημα, όπως αυτά ανιχνεύονται στα αρχεία καταγραφής (log files) του ίδιου του συστήματος. Εστιάζει δε σε συγκεκριμένη κατηγορία επιθέσεων που εντάσσονται στο πλαίσιο του MITRE ATT&CK (T1569.002 – Service Execution), όπως επίσης και σε συγκεκριμένο λειτουργικό σύστημα (Windows 10). Και παρά το γεγονός πως δεν ασχολείται με κάποιο IDS, εντούτοις αναφέρεται αφενός σε ανίχνευση κακόβουλης δραστηριότητας βασισμένη σε αρχεία καταγραφής (log files), αφετέρου στην εφαρμογή του πλαισίου MITRE ATT&CK. Και παρουσιάζει ιδιαίτερο ενδιαφέρον επειδή ως προς το πρώτο σκέλος, ακολουθήσαμε την ίδια μέθοδο στην παρούσα εργασία (στο δεύτερο στάδιο σύμφωνα με την ενότητα 1.3), όπου μελετήσαμε τα αρχεία καταγραφής, ενώ ως προς το δεύτερο σκέλος εντάσσεται στην ενότητα 5.2, κατά την οποία εφαρμόσαμε το συγκεκριμένο πλαίσιο. Η διαφορά είναι πως εμείς μελετήσαμε αρχεία καταγραφής των IDSs και εφαρμόσαμε το συγκεκριμένο πλαίσιο στο σύνολο του δείγματος των επιθέσεων, χωρίς να εστιάσουμε σε κάποιο λειτουργικό σύστημα ή κατηγορία επιθέσεων.

Από τα παραπάνω καθίσταται σαφές, πως η εν λόγω εργασία διαφέρει από τις μέχρι τώρα προσεγγίσεις, κάτι που σημαίνει πως προσφέρει άλλη μία οπτική στην πολυπρισματική θεώρηση του χώρου των συστημάτων ανίχνευσης εισβολών δικτύου.

Στην ενότητα αυτή έγινε παρουσίαση της υπάρχουσας βιβλιογραφίας που εντάσσεται στον ευρύτερο χώρο των IDSs και σχετίζεται με την σύγκριση και την αξιολόγησή τους. Είδαμε πως έχουν γίνει πολλές ερευνητικές προσπάθειες προς την κατεύθυνση αυτή, πράγμα που φανερώνει την αξία του θέματος για την ερευνητική κοινότητα και όχι μόνο. Και αυτό είναι λογικό εφόσον με την αξιολόγηση ανακαλύπτουμε τα τρωτά σημεία τους κι επομένως οδηγούμαστε στην βελτιστοποίησή τους. Και με αυτό ως απώτερο σκοπό, είδαμε να χρησιμοποιούνται διαφορετικά κριτήρια, διαφορετικές τεχνολογίες και διαφορετικές προσεγγίσεις. Η ενότητα που ακολουθεί περιέχει τις απαραίτητες για το θεωρητικό υπόβαθρο έννοιες.

3

Βασικές έννοιες

Στην ενότητα αυτή παροουσιάζονται οι βασικές έννοιες που περιέχονται στην εργασία, έτσι ώστε να υπάρξει ένα κοινό σημείο αναφοράς με τον αναγνώστη και να τεθεί το εύρος της εργασίας σε θεωρητικό επίπεδο.

3.1 Τι είναι IDS (Intrusion Detection System)

Καθώς ο ρυθμός εκδήλωσης επιθέσεων και ο αντίκτυπος που αυτές προκαλούν συνεχώς αυξάνεται τα τελευταία χρόνια, τα Συστήματα Ανίχνευσης Εισβολών (IDSs), για την συντριπτική πλειοψηφία των επιχειρήσεων, αποτελούν σημαντικό πυλώνα στην υποδομή ασφάλειας και στην υλοποίηση του μοντέλου defense-in-depth[2] (NIST, 2011, p. B3). Πριν όμως δούμε τι είναι ένα τέτοιο σύστημα θα πρέπει να εξετάσουμε τι είναι η ανίχνευση εισβολής (intrusion detection).

Ανίχνευση Εισβολής (*intrusion detection*) ορίζεται ως η διαδικασία παρακολούθησης των περιστατικών που συμβαίνουν σε ένα πληροφοριακό σύστημα ή δίκτυο και η ανάλυσή τους για ενδείξεις που αφορούν πιθανά περιστατικά, τα οποία αποτελούν παραβιάσεις ή επικείμενη απειλή για παραβίαση των πολιτικών ασφάλειας, χρήσης και των πρότυπων πρακτικών ασφάλειας (Scarfone & Mell, 2007).

Κατ' επέκταση, με τον όρο *Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System)* αναφερόμαστε σε συστήματα λογισμικού ή υλικού, τα οποία αυτοματοποιούν την διαδικασία παρακολούθησης (monitoring) των περιστατικών που συμβαίνουν στα πληροφοριακά συστήματα ή στα δίκτυα και τα αναλύουν παρέχοντας ενδείξεις για προβλήματα ασφάλειας (Bace & Mell, 2001).

3.2 Γιατί να χρησιμοποιήσουμε ένα IDS

Η ανίχνευση εισβολής επιτρέπει σε οργανισμούς και επιχειρήσεις να προστατεύουν τα συστήματά τους από τις απειλές που συνοδεύουν την ολοένα και αυξανόμενη συνδεσιμότητα του δικτύου (Bace & Mell, 2001). Επομένως, το ερώτημα που προκύπτει δεν είναι το «αν θα πρέπει να

[2] Defense-in-depth: Στρατηγική της ασφάλειας πληροφοριών που ενσωματώνει ανθρώπινο δυναμικό, τεχνολογία και επιχειρησιακές δεξιότητες, με σκοπό την εγκατάσταση μεταβλητών εμποδίων σε πολλαπλά επίπεδα σε έναν οργανισμό. https://csrc.nist.gov/glossary/term/defense_in_depth#

χρησιμοποιήσουμε» IDSs , αλλά μάλλον το «πια από τα χαρακτηριστικά και τις δυνατότητές τους θα πρέπει να χρησιμοποιήσουμε».

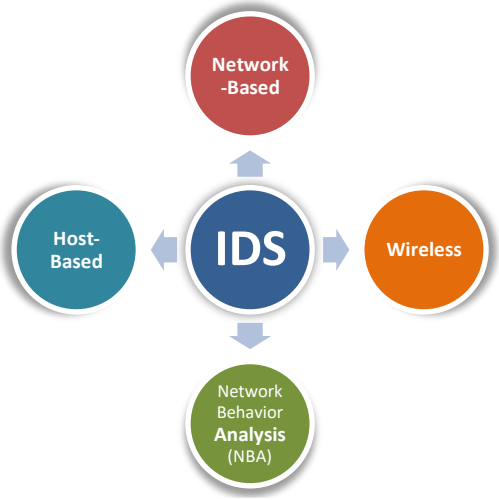
Η εγκατάσταση και αξιοποίηση ενός IDS προσφέρει σημαντικά οφέλη για τους εξής λόγους (Bace & Mell, 2001):

- Με αυτό τον τρόπο αυξάνεται στους εν δυνάμει επιτιθέμενους η πεποίθηση πως μπορεί να αποκαλυφθούν, με αποτέλεσμα να αποτρέπονται κακόβουλες ενέργειες.
- Με τα IDS είμαστε σε θέση να ανιχνεύσουμε επιθέσεις και παραβιάσεις στην ασφάλεια, οι οποίες δεν είναι δυνατόν να αποτραπούν από άλλα μέτρα ασφάλειας.
- Μπορούμε να εντοπίσουμε και να αντιμετωπίσουμε δραστηριότητες όπως η ανίχνευση δικτύου (network scanning), οι οποίες αποτελούν κατ' εξοχήν προοίμιο επίθεσης.
- Μπορούμε να εντοπίσουμε και να στοιχειοθετήσουμε μία απειλή που πιθανόν αντιμετωπίζει ο οργανισμός.
- Μπορεί να λειτουργήσει ως εγγύηση ποιότητας για τους διαχειριστές και σχεδιαστές δικτύων, ειδικότερα σε μεγάλης κλίμακας επιχειρήσεις.
- Μας παρέχει χρήσιμες πληροφορίες σχετικά με εισβολές που λαμβάνουν χώρα, επιτρέποντας την διάγνωση, την ανάκαμψη και την διόρθωση των λαθών που οδήγησαν στην παραβίαση.

Επιπλέον, δεν πρέπει να παραγνωρίζουμε το γεγονός πως τα Συστήματα Ανίχνευσης Εισβολών συμπεριλαμβάνονται στις βέλτιστες πρακτικές διασφάλισης της δικτυακή υποδομής ενός Πληροφοριακού συστήματος (Παππάς, 2021, σ. 51).

3.3 Τύποι IDS

Σύμφωνα με τον οργανισμό NIST (National Institute of Standards and Technology), υπάρχουν πολλοί τύποι ΣΑΕ. Με κριτήριο το είδος των γεγονότων που παρακολουθούν και τον τρόπο με τον οποίο υλοποιούνται διακρίνονται σε τέσσερις κατηγορίες, οι οποίες φαίνοται στην Εικόνα 3 και περιγράφονται συνοπτικά στον Πίνακα 1 (Scarfone & Mell, 2007, σ. 6)



Εικόνα 3. Οι τύποι των IDS με βάση το είδος των γεγονότων που παρακολουθούν και τον τρόπο υλοποίησης

Intrusion Detection Systems	
Network-Based	Παρακολουθεί την κίνηση του δικτύου (σε συγκεκριμένο τμήμα του ή για συγκεκριμένο αριθμό συσκευών) και αναλύει τα πρωτόκολλα επιπέδου δικτύου και εφαρμογής με σκοπό να ανιχνεύσει ύποπτη δραστηριότητα. Συνήθως υλοποιείται σε σημεία (π.χ. firewalls, routers, VPN servers) που βρίσκονται στα όρια του δικτύου.
Wireless	Παρακολουθεί την κίνηση ασύρματων δικτύων και αναλύει τα πρωτόκολλα με σκοπό να ανιχνεύσει ύποπτη δραστηριότητα που αφορά τα ίδια τα πρωτόκολλα. Δεν ανιχνεύει ύποπτη δραστηριότητα σε επίπεδο εφαρμογής ή στα υψηλότερα στρώματα επιπέδου δικτύου (π.χ. TCP, UDP). Τοποθετείται σε σημεία είτε εντός των ορίων του ασύρματου δικτύου της επιχείρησης/οργανισμού, είτε σε σημεία που θα μπορούσε να υπάρξει μη εξουσιοδοτημένο ασύρματο δίκτυο.
Network Behavior Analysis (NBA)	Παρακολουθεί την κίνηση του δικτύου με σκοπό να αναγνωρίσει απειλές προερχόμενες από ασυνήθιστες ροές κίνησης δεδομένων (DDoS επιθέσεις), συγκεκριμένες μορφές κακόβουλου λογισμικού (worms, backdoors), καθώς και παραβιάσεις στην πολιτική (π.χ. ένα σύστημα πελάτη να παρέχει υπηρεσίες σε άλλα συστήματα). Συνήθως χρησιμοποιούνται για τον έλεγχο εσωτερικών δικτύων ή για τον έλεγχο της επικοινωνίας του εσωτερικού με εξωτερικά δίκτυα.
Host-Based	Παρακολουθεί τα χαρακτηριστικά ενός και μόνο host, καθώς και τα γεγονότα που συμβαίνουν σε αυτόν, ώστε να αναγνωρίσει ύποπτη δραστηριότητα (π.χ. αρχεία καταγραφών συστήματος, διαδικασίες και εφαρμογές που εκτελούνται, πρόσβαση και τροποποίηση αρχείων και αλλαγές ρυθμίσεων του συστήματος ή των εφαρμογών).

Πίνακας 1. Συνοπτική περιγραφή των τύπων IDS

Δύο από τα πιο διαδεδομένα open-source IDS είναι τα Zeek και Suricata, που αποτελούν και το αντικείμενο μελέτης της παρούσας εργασίας. Τα δύο αυτά συστήματα ανήκουν στην κατηγορία των *Network-based IDS*, του Πίνακα 1.

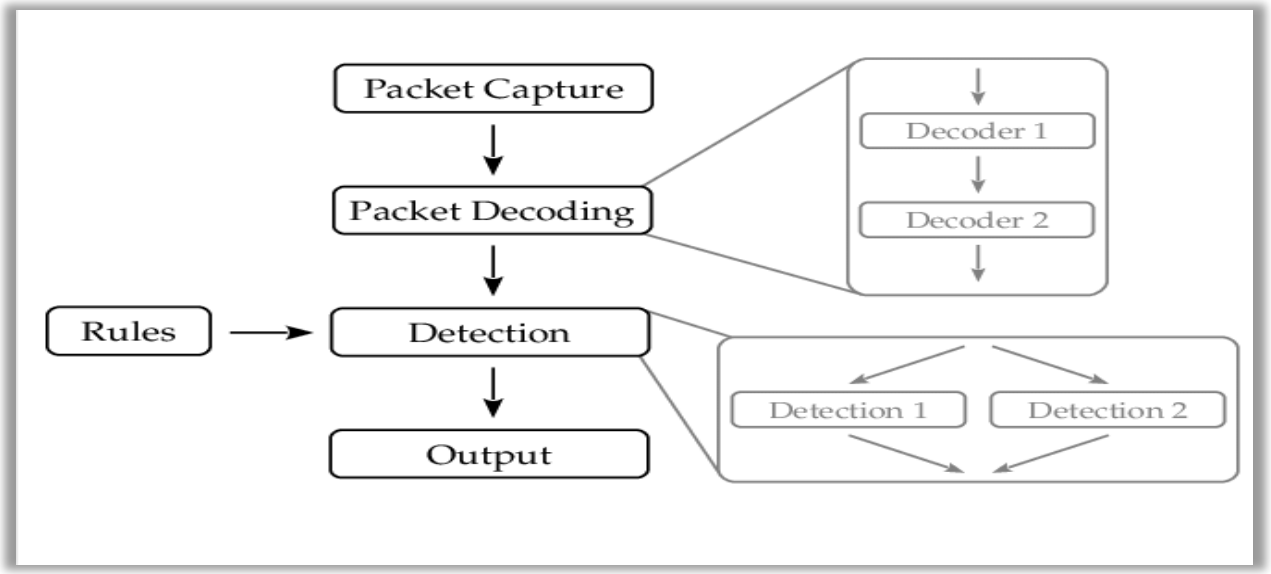
Στην συνέχεια, θα αναφερθούμε συνοπτικά σε αυτά, σκιαγραφόντας ορισμένες τεχνικές διαφορές τους. Δεν θα επεκταθούμε ωστόσο στα τεχνικά χαρακτηριστικά τους, καθώς η μελέτη μας εστιάζει κυρίως στην συμπεριφορά τους απέναντι σε κακόβουλη δικτυακή κίνηση και συγκεκριμένα στα παραγόμενα alerts.

3.4 Suricata IDS

Το Suricata[3] είναι ένα ΣΑΕ, το οποίο εκτελεί *deep packet inspection*[4]*(dpi,)* ταυτίζοντας μοτίβα (pattern matching) δικτυακής κίνησης, με εκείνα κακόβουλων λογισμικών. Στην Εικόνα 4

[3] https://suricata.io/

φαίνεται η multi-threaded αρχιτεκτονική του συστήματος, η οποία το κάνει να υπερέχει σε απόδοση έναντι των υπολοίπων IDSs (Prenosil, Hammoudeh, Ghafir, & Svoboda, 2016).



Εικόνα 4. Η αρχιτεκτονική του Suricata IDS

Έχει υλοποιηθεί με γλώσσα προγραμματισμού C και για τους κανόνες (rules) ανίχνευσης χρησιμοποιείται η Lua.

Πρόκειται για ένα IDS που ανήκει στην κατηγορία των *signature-based*. Αυτό σημαίνει πως για να ανιχνεύσει κάποιο κακόβουλο λογισμικό, θα πρέπει πρώτα αυτό να έχει αποκαλυφθεί (ή ανακαλυφθεί). Με άλλα λόγια, τα IDS της συγκεκριμένης κατηγορίας μειονεκτούν στις 0-day επιθέσεις για τον απλούστατο λόγο πως δεν υπάρχουν ακόμα signatures. Το κενό αυτό έρχεται να καλύψει το Zeek, το οποίο ακολουθεί διαφορετική μέθοδο ανίχνευσης, όπως θα δούμε παρακάτω.

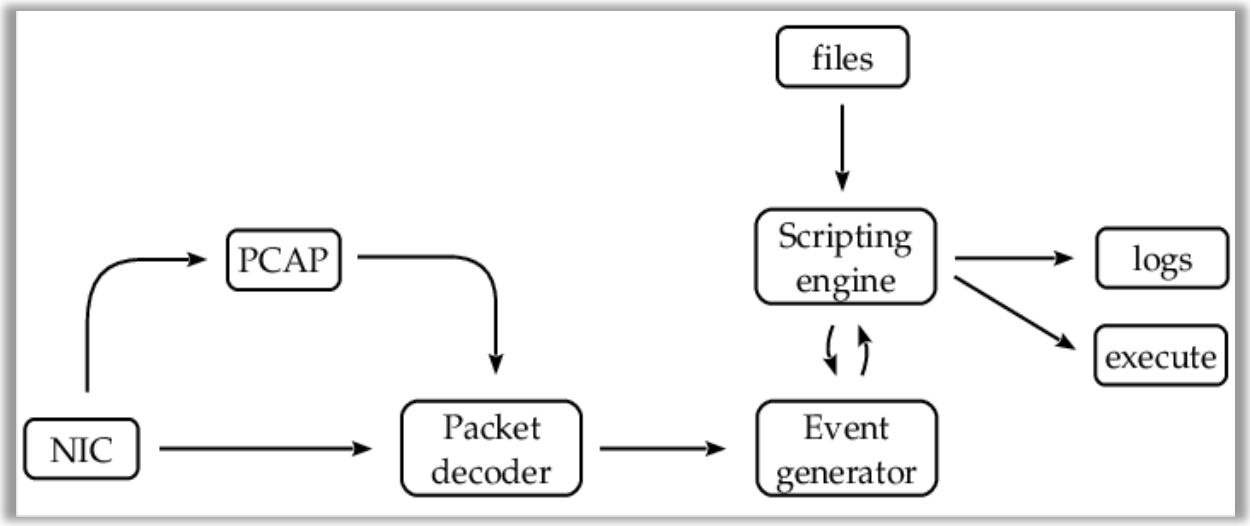
Θα πρέπει να σημειωθεί πως το Suricata διαθέτει και λειτουργία IDPS (Intrusion Detection and Prevention System). Στην λειτουργία αυτή παρέχεται επιπλέον η δυνατότητα αποτροπής (Prevention) της απειλής που ενδεχομένως έχει ανιχνευθεί. Το γεγονός όμως πως το Zeek δεν διαθέτει αυτή την λειτουργία σημαίνει πως δεν υπάρχει σύγκριση και συνεπώς για τον λόγο αυτό δεν λαμβάνεται υπόψιν.

3.5 Zeek IDS

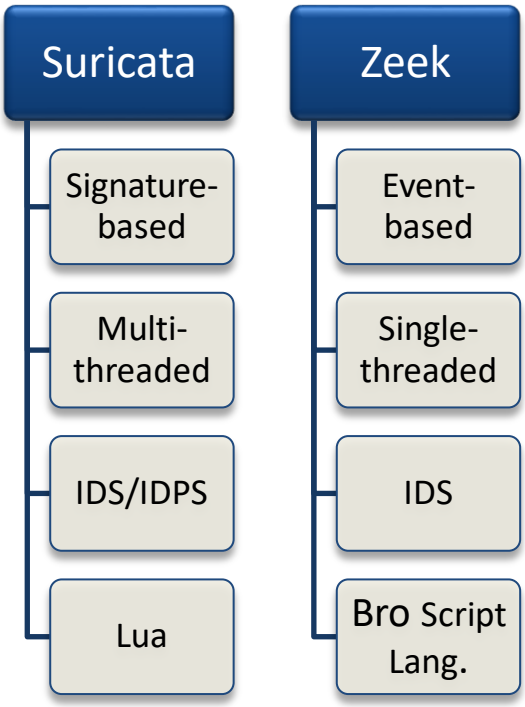
Το Zeek[5] αποτελεί μία άλλη επιλογή στον χώρο των IDSs. Εκτελεί επίσης *deep packet inspection (dpi)* χρησιμοποιώντας όμως ανάλυση event-based. Αυτό σημαίνει πως βασίζεται στα events που λαμβάνουν χώρα ανάλογα με το τι συμβαίνει στην κίνηση του δικτύου. Και αυτό με την σειρά του, πως με αυτόν τον τύπο dpi πραγματοποιείται ανίχνευση με βάση την σημασιολογία (σημασιολογικό ταίριασμα – semantic matching), σε αντίθεση με το Suricata, το οποίο εκτελεί όπως προαναφέρθηκε pattern matching. Στην εικόνα 5 φαίνεται η single-threaded αρχιτεκτονική του συστήματος σε *standalone* λειτουργία (Prenosil, Hammoudeh, Ghafir, & Svoboda, 2016). Επίσης, μπορεί να λειτουργήσει και ως κατανεμημένη multi-threaded εφαρμογή υπό την μορφή *cluster*. Εχει υλοποιηθεί με γλώσσα προγραμματισμού C, ομοίως με το Suricata, ωστόσο για τα

[4] https://www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI
[5] https://zeek.org/

scripts χρησιμοποιείται Bro Language. Στον Εικόνα 6 γίνεται μία συγκεντρωτική παρουσίαση των βασικών τεχνικών διαφορών ανάμεσα στα δύο IDSs.



Εικόνα 5. Η αρχιτεκτονική του Zeek IDS



Εικόνα 6. Οι κυριότερες από τις τεχνικές διαφορές μεταξύ Suricata και Zeek

Στην ενότητα αυτή, είδαμε ορισμένες βασικές έννοιες για τα IDSs. Αρχικά αναφερθήκαμε στο τι είναι, ποια η αξία τους και σε ποιους διαφορετικούς τύπους διακρίνονται με βάση τον τρόπο υλοποίησης και το είδος των γεγονότων που παρακολουθούν. Στην συνέχεια, παρουσιάσαμε τα υπό εξέταση Zeek και Suricata αναφέροντας ορισμένα από τα βασικά χαρακτηριστικά που διαφοροποιούν το ένα από το άλλο.

Τα IDS αποτελούν ένα πολύτιμο εργαλείο που προσφέρει στον διαχειριστή ενός δικτύου την δυνατότητα να αντιδρά έγκαιρα στην ανίχνευση κάποιας ύποπτης δραστηριότητας ή ακόμα και σε μία ενδεχόμενη επίθεση. (Παππάς, 2021)

Η ενότητα που έπεται, περιλαμβάνει την μεθοδολογία που ακολουθήθηκε για την υλοποίηση της εργασίας. Ξεκινά με λεπτομέρειες σχετικά με την υποδομή και το δείγμα και ολοκληρώνεται με μία περίπτωση μελέτης.

4

Μεθοδολογία

Η ενότητα της μεθοδολογίας αποτελείται από 3 μέρη. Στο πρώτο θα αναφερθούμε σε υλικό (hardware) και λογισμικό (software) που χρησιμοποιήσαμε. Ακολουθεί το δεύτερο μέρος, όπου περιγράφουμε λεπτομέρειες για το δείγμα των επιθέσεων, όπως για παράδειγμα τα κριτήρια επιλογής του και κλείνουμε με την περιγραφή ενδεικτικά μίας περίπτωσης μελέτης και των αντίστοιχων ευρημάτων.

4.1 Υποδομή

Για την εκπόνηση της εργασίας χρησιμοποιήθηκαν οι κάτωθι πόροι:

4.1.1 Hardware

Τα πειράματα διεξήχθησαν σε έναν Η/Υ, του οποίου τα χρακτηριστικά βλέπουμε στον Πίνακα 2.

Host PC	
CPU	Intel® Core™ i7 10750H CPU@2.60GHz
RAM	16GB
OS	Windows 10

Πίνακας 2. Τα χαρακτηριστικά του host PC

4.1.2 Software

Στο παραπάνω μηχάνημα εγκαταστήσαμε το εργαλείο *VirtualBox*[6] έκδοση 6.1.16, με σκοπό να εκτελέσουμε τα πειράματά μας σε μία εικονική μηχανή με τα χαρακτηριστικά του Πίνακα 3.

Virtual Machine	
CPU	4 cores
RAM	8GB
OS	Ubuntu Desktop 20.04.05 (Focal Fossa)
HD	100GB

Πίνακας 3. Τα χαρακτηριστικά της εικονικής μηχανής

[6] https://www.virtualbox.org/

Εν συνεχεία, εγκαταστήσαμε τα παρακάτω εργαλεία στην εικονική μηχανή.

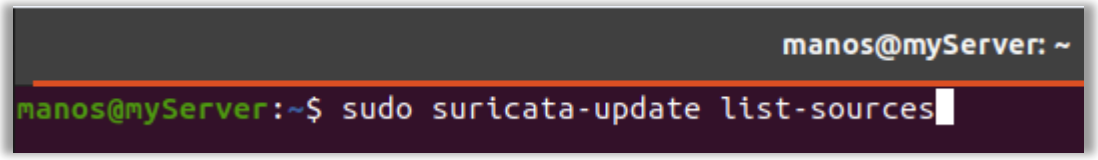
Tools	version
Suricata NIDS	6.0.9
Zeek NIDS	5.0.4
tcpreplay[7]	4.3.2

Πίνακας 4. Τα εργαλεία που εγκαταστάθηκαν στο vm

Δεν θα επεκταθούμε στην διαδικασία εγκατάστασης των εργαλείων καθώς θεωρούμε πως πρόκειται για τετριμμένη διαδικασία. Θα αναφερθούμε όμως σε κανόνες που προσθέσαμε.

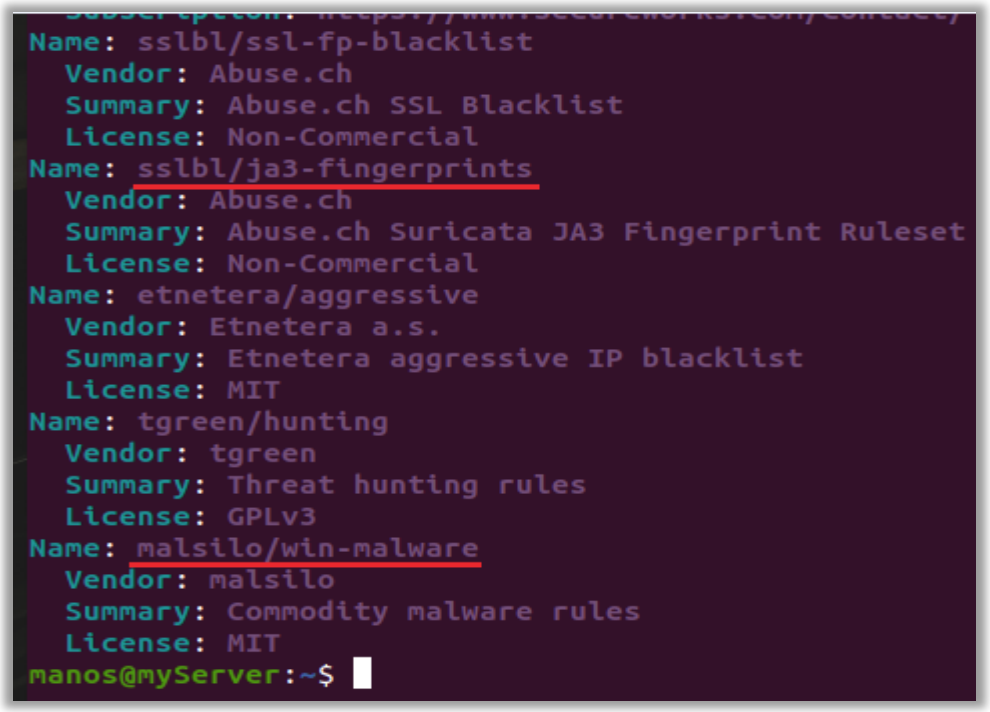
- **Suricata**

Η παρακάτω εντολή επιστρέφει μία λίστα από repositories (δωρεάν και μη), από όπου μπορούμε να εισάγουμε κανόνες (rules) για το Suricata.



Εικόνα 7. Η εντολή για τα repositories με τους κανόνες

Στην Εικόνα 8 εμφανίζονται τα repositories από τα οποία προμηθευτήκαμε τους κανόνες για τις δοκιμές μας.



Εικόνα 8. Τα σύνολα των κανόνων που προσθέσαμε στο Suricata

[7] https://tcpreplay.appneta.com/

Το σύνολο κανόνων *sslbl/ja3-fingerprints* προσφέρει «αποτυπώματα» ή αλλιώς υπογραφές για τον έλεγχο των SSL συνδέσεων και των πιστοποιητικών, ενώ το *malsilo/win-malware* τις αντίστοιχες για επιθέσεις σε Windows λειτουργικά συστήματα. Στην συνέχεια, ενεργοποιούμε τους κανόνες, όπως φαίνεται στην Εικόνα 9

```
manos@myServer:~$ sudo suricata-update enable-source malsilo/win-malware
27/9/2022 -- 18:03:57 - <Info> -- Using data-directory /var/lib/suricata.
27/9/2022 -- 18:03:57 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
27/9/2022 -- 18:03:57 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
27/9/2022 -- 18:03:57 - <Info> -- Found Suricata version 6.0.6 at /usr/bin/suricata.
27/9/2022 -- 18:03:57 - <Info> -- Creating directory /var/lib/suricata/update/sources
27/9/2022 -- 18:03:57 - <Info> -- Enabling default source et/open
27/9/2022 -- 18:03:57 - <Info> -- Source malsilo/win-malware enabled
manos@myServer:~$ sudo suricata-update
```

Εικόνα 9. Ενεργοποίηση των κανόνων

Στο σημείο αυτό, για να ελέγξουμε αν όλα λειτουργούν σωστά, δημιουργούμε πρώτα έναν υποτυπώδη κανόνα που ανιχνεύει ICMP Ping.

```
  GNU nano 4.8
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping"; sid:1; rev:1)
```

Εικόνα 10. Ένας απλός κανόνας (rule) για ICMP ping

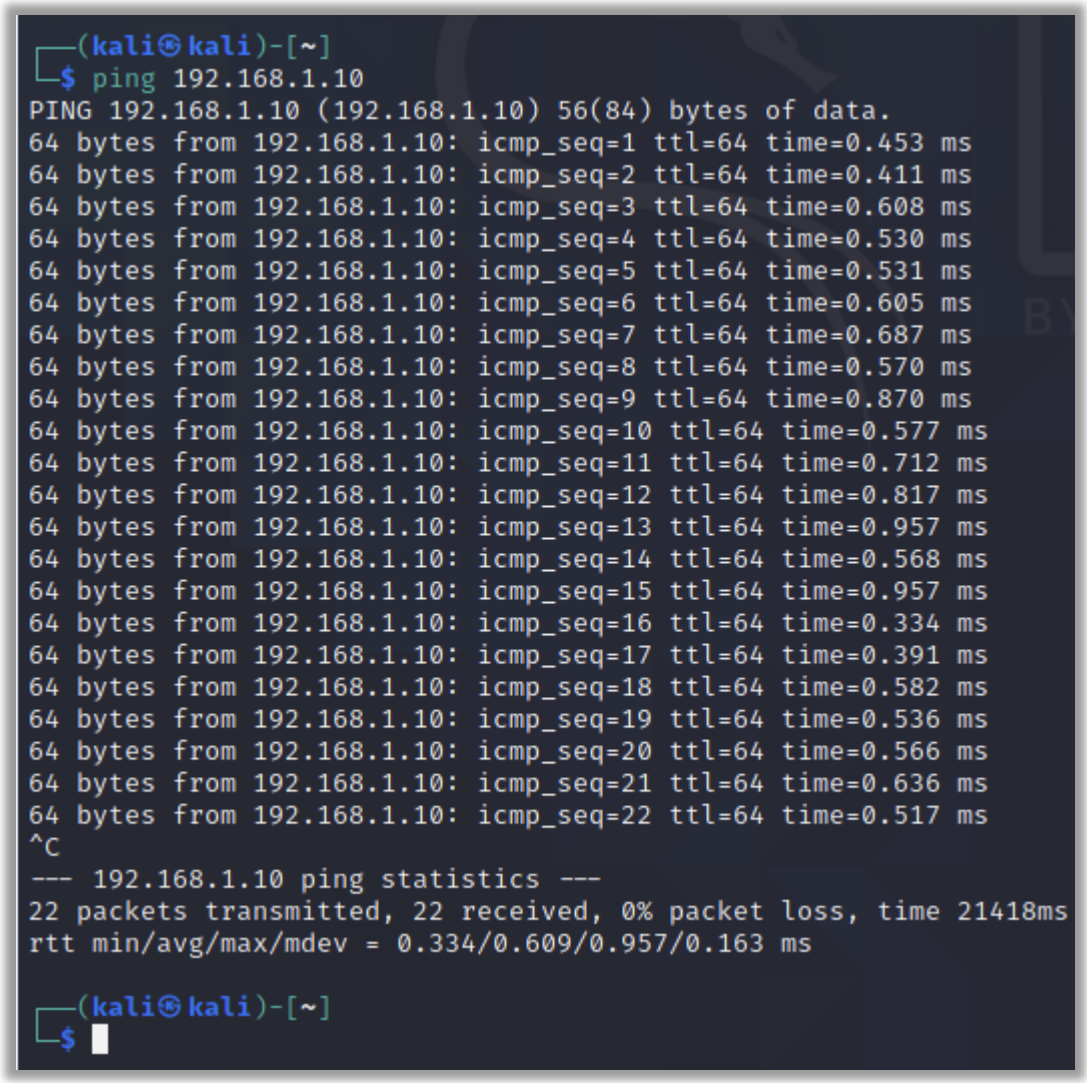
Και στην συνέχεια ενεργοποιούμε το IDS

```
manos@myServer:~$ sudo systemctl start suricata.service
manos@myServer:~$ sudo systemctl status suricata.service
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (running) since Tue 2022-09-27 18:16:25 EEST; 6s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 5893 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
      Tasks: 1 (limit: 9449)
     Memory: 264.1M
     CGroup: /system.slice/suricata.service
             └─5902 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid --af-packet -D -vvv

Σεπ 27 18:16:25 myServer systemd[1]: Starting LSB: Next Generation IDS/IPS...
Σεπ 27 18:16:25 myServer suricata[5893]: Likely stale PID 978 with /var/run/suricata.pid exists, but process is not running!
Σεπ 27 18:16:25 myServer suricata[5893]: Removing stale PID file /var/run/suricata.pid
Σεπ 27 18:16:25 myServer suricata[5893]: Starting suricata in IDS (af-packet) mode... done.
Σεπ 27 18:16:25 myServer systemd[1]: Started LSB: Next Generation IDS/IPS.
manos@myServer:~$
```

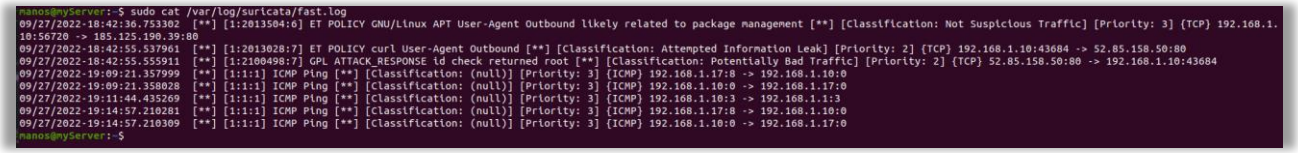
Εικόνα 11. Το Suricata σε λειτουργία

και εκτελούμε μία σειρά από pings από μία άλλη εικονική μηχανή Kali, Εικόνα 12.



Εικόνα 12. Μία σειρά από pings προερχόμενα από Kali Linux

Τέλος, ελέγχουμε το αρχείο *fast.log* για καταγραφές, Εικόνα 13.



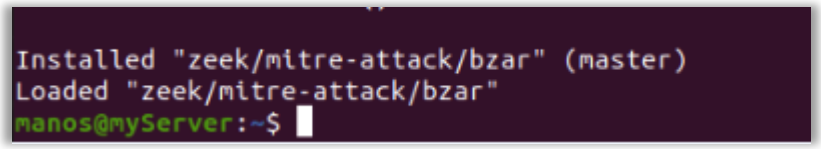
Εικόνα 13. Το αρχείο fast.log με καταγεγραμμένα pings που εκτελέσαμε

Εφόσον όλα λειτουργούν σωστά προχωράμε στο επόμενο IDS που είναι το Zeek.

- **Zeek**

Όσον αφορά στο Zeek, η μόνη προσθήκη που πραγματοποιήσαμε είναι το πακέτο *bzar*[8] (Marx, 2017). Πρόκειται για ένα πακέτο υλοποιημένο από τον Fernandez Mark και την κοινότητα του Zeek, με σκοπό να δημιουργούνται καταγραφές στο *notice.log* κάθε φορά που θα παρατηρείται ύποπτη δραστηριότητα στα SMB logs.

[8] https://docs.zeek.org/en/master/logs/smb.html



Εικόνα 14. Εγκαταστάση του bzar package

Πέρα από αυτές τις προσθήκες δεν πραγματοποιήσαμε καμία άλλη αλλαγή. Επίσης, δεν κάναμε κάποια περαιτέρω ρύθμιση σε αρχεία, εκτός από τις απαραίτητες. Σκόπος μας ήταν να αξιολογήσουμε την συμπεριφορά των IDS με ρυθμίσεις όσο πιο κοντά στις αρχικές. Με αυτό τον τρόπο, θα έχουμε επίσης την δυνατότητα να αξιολογήσουμε και τους κανόνες που προσθέσαμε.

4.2 Δείγμα

Το δείγμα των επιθέσεων που χρησιμοποιήθηκε στα πλαίσια των δοκιμών της διπλωματικής, απαρτίζεται από 91 pcap αρχεία αποκλειστικά με κακόβουλη δικτυακή κίνηση. Στόχος μας είναι η αξιολόγηση να γίνει με πραγματικά περιστατικά.

Επιπλέον, επιθυμούμε να αξιολογήσουμε τα δύο IDSs με όσο το δυνατόν περισσότερα είδη κακόβουλου λογισμικού. Επομένως, και η επιλογή των pcap αρχείων έγινε με το ίδιο σκεπτικό. Επίσης, επιλέξαμε αρχεία κατά το χρονικό διάστημα 2017 – 2022 έτσι ώστε, αφενός να παρατηρήσουμε τυχόν αλλαγές που μπορεί να υφίστανται τα διάφορα είδη κακόβουλου λογισμικού με την πάροδο του χρόνου, αφετέρου να δούμε πως συμπεριφέρονται τα δύο IDSs τόσο με προγενέστερες όσο και με μεταγενέστερες εκδόσεις των λογισμικών αυτών.

Οι πηγές προέλευσης των αρχείων αναφέρονται στο Παράρτημα Ι.

4.3 Περίπτωση μελέτης

4.3.1 Η διαδικασία

Έχοντας πλέον τα pcap αρχεία συγκεντρωμένα και τα απαραίτητα εργαλεία εγκατεστημένα μπορούμε να ξεκινήσουμε τις δοκιμές μας. Η διαδικασία που ακολουθήθηκε περιλαμβάνει τα εξής βήματα:

Για κάθε ένα από τα pcap αρχεία:

1. Αναπαράγουμε την κακόβουλη δικτυακή κίνηση με χρήση του εργαλείου tcpreplay, έχοντας ενεργοποιημένο μόνο το Suricata IDS.
2. Επαναλαμβάνουμε την αναπαραγωγή με ενεργοποιημένο αυτή την φορά μόνο το Zeek IDS.
3. Συλλογή των logfiles που παρήγαγαν τα δύο IDSs και ενδελεχή έρευνά τους με σκοπό την εύρεση στοιχείων και ενδείξεων παραβίασης ή ύπαρξης κακόβουλου λογισμικού. Ενδείξεις, όπως για παράδειγμα τα εκτελέσιμα αρχεία (portable executables) από όπου ξεκίνησε η παραβίαση, τα ηλ. μηνύματα που εστάλησαν κατά την διάρκεια μίας malspam εκστρατείας (malspam campaign) ή ακόμα και τις κινήσεις, στις οποίες προχώρησε το λογισμικό μετά την μόλυνση.

4. Στην συνέχεια, προχωρήσαμε σε καταγραφή και σύγκριση των ευρημάτων ανάμεσα στα δύο IDSs, τα αποτελέσματα της οποίας παρουσιάζονται στην ενότητα 5.

Για λόγους πληρότητας της εργασίας, θα παραθέσουμε ενδεικτικά τα ευρύματα μίας εκ των περιπτώσεων. Φυσικά δεν θα ήταν δυνατόν να συμπεριλάβουμε όλα τα ευρύματα από όλες τις επιθέσεις εντός της εργασίας, λόγω του μεγάλου μεγέθους που θα αποκτούσε. Ωστόσο, είναι διαθέσιμα σε κάθε ενδιαφερόμενο προς μελέτη[9].

4.3.2 Ενδεικτική περίπτωση μελέτης

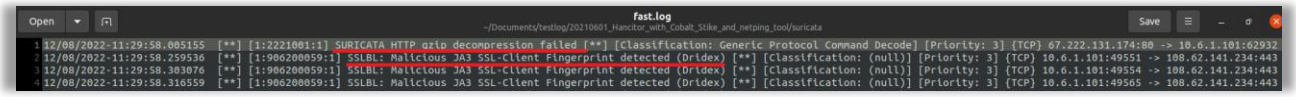
Το pcap αρχείο με το οποίο θα ασχοληθούμε είναι το "81. 20210601_Hancitor_with_Cobalt_Strike_and_netping_tool". Πρόκειται για μία περίπτωση malspam που συνδυάζει downloader[10] (Hancitor), Remote Access Tool (RAT), και απομακρυσμένη εκτέλεση αρχείου (portable executable) με lateral movement. Τα ευρήματα από την επίθεση αυτή παρουσιάζονται παρακάτω.

- ***Suricata***

Το πρώτο αρχείο στο οποίο ανατρέχουμε είναι το *fast.log*. Στο αρχείο αυτό εμφανίζονται τα alerts που παράγει το IDS, χωρίς αυτό να σημαίνει πως alerts εμφανίζονται πάντα. Εκείνα που πήραμε από το συγκεκριμένο pcap αρχείο είναι:

1. `SURICATA HTTP gzip decompression failed`
2. `SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Dridex`[11]`)`
3. `SURICATA HTTP unable to match response to request`

όπως φαίνεται στις Εικόνες 15 και 16 που ακολουθούν.



Εικόνα 15. Suricata alerts – fast.log pt1

Εικόνα 16. Suricata alerts – fast.log pt2

Από το αρχείο αυτό μπορούμε να δούμε μεταξύ άλλων πως ανιχνεύθηκε ένα συμπιεσμένο αρχείο, αναγνωρίστηκε κάποιο malware και να πληροφορηθούμε για τις IP διευθύνσεις των εμπλεκομένων hosts. Επιπλέον, από το δεύτερο alert συμπεραίνουμε πως οι κανόνες JA3 τους οποίους προσθέσαμε, όντως λειτουργούν.

Το επόμενο αρχείο, από το οποίο θα προσπαθήσουμε να αντλήσουμε πληροφορίες είναι το *eve.json*. Στο αρχείο αυτό εμφανίζονται καταγραφές υπό την μορφή "*event_type*". Τα πρώτα που ελέγχουμε είναι τα *event_type alert*. Εδώ βρίσκουμε περαιτέρω πληροφορίες σχετικά με τα alerts που εμφανίστηκαν στο αρχείο *fast.log* που είδαμε προηγουμένως.

[9] https://github.com/Manos01/Network-Intrusion-Detection-Systems-NIDS-Comparison.git
[10] Αυτή η κατηγορία malware χρησιμοποιείται για να μολύνει το σύστημα μεταφέροντας άλλα malwares.
[11] https://attack.mitre.org/software/S0384/

```
{
  "timestamp": "2022-12-08T11:29:58.005155+0200",
  "flow_id": 1449494261879890,
  "in_iface": "enp0s8",
  "event_type": "alert",
  "src_ip": "67.222.131.174",
  "src_port": 80,
  "dest_ip": "10.6.1.101",
  "dest_port": 62932,
  "proto": "TCP",
  "metadata": {
    "flowints": {
      "http.anomaly.count": 1
    }
  },
  "community_id": "1:RzecbLFq+iKlZACXbL50zWSP5N4=",
  "tx_id": 1,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2221001,
    "rev": 1,
    "signature": "SURICATA HTTP gzip decompression failed",
    "category": "Generic Protocol Command Decode",
    "severity": 3
  },
  "http": {
    "hostname": "e-learning.iskandariah.perubatan.org",
    "url": "/swaging.php",
    "http_user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKi
    "http_content_type": "text/html",
    "http_refer": "http://e-learning.iskandariah.perubatan.org/swaging.php",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 804188
  },
```


Εικόνα 17. event type alert pt1

Στην Εικόνα 17 βλέπουμε πληροφορίες σχετικά το συμπιεσμένο αρχείο που μεταφέρθηκε, όπως *hostname* και *http_content_type*, ενώ η Εικόνα 18 μας πληροφορεί για το ποιοι hosts εμπλέκονται στην μετάδοση του κακόβουλου λογισμικού.


```
{
  "timestamp": "2022-12-08T11:30:00.493282+0200",
  "flow_id": 1277420692342083,
  "in_iface": "enp0s8",
  "event_type": "alert",
  "src_ip": "10.6.1.101",
  "src_port": 52877,
  "dest_ip": "108.62.141.234",
  "dest_port": 443,
  "proto": "TCP",
  "community_id": "1:l4IJ8lHcKPFKDPCQzUEhztXuJzM=",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 906200059,
    "rev": 1,
    "signature": "SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Dridex)",
    "category": "",
    "severity": 3
  },
  "tls": {
    "session_resumed": true,
    "version": "TLS 1.2",
    "ja3": {
      "hash": "51c64c77e60f3980eea90869b68c58a8",
      "string": "771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-65281,29-23-24,0"
    },
    "ja3s": {
      "hash": "ae4edc6faf64d08308082ad26be60767",
      "string": "771,49200,23-65281"
```


Εικόνα 18. event type alert pt2

Η Εικόνα 19 που ακολουθεί παρέχει πληροφορίες σχετικά με το τρίτο alert. Ειδικότερα, το πεδίο *http_content_type* αναφέρεται σε ένα binary αρχείο (application/octet-stream).

```
{
  "timestamp": "2022-12-08T11:30:11.360411+0200",
  "flow_id": 1590820160972195,
  "in_iface": "enp0s8",
  "event_type": "alert",
  "src_ip": "108.62.141.234",
  "src_port": 80,
  "dest_ip": "10.6.1.101",
  "dest_port": 53248,
  "proto": "TCP",
  "metadata": {
    "flowints": {
      "http.anomaly.count": 1
    }
  },
  "community_id": "1:vzB8UzZ5ckFliqzp9y05zEyhEjE=",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2221010,
    "rev": 1,
    "signature": "SURICATA HTTP unable to match response to request",
    "category": "Generic Protocol Command Decode",
    "severity": 3
  },
  "http": {
    "http_port": 0,
    "url": "/libhtp::request_uri_not_seen",
    "http_content_type": "application/octet-stream",
    "status": 200,
    "length": 0
```

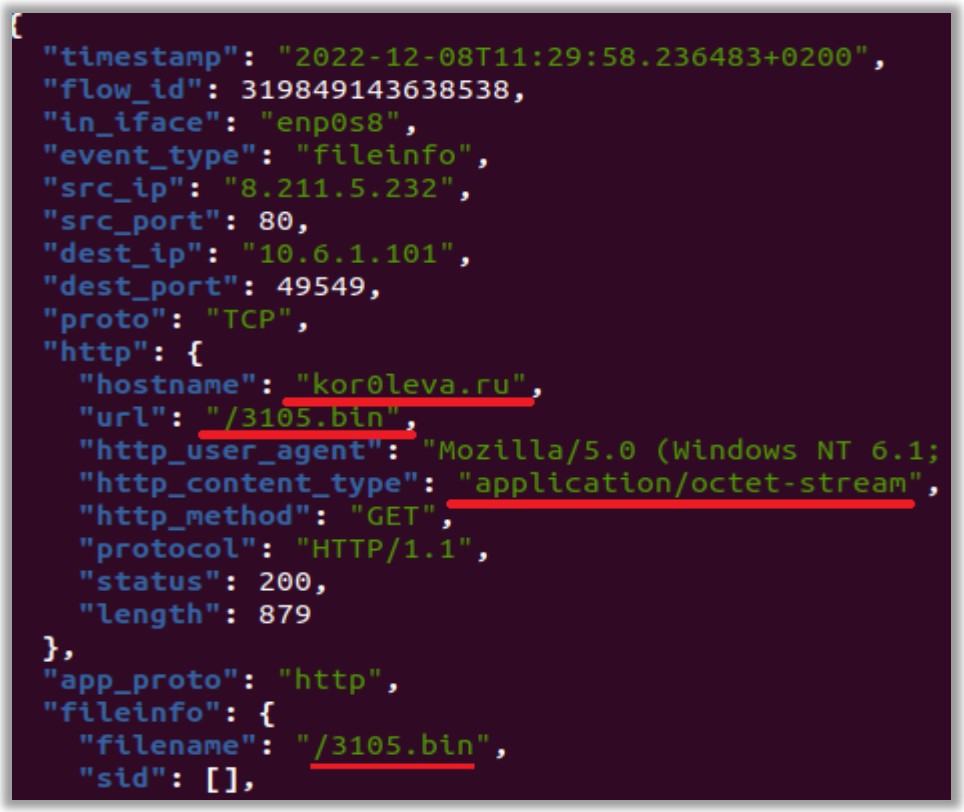

Εικόνα 19. event type alert pt3

Και δια του λόγου το αληθές, ελέγχοντας τα *http event_type* προκύπτει το εύρημα της Εικόνας 20.


```
{
  "timestamp": "2022-12-08T11:29:58.236379+0200",
  "flow_id": 319849143638538,
  "in_iface": "enp0s8",
  "event_type": "http",
  "src_ip": "10.6.1.101",
  "src_port": 49549,
  "dest_ip": "8.211.5.232",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 0,
  "community_id": "1:ObiHIwCQzwPkRRvR6nhx+wmUqEk=",
  "http": {
    "hostname": "kor0leva.ru",
    "url": "/3105.bin",
    "http_user_agent": "Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko",
    "http_content_type": "application/octet-stream",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 879
  }
}
```

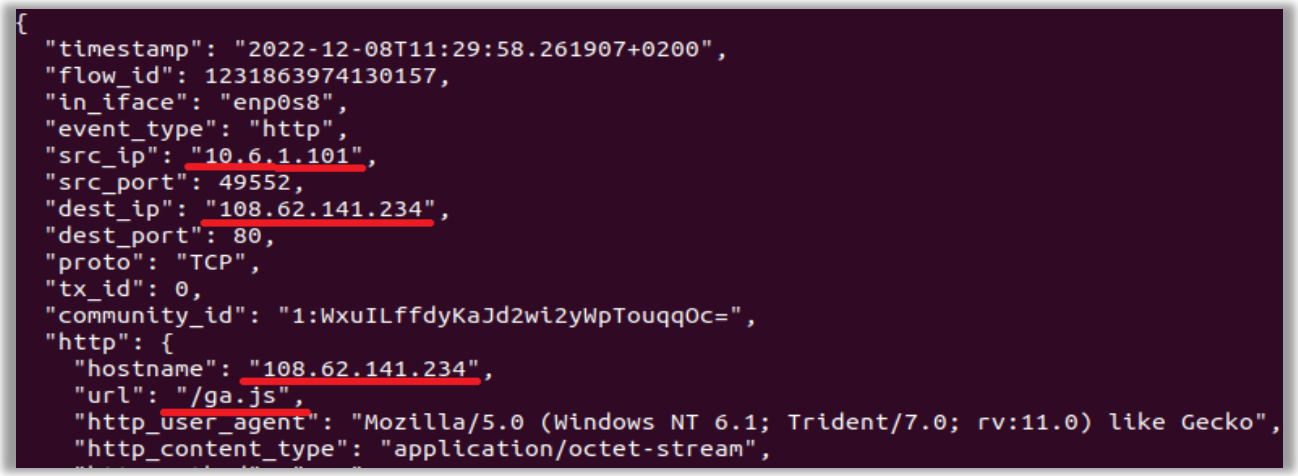

Εικόνα 20. event type http pt1

Το πεδίο *url* στην Εικόνα 20, αντιστοιχεί σε binary αρχείο και αυτό διασταυρώθηκε και από τα *event_type* "*fileinfo*" (Εικόνα 21).



Εικόνα 21. event type fileinfo pt1

Επίσης ανιχνεύθηκαν, ένα εκτελέσιμο αρχείο javascript (Εικόνα 22)



Εικόνα 22. event type http pt2

το συμπιεσμένο αρχείο (Εικόνα 23)

```
{
  "timestamp": "2022-12-08T11:29:58.276793+0200",
  "flow_id": 2031290531844353,
  "in_iface": "enp0s8",
  "event_type": "http",
  "src_ip": "10.6.1.101",
  "src_port": 49553,
  "dest_ip": "23.47.50.232",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 0,
  "community_id": "1:LPq2bRX3lF+95K53FBORXhjgMH8=",
  "http": {
    "hostname": "ctldl.windowsupdate.com",
    "url": "/msdownload/update/v3/static/trustedr/en/authrootstl.cab?c7ba64d52f9213c5",
    "http_user_agent": "Microsoft-CryptoAPI/10.0",
    "http_content_type": "application/vnd.ms-cab-compressed",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 60080
  }
}
```


Εικόνα 23. event type http pt3

και ένα εκτελέσιμο .exe αρχείο (Εικόνα 24).


```
{
  "timestamp": "2022-12-08T11:29:58.283102+0200",
  "flow_id": 319849143638538,
  "in_iface": "enp0s8",
  "event_type": "http",
  "src_ip": "10.6.1.101",
  "src_port": 49549,
  "dest_ip": "8.211.5.232",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 2,
  "community_id": "1:ObiHIwCQzwPkRRvR6nhx+wmUqEk=",
  "http": {
    "hostname": "kor0leva.ru",
    "url": "/6ha8ua.exe",
    "http_user_agent": "Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko",
    "http_content_type": "application/octet-stream",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 273422
  }
}
```


Εικόνα 24. event type http pt4

Το συμπιεσμένο αρχείο σχετίζεται με την υπηρεσία windows update (Εικόνα 23). Αυτό μπορεί να συμβαίνει είτε ως process injection σε κάποια διεργασία του λειτουργικού συστήματος, είτε να είναι απλώς ένα όνομα που χρησιμοποιείται ως πλαστοπροσωπία, έτσι ώστε να περάσει απαρατήρητο το κακόβουλο λογισμικό (από antivirus και χρήστη αντίστοιχα). Σε κάθε περίπτωση, αυτό αποτελεί γνωστή πρακτική (*Defense Evasion*) και η συγκεκριμένη εγγραφή χρήζει περαιτέρω διερεύνησης.

Και αυτό που σίγουρα χρήζει περαιτέρω διερεύνησης είναι και η SMB σύνδεση που φαίνεται παρακάτω να έχει πρόσβαση σε αρχείο Registry.pol. Πρόκειται για αρχεία, στα οποία αποθηκεύονται ρυθμίσεις για τα Group Policies, δηλαδή αρχεία σχετικά με δικαιώματα πρόσβασης. Αυτά βρίσκονται στο Group Policy Template, το οποίο με την σειρά του φιλοξενείται στο sysvol share directory ενός Domain Controller. Και αυτό επαληθεύεται από τα ευρήματα της Εικόνας 25.


```
{
  "timestamp": "2022-12-08T11:29:57.280965+0200",
  "flow_id": 1851958467353339,
  "in_iface": "enp0s8",
  "event_type": "fileinfo",
  "src_ip": "10.6.1.6",
  "src_port": 445,
  "dest_ip": "10.6.1.101",
  "dest_port": 49679,
  "proto": "TCP",
  "smb": {
    "id": 28,
    "dialect": "3.11",
    "command": "SMB2_COMMAND_READ",
    "status": "STATUS_SUCCESS",
    "status_code": "0x0",
    "session_id": 202310139510825,
    "tree_id": 1,
    "filename": "duckkissmixer.com\\Policies\\{31B2F340-016D-11D2-945F-00C04FB984F9}\\Machine\\Registry.pol",
    "share": "\\\\DuckKiss-DC.duckkissmixer.com\\sysvol",
    "fuid": "00000012-002e-0000-0019-00000000002e"
  },
  "app_proto": "smb",
  "fileinfo": {
    "filename": "duckkissmixer.com\\Policies\\{31B2F340-016D-11D2-945F-00C04FB984F9}\\Machine\\Registry.pol",
```


Εικόνα 25. event type fileinfo pt2

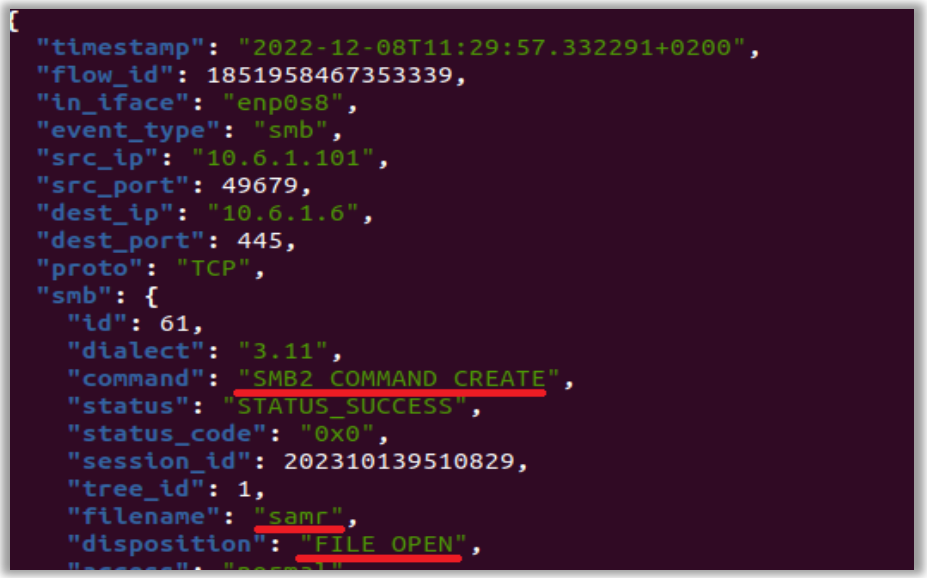
Το εύρημα αυτό μας οδηγεί να ερευνήσουμε τα *event_type smb*. Εκεί βρίσκουμε την εγκαθίδρυση ενός καναλιού επικοινωνίας με IPC (Inter-Process Communication[12]), όπως φαίνεται και στην Εικόνα 26.


```
{
  "timestamp": "2022-12-08T11:29:57.257646+0200",
  "flow_id": 1851958467353339,
  "in_iface": "enp0s8",
  "event_type": "smb",
  "src_ip": "10.6.1.101",
  "src_port": 49679,
  "dest_ip": "10.6.1.6",
  "dest_port": 445,
  "proto": "TCP",
  "smb": {
    "id": 4,
    "dialect": "3.11",
    "command": "SMB2_COMMAND_TREE_CONNECT",
    "status": "STATUS_SUCCESS",
    "status_code": "0x0",
    "session_id": 202310139510821,
    "tree_id": 1,
    "named_pipe": "\\\\DuckKiss-DC.duckkissmixer.com\\IPC$",
    "share_type": "PIPE"
  },
  "community_id": "1:+K5Bz3jvJPYKk8psiTR6k37T61s="
}
```


Εικόνα 26. event type smb pt1

[12] https://attack.mitre.org/techniques/T1559/

Και απόπειρα ανάγνωσης του αρχείου samr (Security Account Manager Remote Protocol) (Εικόνα 27)



```
{
  "timestamp": "2022-12-08T11:29:57.332291+0200",
  "flow_id": 1851958467353339,
  "in_iface": "enp0s8",
  "event_type": "smb",
  "src_ip": "10.6.1.101",
  "src_port": 49679,
  "dest_ip": "10.6.1.6",
  "dest_port": 445,
  "proto": "TCP",
  "smb": {
    "id": 61,
    "dialect": "3.11",
    "command": "SMB2_COMMAND_CREATE",
    "status": "STATUS_SUCCESS",
    "status_code": "0x0",
    "session_id": 202310139510829,
    "tree_id": 1,
    "filename": "samr",
    "disposition": "FILE_OPEN",
```


Εικόνα 27. event type smb pt2

Στην συνέχεια, πρόσβαση στο Shared file του Domain Controller (Εικόνα 28)

```
{
  "timestamp": "2022-12-08T11:29:57.337256+0200",
  "flow_id": 2112551313022435,
  "in_iface": "enp0s8",
  "event_type": "smb",
  "src_ip": "10.6.1.101",
  "src_port": 49721,
  "dest_ip": "10.6.1.6",
  "dest_port": 445,
  "proto": "TCP",
  "smb": {
    "id": 3,
    "dialect": "3.11",
    "command": "SMB2_COMMAND_TREE_CONNECT",
    "status": "STATUS_SUCCESS",
    "status_code": "0x0",
    "session_id": 202310139510833,
    "tree_id": 1,
    "share": "\\\\DuckKiss-DC\\Shared",
    "share_type": "FILE"
  },
  "community_id": "1:cC1TitekNsO99AL2rx52ODpqYEU="
}
```

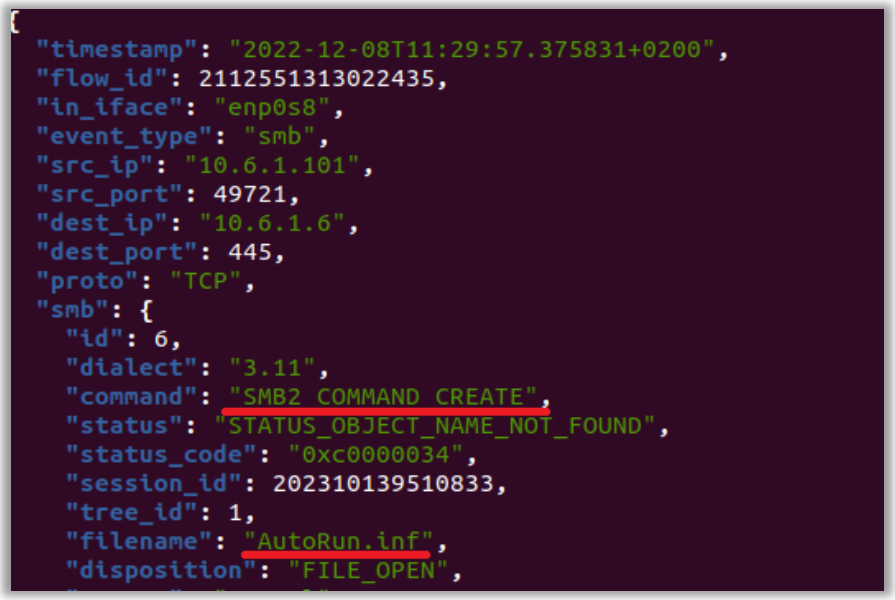

Εικόνα 28. event type smb pt3

και αναζήτηση στο interface του δικτύου για σχετικές πληροφορίες (Εικόνα 29).

```
{
  "timestamp": "2022-12-08T11:29:57.337499+0200",
  "flow_id": 2112551313022435,
  "in_iface": "enp0s8",
  "event_type": "smb",
  "src_ip": "10.6.1.101",
  "src_port": 49721,
  "dest_ip": "10.6.1.6",
  "dest_port": 445,
  "proto": "TCP",
  "smb": {
    "id": 4,
    "dialect": "3.11",
    "command": "SMB2_COMMAND_IOCTL",
    "status": "STATUS_SUCCESS",
    "status_code": "0x0",
    "session_id": 202310139510833,
    "tree_id": 1,
    "function": "FSCTL_QUERY_NETWORK_INTERFACE_INFO"
  },
  "community_id": "1:cC1TitekNsO99AL2rx52ODpqYEU="
}
```


Εικόνα 29. event type smb pt4

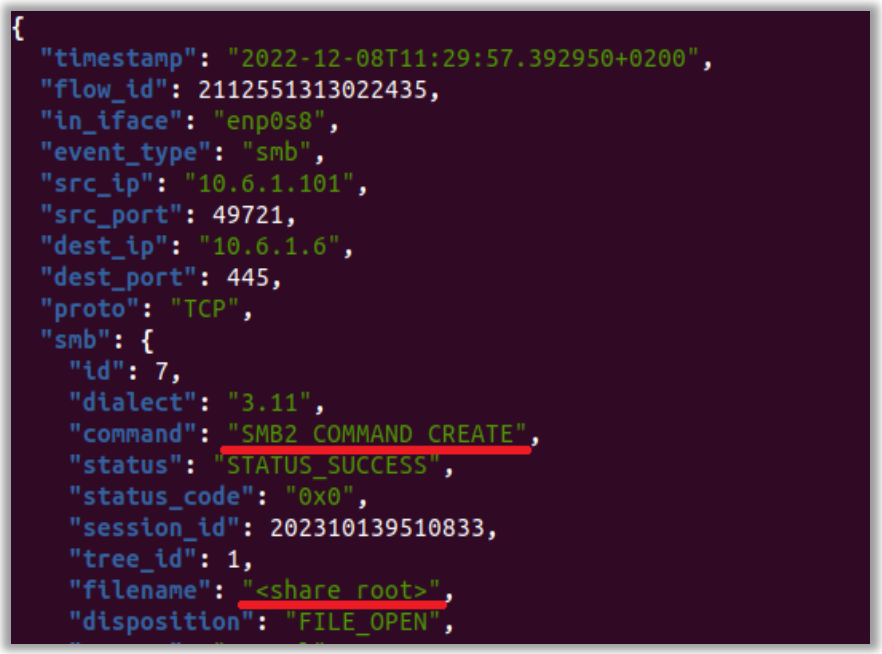
Έπειτα, ακολουθεί απόπειρα για persistence, μέσω του Autorun service (Εικόνα 30)



```
{
  "timestamp": "2022-12-08T11:29:57.375831+0200",
  "flow_id": 2112551313022435,
  "in_iface": "enp0s8",
  "event_type": "smb",
  "src_ip": "10.6.1.101",
  "src_port": 49721,
  "dest_ip": "10.6.1.6",
  "dest_port": 445,
  "proto": "TCP",
  "smb": {
    "id": 6,
    "dialect": "3.11",
    "command": "SMB2_COMMAND_CREATE",
    "status": "STATUS_OBJECT_NAME_NOT_FOUND",
    "status_code": "0xc0000034",
    "session_id": 202310139510833,
    "tree_id": 1,
    "filename": "AutoRun.inf",
    "disposition": "FILE_OPEN",
```


Εικόνα 30. event type smb pt5

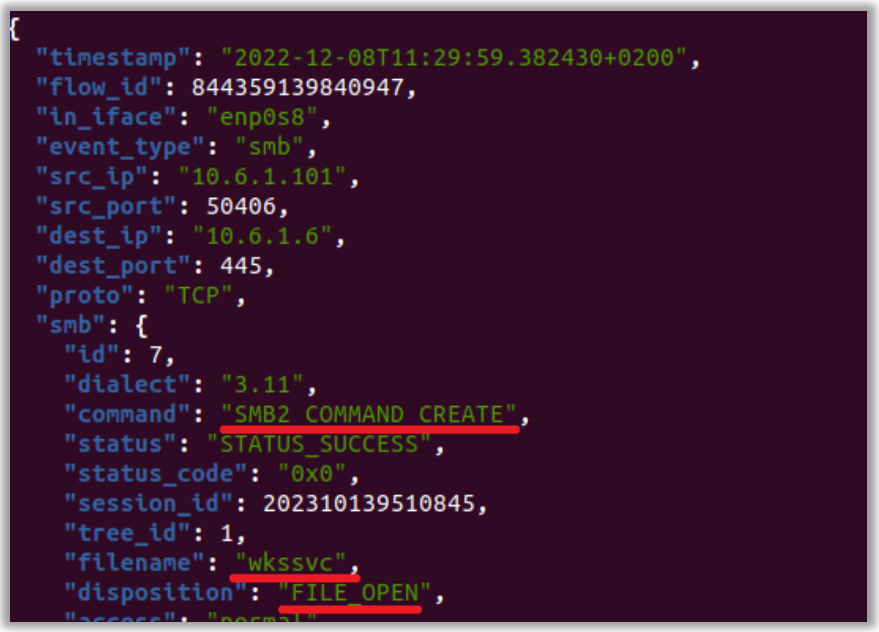
σύνδεση στο <share root> (Εικόνα 31) κι από εκεί πρόσβαση (Session Setup) `host: DESKTOP-41SH6EJ` και `user: "elaine.hammil"` (Εικόνα 32).



Εικόνα 31. event type smb pt6

Εικόνα 32. event type smb pt7

Μετά ακολουθεί απόπειρα για επικοινωνία με αρχείο (wkssvc), σχετικό με service των Windows™, το οποίο είναι υπεύθυνο για απομακρυσμένες συνδέσεις με servers (Εικόνα 33).



```
{
  "timestamp": "2022-12-08T11:29:59.382430+0200",
  "flow_id": 844359139840947,
  "in_iface": "enp0s8",
  "event_type": "smb",
  "src_ip": "10.6.1.101",
  "src_port": 50406,
  "dest_ip": "10.6.1.6",
  "dest_port": 445,
  "proto": "TCP",
  "smb": {
    "id": 7,
    "dialect": "3.11",
    "command": "SMB2_COMMAND_CREATE",
    "status": "STATUS_SUCCESS",
    "status_code": "0x0",
    "session_id": 202310139510845,
    "tree_id": 1,
    "filename": "wkssvc",
    "disposition": "FILE_OPEN",
```


Εικόνα 33. event type smb pt8

Η επόμενη καταγραφή μας, ανήκει στα *event_type krb5* που αφορούν το πρωτόκολλο Kerberos, υπεύθυνο για την αυθεντικοποίηση αιτημάτων υπηρεσιών. Στην Εικόνα 34 παρατηρούμε επικοινωνία με το TGS (Ticket Granting Service) του Kerberos. Πιο συγκεκριμένα το "krbtgt" είναι ένας προκαθορισμένος λογαριασμός (default account) που διαθέτουν όλα τα domains ενός Active Directory. Ο ρόλος του δε, είναι να λειτουργεί ως KDC (Key Distribution Center), δηλαδή την υπηρεσία που διανέμει τα κλειδιά για ασφαλή επικοινωνία.

```
{
  "timestamp": "2022-12-08T11:29:57.246092+0200",
  "flow_id": 1953238091152455,
  "in_iface": "enp0s8",
  "event_type": "krb5",
  "src_ip": "10.6.1.101",
  "src_port": 49676,
  "dest_ip": "10.6.1.6",
  "dest_port": 88,
  "proto": "TCP",
  "community_id": "1:hKJ2Dei6ieym/C5TV1yeaw7o/Hc=",
  "krb5": {
    "msg_type": "KRB_TGS_REP",
    "cname": "DESKTOP-41SH6EJ$",
    "realm": "DUCKKISSMIXER.COM",
    "sname": "ldap/duckkiss-dc.duckkissmixer.com/duckkissmixer.com",
    "encryption": "aes256-cts-hmac-sha1-96",
    "weak_encryption": false
  }
}
```


Εικόνα 34. event type krb5

Επιπρόσθετα, στην Εικόνα 34 παρατηρούμε πως προφανώς πρόκειται για LDAP server. Οι συγκεκριμένοι servers χρησιμοποιούνται για την αποθήκευση usernames, passwords και άλλων στοιχείων των χρηστών, διότι αυτά χρησιμεύουν κατά την αυθεντικοποίησή τους όταν στέλνουν τα ανάλογα αιτήματα (Requests). Με άλλα λόγια, το κακόβουλο λογισμικό επιχειρεί Credential

Access (TA0006[13]) και πιθανόν System Owner/User Discovery (T1033). Ας μην ξεχνάμε πως το λογισμικό που ανιχνεύθηκε είναι το Dridex, το οποίο είναι ένας banking trojan, που χρησιμεύει για την υποκλοπή προσωπικών και δη οικονομικών δεδομένων.

Αυτά μεταξύ άλλων ήταν τα ευρήματα που ανακαλύψαμε από τα log files του Suricata. Στην συνέχεια θα ασχοληθούμε με τα αντίστοιχα που προέκυψαν από το Zeek για να ανακαλύψουμε αν μεταξύ τους συμφωνούν ή αν μπορούμε να αποκομίσουμε κάποιο στοιχείο παραπάνω.

- ***Zeek***

Το Zeek ακολουθεί ένα άλλο σχήμα ως προς την παρουσίαση των log files, το οποίο έχει να κάνει με την αρχιτεκτονική και τον τρόπο λειτουργίας του. Δεν θα επεκταθούμε σε αυτό, αλλά αποτελεί μία ειδοποιό διαφορά το γεγονός πως κατά κάποιο τρόπο για κάθε *event_type* του Suricata, το Zeek παράγει ξεχωριστό log file. Ή αλλιώς, όλα τα log files του Zeek είναι ενσωματωμένα σε ένα eve.json στο Suricata χωρισμένα ανά *event_type*.

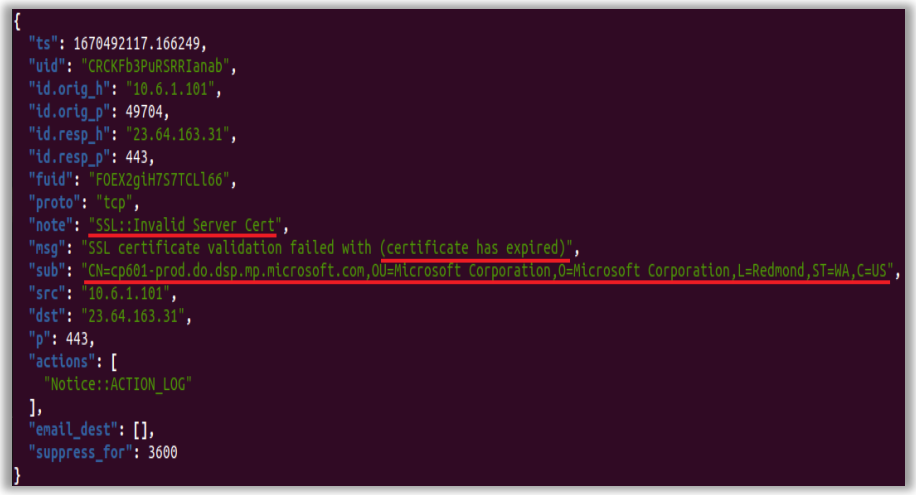
Στην περίπτωση του Zeek το πρώτο αρχείο στο οποίο ανατρέχουμε είναι το *notice.log* και είναι αντίστοιχο με το *fast.log* του Suricata. Δηλάδη εδώ εμφανίζονται τα alerts που παράγει το IDS. Εκείνα που προέκυψαν από το συγκεκριμένο pcap αρχείο είναι (Εικόνες 35 – 36):

1. `SSL certificate validation failed with (unable to get local issuer certificate)`
2. `SSL certificate validation failed with (certificate has expired)`


```
{
  "ts": 1670492117.166249,
  "uid": "CXKZYR3DSZTuG5H6sj",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49699,
  "id.resp_h": "51.104.167.186",
  "id.resp_p": 443,
  "fuid": "Fv7jfg1FIkqVuLFs59",
  "proto": "tcp",
  "note": "SSL::Invalid Server Cert",
  "msg": "SSL certificate validation failed with (unable to get local issuer certificate)",
  "sub": "CN=*.prod.do.dsp.mp.microsoft.com,OU=DSP,O=Microsoft,L=Redmond,ST=WA,C=US",
  "src": "10.6.1.101",
  "dst": "51.104.167.186",
  "p": 443,
  "actions": [
    "Notice::ACTION_LOG"
  ],
  "email_dest": [],
  "suppress_for": 3600
}
```


Εικόνα 35. notice.log pt1

[13] https://attack.mitre.org/

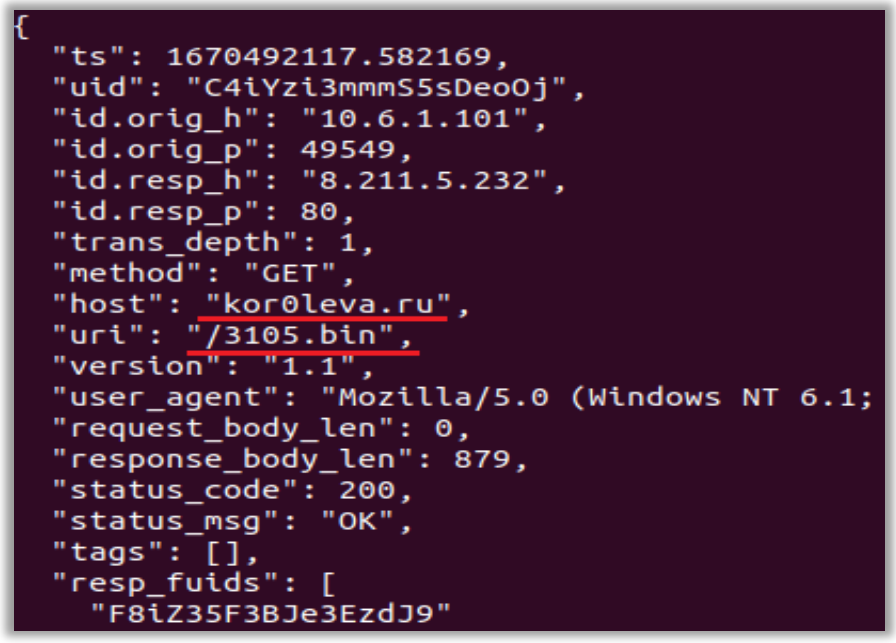


```
{
  "ts": 1670492117.166249,
  "uid": "CRCKFb3PuRSRRIanab",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49704,
  "id.resp_h": "23.64.163.31",
  "id.resp_p": 443,
  "fuid": "FOEX2giH7S7TCLl66",
  "proto": "tcp",
  "note": "SSL::Invalid Server Cert",
  "msg": "SSL certificate validation failed with (certificate has expired)",
  "sub": "CN=cp601-prod.do.dsp.mp.microsoft.com,OU=Microsoft Corporation,O=Microsoft Corporation,L=Redmond,ST=WA,C=US",
  "src": "10.6.1.101",
  "dst": "23.64.163.31",
  "p": 443,
  "actions": [
    "Notice::ACTION_LOG"
  ],
  "email_dest": [],
  "suppress_for": 3600
}
```


Εικόνα 36. notice.log pt2

Παρατηρούμε πως τα alerts του Zeek επικεντρώνονται σε ληγμένα και μη έγκυρα πιστοποιητικά. Σε πολλές περιπτώσεις οι επιτιθέμενοι αγοράζουν και/ή κλέβουν SSL/TLS πιστοποιητικά, τα οποία και μετέπειτα χρησιμοποιούν σε επιθέσεις (T1588.004[14]).

Προχωρώντας στο *http.log* παρατηρούμε πως ανιχνεύθηκαν όλα εκείνα τα αρχεία που ανακάλυψε και το Suricata (παρά το γεγονός πως μόνο τα πιστοποιητικά εμφανίστηκαν ως alerts). Συνεπώς ξεκινάμε με το binary file από τον host, που σύμφωνα με την κατάληξη φέρεται να είναι από Ρωσία (Εικόνα 37).

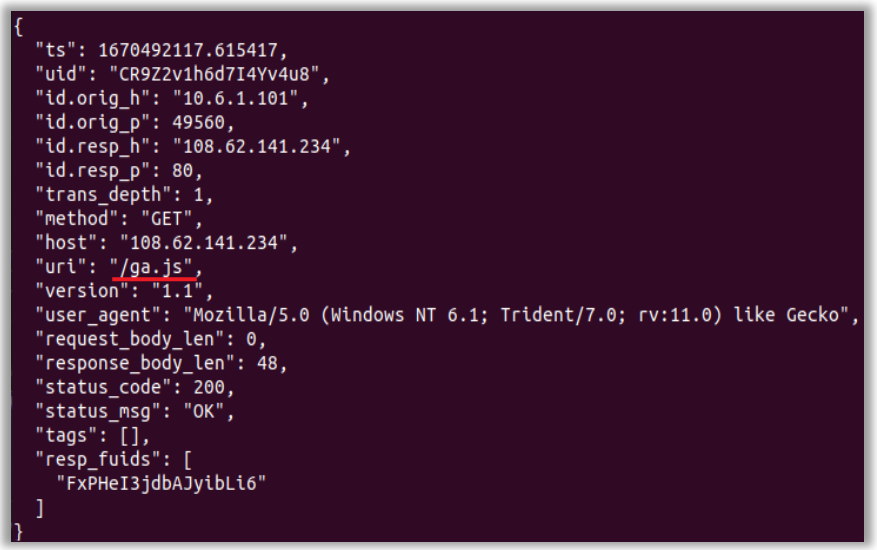


```
{
  "ts": 1670492117.582169,
  "uid": "C4iYzi3mmmS5sDeoOj",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49549,
  "id.resp_h": "8.211.5.232",
  "id.resp_p": 80,
  "trans_depth": 1,
  "method": "GET",
  "host": "kor0leva.ru",
  "uri": "/3105.bin",
  "version": "1.1",
  "user_agent": "Mozilla/5.0 (Windows NT 6.1;
  "request_body_len": 0,
  "response_body_len": 879,
  "status_code": 200,
  "status_msg": "OK",
  "tags": [],
  "resp_fuids": [
    "F8iZ35F3BJe3EzdJ9"
```


Εικόνα 37. http.log pt1

Συνεχίζουμε με το javascript file (Εικόνα 38)

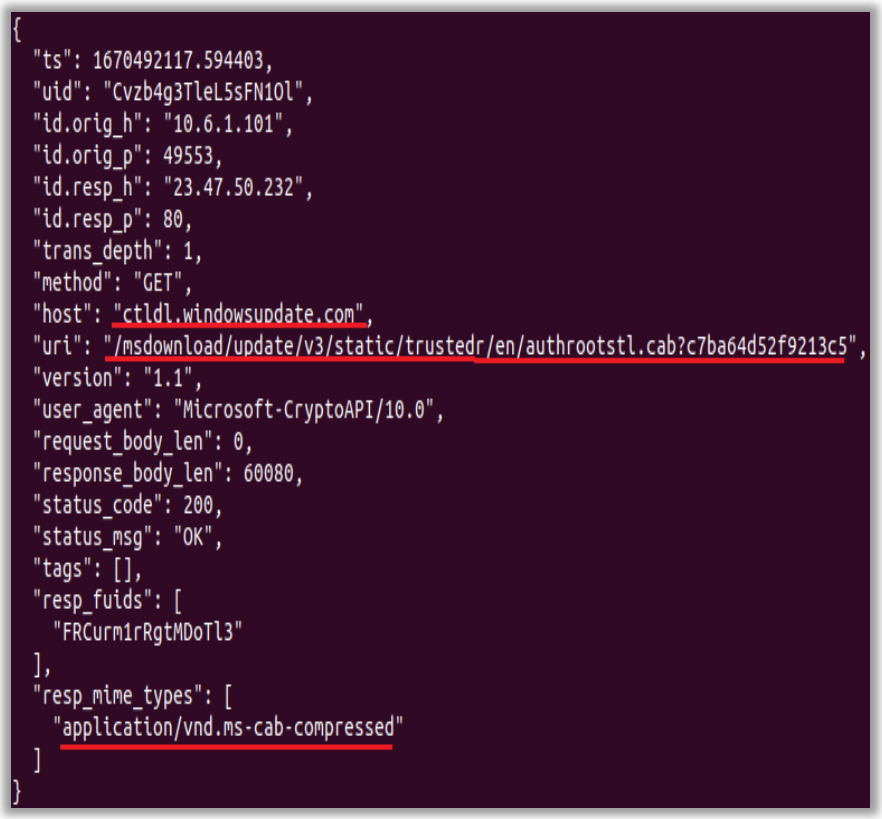
[14] https://attack.mitre.org/techniques/T1588/004/



```
{
  "ts": 1670492117.615417,
  "uid": "CR9Z2v1h6d7I4Yv4u8",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49560,
  "id.resp_h": "108.62.141.234",
  "id.resp_p": 80,
  "trans_depth": 1,
  "method": "GET",
  "host": "108.62.141.234",
  "uri": "/ga.js",
  "version": "1.1",
  "user_agent": "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko",
  "request_body_len": 0,
  "response_body_len": 48,
  "status_code": 200,
  "status_msg": "OK",
  "tags": [],
  "resp_fuids": [
    "FxPHeI3jdbAJyibLi6"
  ]
}
```


Εικόνα 38. http.log pt2

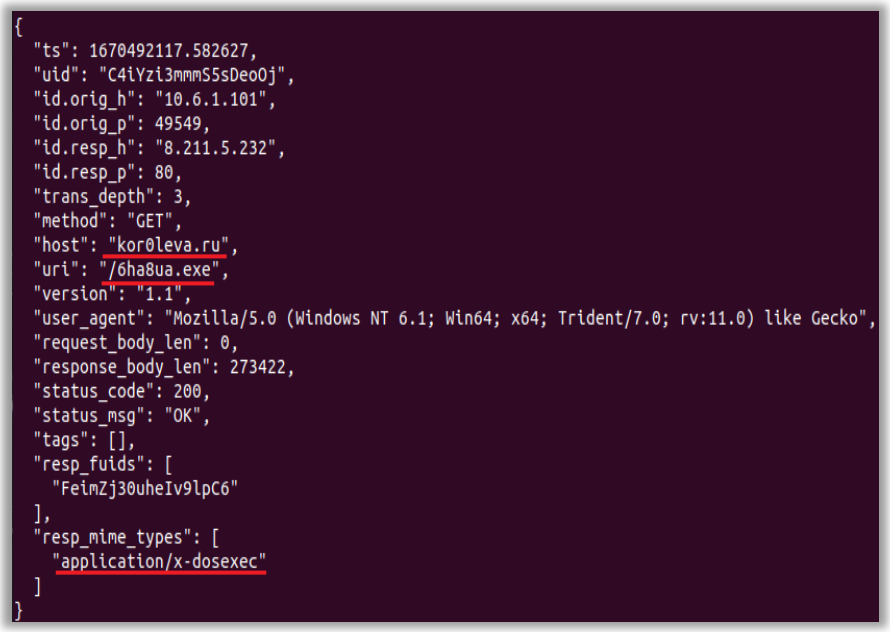
ακολουθεί το συμπιεσμένο αρχείο (Εικόνα 39)



```
{
  "ts": 1670492117.594403,
  "uid": "Cvzb4g3TleL5sFN10l",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49553,
  "id.resp_h": "23.47.50.232",
  "id.resp_p": 80,
  "trans_depth": 1,
  "method": "GET",
  "host": "ctldl.windowsupdate.com",
  "uri": "/msdownload/update/v3/static/trustedr/en/authrootstl.cab?c7ba64d52f9213c5",
  "version": "1.1",
  "user_agent": "Microsoft-CryptoAPI/10.0",
  "request_body_len": 0,
  "response_body_len": 60080,
  "status_code": 200,
  "status_msg": "OK",
  "tags": [],
  "resp_fuids": [
    "FRCurm1rRgtMDoTl3"
  ],
  "resp_mime_types": [
    "application/vnd.ms-cab-compressed"
  ]
}
```


Εικόνα 39. http.log pt3

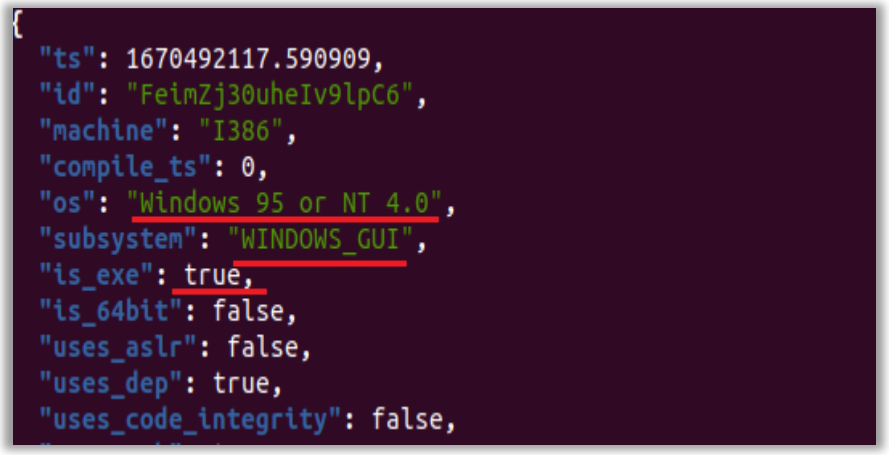
και το .exe εκτελέσιμο (Εικόνα 40)



```
{
  "ts": 1670492117.582627,
  "uid": "C4iYzi3mmmS5sDeoOj",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49549,
  "id.resp_h": "8.211.5.232",
  "id.resp_p": 80,
  "trans_depth": 3,
  "method": "GET",
  "host": "kor0leva.ru",
  "uri": "/6ha8ua.exe",
  "version": "1.1",
  "user_agent": "Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko",
  "request_body_len": 0,
  "response_body_len": 273422,
  "status_code": 200,
  "status_msg": "OK",
  "tags": [],
  "resp_fuids": [
    "FeimZj30uheIv9lpC6"
  ],
  "resp_mime_types": [
    "application/x-dosexec"
  ]
}
```


Εικόνα 40. http.log pt4

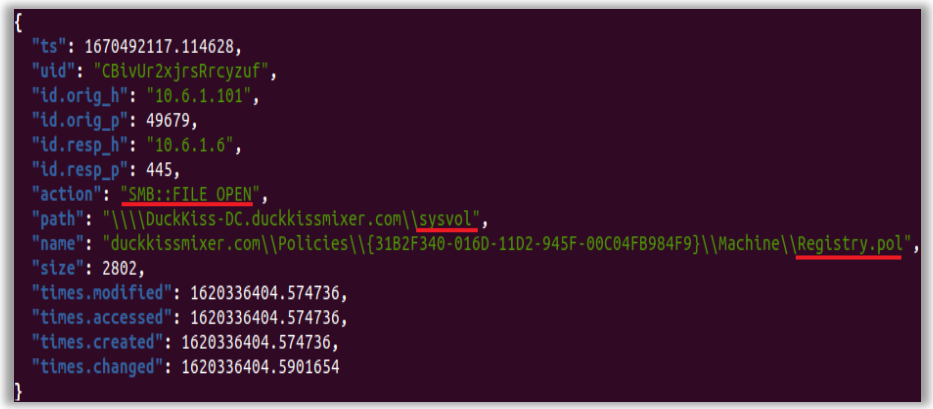
Στην συνέχεια το Zeek διαφοροποιείται λιγάκι. Η ύπαρξη του *pe.log* υποδηλώνει την ανίχνευση ενός portable executable αρχείου (Εικόνα 41)



```
{
  "ts": 1670492117.590909,
  "id": "FeimZj30uheIv9lpC6",
  "machine": "I386",
  "compile_ts": 0,
  "os": "Windows 95 or NT 4.0",
  "subsystem": "WINDOWS_GUI",
  "is_exe": true,
  "is_64bit": false,
  "uses_aslr": false,
  "uses_dep": true,
  "uses_code_integrity": false,
```


Εικόνα 41. pe.log

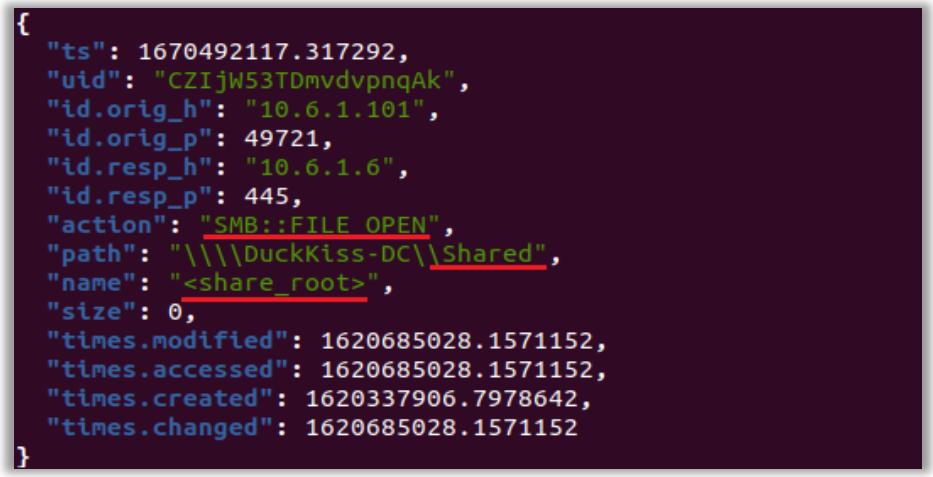
Συνεχίζοντας την έρευνα με το *smb_files.log* παρατηρούμε τα ίδια ευρήματα με το Suricata. Απόπειρα πρόσβασης στο Registry.pol (Εικόνα 42)



```
{
  "ts": 1670492117.114628,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "action": "SMB::FILE_OPEN",
  "path": "\\\\DuckKiss-DC.duckkissmixer.com\\sysvol",
  "name": "duckkissmixer.com\\Policies\\{31B2F340-016D-11D2-945F-00C04FB984F9}\\Machine\\Registry.pol",
  "size": 2802,
  "times.modified": 1620336404.574736,
  "times.accessed": 1620336404.574736,
  "times.created": 1620336404.574736,
  "times.changed": 1620336404.5901654
}
```


Εικόνα 42. smb_files.log pt1

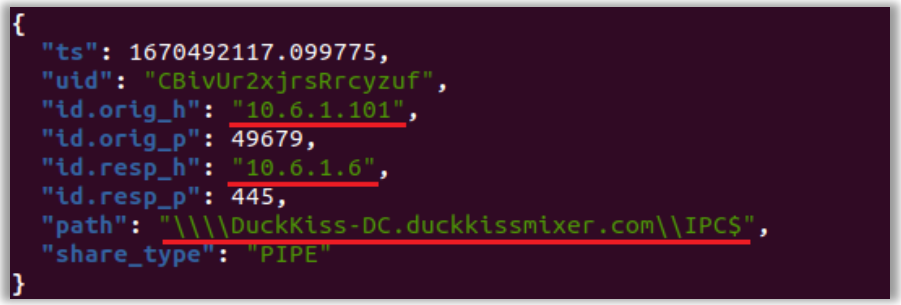
και πρόσβαση στον Shared file του domain controller (Εικόνα 43)



```
{
  "ts": 1670492117.317292,
  "uid": "CZIjW53TDmvdvpnqAk",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49721,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "action": "SMB::FILE_OPEN",
  "path": "\\\\DuckKiss-DC\\Shared",
  "name": "<share_root>",
  "size": 0,
  "times.modified": 1620685028.1571152,
  "times.accessed": 1620685028.1571152,
  "times.created": 1620337906.7978642,
  "times.changed": 1620685028.1571152
}
```


Εικόνα 43. smb_files.log pt2

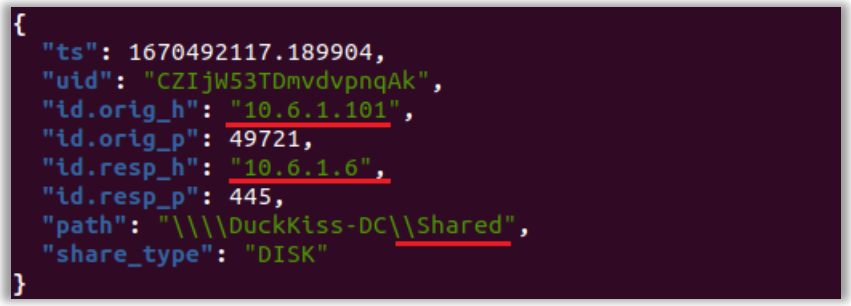
Το επόμενο αρχείο προς έρευνα είναι το *smb_mapping.log*. Εδώ έχουμε την πρόσβαση στο IPC (Εικόνα 44)



```
{
  "ts": 1670492117.099775,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "path": "\\\\DuckKiss-DC.duckkissmixer.com\\IPC$",
  "share_type": "PIPE"
}
```


Εικόνα 44. smb_mapping.log pt1

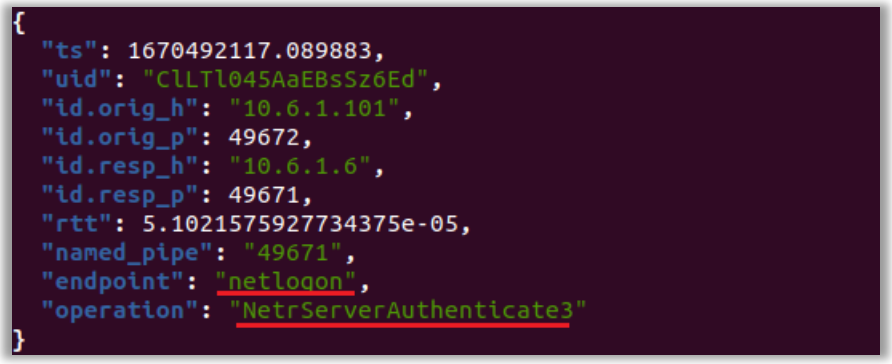
καθώς και στον Shared file του domain controller (Εικόνα 45)



```
{
  "ts": 1670492117.189904,
  "uid": "CZIjW53TDmvdvpnqAk",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49721,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "path": "\\\\DuckKiss-DC\\Shared",
  "share_type": "DISK"
}
```


Εικόνα 45. smb_mapping.log pt2

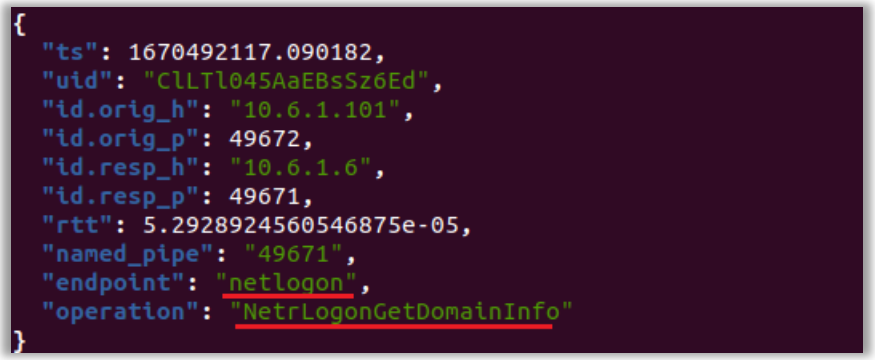
Σειρά έχει το αρχείο *dce_rpc.log* (Distributed Computing Environment / Remote Procedure Call), στο οποίο ανακαλύπτουμε ενδιαφέρουσες πληροφορίες που δεν είχε ανιχνεύσει προηγουμένως το Suricata. Έτσι παρατηρούμε καταγραφή που αναφέρει αυθεντικοποίηση με το netlogon service (Εικόνα 46). Το netlogon είναι ένα Local Security Authority service, το οποίο αυθεντικοποιεί τους χρήστες εντός του domain.



```
{
  "ts": 1670492117.089883,
  "uid": "ClLTl045AaEBsSz6Ed",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49672,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 49671,
  "rtt": 5.1021575927734375e-05,
  "named_pipe": "49671",
  "endpoint": "netlogon",
  "operation": "NetrServerAuthenticate3"
}
```


Εικόνα 46. dce_rpc.log pt1

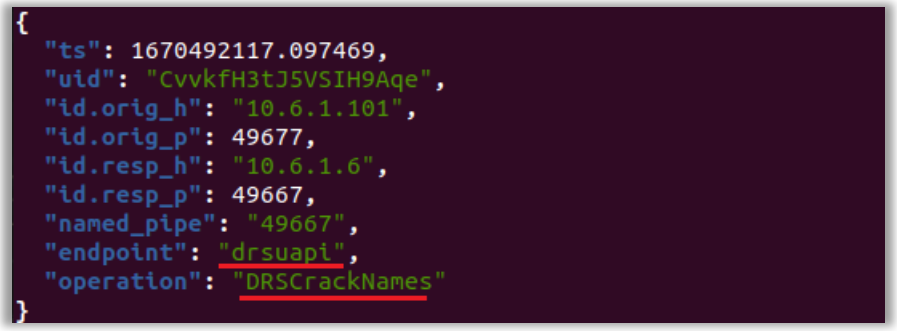
Έπειτα, αναζητά πληροφορίες για τον domain. Ίσως κάποια scripts του netlogon τα οποία χρησιμοποιούν οι χρήστες για την αυθεντικοποίησή τους.



```
{
  "ts": 1670492117.090182,
  "uid": "ClLTl045AaEBsSz6Ed",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49672,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 49671,
  "rtt": 5.2928924560546875e-05,
  "named_pipe": "49671",
  "endpoint": "netlogon",
  "operation": "NetrLogonGetDomainInfo"
}
```


Εικόνα 47. dce_rpc.log pt2

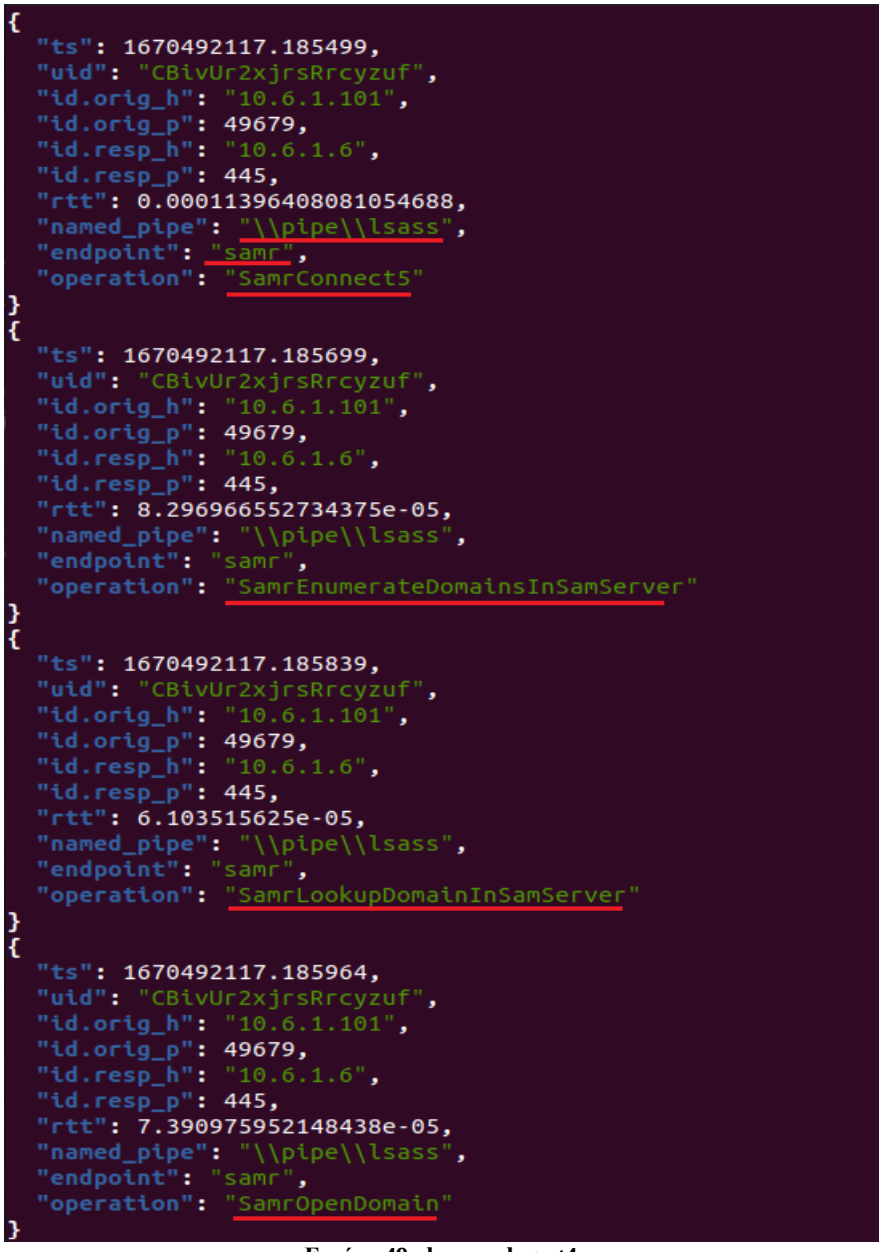
Μία άλλη καταγραφή αναφέρεται στο *drsuapi* (Εικόνα 48). Πρόκειται για API της Microsoft, το οποίο υλοποιεί το πρωτόκολλο MS-DRSR (Microsoft Directory Replication Service Remote Protocol). Για να υπάρχει συνέπεια στην πληροφορία μεταξύ των Domain Controllers, πρέπει τα αντικείμενα του Active Directory να αναπαράγονται σε όλους τους Domain Controllers. Το προαναφερθέν πρωτόκολλο αφορά αυτή την διαδικασία.



```
{
  "ts": 1670492117.097469,
  "uid": "CvvkfH3tJ5VSIH9Aqe",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49677,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 49667,
  "named_pipe": "49667",
  "endpoint": "drsuapi",
  "operation": "DRSCrackNames"
}
```


Εικόνα 48. dce_rpc.log pt3

Συνεχίζοντας, στο ίδιο αρχείο παρατηρούμε μία σύνδεση στο Security Account Manager (SAM), ένα σημείο όπου αποθηκεύονται usernames και passwords (Εικόνα 49).



```
{
  "ts": 1670492117.185499,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "rtt": 0.00011396408081054688,
  "named_pipe": "\\pipe\\lsass",
  "endpoint": "samr",
  "operation": "SamrConnect5"
}
{
  "ts": 1670492117.185699,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "rtt": 8.296966552734375e-05,
  "named_pipe": "\\pipe\\lsass",
  "endpoint": "samr",
  "operation": "SamrEnumerateDomainsInSamServer"
}
{
  "ts": 1670492117.185839,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "rtt": 6.103515625e-05,
  "named_pipe": "\\pipe\\lsass",
  "endpoint": "samr",
  "operation": "SamrLookupDomainInSamServer"
}
{
  "ts": 1670492117.185964,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "rtt": 7.390975952148438e-05,
  "named_pipe": "\\pipe\\lsass",
  "endpoint": "samr",
  "operation": "SamrOpenDomain"
}
```

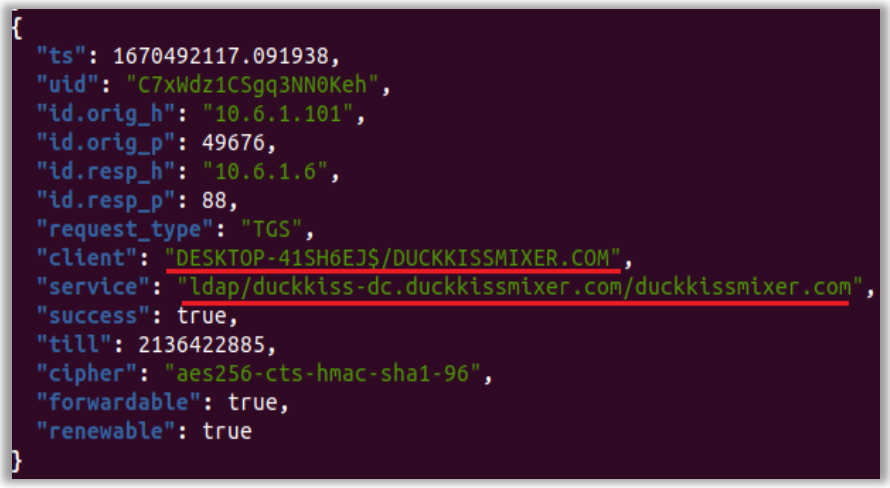

Εικόνα 49. dce_rpc.log pt4

Στην παραπάνω εικόνα πέρα από την σύνδεση φαίνεται μία αναζήτηση για τον αριθμό των domains στον server, έπειτα μία άλλη αναζήτηση για συγκεκριμένο domain και απόπειρα ανάγνωσης αρχείου για συγκεκριμένο domain. Ακολουθεί αναζήτηση της λίστας των ονομάτων που συμπεριλαμβάνονται στον domain, ανάγνωση αρχείου συγκεκριμένου χρήστη και αναζήτηση για πληροφορίες που τον αφορούν (Εικόνα 50)


```
{
  "ts": 1670492117.186274,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "rtt": 6.29425048828125e-05,
  "named_pipe": "\\pipe\\lsass",
  "endpoint": "samr",
  "operation": "SamrLookupNamesInDomain"
}
{
  "ts": 1670492117.186392,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "rtt": 5.3882598876953125e-05,
  "named_pipe": "\\pipe\\lsass",
  "endpoint": "samr",
  "operation": "SamrOpenUser"
}
{
  "ts": 1670492117.186516,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "rtt": 5.2928924560546875e-05,
  "named_pipe": "\\pipe\\lsass",
  "endpoint": "samr",
  "operation": "SamrQueryInformationUser"
}
{
  "ts": 1670492117.186629,
  "uid": "CBivUr2xjrsRrcyzuf",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49679,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "rtt": 5.1975250244140625e-05,
  "named_pipe": "\\pipe\\lsass",
  "endpoint": "samr",
  "operation": "SamrQuerySecurityObject"
}
```

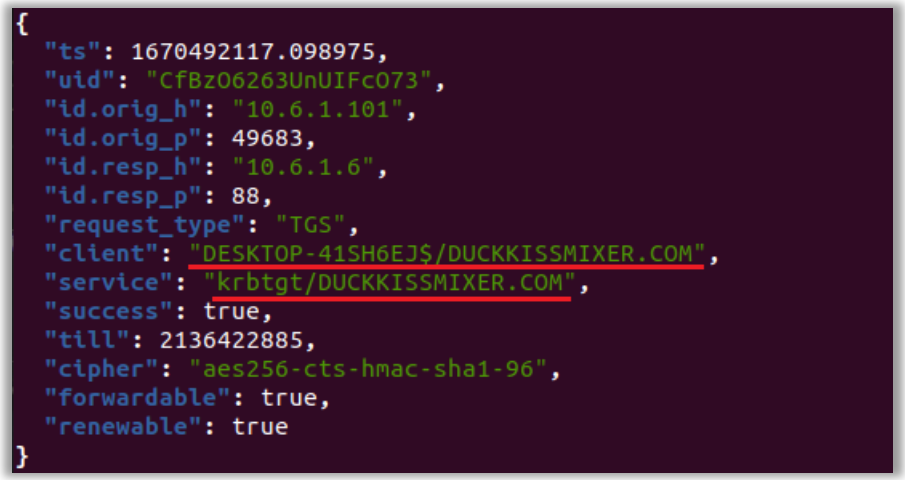

Εικόνα 50. dce_rpc.log pt5

Στο αρχείο *kerberos.log* βρίσκουμε ενδείξεις για πρόσβαση στον LDAP server (Εικόνα 51) και στο kerberos service (Εικόνα 52), όμοιες με εκείνες του Suricata.



```
{
  "ts": 1670492117.091938,
  "uid": "C7xWdz1CSgq3NN0Keh",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49676,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 88,
  "request_type": "TGS",
  "client": "DESKTOP-41SH6EJ$/DUCKKISSMIXER.COM",
  "service": "ldap/duckkiss-dc.duckkissmixer.com/duckkissmixer.com",
  "success": true,
  "till": 2136422885,
  "cipher": "aes256-cts-hmac-sha1-96",
  "forwardable": true,
  "renewable": true
}
```


Εικόνα 51. kerberos.log pt1



```
{
  "ts": 1670492117.098975,
  "uid": "CfBzO6263UnUIFcO73",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 49683,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 88,
  "request_type": "TGS",
  "client": "DESKTOP-41SH6EJ$/DUCKKISSMIXER.COM",
  "service": "krbtgt/DUCKKISSMIXER.COM",
  "success": true,
  "till": 2136422885,
  "cipher": "aes256-cts-hmac-sha1-96",
  "forwardable": true,
  "renewable": true
}
```


Εικόνα 52. kerberos.log pt2

Τέλος, στο *ntlm.log*, βρίσκουμε τις πληροφορίες για τα username και hostname (Εικόνα 53)

```
{
  "ts": 1670492117.938756,
  "uid": "CANYC1mvNpOu8t8W",
  "id.orig_h": "10.6.1.101",
  "id.orig_p": 50406,
  "id.resp_h": "10.6.1.6",
  "id.resp_p": 445,
  "username": "elaine.hammil",
  "hostname": "DESKTOP-41SH6EJ",
  "domainname": "DUCKKISSMIXER",
  "server_nb_computer_name": "DUCKKISS-DC",
  "server_dns_computer_name": "DuckKiss-DC.duckkissmixer.com",
  "server_tree_name": "duckkissmixer.com",
  "success": true
}
```


Εικόνα 53. ntlm.log

Αυτά ήταν τα κυριότερα από τα ευρήματα που προέκυψαν από τα log files των δύο IDS. Αυτό που παρατηρήσαμε σε γενικές γραμμές είναι πως το Suricata υπερτερεί έναντι του Zeek ως

προς τα alerts, έχοντας καλύτερα αποτελέσματα, ωστόσο ερευνώντας τις καταγραφές των αρχείων είμασταν σε θέση να αποκομίσουμε περισσότερες πληροφορίες από το Zeek, σε σχέση με εκείνες από το Suricata, τουλάχιστον όσον αφορά τις ενέργειες του κακόβουλου λογισμικού μετά την μόλυνση του συστήματος.

Στην ενότητα αυτή ασχοληθήκαμε με την μεθοδολογία που ακολουθήθηκε για την εκπόνηση της εργασίας. Ξεκινήσαμε με την παρουσίαση της υποδομής και συνεχίσαμε αναφέροντας πληροφορίες για το δείγμα, όπως τις πηγές και τους λόγους που επιλέξαμε τα αρχεία που το απαρτίζουν. Έπειτα ασχοληθήκαμε με μία περίπτωση μελέτης, επίλέγοντας μία εκ των επιθέσεων που περιλαμβάνονται στα pcap αρχεία και παραθέσαμε τα κυριότερα ευρήματα που αντλήσαμε από τα log files και μόνο. Στόχος μας ήταν αφενός να δείξουμε την μεθοδολογία που ακολουθήσαμε για την συλλογή των ενδείξεων παραβίασης, αφετέρου να υπογραμμίσουμε το γεγονός πως για την εξαγωγή συμπερασμάτων σε μία επίθεση απαιτείται ο συνδυασμός πληροφοριών και στοιχείων από διαφορετικά log files και όχι μόνο. Με αυτό τον τρόπο καταλήγουμε να απαντήσουμε σε ερωτήσεις όπως το ποιος εμπλέκεται στο περιστατικό ασφάλειας, τι συνέβη, πότε συνέβη, γιατί συνέβη, πως συνέβη και που;

Στην επόμενη ενότητα θα γίνει παρουσίαση των αποτελεσμάτων όπως προέκυψαν από το σύνολο των επιθέσεων.

5

Αποτελέσματα και ανάλυση

Συνεχίζουμε στην ενότητα αυτή, με την παρουσίαση των αποτελεσμάτων που προέκυψαν με βάση την μεθοδολογία που περιγράψαμε παραπάνω. Θα πρέπει να σημειώσουμε πως πρόκειται για μία ποιοτική μελέτη σύγκρισης ανάμεσα στα δύο IDS. Ως εκ τούτου, στο πλαίσιο αυτό διακρίνουμε τρεις υπό-ενότητες.

5.1 Σύγκριση ως προς το πλήθος των alerts

Η πρώτη από τις τρεις υπο-ενότητες ασχολείται με την αποτελεσματικότητα των δύο IDS ως προς τα alerts. Ένα IDS είναι χρήσιμο, όταν είναι σε θέση να ανιχνεύει και να προειδοποιεί για κακόβουλες δραστηριότητες, χωρίς φυσικά να υποτιμούμε την αξία της καταγραφής των συμβάντων. Επιπλέον, κρίνεται σκόπιμο να αναφέρουμε πως δεν λαμβάνουμε υπόψιν την ακρίβεια των IDSs, δηλαδή το κατά πόσο είναι ακριβή τα αποτελέσματα και αν έχουμε Ψευδώς-Αληθείς περιπτώσεις αποτελεσμάτων. Εργαστήκαμε κάνοντας την παραδοχή πως τα αποτελέσματα που προέκυψαν είναι έγκυρα.

Κάτι άλλο που θα πρέπει να ορίσουμε είναι την «αποτελεσματικότητα». Θεωρούμε λοιπόν, για την εν λόγω εργασία, πως το μέγεθος της αποτελεσματικότητας παίρνει τις τιμές *low, medium* και *high*, σύμφωνα με τον πίνακα που ακολουθεί.

Alerts	IoCs	Effectiveness
No	No	**Low**
No	Yes	**Medium**
Yes	No	**Medium**
Yes	Yes	**High**

Πίνακας 5. Η αποτελεσματικότητα όπως ορίζεται στα πλαίσια της εργασίας

Με άλλα λόγια, θεωρούμε πως όταν το IDS παράγει alerts για μία επίθεση και επιπλέον βρίσκουμε ενδείξεις παραβίασης (IoCs – Indicators of Compromise) στα log files, τότε έχει υψηλή αποτελεσματικότητα. Στην αντίθετη περίπτωση που δεν έχουμε alerts και δεν υπάρχουν IoCs, τότε το IDS εμφανίζει χαμηλή αποτελεσματικότητα. Σε οποιαδήποτε άλλη περίπτωση, η αποτελεσματικότητά του είναι μέτρια. Ακόμα και στην περίπτωση που προκύψει alert, αλλά δεν είμαστε σε θέση να βρούμε IoCs, θεωρούμε μέτρια την αποτελεσματικότητα γιατί και το alert

είναι ένα είδος ένδειξης (IoC) από μόνο του. Τα ερωτήματα που καλείται να απαντήσει αυτή η υπο-ενότητα είναι «σε ποιες και σε πόσες από τις επιθέσεις εμφάνισε alerts το κάθε IDS;», «σε ποιες και σε πόσες από τις επιθέσεις είχαμε IoCs από το κάθε IDS;», «σε πόσες επιθέσεις τα δύο IDS παρουσιάζουν αποτελεσματικότητα High/Medium/Low;»

Ξεκινάμε λοιπόν με τον πίνακα που εμφανίζει την αποτελεσματικότητα των δύο IDS στο σύνολο των επιθέσεων, δηλαδή σε ποιες από τις επιθέσεις πήραμε alerts και σε ποιες IoCs.

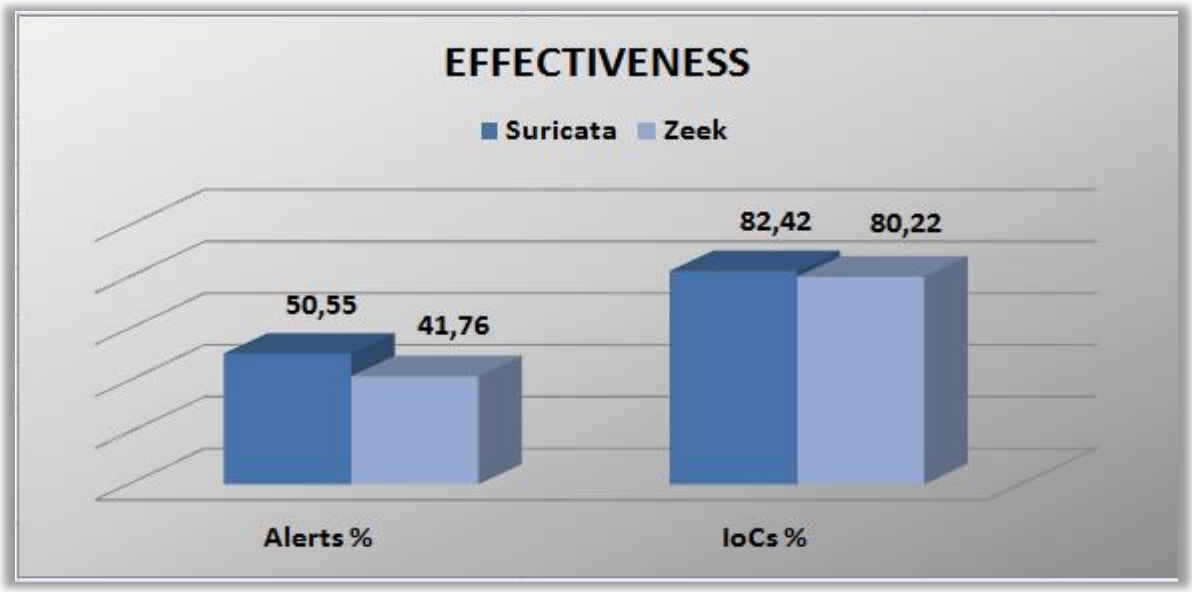
Pcap Name	Alerts		IoCs		Effectiveness	
	Suricata	Zeek	Suricata	Zeek	Suricata	Zeek
1. 20161215_ccnotice.net_malspam_traffic			✓	✓	Medium	Medium
2. 20161216_Locky_malspam_traffic_example					Low	Low
3. 20161222_Cerber_from_malspam_traffic			✓	✓	Medium	Medium
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware			✓	✓	Medium	Medium
5. 20161228_1st_run_Sundown_EK_sends_Chthonic			✓	✓	Medium	Medium
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader			✓	✓	Medium	Medium
7. 20170201_Hancitor_Pony_malspam_traffic	✓	✓	✓	✓	High	High
8. 20170202_Cerber_from_adibas.top			✓	✓	Medium	Medium
9.20170215_EITest_HoeflerText_Chrome_popup_traffic_1_of_6	✓		✓	✓	High	Medium
10.20170215_EITest_HoeflerText_Chrome_popup_traffic_2_of_6	✓		✓	✓	High	Medium
11. 20170221_Hancitor_malspam_traffic			✓	✓	Medium	Medium
12. 20170221_ZeusPandaBanker_malspam_traffic		✓	✓	✓	Medium	High
13. 20170302_Nebula_EK_1st_run	✓		✓	✓	High	Medium
14. 20170302_Nebula_EK_2nd_run			✓	✓	Medium	Medium
15. 20170302_Nebula_EK_3rd_run	✓		✓	✓	High	Medium
16. 20170313_Kovter_Locky_malspam_traffic	✓	✓	✓	✓	High	High
17. 20170314_Kovter_malspam_traffic	✓	✓	✓	✓	High	High
18. 20170315_EITest_Rig_EK_sends_Revenge_ransomware	✓		✓		High	Low
19. 20170330_Dridex_confirmation_letter_Dridex_traffic	✓	✓	✓	✓	High	High
20. 20170405_Terror_EK_sends_Andromeda_1st_run			✓	✓	Medium	Medium
21. 20170405_Terror_EK_sends_Andromeda_2nd_run			✓	✓	Medium	Medium
22. 20170421_Locky_malspam_traffic					Low	Low
23. 20170429_CVE_2017_0199_attempt_from_horsezangd			✓	✓	Medium	Medium
24. 20170516_Jaff_ransomware_malspam_traffic	✓		✓		High	Low
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit	✓		✓	✓	High	Medium
26. 20170601_ZeusPandaBanker_malspam_traffic	✓	✓	✓	✓	High	High
27. 20170612_Loki_Bot_malspam_traffic					Low	Low
28. 20170612_Trickbot_malspam_traffic					Low	Low
29. 20170612_Ursnif_malspam_traffic			✓	✓	Medium	Medium
30. 20170710_Kovter_Nemucod_malspam_traffic	✓	✓	✓	✓	High	High
31. 20170724_Trickbot_malspam_traffic		✓			Low	Medium
32. 20170726_Emotet_malspam_traffic			✓	✓	Medium	Medium
33. 20170803_Hancitor_malspam_traffic	✓	✓	✓	✓	High	High
34.20170812_Trickbot_infection_from_carriereiserphotography.com		✓	✓	✓	Medium	High
35. 20170812_Trickbot_infection_from_carriereiter.com.exe		✓	✓	✓	Medium	High
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu			✓		Medium	Low
37. 20171010_Emotet_malspam_traffic	✓	✓	✓	✓	High	High
38.20171017_post_infection_traffic_from_Terror_EK_payload	✓	✓	✓	✓	High	High

39. 20171017_Terror_EK_example			✓	✓	Medium	Medium
40. 20171018_Locky_Bot_traffic					Low	Low
41. 20171031_Necurs_Botnet_malspam_pushing_Locky			✓	✓	Medium	Medium
42. 20171102_Smoke_Loader_traffic	✓	✓	✓	✓	High	High
43. 20171129_Emotet_malspam_1st_run	✓		✓	✓	High	Medium
44. 20171204_Dridex_malspam_trafic	✓	✓	✓	✓	High	High
45. 20171220_smb_at_schedule				✓	Low	Medium
46.20171220_smb_metasploit_psexec_pth_download_meterpreter	✓		✓	✓	High	Medium
47. 20171220_smb_mimikatz_copy					Low	Low
48. 20171220_smb_mimikatz_copy_to_host			✓	✓	Medium	Medium
49. 20171220_smb_net_user					Low	Low
50. 20171220_smb_psexec_add_user	✓		✓		High	Low
51. 20171220_smb_psexec_mimikatz_ticket_dump					Low	Low
52. 20171222_malspam_pushing_RemcosRAT	✓	✓	✓	✓	High	High
53. 20180102_fake_Flash_player_installs_coinminer_malware	✓	✓	✓	✓	High	High
54. 20180104_PCRat_gh0st_traffic					Low	Low
55. 20180104_PCRat_gh0st_traffic_pcap					Low	Low
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic	✓	✓	✓	✓	High	High
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_coin_miner	✓	✓	✓	✓	High	High
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffic					Low	Low
59.20180821_Neutrino_infection_traffic_from_password_protected_Word_doc	✓		✓	✓	High	Medium
60.20181008_Trickbot_sat75_infection_with_powershell_empire_traffic		✓	✓	✓	Medium	High
61. 20181019_malspam_pushing_Nymaim_infection_traffic			✓	✓	Medium	Medium
62. 20181210_Imminent_Monitor_RAT_infection	✓	✓	✓	✓	High	High
63. 20181227_shade_malspam_infection	✓	✓	✓	✓	High	High
64. 20190104_Nanocore_RAT_infection_traffic					Low	Low
65. 20190207_cred_stealer_via_FTP_traffic			✓	✓	Medium	Medium
66. 20190306_Flawed_Ammyy_traffic	✓		✓	✓	High	Medium
67. 20190522_Rig_EK_sends_Gandcrab_ransomware	✓	✓	✓	✓	High	High
68. 20190802_Lord_EK_sends_Eris_Ransomware	✓	✓	✓	✓	High	High
69. 20190812_Rig_EK_sends_MedusaHTTP_malware			✓		Medium	Low
70. 20190904_Ursnif_infection_with_Trickbot	✓	✓	✓	✓	High	High
71. 20190913_WSHRAT_infection_traffic	✓		✓	✓	High	Medium
72. 20200115_RevengeRAT_infection_traffic	✓	✓	✓	✓	High	High

73. 20200226_Trickbot_spreads_from_infected_client_to_DC	✓	✓	✓	✓	High	High
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps		✓	✓	✓	Medium	High
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps		✓	✓	✓	Medium	High
75. 20200701_pitty_tiger_1hr	✓	✓	✓	✓	High	High
76. 20200701_Valak_infection_with_IcedID		✓	✓	✓	Medium	High
77.20201229_Emotet_infection_with_Trickbot_and_spambot_activity	✓	✓	✓	✓	High	High
78. 20210105_PurpleFox_EK_and_post_infection_traffic	✓	✓	✓	✓	High	High
79. 20210223_lateral_backup_c2_1hr			✓	✓	Medium	Medium
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cobalt_Strike	✓	✓	✓	✓	High	High
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	✓	✓	✓	✓	High	High
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike	✓	✓	✓	✓	High	High
83. 20220101_thru_03_server_activity_with_log4j_attempts	✓		✓	✓	High	Medium
eternalblue_success_unpatched_win7			✓	✓	Medium	Medium
85. LM_psexec_smb_dcerpc_epm_svcctl				✓	Low	Medium
86. LM_smbexec_smb_dcerpc_svcctl_epm				✓	Low	Medium
87. mmcexec	✓		✓	✓	High	Medium
88. 20211215_thru_20_server_activity_with_log4j_attempts	✓		✓	✓	High	Medium
89. usecase4_spearphishing_EKC2_lateral_move	✓	✓	✓	✓	High	High
90. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike	✓	✓	✓	✓	High	High
Total	46	38	75	73	Low:16 Med:29 High:46	Low:17 Med:37 High:37

Πίνακας 6. Η αποτελεσματικότητα των δύο IDS στο σύνολο των επιθέσεων

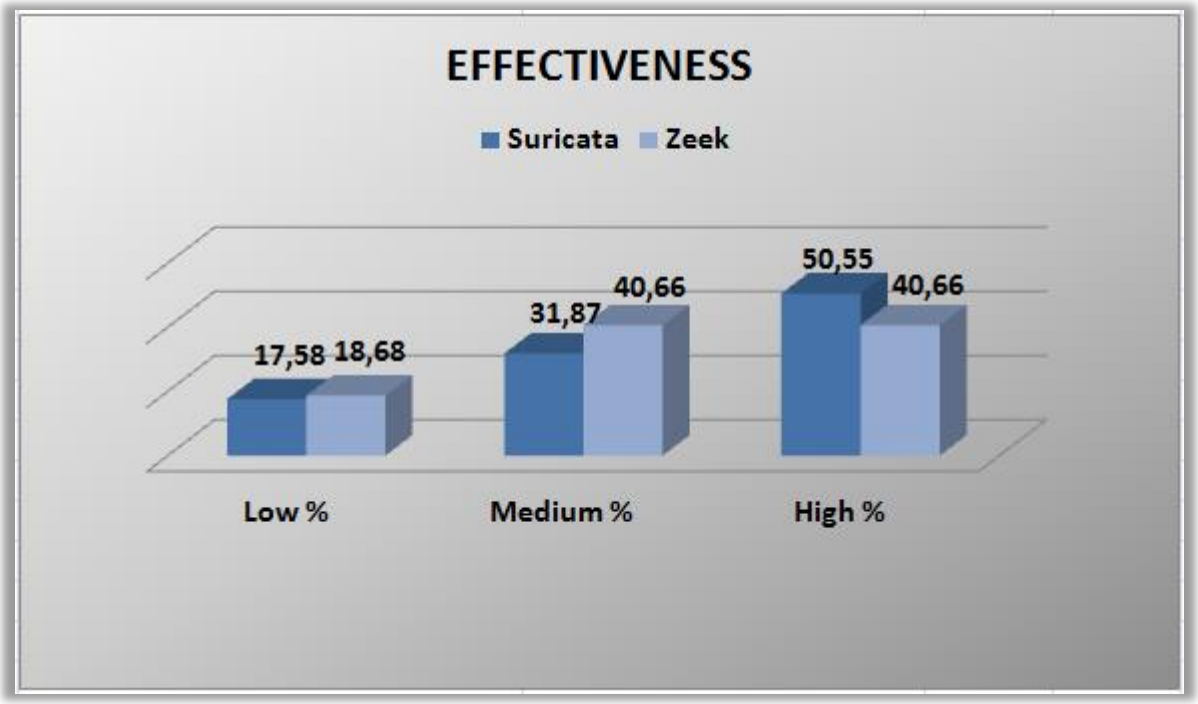
Τα διαγράμματα που ακολουθούν οπτικοποιούν τον παραπάνω πίνακα και προσφέρουν μία εικόνα για την συμπεριφορά των δύο IDS.



Εικόνα 54. Το ποσοστό των επιθέσεων στις οποίες εμφάνισαν alerts ή/και IoCs

Στο γράφημα της Εικόνας 54 βλέπουμε πως το Suricata υπερτερεί στην συχνότητα εμφάνισης των alerts με ποσοστό 50.55%, έναντι 41.76% του Zeek. Ενώ στο θέμα των IoCs τα δύο IDS βρίσκονται πολύ κοντά, 82% και 80% αντίστοιχα. Αυτά ακριβώς τα χαρακτηριστικά συμπεράναμε και κατά την περίπτωση μελέτης στην ενότητα 4.3.

Το επόμενο γράφημα (Εικόνα 55) είναι εκείνο που αντικατοπτρίζει την αποτελεσματικότητα με την κλίμακα των τριών βαθμίδων.



Εικόνα 55. Η αποτελεσματικότητα των δύο IDS σύμφωνα με την κλίμακα Low – Medium – High

Εδώ είναι φανερό πως τα δύο IDS – εξαιρουμένης της βαθμίδας "Low" – εμφανίζουν μία διαφορά της τάξεως του 9 – 10% στην αποτελεσματικότητά τους. Την στιγμή που το Suricata παρουσιάζει υψηλή αποτελεσματικότητα στο 50% των επιθέσεων, το Zeek έχει την ίδια στο 40% των επιθέσεων. Το αντίστροφο παρατηρούμε για τις περιπτώσεις όπου τα δύο IDSs εμφανίζουν μέτρια απόδοση. Τέσσερις στις δέκα φορές το Zeek είχε μέτρια απόδοση, ενώ το Suricata εμφάνιζε τρεις στις δέκα φορές.

5.2 Σύγκριση ως προς τον τύπο των alerts

Η υπο-ενότητα αυτή έρχεται να απαντήσει σε ερωτήματα όπως, «τι alerts εμφάνισε το κάθε IDS;», «υπάρχουν κάποια που εμφανίστηκαν περισσότερες από μία φορές και αν ναι πόσες;».

Στον πίνακα που ακολουθεί παρουσιάζονται μόνο οι επιθέσεις, στις οποίες είχαμε την εμφάνιση κάποιου alert, καθώς επίσης και τι alerts προέκυψαν και από τα δύο IDSs.

Pcaps	Suricata Alerts	Zeek Alerts
7. 20170201_Hancitor_Pony_malspam_traffic	SURICATA STREAM excessive retransmissions	SSL certificate validation failed with (self signed certificate)
	SURICATA Applayer Detect protocol only one direction	
9.20170215_EITest_HoeflerText_Chrome_popup_traffic_1_of_6	SURICATA HTTP Request abnormal Content-Encoding header	
10.20170215_EITest_HoeflerText_Chrome_popup_traffic_2_of_6	SURICATA HTTP Request abnormal Content-Encoding header	
12. 20170221_ZeusPandaBanker_malspam_traffic		SSL certificate validation failed with (unable to get local issuer certificate)
13. 20170302_Nebula_EK_1st_run	SURICATA HTTP invalid response chunk len	
15. 20170302_Nebula_EK_3rd_run	SURICATA HTTP invalid response chunk len	
	SURICATA HTTP gzip decompression failed	
16. 20170313_Kovter_Locky_malspam_traffic	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
	SURICATA Applayer Detect protocol only one direction	
	SURICATA HTTP Request line incomplete	
17. 20170314_Kovter_malspam_traffic	SURICATA HTTP unable to match response to request	SSL certificate validation failed with (self signed certificate)
	SURICATA Applayer Detect protocol only one direction	SSL certificate validation failed with (certificate has expired)
	SURICATA HTTP Request line incomplete	
18. 20170315_EITest_Rig_EK_sends_Revenge_ransomware	SURICATA HTTP Request abnormal Content-Encoding header	
	SURICATA HTTP gzip decompression failed	
	SURICATA HTTP invalid response chunk len	
19. 20170330_Dridex_confirmation_letter_Dridex_traffic	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (self signed certificate)
		SSL certificate validation failed with (unable to get local issuer certificate)
24. 20170516_Jaff_ransomware_malspam_traffic	SURICATA HTTP invalid response chunk len	
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit	SURICATA ICMPv6 invalid checksum	
	ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010 / Attempted Administrator Privilege Gain	
26. 20170601_ZeusPandaBanker_malspam_traffic	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
		SSL certificate validation failed with (self signed certificate)
30. 20170710_Kovter_Nemucod_malspam_traffic	SURICATA HTTP Request line incomplete	SSL certificate validation failed with (unable to get local issuer certificate)
	SURICATA Applayer Detect protocol only one direction	SSL certificate validation failed with (self signed certificate)
	SURICATA HTTP METHOD terminated by non-compliant character	SSL certificate validation failed with (certificate has expired)
31. 20170724_Trickbot_malspam_traffic		SSL certificate validation failed with (self signed certificate)
33. 20170803_Hancitor_malspam_traffic	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Ransomware)	SSL certificate validation failed with (unable to get local issuer certificate)

34.20170812_Trickbot_infection_from_carriereiserphotography.com		SSL certificate validation failed with (certificate has expired)
35. 20170812_Trickbot_infection_from_carriereiter.com.exe		SSL certificate validation failed with (self signed certificate)
37. 20171010_Emotet_malspam_traffic	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Ransomware)	SSL certificate validation failed with (certificate has expired)
	SURICATA HTTP invalid response chunk len	
	SURICATA Applayer Detect protocol only one direction	
	SURICATA SMTP invalid reply	SSL certificate validation failed with (unable to get local issuer certificate)
	ET POLICY Outbound Multiple Non-SMTP Server Emails / Misc activity	
	SURICATA STREAM FIN1 FIN with wrong seq	
	SURICATA TLS invalid record/traffic	
38.20171017_post_infection_traffic_from_Terror_EK_payload	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (certificate has expired)
42. 20171102_Smoke_Loader_traffic	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
43. 20171129_Emotet_malspam_1st_run	SURICATA HTTP invalid response chunk len	
44. 20171204_Dridex_malspam_trafic	SURICATA HTTP invalid response chunk len	SSL certificate validation failed with (self signed certificate)
46.20171220_smb_metasploit_psexec_pth_download_meterpreter	SURICATA SMB malformed response data	
50. 20171220_smb_psexec_add_user	SURICATA IPv4 invalid checksum	
52. 20171222_malspam_pushing_RemcosRAT	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
53. 20180102_fake_Flash_player_installs_coinminer_malware	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (certificate has expired)
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic	SURICATA HTTP invalid response chunk len	SSL certificate validation failed with (self signed certificate)
	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_coin_miner	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
		SSL certificate validation failed with (certificate has expired)
59.20180821_Neutrino_infection_traffic_from_password_protected_Word_doc	SURICATA STREAM ESTABLISHED invalid ack	
	SURICATA STREAM Packet with invalid ack	
	SURICATA STREAM FIN invalid ack	
	SURICATA STREAM ESTABLISHED packet out of window	
	SURICATA STREAM FIN out of window	

60.20181008_Trickbot_sat75_infection_with_powershell_empire_traffic		SSL certificate validation failed with (self signed certificate)
62. 20181210_Imminent_Monitor_RAT_infection	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
63. 20181227_shade_malspam_infection	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Ransomware.Troldesh)	SSL certificate validation failed with (unable to get local issuer certificate)
	ET POLICY TLS possible TOR SSL traffic / Misc activity	
	ET POLICY Cleartext WordPress Login / Potential Corporate Privacy Violation	SSL certificate validation failed with (certificate has expired)
66. 20190306_Flawed_Ammyy_traffic	SURICATA STREAM bad window update	
67. 20190522_Rig_EK_sends_Gandcrab_ransomware	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
68. 20190802_Lord_EK_sends_Eris_Ransomware	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
70. 20190904_Ursnif_infection_with_Trickbot	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (self signed certificate)
	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Adware)	SSL certificate validation failed with (unable to get local issuer certificate)
		SSL certificate validation failed with (certificate has expired)
71. 20190913_WSHRAT_infection_traffic	SURICATA Applayer Detect protocol only one direction	
72. 20200115_RevengeRAT_infection_traffic	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
73. 20200226_Trickbot_spreads_from_infected_client_to_DC	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (self signed certificate)
	SURICATA STREAM Last ACK with wrong seq	SSL certificate validation failed with (certificate has expired)
		SSL certificate validation failed with (unable to get local issuer certificate)
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps		SSL certificate validation failed with (certificate has expired)
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps		SSL certificate validation failed with (certificate has expired)
75. 20200701_pitty_tiger_1hr	SURICATA IPv4 invalid checksum	SSL certificate validation failed with (unable to get local issuer certificate)
	SURICATA UDPv4 invalid checksum	SSL certificate validation failed with (certificate has expired)
76. 20200701_Valak_infection_with_IcedID		SSL certificate validation failed with (self signed certificate)

77.20201229_Emotet_infection_with_Trickbot_and_spambot_activity	SURICATA Applayer Mismatch protocol both directions	SSL certificate validation failed with (self signed certificate)
	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (TrickBot)	
	SURICATA Applayer Detect protocol only one direction	SSL certificate validation failed with (unable to get local issuer certificate)
	SURICATA SMTP invalid reply	
	SURICATA SMTP tls rejected	SSL certificate validation failed with (certificate has expired)
	SURICATA SMTP data command rejected	
	ET POLICY Outbound Multiple Non-SMTP Server Emails / Misc activity	
78. 20210105_PurpleFox_EK_and_post_infection_traffic	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	SSL certificate validation failed with (unable to get local issuer certificate)
		SSL certificate validation failed with (certificate has expired)
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cobalt_Strike	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Dridex)	SSL certificate validation failed with (unable to get local issuer certificate)
		SSL certificate validation failed with (certificate has expired)
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	SURICATA HTTP gzip decompression failed	SSL certificate validation failed with (unable to get local issuer certificate)
	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Dridex)	SSL certificate validation failed with (certificate has expired)
	SURICATA HTTP unable to match response to request	
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike	SURICATA Applayer Wrong direction first Data	SSL certificate validation failed with (certificate has expired)
		SSL certificate validation failed with (self signed certificate)
83. 20220101_thru_03_server_activity_with_log4j_attempts	ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03 / Attempted Denial of Service	
	SURICATA UDPv4 invalid checksum	
87. mmcexec	ICMP Ping	
	ET NETBIOS DCERPC DCOM ExecuteShellCommand Call - Likely Lateral Movement / Potentially Bad Traffic	

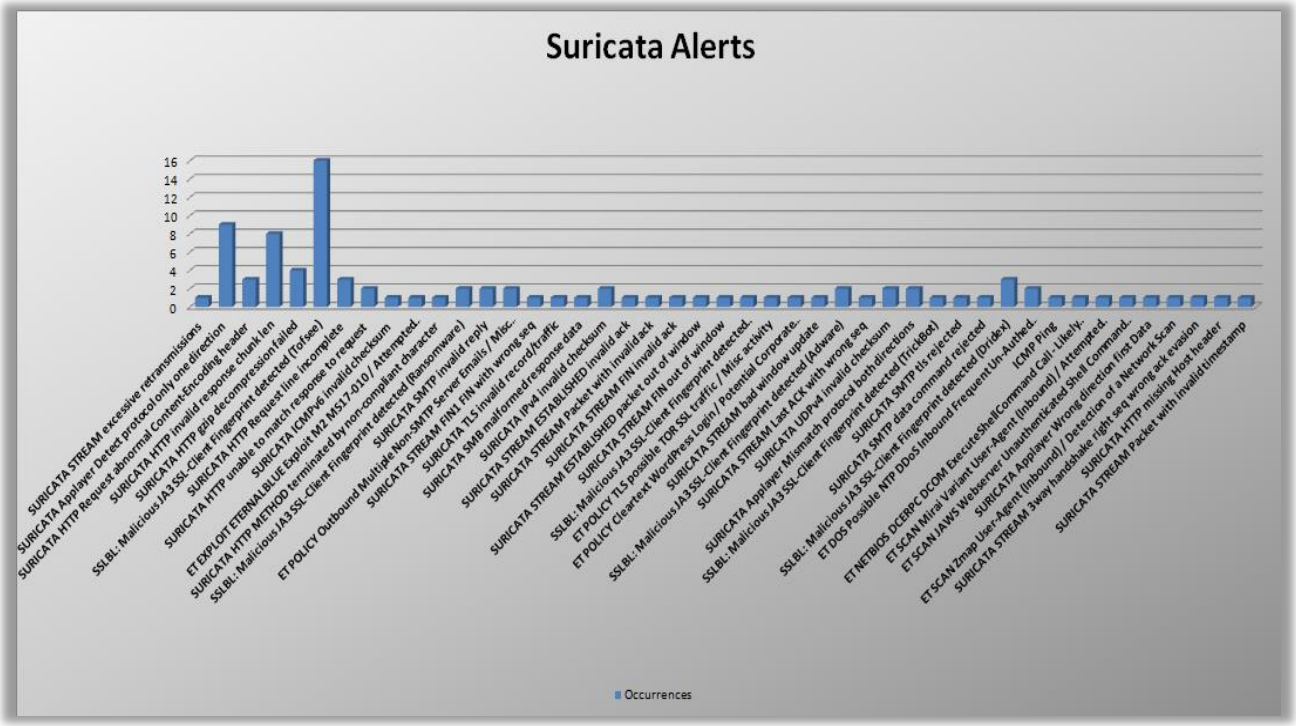
88. 20211215_thru_20_server_activity_with_log4j_atten	SURICATA UDPv4 invalid checksum	
	ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03 / Attempted Denial of Service	
	ET SCAN Mirai Variant User-Agent (Inbound) / Attempted Administrator Privilege Gain	
	ET SCAN JAWS Webserver Unauthenticated Shell Command Execution / Web Application Attack	
	SURICATA ICMPv4 invalid checksum	
	ET SCAN Zmap User-Agent (Inbound) / Detection of a Network Scan	
	URICATA STREAM 3way handshake right seq wrong ack evasio	
	SURICATA Applayer Mismatch protocol both directions	
	SURICATA HTTP missing Host header	
	SURICATA STREAM Packet with invalid timestamp	
	SURICATA Applayer Detect protocol only one direction	
89. usecase4_spearphishing_EKC2_lateral_move	SURICATA IPv4 invalid checksum	SSL certificate validation failed with (certificate has expired)
	SURICATA UDPv4 invalid checksum	SSL certificate validation failed with (unable to get local issuer certificate)
	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Adware)	
90. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike	SURICATA Applayer Detect protocol only one direction	SSL certificate validation failed with (certificate has expired)
	SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Dridex)	SSL certificate validation failed with (self signed certificate)
		SSL certificate validation failed with (unable to get local issuer certificate)

Πίνακας 7. Συγκεντρωτικά τα alerts των δύο IDS στο σύνολο των επιθέσεων

Αυτό που σίγουρα μπορούμε να συμπεράνουμε από τον παραπάνω πίνακα είναι πως το Suricata εμφανίζει μία ποικιλομορφία ως προς τα alerts και καλύτερη συμπεριφορά στην ανίχνευση κακόβουλου λογισμικού.

- ***Suricata***

Στην συνέχεια, ακολουθεί το γράφημα της Εικόνας 57, με στοιχεία για τον αριθμό εμφανίσεων για κάθε alert που πήραμε μόνο από το Suricata.



Εικόνα 56. Ο αριθμός εμφανίσεων για κάθε alert του Suricata

Suricata Alerts	Occurrences	Malware
SURICATA STREAM excessive retransmissions	1	Hancitor_Pony
SURICATA Applayer Detect protocol only one direction	9	Hancitor_Pony, Kovter_Locky, Kovter_Nemucod, Emotet, WSHRAT, Trickbot, log4j, IcedID, DarkVNC, Cobalt Strike
SURICATA HTTP Request abnormal Content-Encoding header	3	ElTest
SURICATA HTTP invalid response chunk len	8	Nebula, ElTest, Rig_EK_Revenge_Ransomware, Jaff_Ransomware, Emotet, Dridex, ZeusPanda
SURICATA HTTP gzip decompression failed	4	Nebula, Emotet, ElTest_Rig_EK_Revenge_Ransomware, Hancitor_Cobalt_Strike_netping_tool
SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)	16	Kovter_Locky, Dridex, ZeusPandaBanker, Terror_EK, Smoke_Loader, Remcos_RAT, coinminer, Emotet, Monero_coinminer, Rig_EK, Imminent_monitor_RAT, Gandcrab_ransomware, Eris_ransomware, Ursnif, Lord_EK,
SURICATA HTTP Request line incomplete	3	Kovter/Kovter_Nemucod
SURICATA HTTP unable to match response to request	2	Kovter, Hancitor_Cobalt Strike_netping tool
SURICATA ICMPv6 invalid checksum	1	WannaCry_EternalBlue
ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010 / Attempted Administrator Privilege Gain	1	WannaCry_EternalBlue
SURICATA HTTP METHOD terminated by non-compliant character	1	Kovter_Nemucod
SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Ransomware)	2	Hancitor, Emotet
SURICATA SMTP invalid reply	2	Emotet, Trickbot
ET POLICY Outbound Multiple Non-SMTP Server Emails / Misc Activity	2	Emotet, Trickbot
SURICATA STREAM FIN1 FIN with wrong seq	1	Emotet
SURICATA TLS invalid record/traffic	1	Emotet
SURICATA SMB malformed response data	1	psexec
SURICATA IPv4 invalid checksum	2	psexec, EK_C2_lateral_move
SURICATA STREAM ESTABLISHED invalid ack	1	Neutrino
SURICATA STREAM Packet with invalid ack	1	Neutrino
SURICATA STREAM FIN invalid ack	1	Neutrino
SURICATA STREAM ESTABLISHED packet out of window	1	Neutrino
SURICATA STREAM FIN out of window	1	Neutrino
SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Ransomware.Troldesh)	1	Shade
ET POLICY TLS possible TOR SSL traffic / Misc activity	1	Shade
ET POLICY Cleartext WordPress Login / Potential Corporate Privacy Violation	1	Shade
SURICATA STREAM bad window update	1	Flawed_Ammyy
SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Adware)	2	Ursnif, Trickbot, EKC2_LM
SURICATA STREAM Last ACK with wrong seq	1	Trickbot
SURICATA UDPv4 invalid checksum	2	Pitty_tiger, EKC2_LM
SURICATA Applayer Mismatch protocol both directions	2	Emotet, Trickbot, log4j
SSLBL: Malicious JA3 SSL-Client Fingerprint detected (TrickBot)	1	Emotet, Trickbot
SURICATA SMTP tls rejected	1	Emotet, Trickbot
SURICATA SMTP data command rejected	1	Emotet, Trickbot
SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Dridex)	3	Hancitor_FickerStealer_Cobalt_Strike, Hancitor_Cobalt_Strike_netping_tool, IcedID_DarkVNC_Cobalt_Strike
ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03 / Attempted Denial of Service	2	log4j
ICMP Ping	1	mmcexec
ET NETBIOS DCERPC DCOM ExecuteShellCommand Call - Likely Lateral Movement / Potentially Bad Traffic	1	mmcexec
ET SCAN Mirai Variant User-Agent (Inbound) / Attempted Administrator Privilege Gain	1	jog4j
ET SCAN JAWS Webserver Unauthenticated Shell Command Execution / Web Application Attack	1	jog4j
SURICATA Applayer Wrong direction first Data	1	TA551
ET SCAN Zmap User-Agent (Inbound) / Detection of a Network Scan	1	jog4j
SURICATA STREAM 3way handshake right seq wrong ack evasion	1	jog4j
SURICATA HTTP missing Host header	1	jog4j
SURICATA STREAM Packet with invalid timestamp	1	jog4j

Πίνακας 8. Τα alerts του Suricata μαζί με τον αριθμό εμφανίσεων και το malware, στο οποίο εμφανίστηκε το καθένα

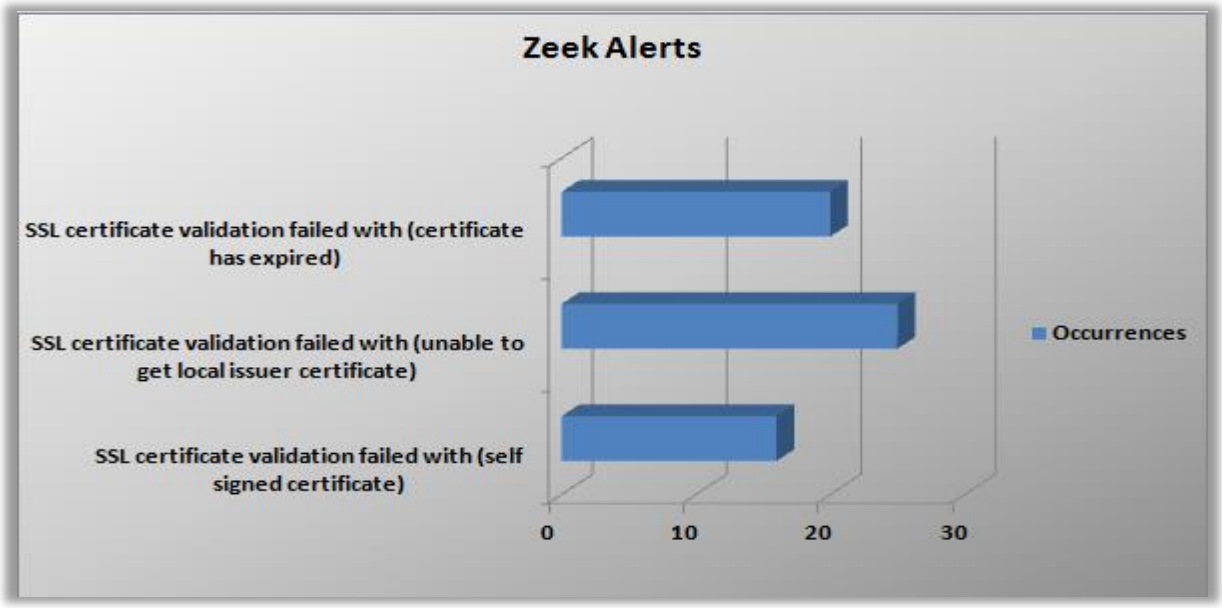
Στο γράφημα της Εικόνας 57 παρατηρούμε πως το alert εκείνο που έχει τις περισσότερες εμφανίσει είναι το «*SSLBL: Malicious JA3 SSL-Client Fingerprint Detected (Tofsee*[15]*)*» με 16 εμφανίσεις, ενώ το αμέσως επόμενο είναι το «*Suricata Applayer Detect protocol only one direction*» με 9 εμφανίσεις. Στον Πίνακα 8, εκτός από τον αριθμό των εμφανίσεων για κάθε τύπο alert, βλέπουμε και σε ποιο κακόβουλο λογισμικό παρουσιάστηκε το καθένα. Αυτό που μπορούμε να συμπεράνουμε από τα παραπάνω είναι πως – στο δείγμα των επιθέσεων – το είδος malware που χρησιμοποιήθηκε περισσότερο από τους επιτιθέμενους είναι *trojan* (Tofsee). Και είναι λογικό διότι αποτελούν εξαιρετικό μέσο μετάδοσης άλλων malwares. Επιπλέον, παρατηρούμε πως κάποια alerts έκαναν την εμφάνισή τους μία και μόνη φορά με συγκεκριμένο malware και ίσως να μπορούμε να τα ταυτίσουμε μεταξύ τους, έτσι ώστε να γνωρίζουμε άμεσα βλέποντας ένα alert, με ποιο malware έχουμε έρθει αντιμέτωποι. Αυτό όμως είναι κάτι που για να πραγματοποιηθεί θα πρέπει να γίνει έρευνα σε βάθος χρόνου και με μεγαλύτερο εύρος ως προς το δείγμα της έρευνας.

Συνεχίζουμε με τα στοιχεία για το Zeek. Ο Πίνακας 9 παρουσιάζει τα alerts που προέκυψαν, καθώς επίσης και τα malware στα οποία εμφανίστηκε το καθένα.

Zeek Alerts	Occurrences	Malware
SSL certificate validation failed with (self signed certificate)	16	Hancitor_Pony, Kovter, Dridex, ZeusPandaBanker, Kovter_Nemucod, Trickbot, Emotet, Ursnif, Valak_IcedID, TA551_Trickbot_Cobalt_Strike, IcedID_DarkVNC_Cobalt_Strike
SSL certificate validation failed with (unable to get local issuer certificate)	25	ZeusPandaBanker, Kovter_Locky, Dridex, Kovter_Nemucod, Hancitor, Emotet, Smoke_Loader, RemcosRAT, RIG_EK_Smoke_Loader_Monero_coin_miner, Imminent_monitor_RAT, shade, RIG_EK_Gandcrab, Lord_EK_Eris_ransomware, Ursnif, Trickbot, Revenge_RAT, Pitty_Tiger, PurpleFox_EK, Hancitor_Ficker_stealer_Cobalt_Strike, Hancitor_Cobalt_Strike_netping_tool, EKC2, IcedID_DarkVNC_Cobalt_Strike
SSL certificate validation failed with (certificate has expired)	20	Kovter, Kovter_Nemucod, Trickbot, Emotet, Terror_EK, coinminer, Rig_EK_Smoke_Loader_Monero_coin_miner, shade, Ursnif, GULoader_NetWire_RAT, pitty_tiger, PurpleFox_EK, Hancitor_Ficker_stealer_Cobalt_Strike, Hancitor_Cobalt_Strike_netping_tool, TA551_Trickbot_Cobalt_Strike, EKC2, IcedID_DarkVNC_Cobalt_Strike

Πίνακας 9. Τα alerts του Zeek μαζί με τον αριθμό εμφανίσεων και το malware, στο οποίο εμφανίστηκε το καθένα

Ενώ το παρακάτω γράφημα παρέχει μία εικόνα για τις εμφανίσεις των alerts που πήραμε από το Zeek.



Εικόνα 57. Ο αριθμός εμφανίσεων για κάθε alert του Zeek

[15] https://www.f-secure.com/v-descs/backdoor_w32_tofsee.shtml

Από τα παραπάνω γίνεται φανερό πως το alert που επικράτησε στα log files του Zeek είναι το «*SSL certificate validation failed with (unable to get local issuer certificate)*», με 25 παρουσίες, και δεύτερο το «*SSL certificate validation failed with (certificate has expired)*» με 20. Το πρώτο αφορά λανθασμένες ρυθμίσεις στο SSL πιστοποιητικό του host και συνήθως προκαλείται από self-signed πιστοποιητικά και το δεύτερο αφορά πιστοποιητικά που έχουν λήξει.

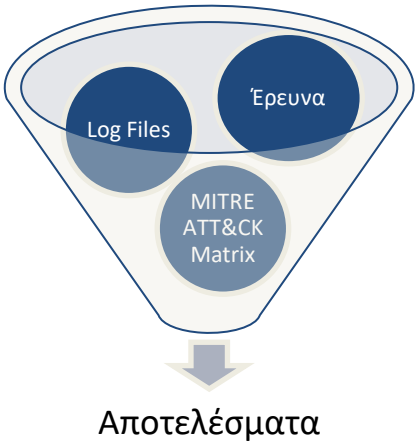
Στην υπο-ενότητα 5.1 ασχοληθήκαμε με τα υπό μελέτη IDSs και την αποτελεσματικότητά τους (*Low –Medium – High*). Έπειτα, στην υπο-ενότητα 5.2 μελετήσαμε τα alert που προέκυψαν. Στην επόμενη υπο-ενότητα θα ασχοληθούμε με τις επιθέσεις και το κακόβουλο λογισμικό που χρησιμοποιήθηκε.

5.3 Ταξινόμηση των επιθέσεων στο πλαίσιο του MITRE ATT&CK

Ξεκινώντας αυτή την υπο-ενότητα κρίνεται σκόπιμο να αναφερθούμε λίγο πιο συγκεκριμένα στο πως καταλήξαμε στα στοιχεία που θα παρουσιάσουμε. Στόχος μας ήταν να μελετήσουμε το κακόβουλο λογισμικό και να καταγράψουμε τις τακτικές και τεχνικές (*Tactics, Techniques and Procedures – TTPs*), σύμφωνα με το μοντέλο MITRE ATT&CK, οι οποίες χρησιμοποιούνται από τα συγκεκριμένα λογισμικά. Απώτερος σκοπός της όλης διαδικασίας είναι να συμπεράνουμε ποια τεχνική από κάθε τακτική είναι η συνηθέστερη ή αλλιώς με ποιες ερχόμαστε πιο συχνά αντιμέτωποι. Οι τεχνικές που εντοπίστηκαν αναφέρονται στο Παράρτημα ΙΙ.

Τα αποτελέσματα που παρουσιάζονται σε αυτή την υπο-ενότητα βασίζονται σε τρεις συνιστώσες:

1. Αναζήτηση σε βιβλιογραφικές και διαδικτυακές πηγές για πληροφορίες σχετικά με το κακόβουλο λογισμικό της κάθε επίθεσης και αναφορές ανάλυσης επιθέσεων με το ανάλογο κακόβουλο λογισμικό. Ενδεικτικά αναφέρουμε την εργασία των Akbanov M., Vassilakis V. και Logothetis D. (Akbanov, Vassilakis, & Logothetis, 2019)
2. Τις ενδείξεις παραβίασης που είχαμε από τα log files.
3. Το MITRE ATT&CK[16] (ATT&CK Matrix for Enterprise)



Εικόνα 58. Η μεθοδολογία που ακολουθήσαμε για την εξαγωγή των συμπερασμάτων

Εν συνεχεία, παρουσιάζουμε τα ευρήματα και εξάγουμε συμπεράσματα ανά τακτική.

[16] https://attack.mitre.org/

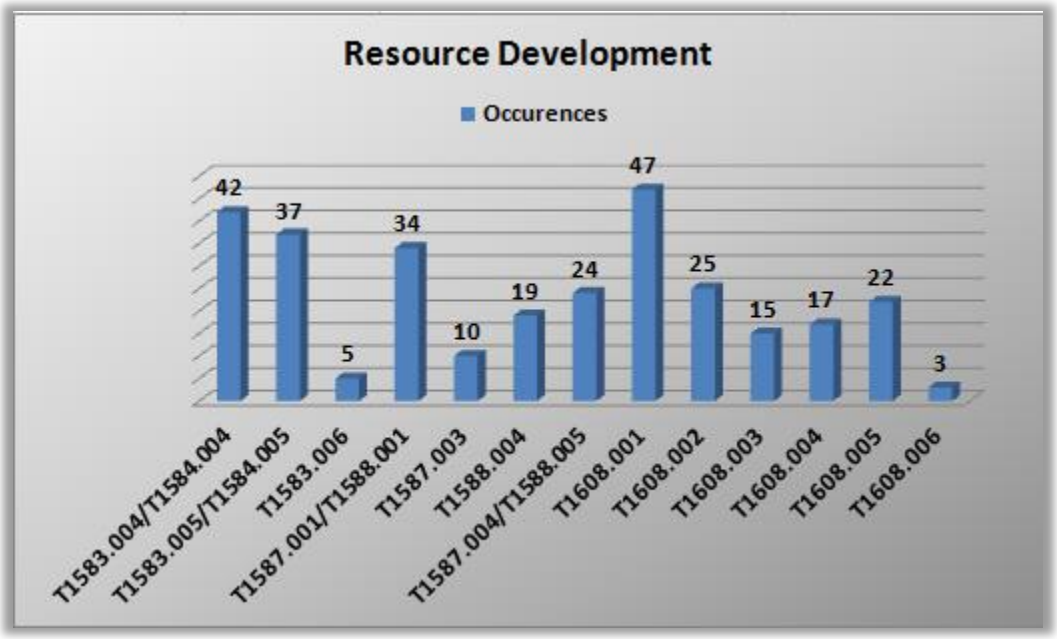
Pcap Name / Mitre Attack Tactic	Resource Development												
	T1583.004/ T1584.004	T1583.005/ T1584.005	T1583.006	T1587.001/ T1588.001	T1587.003	T1588.004	T1587.004/ T1588.005	T1608.001	T1608.002	T1608.003	T1608.004	T1608.005	T1608.006
1. 20161215_ccnotice.net_malspam_traffic		✔										✔	
2. 20161216_Locky_malspam_traffic_example		✔		✔				✔					
3. 20161222_Cerber_from_malspam_traffic		✔		✔								✔	
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware	✔						✔					✔	
5. 20161228_1st_run_Sundown_EK_sends_Chthonic	✔						✔					✔	
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader	✔						✔					✔	
7. 20170201_Hancitor_Pony_malspam_traffic		✔		✔				✔		✔		✔	
8. 20170202_Cerber_from_edibas.top	✔			✔								✔	
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6		✔						✔					
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6		✔						✔					
11. 20170221_Hancitor_malspam_traffic		✔		✔				✔				✔	
12. 20170221_ZeusPandaBanker_malspam_traffic		✔				✔	✔			✔		✔	✔
13. 20170302_Nebula_EK_1st_run	✔						✔	✔			✔		
14. 20170302_Nebula_EK_2nd_run	✔						✔	✔			✔		
15. 20170302_Nebula_EK_3rd_run	✔						✔	✔			✔		
16. 20170313_Kovter_Locky_malspam_traffic	✔			✔		✔		✔		✔		✔	
17. 20170314_Kovter_malspam_traffic	✔				✔	✔		✔		✔			
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware	✔						✔	✔			✔		
19. 20170330_Dridex_confirmation_letter_Dridex_traffic		✔			✔	✔				✔		✔	
20. 20170405_Terror_EK_sends_Andromeda_1st_run	✔	✔					✔	✔		✔	✔		
21. 20170405_Terror_EK_sends_Andromeda_2nd_run	✔	✔					✔	✔		✔	✔		
22. 20170421_Locky_malspam_traffic		✔		✔				✔					
23. 20170429_CVE_2017_0199_attempt_from_horsezangd	✔						✔	✔			✔		
24. 20170516_Jaff_ransomware_malspam_traffic	✔			✔				✔					
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit	✔			✔			✔	✔	✔				
26. 20170601_ZeusPandaBanker_malspam_traffic		✔			✔	✔	✔			✔		✔	✔
27. 20170612_Loki_Bot_malspam_traffic		✔											
28. 20170612_Trickbot_malspam_traffic		✔		✔				✔	✔				
29. 20170612_Ursnif_malspam_traffic	✔			✔				✔	✔				
30. 20170710_Kovter_Nemucod_malspam_traffic	✔				✔	✔		✔		✔			
31. 20170724_Trickbot_malspam_traffic		✔		✔				✔	✔				
32. 20170726_Emotet_malspam_traffic	✔							✔				✔	
33. 20170803_Hancitor_malspam_traffic		✔		✔				✔				✔	
34.20170812_Trickbot_infection_from_carriereiserphotography.com		✔		✔				✔	✔				
35. 20170812_Trickbot_infection_from_carriereiter.com.exe		✔		✔				✔	✔				
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu	✔			✔			✔	✔			✔		

37. 20171010_Emotet_malspam_traffic	✔							✔				✔	
38.20171017_post_infection_traffic_from_Terror_EK_payloa	✔					✔	✔			✔	✔		
39. 20171017_Terror_EK_example	✔						✔				✔		
40. 20171018_Loki_Bot_traffic		✔											
41. 20171031_Necurs_Botnet_malspam_pushing_Locky		✔		✔				✔			✔		
42. 20171102_Smoke_Loader_traffic	✔			✔		✔		✔					
43. 20171129_Emotet_malspam_1st_run	✔							✔				✔	
44. 20171204_Dridex_malspam_trafic		✔			✔	✔				✔		✔	
45. 20171220_smb_at_schedule													
46.20171220_smb_metasploit_psexec_pth_download_mete rpreter									✔				
47. 20171220_smb_mimikatz_copy													
48. 20171220_smb_mimikatz_copy_to_host													
49. 20171220_smb_net_user													
50. 20171220_smb_psexec_add_user									✔				
51. 20171220_smb_psexec_mimikatz_ticket_dump									✔				
52. 20171222_malspam_pushing_RemcosRAT				✔					✔				
53.20180102_fake_Flash_player_installs_coinminer_malware	✔					✔		✔					
54. 20180104_PCRat_gh0st_traffic	✔												
55. 20180104_PCRat_gh0st_traffic_pcap	✔												
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic	✔	✔			✔	✔	✔	✔		✔		✔	✔
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_c oin_miner	✔		✔	✔		✔	✔	✔					
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffi c		✔	✔					✔			✔		
59.20180821_Neutrino_infection_traffic_from_password_pr otected_Word_doc	✔						✔		✔		✔		
60.20181008_Trickbot_set75_infection_with_powershell_e mpire_traffic		✔		✔	✔			✔	✔				
61. 20181019_malspam_pushing_Nymaim_infection_traffic	✔	✔		✔				✔				✔	
62. 20181210_Imminent_Monitor_RAT_infection				✔		✔							
63. 20181227_shade_malspam_infection	✔				✔	✔			✔	✔			
64. 20190104_Nanocore_RAT_infection_traffic									✔				
65. 20190207_cred_stealer_via_FTP_traffic													
66. 20190306_Flawed_Ammyy_traffic	✔			✔				✔			✔		
67. 20190522_Rig_EK_sends_Gandcrab_ransomware	✔			✔		✔	✔	✔			✔		
68. 20190802_Lord_EK_sends_Eris_Ransomware	✔						✔				✔		
69. 20190812_Rig_EK_sends_MeduseHTTP_malware	✔						✔	✔			✔		
70. 20190904_Ursnif_infection_with_Trickbot	✔	✔		✔				✔	✔				
71. 20190913_WSHRAT_infection_traffic	✔		✔	✔				✔	✔				
72. 20200115_RevengeRAT_infection_traffic	✔			✔				✔					
73.20200226_Trickbot_spreads_from_infected_client_to_DC		✔		✔				✔	✔				
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps	✔					✔			✔	✔			
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps	✔					✔	✔		✔	✔			
75. 20200701_pitty_tiger_1hr													
76. 20200701_Valak_infection_with_IcedID		✔			✔	✔							

77.20201229_Emotet_infection_with_Trickbot_and_spambot _activity	✔	✔		✔				✔	✔			✔	
78. 20210105_PurpleFox_EK_and_post_infection_traffic		✔			✔	✔	✔						
79. 20210223_lateral_backup_c2_1hr													
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cob alt_Strike		✔		✔				✔	✔			✔	
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool		✔		✔				✔	✔			✔	
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike		✔		✔				✔	✔				
83. 20220101_thru_03_server_activity_with_log4j_attempts		✔	✔										
eternalblue_success_unpatched_win7													
85. LM_psexec_smb_dcerpc_epm_svcctl									✔				
86. LM_smbexec_smb_dcerpc_svcctl_epm													
88. mmcexec													
89. 20211215_thru_20_server_activity_with_log4j_attempts		✔	✔										
90. usecase4_spearphishing_EKC2_lateral_move													
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike		✔		✔					✔				

Πίνακας 10. Οι τεχνικές της κατηγορίας Resource Development στο σύνολο των επιθέσεων

Τα αποτελέσματα του Πίνακα 10 συνοψίζονται στο γράφημα της Εικόνα 59.



Εικόνα 59. Resource Development techniques

Παρατηρούμε πως η τεχνική που ξεχωρίζει είναι η ***T1608.001:*** *Stage Capabilities/**Upload Malware***, ακολουθούμενη από τις ***T1583.004/1584.004:*** *Acquire Infrastructure/Server – Compromise Infrastructure/**Server*** και ***T1583.005:*** *Resource Development/Acquire Infrastructure/**Botnet.***

Συνεχίζουμε με την τακτική Initial Access. Ο επόμενος πίνακας παρουσιάζει τις αντίστοιχες τεχνικές αυτής της κατηγορίας.

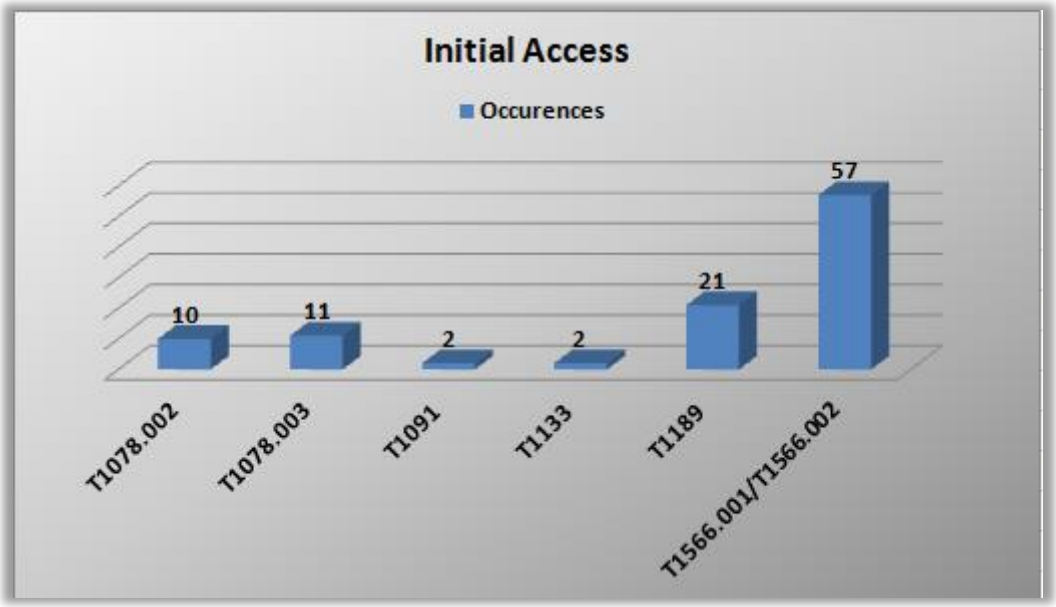
Pcap Name / Mitre Attack Tactic	Initial Access					
	T1078.002	T1078.003	T1091	T1133	T1189	T1566.001/ T1566.002
1. 20161215_ccnotice.net_malspam_traffic					✔	✔
2. 20161216_Locky_malspam_traffic_example						✔
3. 20161222_Cerber_from_malspam_traffic						✔
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware						✔
5. 20161228_1st_run_Sundown_EK_sends_Chthonic						✔
6.20161230_Sundown_EK_1st_run_sends_TerdotA_Zloader						✔
7. 20170201_Hancitor_Pony_malspam_traffic						✔
8. 20170202_Cerber_from_edibas.top						✔
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6					✔	
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6					✔	
11. 20170221_Hancitor_malspam_traffic						✔
12. 20170221_ZeusPandaBanker_malspam_traffic						✔
13. 20170302_Nebula_EK_1st_run					✔	
14. 20170302_Nebula_EK_2nd_run					✔	
15. 20170302_Nebula_EK_3rd_run					✔	
16. 20170313_Kovter_Locky_malspam_traffic						✔
17. 20170314_Kovter_malspam_traffic						✔
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware					✔	
19. 20170330_Dridex_confirmation_letter_Dridex_traffic						✔
20. 20170405_Terror_EK_sends_Andromeda_1st_run	✔				✔	✔
21. 20170405_Terror_EK_sends_Andromeda_2nd_run	✔				✔	✔
22. 20170421_Locky_malspam_traffic						✔
23. 20170429_CVE_2017_0199_attempt_from_horsezangd					✔	✔
24. 20170516_Jeff_ransomware_malspam_traffic						✔
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit				✔		✔
26. 20170601_ZeusPandaBanker_malspam_traffic						✔
27. 20170612_Loki_Bot_malspam_traffic						✔
28. 20170612_Trickbot_malspam_traffic						✔
29. 20170612_Ursnif_malspam_traffic			✔			✔
30. 20170710_Kovter_Nemucod_malspam_traffic						✔
31. 20170724_Trickbot_malspam_traffic						✔
32. 20170726_Emotet_malspam_traffic		✔				✔
33. 20170803_Hancitor_malspam_traffic						✔
34.20170812_Trickbot_infection_from_carriereiserphotography.com						✔
35. 20170812_Trickbot_infection_from_carriereiter.com.exe						✔
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu					✔	

37. 20171010_Emotet_malspam_traffic		✔				✔
38.20171017_post_infection_traffic_from_Terror_EK_payloa	✔				✔	
39. 20171017_Terror_EK_example	✔				✔	
40. 20171018_Loki_Bot_traffic						✔
41. 20171031_Necurs_Botnet_malspam_pushing_Locky						✔
42. 20171102_Smoke_Loader_traffic						✔
43. 20171129_Emotet_malspam_1st_run		✔				✔
44. 20171204_Dridex_malspam_trafic						✔
45. 20171220_smb_at_schedule						
46.20171220_smb_metasploit_psexec_pth_download_meterpreter						
47. 20171220_smb_mimikatz_copy						
48. 20171220_smb_mimikatz_copy_to_host						
49. 20171220_smb_net_user						
50. 20171220_smb_psexec_add_user						
51. 20171220_smb_psexec_mimikatz_ticket_dump						
52. 20171222_malspam_pushing_RemcosRAT						✔
53.20180102_fake_Flash_player_installs_coinminer_malware					✔	
54. 20180104_PCRat_gh0st_traffic						✔
55. 20180104_PCRat_gh0st_traffic_pcap						
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic		✔				✔
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_coin_miner						✔
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffic						
59.20180821_Neutrino_infection_traffic_from_password_protected_Word_doc					✔	
60.20181008_Trickbot_sat75_infection_with_powershell_empire_traffic						✔
61. 20181019_malspam_pushing_Nymaim_infection_traffic						✔
62. 20181210_Imminent_Monitor_RAT_infection						
63. 20181227_shade_malspam_infection						✔
64. 20190104_Nanocore_RAT_infection_traffic						
65. 20190207_cred_stealer_via_FTP_traffic						
66. 20190306_Flawed_Ammyy_traffic					✔	
67. 20190522_Rig_EK_sends_Gandcrab_ransomware					✔	✔
68. 20190802_Lord_EK_sends_Eris_Ransomware	✔	✔			✔	✔
69. 20190812_Rig_EK_sends_MedusaHTTP_malware	✔	✔		✔	✔	✔
70. 20190904_Ursnif_infection_with_Trickbot			✔			✔
71. 20190913_WSHRAT_infection_traffic						✔
72. 20200115_RevengeRAT_infection_traffic						✔
73.20200226_Trickbot_spreads_from_infected_client_to_DC						✔
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps						✔
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps						✔
75. 20200701_pitty_tiger_1hr						
76. 20200701_Valak_infection_with_IcedID						✔

77.20201229_Emotet_infection_with_Trickbot_and_spambot_activity		✔				✔
78. 20210105_PurpleFox_EK_and_post_infection_traffic						
79. 20210223_lateral_backup_c2_1hr						
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cobalt_Strike	✔	✔				✔
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	✔	✔				✔
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike	✔	✔				✔
83. 20220101_thru_03_server_activity_with_log4j_attempts					✔	
eternalblue_success_unpatched_win7						
85. LM_psexec_smb_dcerpc_epm_svcctl						
86. LM_smbexec_smb_dcerpc_svcctl_epm						
88. mmcexec						
89. 20211215_thru_20_server_activity_with_log4j_attempts					✔	
90. usecase4_spearphishing_EKC2_lateral_move						
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike	✔	✔				✔

Πίνακας 11. Οι τεχνικές της κατηγορίας Initial Access στο σύνολο των επιθέσεων

Και το γράφημα της Εικόνας 60 οπτικοποιεί τα αποτελέσματα.

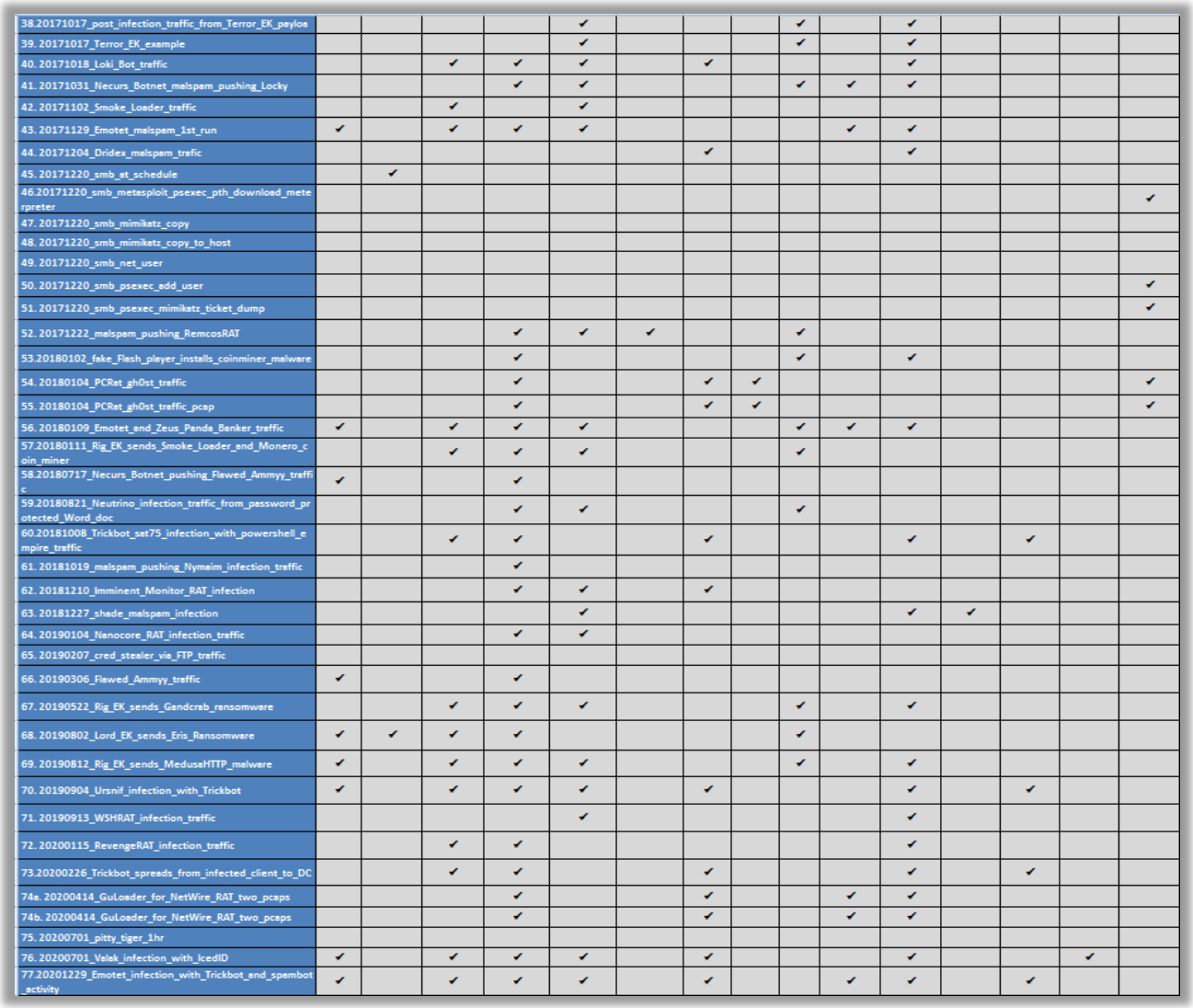


Εικόνα 60. Initial Access techniques

Εδώ είναι ξεκάθαρο πως υπερτερούν οι τεχνικές ***T1566.001:*** *Initial Access/Phishing/**Spearphishing Attachment*** και ***T1566.002:*** *Initial Access/Phishing/**Spearphishing Link***.

Συνεχίζουμε με την κατηγορία Execution του πίνακα MITRE ATT&CK. Οι τεχνικές που καταγράψαμε σε αυτή την τακτική εμφανίζονται στον Πίνακα 12.

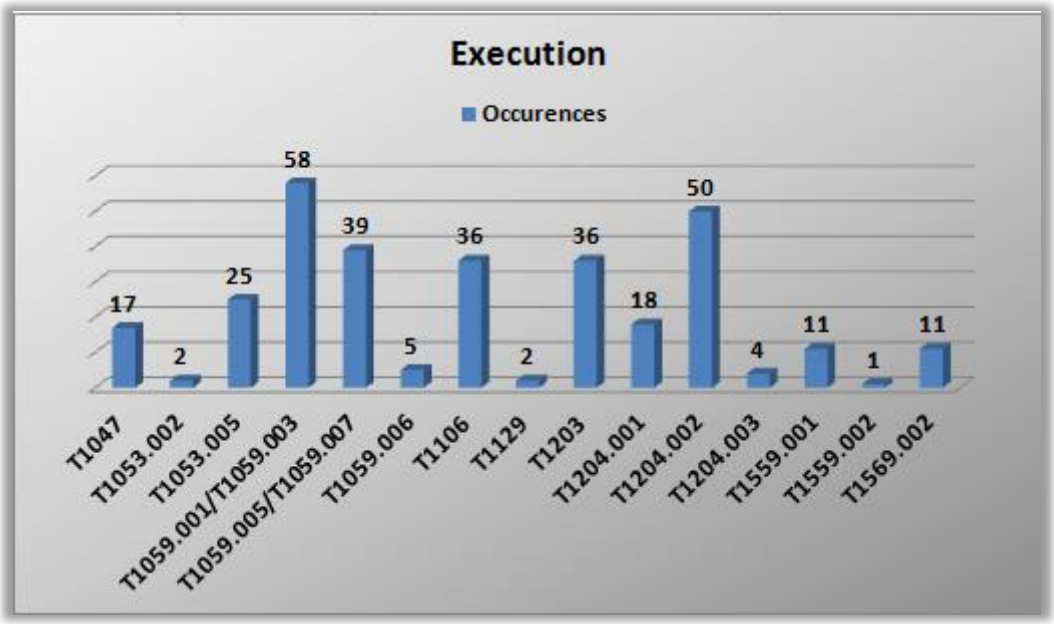
Pcap Name / Mitre Attack Tactic	Execution														
	T1047	T1053.002	T1053.005	T1059.001/ T1059.003	T1059.005/ T1059.007	T1059.006	T1106	T1129	T1203	T1204.001	T1204.002	T1204.003	T1559.001	T1559.002	T1569.002
1. 20161215_ccnotice.net_malspam_traffic											✔				
2. 20161216_Locky_malspam_traffic_example				✔	✔				✔	✔	✔				
3. 20161222_Cerber_from_malspam_traffic											✔				
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware					✔				✔						
5. 20161228_1st_run_Sundown_EK_sends_Chthonic				✔					✔		✔				
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader									✔						
7. 20170201_Hancitor_Pony_malspam_traffic				✔			✔		✔	✔	✔				
8. 20170202_Cerber_from_sdibes.top										✔					
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6											✔				
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6											✔				
11. 20170221_Hancitor_malspam_traffic				✔			✔		✔	✔	✔				
12. 20170221_ZeusPandaBanker_malspam_traffic				✔	✔				✔	✔	✔				
13. 20170302_Nebula_EK_1st_run				✔			✔		✔						
14. 20170302_Nebula_EK_2nd_run				✔			✔		✔						
15. 20170302_Nebula_EK_3rd_run				✔			✔		✔						
16. 20170313_Kovter_Locky_malspam_traffic				✔	✔		✔					✔			
17. 20170314_Kovter_malspam_traffic				✔	✔		✔		✔			✔			
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware			✔	✔	✔				✔						
19. 20170330_Dridex_confirmation_letter_Dridex_traffic							✔				✔				
20. 20170405_Terror_EK_sends_Andromeda_1st_run							✔				✔				
21. 20170405_Terror_EK_sends_Andromeda_2nd_run							✔				✔				
22. 20170421_Locky_malspam_traffic				✔	✔				✔	✔	✔				
23. 20170429_CVE_2017_0199_attempt_from_horsezangd					✔		✔		✔		✔		✔		
24. 20170516_Jaff_ransomware_malspam_traffic					✔				✔		✔				✔
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit	✔			✔			✔			✔	✔				
26. 20170601_ZeusPandaBanker_malspam_traffic				✔	✔				✔		✔				
27. 20170612_Loki_Bot_malspam_traffic			✔	✔	✔		✔				✔				
28. 20170612_Trickbot_malspam_traffic			✔	✔			✔				✔		✔		
29. 20170612_Ursnif_malspam_traffic	✔			✔	✔		✔						✔		
30. 20170710_Kovter_Nemucod_malspam_traffic				✔	✔		✔		✔			✔			
31. 20170724_Trickbot_malspam_traffic			✔	✔			✔				✔		✔		
32. 20170726_Emotet_malspam_traffic	✔		✔	✔	✔					✔	✔				
33. 20170803_Hancitor_malspam_traffic				✔			✔		✔	✔	✔				
34.20170812_Trickbot_infection_from_carriereiserphotography.com			✔	✔			✔				✔		✔		
35. 20170812_Trickbot_infection_from_carriereiter.com.exe			✔	✔			✔				✔		✔		
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu			✔	✔	✔				✔		✔				
37. 20171010_Emotet_malspam_traffic	✔		✔	✔	✔					✔	✔				



38.20171017_post_infection_traffic_from_Terror_EK_payloa					✔				✔		✔				
39. 20171017_Terror_EK_example					✔				✔		✔				
40. 20171018_Loki_Bot_traffic			✔	✔	✔		✔				✔				
41. 20171031_Necurs_Botnet_malspam_pushing_Locky				✔	✔				✔	✔	✔				
42. 20171102_Smoke_Loader_traffic			✔		✔										
43. 20171129_Emotet_malspam_1st_run	✔		✔	✔	✔					✔	✔				
44. 20171204_Dridex_malspam_trafic							✔				✔				
45. 20171220_smb_at_schedule		✔													
46.20171220_smb_metasploit_psexec_pth_download_mete rpreter															✔
47. 20171220_smb_mimikatz_copy															
48. 20171220_smb_mimikatz_copy_to_host															
49. 20171220_smb_net_user															
50. 20171220_smb_psexec_add_user															✔
51. 20171220_smb_psexec_mimikatz_ticket_dump															✔
52. 20171222_malspam_pushing_RemcosRAT				✔	✔	✔			✔						
53.20180102_fake_Flash_player_installs_coinminer_malware				✔					✔		✔				
54. 20180104_PCRat_gh0st_traffic				✔			✔	✔							✔
55. 20180104_PCRat_gh0st_traffic_pcap				✔			✔	✔							✔
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic	✔		✔	✔	✔				✔	✔	✔				
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_c oin_miner			✔	✔	✔				✔						
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffi c	✔			✔											
59.20180821_Neutrino_infection_traffic_from_password_pr otected_Word_doc				✔	✔				✔						
60.20181008_Trickbot_sat75_infection_with_powershell_e mpire_traffic			✔	✔			✔				✔		✔		
61. 20181019_malspam_pushing_Nymaim_infection_traffic				✔											
62. 20181210_Imminent_Monitor_RAT_infection				✔	✔		✔								
63. 20181227_shade_malspam_infection					✔						✔	✔			
64. 20190104_Nanocore_RAT_infection_traffic				✔	✔										
65. 20190207_cred_stealer_via_FTP_traffic															
66. 20190306_Flawed_Ammyy_traffic	✔			✔											
67. 20190522_Rig_EK_sends_Gandcrab_ransomware			✔	✔	✔				✔		✔				
68. 20190802_Lord_EK_sends_Eris_Ransomware	✔	✔	✔	✔					✔						
69. 20190812_Rig_EK_sends_MedusaHTTP_malware	✔		✔	✔	✔				✔		✔				
70. 20190904_Ursnif_infection_with_Trickbot	✔		✔	✔	✔		✔				✔		✔		
71. 20190913_WSHRAT_infection_traffic					✔						✔				
72. 20200115_RevengeRAT_infection_traffic			✔	✔							✔				
73.20200226_Trickbot_spreads_from_infected_client_to_DC			✔	✔			✔				✔		✔		
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps				✔			✔			✔	✔				
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps				✔			✔			✔	✔				
75. 20200701_pitty_tiger_1hr															
76. 20200701_Valak_infection_with_IcedID	✔		✔	✔	✔		✔				✔			✔	
77.20201229_Emotet_infection_with_Trickbot_and_spambot _activity	✔		✔	✔	✔		✔			✔	✔		✔		
78. 20210105_PurpleFox_EK_and_post_infection_traffic				✔											
79. 20210223_lateral_backup_c2_1hr															
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cob alt_Strike	✔			✔	✔	✔	✔		✔	✔	✔				✔
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	✔			✔	✔	✔	✔		✔	✔	✔				✔
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike	✔		✔	✔	✔	✔	✔		✔		✔		✔		✔
83. 20220101_thru_03_server_activity_with_log4j_attempts				✔					✔						
eternalblue_success_unpatched_win7															
85. LM_psexec_smb_dcerpc_epm_svcctl															✔
86. LM_smbexec_smb_dcerpc_svcctl_epm															
88. mmcexec															
89. 20211215_thru_20_server_activity_with_log4j_attempts				✔					✔						
90. usecase4_speerphishing_EKC2_lateral_move															
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike	✔		✔	✔	✔	✔	✔		✔		✔				✔

Πίνακας 12. Οι τεχνικές της κατηγορίας Execution στο σύνολο των επιθέσεων

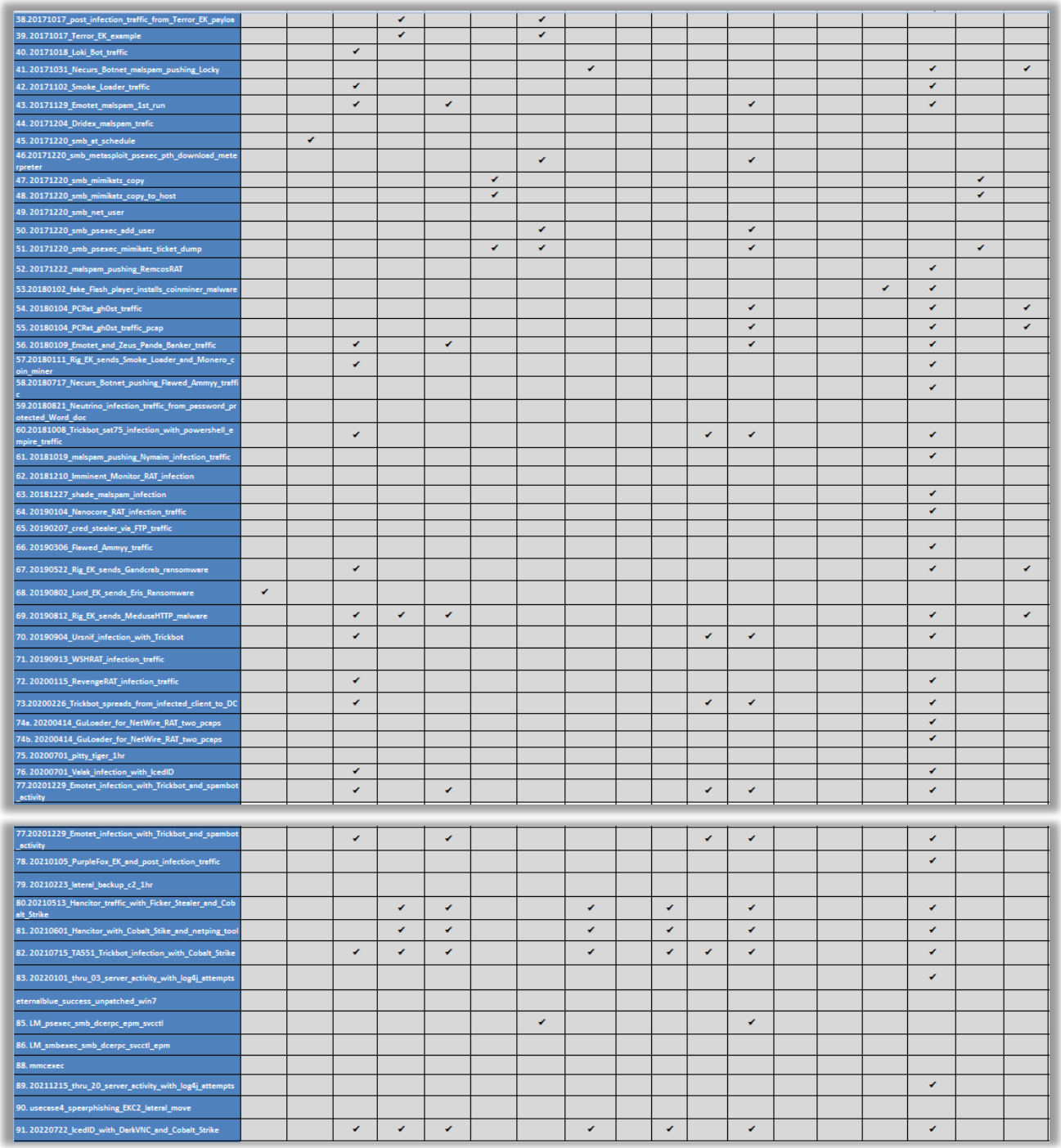
Και τα αποτελέσματα συνοψίζονται στο παρακάτω γράφημα, όπου φαίνεται πως οι επιτιθέμενοι χρησιμοποιούν ως επί το πλείστον *Powershell* και *Windows Command Shell* (***T1059.001:*** *Execution/Command and Scripting Interpreter/**Powershell*** – ***T1059.003:*** *Execution/Command and Scripting Interpreter/**Windows Command Shell***) και βασίζονται στο λάθος των χρηστών για την εκτέλεση του malware (***T1204.002:*** *Execution/User Execution/**Malicious File***) και την έναρξη της αλυσίδας μόλυνσης (infection chain).



Εικόνα 61. Execution techniques

Επόμενη κατηγορία είναι Persistence. Και πάλι τα ευρήματα παρουσιάζονται και συνοψίζονται στο γράφημα.

Pcap Name / Mitre Attack Tactic	Persistence																	
	T1037.001	T1053.002	T1053.005	T1078.002	T1078.003	T1098	T1136.002	T1137.001/ T1137.006	T1176	T1197	T1542.003	T1543.003	T1546.012	T1546.015	T1546.016	T1547.001	T1547.005	T1574.002
1. 20161215_ccnotice.net_malspam_traffic								✔										
2. 20161216_Locky_malspam_traffic_example								✔								✔		✔
3. 20161222_Cerber_from_malspam_traffic								✔										
4.20161226_pseudoDerkleech_Rig_V_sends_Cerber_ransomware									✔									
5. 20161228_1st_run_Sundown_EK_sends_Chthonic																		
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader																		
7. 20170201_Hancitor_Pony_malspam_traffic								✔								✔		
8. 20170202_Cerber_from_adibes.top																		
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6									✔									
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6									✔									
11. 20170221_Hancitor_malspam_traffic								✔								✔		
12. 20170221_ZeusPandaBanker_malspam_traffic																✔		
13. 20170302_Nebula_EK_1st_run												✔				✔		
14. 20170302_Nebula_EK_2nd_run												✔				✔		
15. 20170302_Nebula_EK_3rd_run												✔				✔		
16. 20170313_Kovter_Locky_malspam_traffic			✔															
17. 20170314_Kovter_malspam_traffic													✔			✔		
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware			✔						✔							✔		
19. 20170330_Dridex_confirmation_letter_Dridex_traffic																		
20. 20170405_Terror_EK_sends_Andromeda_1st_run				✔			✔									✔		
21. 20170405_Terror_EK_sends_Andromeda_2nd_run				✔			✔									✔		
22. 20170421_Locky_malspam_traffic								✔								✔		✔
23. 20170429_CVE_2017_0199_attempt_from_horsezangd								✔				✔		✔				
24. 20170516_Jaff_ransomware_malspam_traffic												✔						
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit												✔				✔		
26. 20170601_ZeusPandaBanker_malspam_traffic																✔		
27. 20170612_Loki_Bot_malspam_traffic			✔															
28. 20170612_Trickbot_malspam_traffic			✔								✔	✔				✔		
29. 20170612_Ursnif_malspam_traffic												✔				✔		
30. 20170710_Kovter_Nemucod_malspam_traffic													✔			✔		
31. 20170724_Trickbot_malspam_traffic			✔								✔	✔				✔		
32. 20170726_Emotet_malspam_traffic			✔		✔							✔				✔		
33. 20170803_Hancitor_malspam_traffic								✔								✔		
34.20170812_Trickbot_infection_from_carriereiserphotography.com			✔								✔	✔				✔		
35. 20170812_Trickbot_infection_from_carriereiter.com.exe			✔								✔	✔				✔		
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu			✔													✔		✔
37. 20171010_Emotet_malspam_traffic			✔		✔							✔				✔		

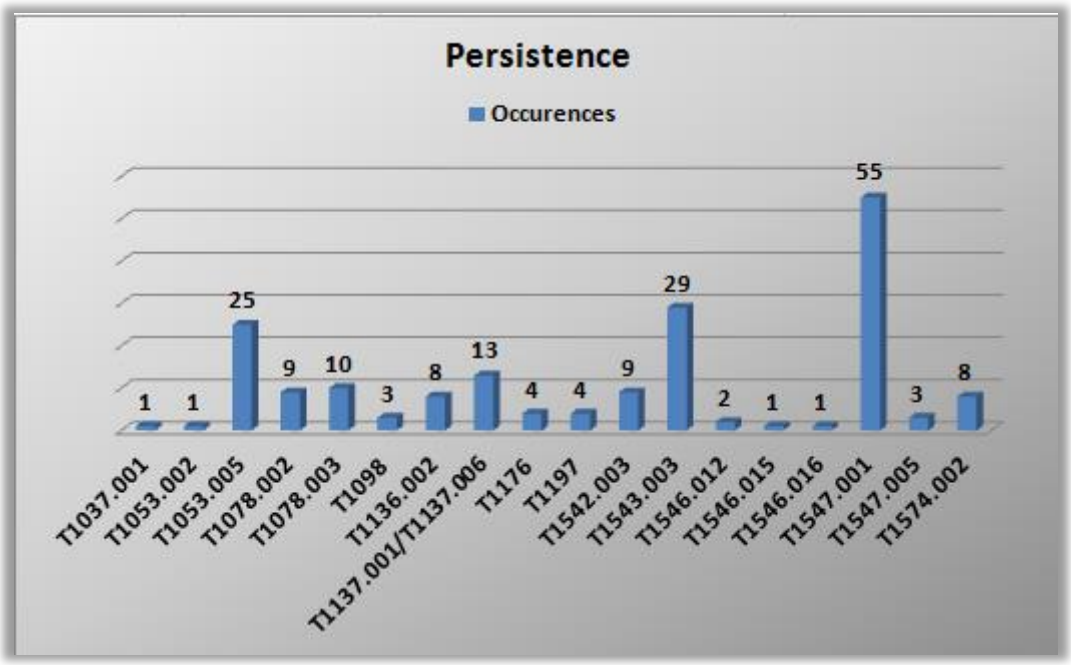


38.20171017_post_infection_traffic_from_Terror_EK_payloa				✔			✔										
39. 20171017_Terror_EK_example				✔			✔										
40. 20171018_Loki_Bot_traffic			✔														
41. 20171031_Necurs_Botnet_malspam_pushing_Locky								✔							✔		✔
42. 20171102_Smoke_Loader_traffic			✔												✔		
43. 20171129_Emotet_malspam_1st_run			✔		✔						✔				✔		
44. 20171204_Dridex_malspam_trafic																	
45. 20171220_smb_at_schedule		✔															
46.20171220_smb_metesploit_psexec_pth_download_mete rpreter							✔				✔						
47. 20171220_smb_mimikatz_copy						✔										✔	
48. 20171220_smb_mimikatz_copy_to_host						✔										✔	
49. 20171220_smb_net_user																	
50. 20171220_smb_psexec_add_user							✔				✔						
51. 20171220_smb_psexec_mimikatz_ticket_dump						✔	✔				✔					✔	
52. 20171222_malspam_pushing_RemcosRAT															✔		
53.20180102_fake_Flash_player_installs_coinminer_malware														✔	✔		
54. 20180104_PCRat_gh0st_traffic											✔				✔		✔
55. 20180104_PCRat_gh0st_traffic_pcap											✔				✔		✔
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic			✔		✔						✔				✔		
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_c oin_miner			✔												✔		
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffi c															✔		
59.20180821_Neutrino_infection_traffic_from_password_pr otected_Word_doc																	
60.20181008_Trickbot_sat75_infection_with_powershell_e mpire_traffic			✔							✔	✔				✔		
61. 20181019_malspam_pushing_Nymaim_infection_traffic															✔		
62. 20181210_Imminent_Monitor_RAT_infection																	
63. 20181227_shade_malspam_infection															✔		
64. 20190104_Nanocore_RAT_infection_traffic															✔		
65. 20190207_cred_stealer_via_FTP_traffic																	
66. 20190306_Flawed_Ammyy_traffic															✔		
67. 20190522_Rig_EK_sends_Gandcrab_ransomware			✔												✔		✔
68. 20190802_Lord_EK_sends_Eris_Ransomware	✔																
69. 20190812_Rig_EK_sends_MeduseHTTP_malware			✔	✔	✔										✔		✔
70. 20190904_Ursnif_infection_with_Trickbot			✔							✔	✔				✔		
71. 20190913_WSHRAT_infection_traffic																	
72. 20200115_RevengeRAT_infection_traffic			✔												✔		
73.20200226_Trickbot_spreads_from_infected_client_to_DC			✔							✔	✔				✔		
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps															✔		
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps															✔		
75. 20200701_pitty_tiger_1hr																	
76. 20200701_Valak_infection_with_IcedID			✔												✔		
77.20201229_Emotet_infection_with_Trickbot_and_spambot _activity			✔		✔					✔	✔				✔		

77.20201229_Emotet_infection_with_Trickbot_and_spambot _activity			✔		✔						✔	✔				✔		
78. 20210105_PurpleFox_EK_and_post_infection_traffic																✔		
79. 20210223_lateral_backup_c2_1hr																		
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cob alt_Strike				✔	✔			✔		✔		✔				✔		
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool				✔	✔			✔		✔		✔				✔		
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike			✔	✔	✔			✔		✔	✔	✔				✔		
83. 20220101_thru_03_server_activity_with_log4j_attempts																✔		
eternalblue_success_unpatched_win7																		
85. LM_psexec_smb_dcerpc_epm_svcctl							✔					✔						
86. LM_smbexec_smb_dcerpc_svcctl_epm																		
88. mmcexec																		
89. 20211215_thru_20_server_activity_with_log4j_attempts																✔		
90. usecase4_spearphishing_EKC2_lateral_move																		
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike			✔	✔	✔			✔		✔		✔				✔		

Πίνακας 13. Οι τεχνικές της κατηγορίας Persistence στο σύνολο των επιθέσεων

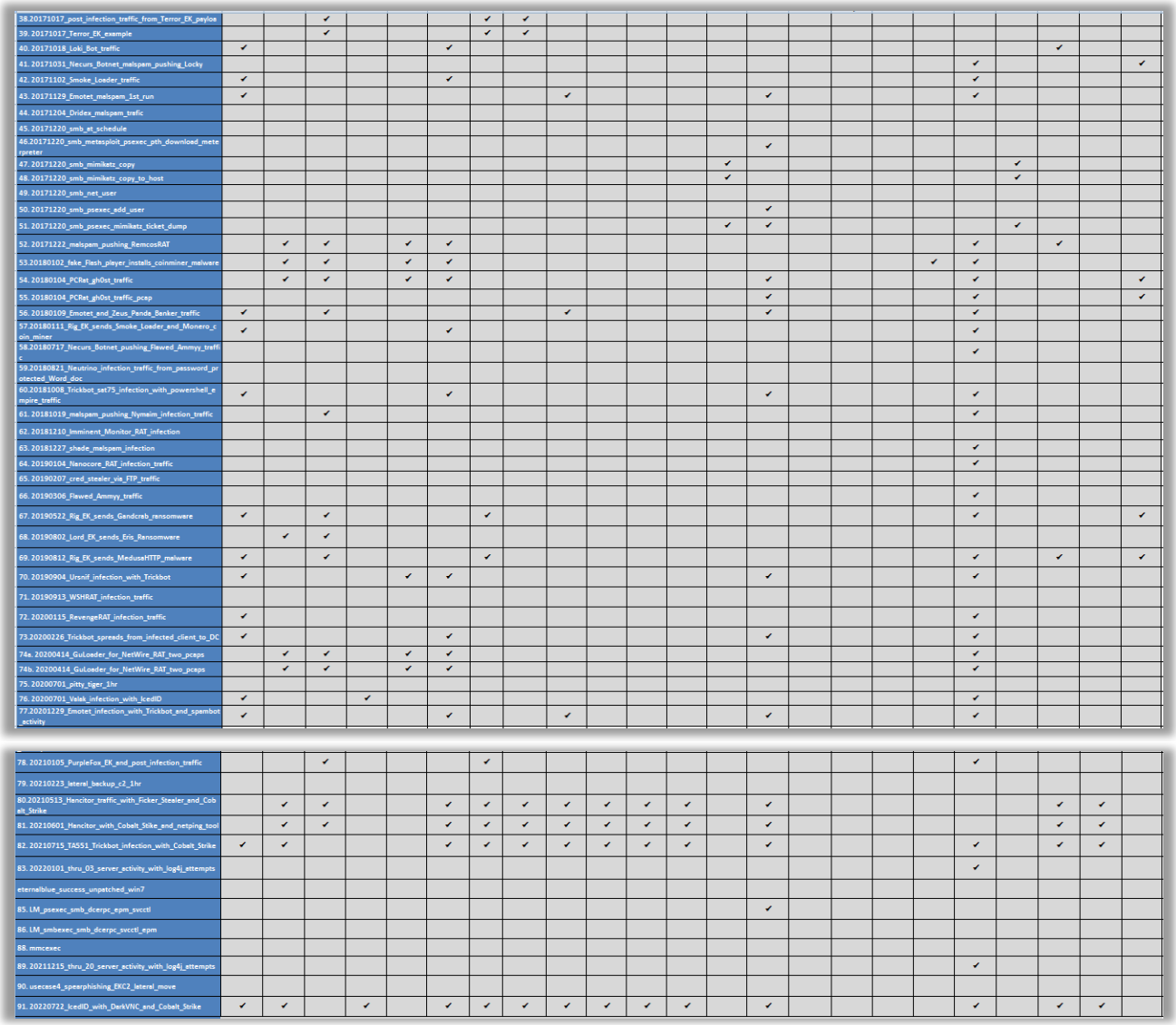
Στην κατηγορία αυτή ξεχώρισε η τεχνική ***T1547.001:*** *Persistence/Boot or Logon Autostart Execution/**Registry Run Keys-Startup Folder***. Η βασική τεχνική για εξασφάλιση persistence (παραμονής στο σύστημα) είναι η δημιουργία registry keys, έτσι ώστε να παραμένουν εντός συστήματος ακόμα και μετά την επανέναρξή του.



Εικόνα 62. Persistence techniques

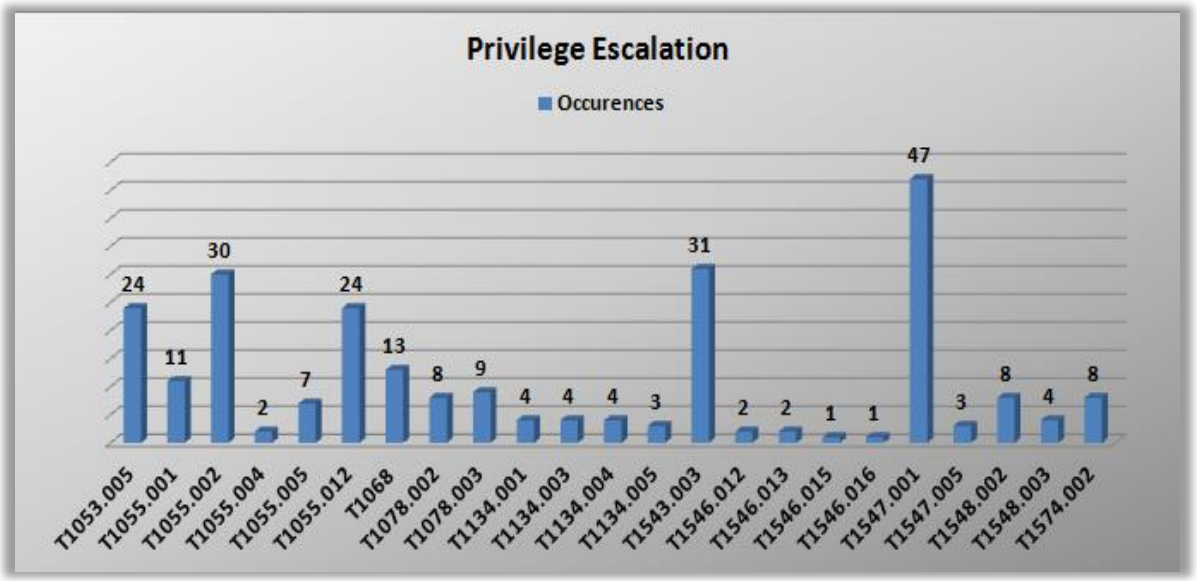
Επόμενη κατηγορία, της οποίας παραθέτουμε τα ευρήματα είναι Privilege Escalation. Οι επιτιθέμενοι, με σκοπό να κλιμακώσουν τα δικαιώματα πρόσβασης που διαθέτουν χρησιμοποιούν τις τεχνικές που παρουσιάζονται στον παρακάτω πίνακα.

Pcap Name / Mitre Attack Tactic	Privilege Escalation																						
	T1053.005	T1055.001	T1055.002	T1055.004	T1055.005	T1055.012	T1068	T1078.002	T1078.003	T1134.001	T1134.003	T1134.004	T1134.005	T1543.003	T1546.012	T1546.013	T1546.015	T1546.016	T1547.001	T1547.005	T1548.002	T1548.003	T1574.002
1. 20161215_ccnotice.net_malspam_traffic			✔																				
2. 20161216_Locky_malspam_traffic_example																			✔				✔
3. 20161222_Cerber_from_malspam_traffic			✔																				
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware																✔							
5. 20161228_1st_run_Sundown_EK_sends_Chthonic																✔							
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader			✔																				
7. 20170201_Hancitor_Pony_malspam_traffic			✔																				
8. 20170202_Cerber_from_edibes.top			✔																				
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6			✔																				
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6			✔																				
11. 20170221_Hancitor_malspam_traffic			✔																				
12. 20170221_ZeusPandaBanker_malspam_traffic			✔																✔				
13. 20170302_Nebula_EK_1st_run														✔									
14. 20170302_Nebula_EK_2nd_run														✔									
15. 20170302_Nebula_EK_3rd_run														✔									
16. 20170313_Kovter_Locky_malspam_traffic			✔			✔																	
17. 20170314_Kovter_malspam_traffic														✔	✔				✔				
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware	✔						✔												✔				
19. 20170330_Dridex_confirmation_letter_Dridex_traffic																							
20. 20170405_Terror_EK_sends_Andromeda_1st_run			✔					✔											✔				
21. 20170405_Terror_EK_sends_Andromeda_2nd_run			✔					✔											✔				
22. 20170421_Locky_malspam_traffic																			✔				✔
23. 20170429_CVE_2017_0199_attempt_from_horsezangd							✔							✔			✔						
24. 20170516_Jaff_ransomware_malspam_traffic						✔								✔									
25.20170518_WanneCry_ransomware_using_EnternalBlue_exploit		✔					✔							✔					✔				
26. 20170601_ZeusPandaBanker_malspam_traffic			✔																✔				
27. 20170612_Loki_Bot_malspam_traffic	✔					✔															✔		
28. 20170612_Trickbot_malspam_traffic	✔					✔								✔					✔				
29. 20170612_Ursnif_malspam_traffic					✔	✔								✔					✔				
30. 20170710_Kovter_Nemucod_malspam_traffic														✔	✔				✔				
31. 20170724_Trickbot_malspam_traffic	✔					✔								✔					✔				
32. 20170726_Emotet_malspam_traffic	✔								✔					✔					✔				
33. 20170803_Hancitor_malspam_traffic			✔																				
34.20170812_Trickbot_infection_from_carriereiserphotography.com	✔					✔								✔					✔				
35. 20170812_Trickbot_infection_from_carriereiter.com.exe	✔					✔								✔					✔				
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu	✔		✔				✔												✔				✔
37. 20171010_Emotet_malspam_traffic	✔								✔					✔					✔				



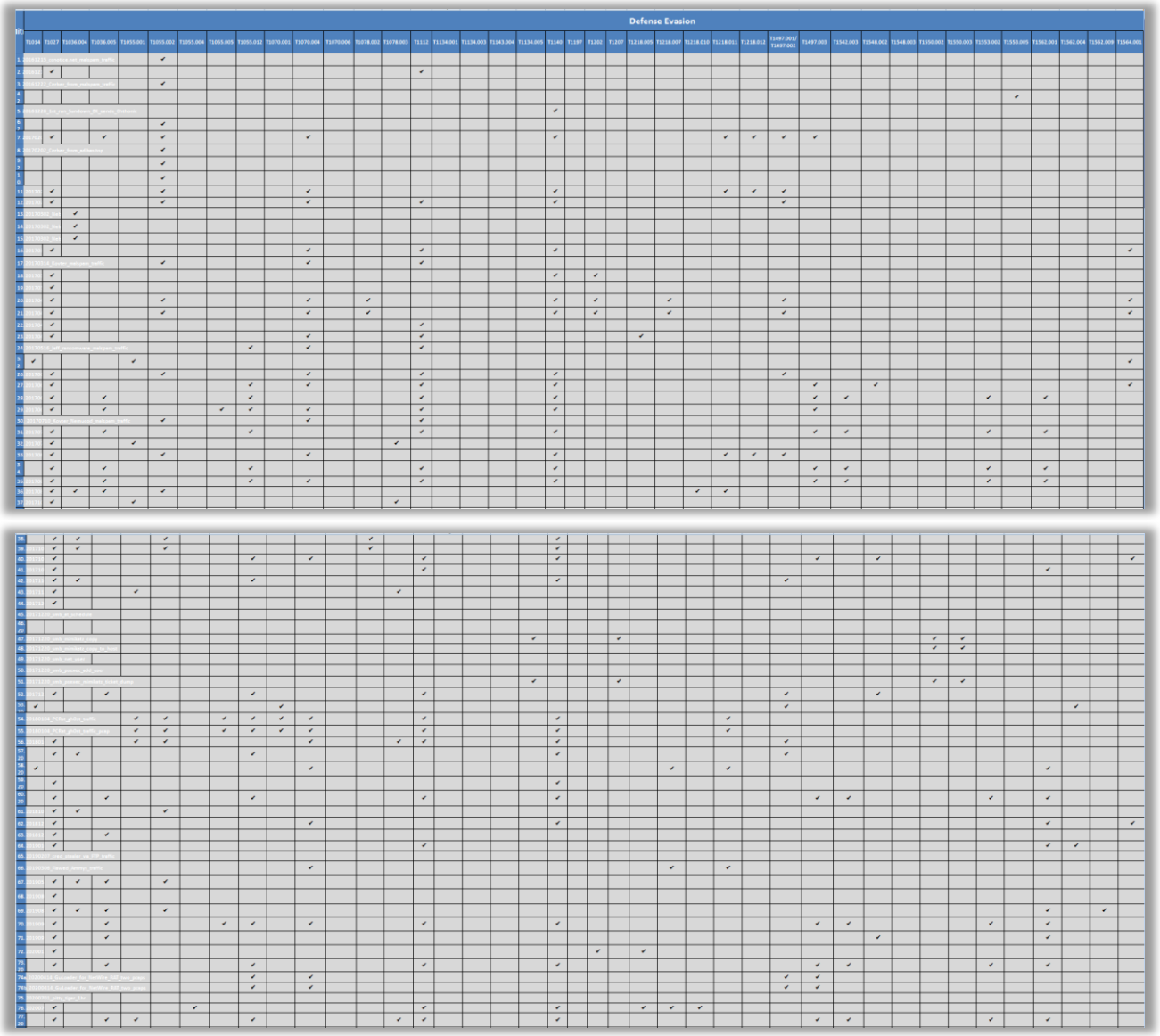
Πίνακας 14. Οι τεχνικές της κατηγορίας Privilege Escalation στο σύνολο των επιθέσεων

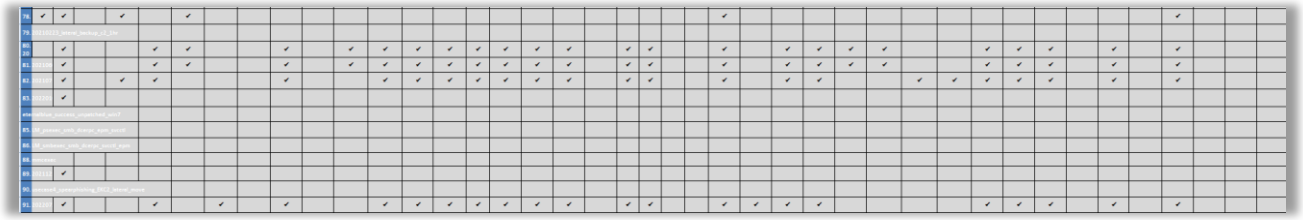
Η «αγαπημένη» τεχνική για Privilege Escalation είναι ***T1547.001:*** *Privilege Escalation/Boot or Logon Autostart Execution/**Registry Run Keys-Startup Folder***, ακολουθούμενη από την ***T1543.003:*** *Privilege Escalation/Create or Modify System Process/**Windows Service***.



Εικόνα 63. Privilege Escalation techniques

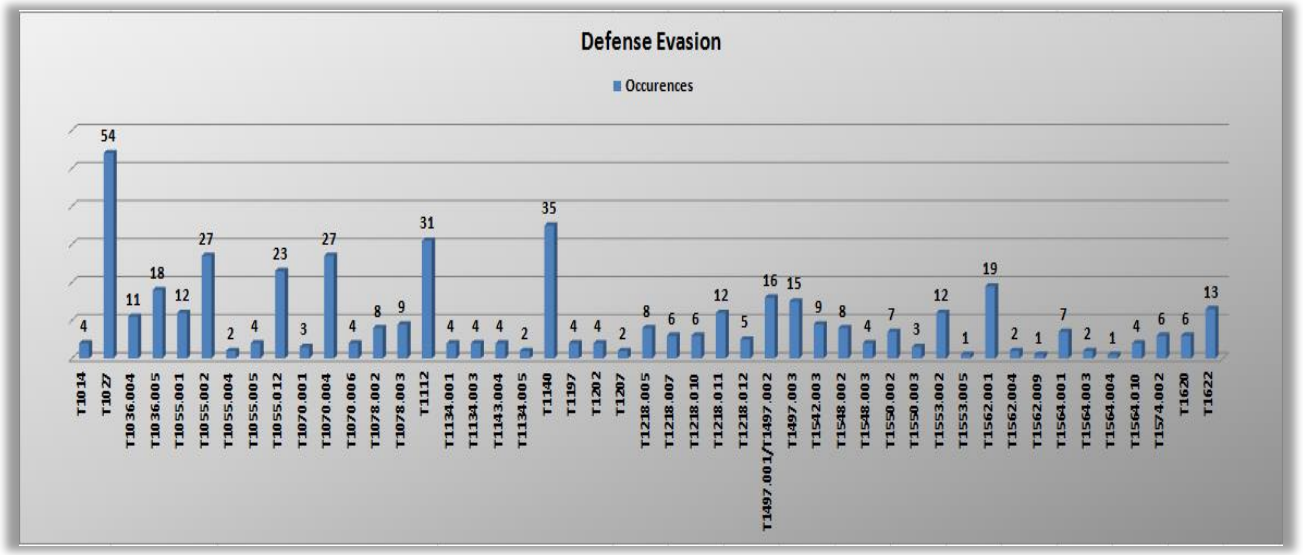
Συνεχίζουμε με τις τεχνικές που συγκαταλέγονται στην τακτική Defense Evasion.





Πίνακας 15. Οι τεχνικές της κατηγορίας Defense Evasion στο σύνολο των επιθέσεων

Οι τεχνικές στην περίπτωση αυτή ήταν περισσότερες από κάθε άλλη κατηγορία. Ωστόσο, ξεχώρισε η ***T1027:*** *Defense Evasion/****Obfuscated Files or Information***.



Εικόνα 64. Defense Evasion techniques

Στον Πίνακα 16 βλέπουμε τις τεχνικές που αφορούν την κατηγορία τακτικών Credential Access.

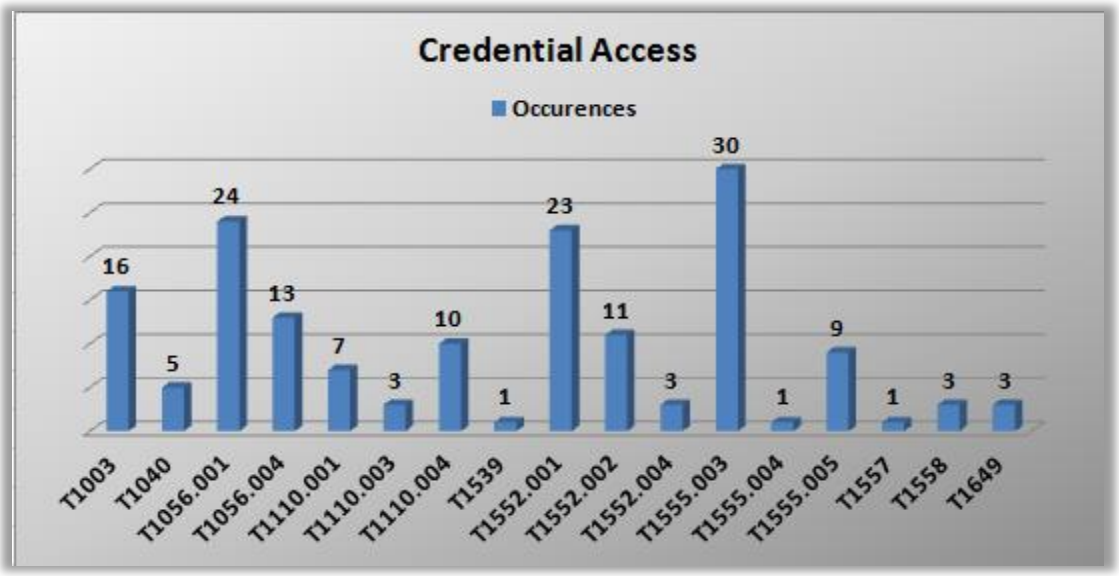
Pcap Name / Mitre Attack Tactic	Credential Access																
	T1003	T1040	T1056.001	T1056.004	T1110.001	T1110.003	T1110.004	T1539	T1552.001	T1552.002	T1552.004	T1555.003	T1555.004	T1555.005	T1557	T1558	T1649
1. 20161215_ccnotice.net_malspam_traffic																	
2. 20161216_Locky_malspam_traffic_example									✔								
3. 20161222_Cerber_from_malspam_traffic																	
4.20161226_pseudoDerkleech_Rig_V_sends_Cerber_ransomware																	
5. 20161228_1st_run_Sundown_EK_sends_Chthonic									✔			✔					
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader								✔				✔					
7. 20170201_Hancitor_Pony_malspam_traffic					✔				✔			✔					
8. 20170202_Cerber_from_edibas.top																	
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6																	
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6																	
11. 20170221_Hancitor_malspam_traffic																	
12. 20170221_ZeusPandaBanker_malspam_traffic			✔	✔													
13. 20170302_Nebula_EK_1st_run			✔														
14. 20170302_Nebula_EK_2nd_run			✔														
15. 20170302_Nebula_EK_3rd_run			✔														
16. 20170313_Kovter_Locky_malspam_traffic			✔									✔					
17. 20170314_Kovter_malspam_traffic																	
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomwere	✔		✔									✔					
19. 20170330_Dridex_confirmation_letter_Dridex_traffic																	
20. 20170405_Terror_EK_sends_Andromeda_1st_run																	
21. 20170405_Terror_EK_sends_Andromeda_2nd_run																	
22. 20170421_Locky_malspam_traffic									✔								
23. 20170429_CVE_2017_0199_attempt_from_horsexangd	✔								✔						✔		
24. 20170516_Jeff_ransomware_malspam_traffic									✔	✔							
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit																	
26. 20170601_ZeusPandaBanker_malspam_traffic			✔	✔													
27. 20170612_Loki_Bot_malspam_traffic			✔									✔					
28. 20170612_Trickbot_malspam_traffic				✔			✔		✔	✔		✔		✔			
29. 20170612_Ursnif_malspam_traffic				✔													
30. 20170710_Kovter_Nemucod_malspam_traffic																	
31. 20170724_Trickbot_malspam_traffic				✔			✔		✔	✔		✔		✔			
32. 20170726_Emotet_malspam_traffic	✔	✔			✔				✔			✔					
33. 20170803_Hancitor_malspam_traffic																	
34.20170812_Trickbot_infection_from_carriereiserphotography.com				✔			✔		✔	✔		✔		✔			
35. 20170812_Trickbot_infection_from_carriereiter.com.exe				✔			✔		✔	✔		✔		✔			
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu																	
37. 20171010_Emotet_malspam_traffic	✔	✔			✔				✔			✔					

38.20171017_post_infection_traffic_from_Terror_EK_payloa																	
39. 20171017_Terror_EK_example																	
40. 20171018_Loki_Bot_traffic			✔									✔					
41. 20171031_Necurs_Botnet_malspam_pushing_Locky									✔								
42. 20171102_Smoke_Loader_traffic									✔			✔					
43. 20171129_Emotet_malspam_1st_run	✔	✔			✔				✔			✔					
44. 20171204_Dridex_malspam_trafic																	
45. 20171220_smb_at_schedule																	
46.20171220_smb_metasploit_psexec_pth_download_mete rpreter																	
47. 20171220_smb_mimikatz_copy	✔										✔	✔				✔	✔
48. 20171220_smb_mimikatz_copy_to_host	✔										✔	✔				✔	✔
49. 20171220_smb_net_user																	
50. 20171220_smb_psexec_add_user																	
51. 20171220_smb_psexec_mimikatz_ticket_dump	✔										✔	✔				✔	✔
52. 20171222_malspam_pushing_RemcosRAT			✔														
53.20180102_fake_Flash_player_installs_coinminer_malware	✔																
54. 20180104_PCRat_gh0st_traffic			✔														
55. 20180104_PCRat_gh0st_traffic_pcap			✔														
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic	✔	✔	✔	✔	✔				✔			✔					
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_c oin_miner									✔			✔					
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffi c			✔														
59.20180821_Neutrino_infection_traffic_from_passsword_pr otected_Word_doc																	
60.20181008_Trickbot_set75_infection_with_powershell_e mpire_traffic				✔			✔		✔	✔		✔		✔			
61. 20181019_malspam_pushing_Nymaim_infection_traffic																	
62. 20181210_Imminent_Monitor_RAT_infection			✔									✔					
63. 20181227_shade_malspam_infection																	
64. 20190104_Nanocore_RAT_infection_traffic			✔														
65. 20190207_cred_stealer_via_FTP_traffic																	
66. 20190306_Flawed_Ammyy_traffic			✔														
67. 20190522_Rig_EK_sends_Gandcrab_ransomware																	
68. 20190802_Lord_EK_sends_Eris_Ransomware																	
69. 20190812_Rig_EK_sends_MeduseHTTP_malware					✔	✔	✔										
70. 20190904_Ursnif_infection_with_Trickbot				✔			✔		✔	✔		✔		✔			
71. 20190913_WSHRAT_infection_traffic												✔					
72. 20200115_RevengeRAT_infection_traffic	✔		✔														
73.20200226_Trickbot_spreads_from_infected_client_to_DC				✔			✔		✔	✔		✔		✔			
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps			✔									✔					
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps			✔									✔					
75. 20200701_pitty_tiger_1hr																	
76. 20200701_Valak_infection_with_IcedID										✔			✔				
77.20201229_Emotet_infection_with_Trickbot_and_spambot _activity	✔	✔		✔	✔		✔		✔	✔		✔		✔			

78. 20210105_PurpleFox_EK_and_post_infection_traffic																	
79. 20210223_lateral_backup_c2_1hr																	
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cob alt_Strike	✔		✔						✔			✔					
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	✔		✔														
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike	✔		✔	✔			✔		✔	✔		✔		✔			
83. 20220101_thru_03_server_activity_with_log4j_attempts						✔											
eternalblue_success_unpatched_win7																	
85. LM_psexec_smb_dcerpc_epm_svcctl																	
86. LM_smbexec_smb_dcerpc_svcctl_epm																	
88. mmcexec																	
89. 20211215_thru_20_server_activity_with_log4j_attempts						✔											
90. usecase4_spearphishing_EKC2_lateral_move																	
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike	✔		✔														

Πίνακας 16. Οι τεχνικές της κατηγορίας Credential Access στο σύνολο των επιθέσεων

Από τα αποτελέσματα προκύπτει πως η συνηθέστερη τεχνική είναι η ***T1555.003:*** *Credential Access/Credentials from Password Stores/****Credentials from Web Browsers*** με 30 εμφανίσεις. Με άλλα λόγια, περίπου μία στις τρεις επιθέσεις προσβάλει τον web browser. Μία επίσης προσφιλής τεχνική είναι η ***T1056.001:*** *Credential Access/****Keylogging***. Χρησιμοποιείται κατά κόρον για κλοπή οικονομικών και προσωπικών δεδομένων από κακόβουλα λογισμικά γνωστά και ως *credential stealers*.



Εικόνα 65. Credential Access techniques

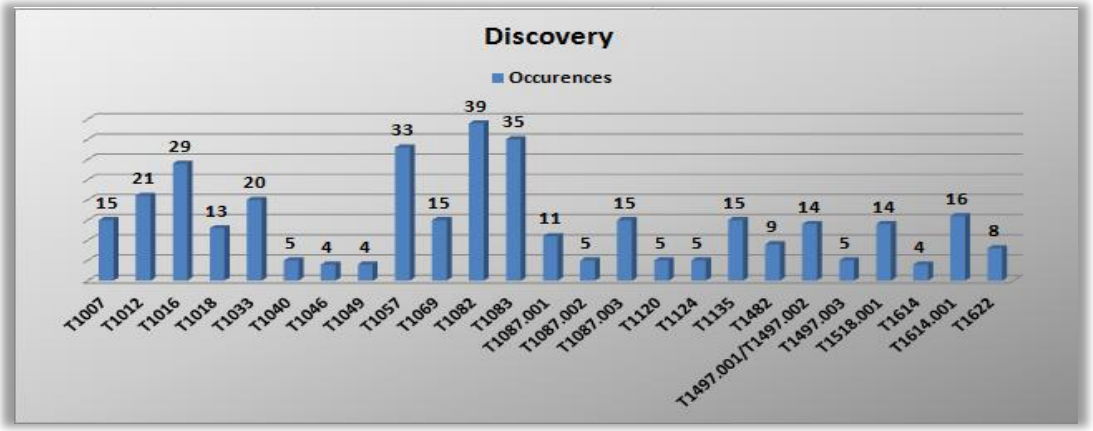
Συνεχίζουμε με τις τεχνικές της κατηγορίας Discovery.

Pcap Name / Mitre Attack Tactic	Discovery																							
	T1007	T1012	T1016	T1018	T1033	T1040	T1046	T1049	T1057	T1069	T1082	T1083	T1087.001	T1087.002	T1087.003	T1120	T1124	T1135	T1482	T1497.001/ T1497.002	T1497.003	T1518.001	T1614	T1614.001	T1622
1. 20161215_ccnotice.net_malspam_traffic																									
2. 20161216_Locky_malspam_traffic_example																									
3. 20161222_Cerber_from_malspam_traffic																									
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware																									
5. 20161228_1st_run_Sundown_EK_sends_Chthonic																									
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader																									
7. 20170201_Hancitor_Pony_malspam_traffic			✔								✔		✔							✔	✔				
8. 20170202_Cerber_from_adibes.top																									
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6																									
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6																									
11. 20170221_Hancitor_malspam_traffic			✔																	✔					
12. 20170221_ZeusPandaBanker_malspam_traffic		✔							✔		✔	✔										✔		✔	
13. 20170302_Nebula_EK_1st_run											✔	✔												✔	
14. 20170302_Nebula_EK_2nd_run											✔	✔												✔	
15. 20170302_Nebula_EK_3rd_run											✔	✔												✔	
16. 20170313_Kovter_Locky_malspam_traffic			✔								✔	✔													
17. 20170314_Kovter_malspam_traffic		✔							✔		✔														
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware			✔		✔						✔														
19. 20170330_Dridex_confirmation_letter_Dridex_traffic											✔											✔			
20. 20170405_Terror_EK_sends_Andromeda_1st_run			✔		✔						✔	✔					✔							✔	✔
21. 20170405_Terror_EK_sends_Andromeda_2nd_run			✔		✔						✔	✔					✔							✔	✔
22. 20170421_Locky_malspam_traffic			✔								✔	✔						✔						✔	
23. 20170429_CVE_2017_0199_attempt_from_horsezangd		✔			✔				✔		✔	✔													
24. 20170516_Jaff_ransomware_malspam_traffic	✔	✔			✔				✔			✔												✔	
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit			✔	✔								✔				✔									
26. 20170601_ZeusPandaBanker_malspam_traffic		✔							✔		✔	✔					✔					✔		✔	
27. 20170612_Loki_Bot_malspam_traffic			✔		✔						✔	✔													
28. 20170612_Trickbot_malspam_traffic	✔		✔	✔	✔				✔	✔	✔	✔	✔		✔			✔	✔						
29. 20170612_Ursnif_malspam_traffic	✔	✔							✔		✔										✔				
30. 20170710_Kovter_Nemucod_malspam_traffic		✔							✔		✔														
31. 20170724_Trickbot_malspam_traffic	✔		✔	✔	✔				✔	✔	✔	✔	✔		✔			✔	✔						
32. 20170726_Emotet_malspam_traffic						✔			✔						✔										
33. 20170803_Hancitor_malspam_traffic			✔																	✔					
34.20170812_Trickbot_infection_from_carriereiserphotography.com	✔		✔	✔	✔				✔	✔	✔	✔	✔		✔			✔	✔						
35. 20170812_Trickbot_infection_from_carriereiter.com.exe	✔		✔	✔	✔				✔	✔	✔	✔	✔		✔			✔	✔						
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu		✔							✔									✔		✔					✔
37. 20171010_Emotet_malspam_traffic						✔			✔						✔										

38.20171017_post_infection_traffic_from_Terror_EK_payloa																							
39. 20171017_Terror_EK_example																							
40. 20171018_Loki_Bot_treffic			✔		✔					✔	✔												
41. 20171031_Necurs_Botnet_malspam_pushing_Locky			✔																				
42. 20171102_Smoke_Loader_traffic											✔							✔				✔	
43. 20171129_Emotet_malspam_1st_run						✔		✔						✔									
44. 20171204_Dridex_malspam_trafic										✔										✔			
45. 20171220_smb_at_schedule																							
46.20171220_smb_metasploit_psexec_pth_download_mete rpreter																							
47. 20171220_smb_mimikatz_copy																							
48. 20171220_smb_mimikatz_copy_to_host																							
49. 20171220_smb_net_user																							
50. 20171220_smb_psexec_add_user																							
51. 20171220_smb_psexec_mimikatz_ticket_dump																							
52. 20171222_malspam_pushing_RemcosRAT											✔							✔					
53.20180102_fake_Flash_player_installs_coinminer_malware										✔	✔							✔		✔			
54. 20180104_PCRat_gh0st_traffic		✔						✔		✔													
55. 20180104_PCRat_gh0st_traffic_pcap		✔						✔		✔													
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic		✔				✔		✔		✔	✔			✔		✔				✔		✔	
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_c oin_miner	✔										✔							✔				✔	
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffi c					✔				✔	✔				✔						✔			
59.20180821_Neutrino_infection_traffic_from_password_pr otected_Word_doc			✔																		✔		
60.20181008_Trickbot_sat75_infection_with_powershell_e mpire_traffic	✔		✔	✔	✔			✔	✔	✔	✔	✔		✔			✔	✔					
61. 20181019_malspam_pushing_Nymaim_infection_traffic								✔												✔		✔	✔
62. 20181210_Imminent_Monitor_RAT_infection								✔			✔												
63. 20181227_shade_malspam_infection																							
64. 20190104_Nanocore_RAT_infection_treffic			✔																				
65. 20190207_cred_stealer_via_FTP_traffic																							
66. 20190306_Flawed_Ammyy_traffic					✔				✔	✔				✔						✔			
67. 20190522_Rig_EK_sends_Gandcrab_ransomware		✔						✔		✔								✔			✔	✔	✔
68. 20190802_Lord_EK_sends_Eris_Ransomware			✔							✔											✔	✔	
69. 20190812_Rig_EK_sends_MedusaHTTP_malware		✔						✔			✔					✔		✔					✔
70. 20190904_Ursnif_infection_with_Trickbot	✔	✔	✔	✔	✔			✔	✔	✔	✔	✔		✔			✔	✔		✔			
71. 20190913_WSHRAT_infection_treffic								✔															
72. 20200115_RevengeRAT_infection_traffic			✔		✔					✔													
73.20200226_Trickbot_spreads_from_infected_client_to_DC	✔		✔	✔	✔			✔	✔	✔	✔	✔		✔			✔	✔					
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps		✔						✔			✔			✔					✔	✔			✔
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps		✔									✔			✔					✔	✔			✔
75. 20200701_pitty_tiger_1hr																							
76. 20200701_Valak_infection_with_IcedID		✔	✔		✔			✔	✔	✔		✔	✔							✔			
77.20201229_Emotet_infection_with_Trickbot_and_spambot _activity	✔		✔	✔	✔	✔		✔	✔	✔	✔	✔		✔			✔	✔					

78. 20210105_PurpleFox_EK_and_post_infection_treffic																							
79. 20210223_lateral_backup_c2_1hr																							
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cob alt_Strike	✔	✔	✔	✔			✔	✔	✔	✔	✔	✔		✔			✔	✔		✔		✔	✔	
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	✔	✔	✔	✔			✔	✔	✔	✔		✔		✔				✔		✔		✔		
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔			✔		
83. 20220101_thru_03_server_activity_with_log4j_attempts																✔								
eternalblue_success_unpatched_win7																								
85. LM_psexec_smb_dcerpc_epm_svcctl																								
86. LM_smbexec_smb_dcerpc_svcctl_epm																								
88. mmcexec																								
89. 20211215_thru_20_server_activity_with_log4j_attempts																✔								
90. usecase4_spearphishing_EKC2_lateral_move																								
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike	✔	✔	✔	✔			✔	✔	✔	✔	✔	✔		✔				✔				✔		

Πίνακας 17. Οι τεχνικές της κατηγορίας Discovery στο σύνολο των επιθέσεων



Εικόνα 66. Discovery techniques

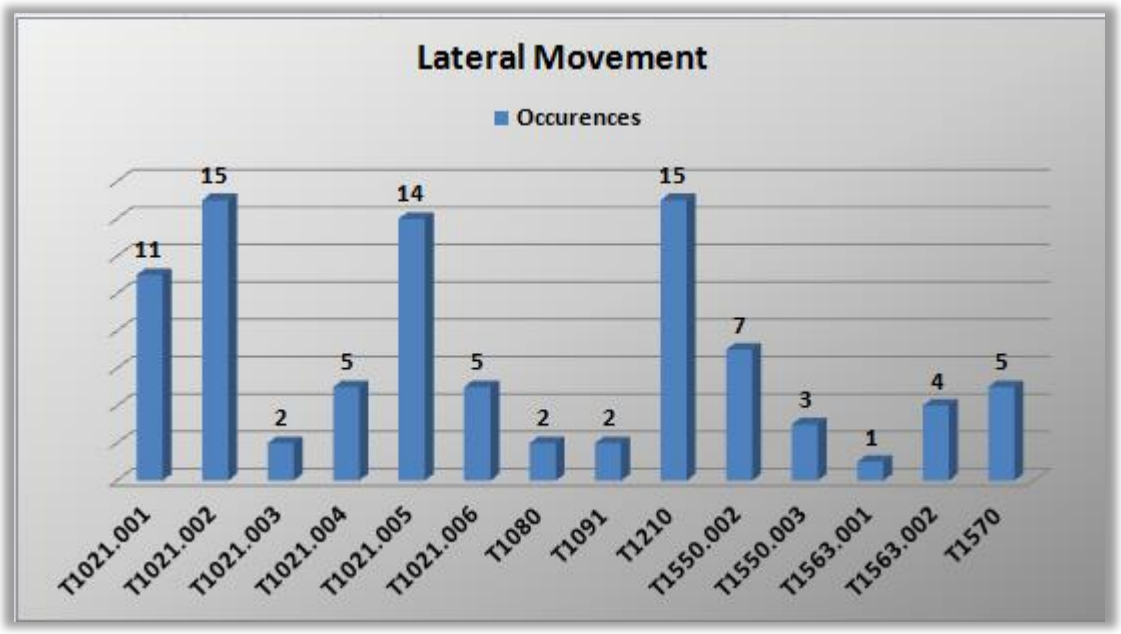
Στην περίπτωση αυτή ξεχώρισαν οι ***T1082***: *Discovery/**System Information Discovery*** και ***T1083:*** *Discovery/**File and Directory Discovery*** με 39 και 35 παρουσίες στα log files αντίστοιχα. Ακολουθεί η κατηγορία Lateral Movement και οι τεχνικές που χρησιμοποιούνται στον Πίνακα 18.

Pcap Name / Mitre Attack Tactic	Lateral Movement													
	T1021.001	T1021.002	T1021.003	T1021.004	T1021.005	T1021.006	T1080	T1091	T1210	T1550.002	T1550.003	T1563.001	T1563.002	T1570
1. 20161215_ccnotice.net_malspam_traffic														
2. 20161216_Locky_malspam_traffic_example														
3. 20161222_Cerber_from_malspam_traffic														
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware														
5. 20161228_1st_run_Sundown_EK_sends_Chthonic														
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader														
7. 20170201_Hancitor_Pony_malspam_traffic														
8. 20170202_Cerber_from_adibas.top														
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6														
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6														
11. 20170221_Hancitor_malspam_traffic														
12. 20170221_ZeusPandaBanker_malspam_traffic					✔									
13. 20170302_Nebula_EK_1st_run														
14. 20170302_Nebula_EK_2nd_run														
15. 20170302_Nebula_EK_3rd_run														
16. 20170313_Kovter_Locky_malspam_traffic														
17. 20170314_Kovter_malspam_traffic														
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware	✔													
19. 20170330_Dridex_confirmation_letter_Dridex_traffic														
20. 20170405_Terror_EK_sends_Andromeda_1st_run														
21. 20170405_Terror_EK_sends_Andromeda_2nd_run														
22. 20170421_Locky_malspam_traffic														
23. 20170429_CVE_2017_0199_attempt_from_horsezangd									✔			✔		
24. 20170516_Jeff_ransomware_malspam_traffic														
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit									✔				✔	✔
26. 20170601_ZeusPandaBanker_malspam_traffic					✔									
27. 20170612_Loki_Bot_malspam_traffic														
28. 20170612_Trickbot_malspam_traffic					✔				✔					
29. 20170612_Ursnif_malspam_traffic							✔	✔						
30. 20170710_Kovter_Nemucod_malspam_traffic														
31. 20170724_Trickbot_malspam_traffic					✔				✔					
32. 20170726_Emotet_malspam_traffic		✔							✔					
33. 20170803_Hancitor_malspam_traffic														
34.20170812_Trickbot_infection_from_carriereiserphotography.com					✔				✔					
35. 20170812_Trickbot_infection_from_carriereiter.com.exe					✔				✔					
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu	✔												✔	
37. 20171010_Emotet_malspam_traffic		✔							✔					

38.20171017_post_infection_traffic_from_Terror_EK_payloe														
39. 20171017_Terror_EK_example														
40. 20171018_Loki_Bot_traffic														
41. 20171031_Necurs_Botnet_malspam_pushing_Locky														
42. 20171102_Smoke_Loader_traffic														
43. 20171129_Emotet_malspam_1st_run		✔							✔					
44. 20171204_Dridex_malspam_trafic														
45. 20171220_smb_at_schedule														
46.20171220_smb_metasploit_psexec_pth_download_meterpreter		✔												✔
47. 20171220_smb_mimikatz_copy										✔	✔			
48. 20171220_smb_mimikatz_copy_to_host										✔	✔			
49. 20171220_smb_net_user														
50. 20171220_smb_psexec_add_user		✔												✔
51. 20171220_smb_psexec_mimikatz_ticket_dump		✔								✔	✔			✔
52. 20171222_malspam_pushing_RemcosRAT														
53.20180102_fake_Flash_player_installs_coinminer_malware	✔	✔												
54. 20180104_PCRat_gh0st_traffic														
55. 20180104_PCRat_gh0st_traffic_pcap														
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic		✔			✔				✔					
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_coin_miner														
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffic														
59.20180821_Neutrino_infection_traffic_from_password_protected_Word_doc														
60.20181008_Trickbot_sat75_infection_with_powershell_empire_traffic					✔				✔					
61. 20181019_malspam_pushing_Nymaim_infection_traffic														
62. 20181210_Imminent_Monitor_RAT_infection	✔													
63. 20181227_shade_malspam_infection														
64. 20190104_Nanocore_RAT_infection_traffic														
65. 20190207_cred_stealer_via_FTP_traffic														
66. 20190306_Flawed_Ammyy_traffic														
67. 20190522_Rig_EK_sends_Gandcrab_ransomware	✔												✔	
68. 20190802_Lord_EK_sends_Eris_Ransomware														
69. 20190812_Rig_EK_sends_MedusaHTTP_malware	✔	✔	✔	✔	✔	✔							✔	
70. 20190904_Ursnif_infection_with_Trickbot					✔		✔	✔	✔					
71. 20190913_WSHRAT_infection_traffic														
72. 20200115_RevengeRAT_infection_traffic	✔													
73.20200226_Trickbot_spreads_from_infected_client_to_DC					✔				✔					
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps														
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps														
75. 20200701_pitty_tiger_1hr														
76. 20200701_Valak_infection_with_IcedID														
77.20201229_Emotet_infection_with_Trickbot_and_spambot_activity		✔			✔				✔					

78. 20210105_PurpleFox_EK_and_post_infection_traffic														
79. 20210223_lateral_backup_c2_1hr														
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cobalt_Strike	✔	✔		✔		✔				✔				
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	✔	✔		✔		✔				✔				
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike	✔	✔		✔	✔	✔			✔	✔				
83. 20220101_thru_03_server_activity_with_log4j_attempts														
eternalblue_success_unpatched_win7														
85. LM_psexec_smb_dcerpc_epm_svcctl		✔												✔
86. LM_smbexec_smb_dcerpc_svcctl_epm														
88. mmcexec														
89. 20211215_thru_20_server_activity_with_log4j_attempts														
90. usecase4_spearphishing_EKC2_lateral_move														
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike	✔	✔	✔	✔	✔	✔				✔				

Πίνακας 18. Οι τεχνικές της κατηγορίας Lateral Movement στο σύνολο των επιθέσεων



Εικόνα 67. Lateral Movement techniques

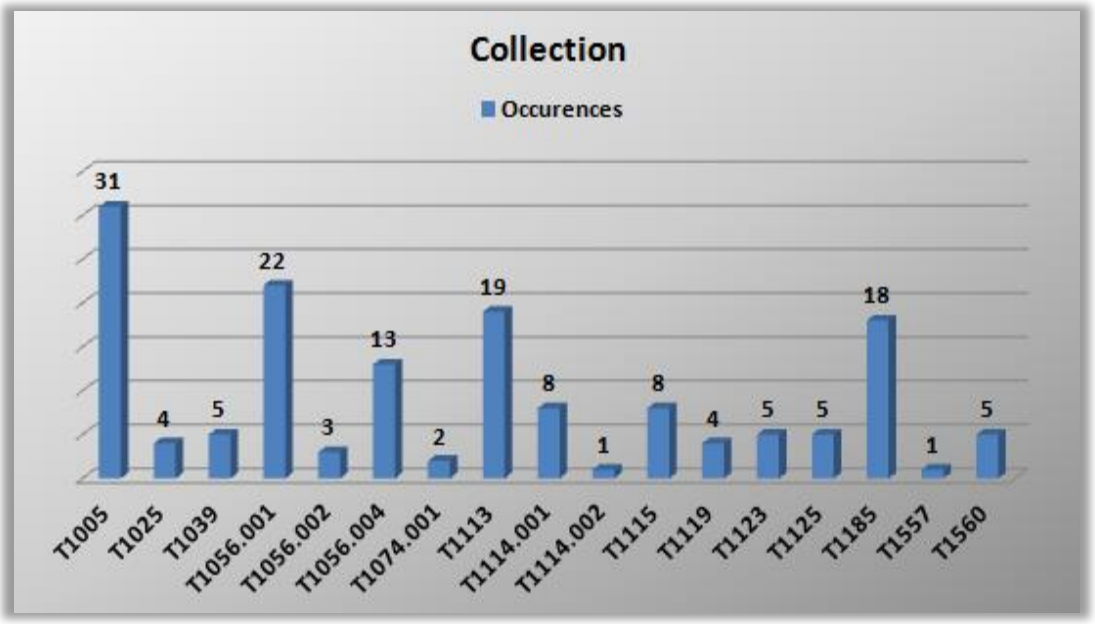
Στην περίπτωση αυτή παρατηρήθηκε ισοψηφία ανάμεσα στην ***T1021.002:*** *Lateral Movement/Remote Services/**SMB-Windows Admin Shares*** και την ***T1210:*** *Lateral Movement/**Exploitation of Remote Services*** με 15 εμφανίσεις. Ακολουθεί η κατηγορία Collection.

Pcap Name / Mitre Attack Tactic	Collection															
	T1005	T1025	T1039	T1056.001	T1056.002	T1056.004	T1074.001	T1113	T1114.001	T1114.002	T1115	T1119	T1123	T1125	T1185	T1557	T1560
1. 20161215_ccnotice.net_malspam_traffic																	
2. 20161216_Locky_malspam_traffic_example	✔	✔	✔														
3. 20161222_Cerber_from_malspam_traffic																	
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware																	
5. 20161228_1st_run_Sundown_EK_sends_Chthonic												✔					
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader															✔		
7. 20170201_Hancitor_Pony_malspam_traffic																	
8. 20170202_Cerber_from_edibas.top																	
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6																	
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6																	
11. 20170221_Hancitor_malspam_traffic																	
12. 20170221_ZeusPandaBanker_malspam_traffic				✔	✔	✔		✔			✔						
13. 20170302_Nebula_EK_1st_run	✔																
14. 20170302_Nebula_EK_2nd_run	✔																
15. 20170302_Nebula_EK_3rd_run	✔																
16. 20170313_Kovter_Locky_malspam_traffic																	
17. 20170314_Kovter_malspam_traffic																	
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware				✔				✔					✔	✔			
19. 20170330_Dridex_confirmation_letter_Dridex_traffic															✔		
20. 20170405_Terror_EK_sends_Andromeda_1st_run	✔																
21. 20170405_Terror_EK_sends_Andromeda_2nd_run	✔																
22. 20170421_Locky_malspam_traffic	✔	✔	✔														
23. 20170429_CVE_2017_0199_attempt_from_horsezangd	✔			✔								✔				✔	
24. 20170516_Jaff_ransomware_malspam_traffic	✔											✔					
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit																	
26. 20170601_ZeusPandaBanker_malspam_traffic				✔	✔	✔		✔			✔						
27. 20170612_Loki_Bot_malspam_traffic				✔													
28. 20170612_Trickbot_malspam_traffic	✔					✔									✔		
29. 20170612_Ursnif_malspam_traffic	✔					✔	✔	✔							✔		
30. 20170710_Kovter_Nemucod_malspam_traffic																	
31. 20170724_Trickbot_malspam_traffic	✔					✔									✔		
32. 20170726_Emotet_malspam_traffic									✔								✔
33. 20170803_Hancitor_malspam_traffic																	
34.20170812_Trickbot_infection_from_carriereiserphotography.com	✔					✔									✔		
35. 20170812_Trickbot_infection_from_carriereiter.com.exe	✔					✔									✔		
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu			✔														
37. 20171010_Emotet_malspam_traffic									✔								✔

38.20171017_post_infection_traffic_from_Terror_EK_payloa	✔															
39. 20171017_Terror_EK_example	✔															
40. 20171018_Loki_Bot_traffic				✔												
41. 20171031_Necurs_Botnet_malspam_pushing_Locky	✔	✔	✔													
42. 20171102_Smoke_Loader_traffic									✔							
43. 20171129_Emotet_malspam_1st_run	✔								✔							✔
44. 20171204_Dridex_malspam_trafic														✔		
45. 20171220_smb_at_schedule																
46.20171220_smb_metasploit_psexec_pth_download_meterpreter																
47. 20171220_smb_mimikatz_copy																
48. 20171220_smb_mimikatz_copy_to_host																
49. 20171220_smb_net_user																
50. 20171220_smb_psexec_add_user																
51. 20171220_smb_psexec_mimikatz_ticket_dump																
52. 20171222_malspam_pushing_RemcosRAT	✔			✔				✔			✔		✔	✔		
53.20180102_fake_Flash_player_installs_coinminer_malware	✔	✔	✔													
54. 20180104_PCRat_gh0st_traffic				✔				✔								
55. 20180104_PCRat_gh0st_traffic_pcap				✔				✔								
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic	✔			✔	✔	✔		✔	✔		✔					✔
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_coin_miner									✔							
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffic	✔			✔				✔			✔					
59.20180821_Neutrino_infection_traffic_from_password_protected_Word_doc								✔								
60.20181008_Trickbot_sat75_infection_with_powershell_empire_traffic	✔					✔								✔		
61. 20181019_malspam_pushing_Nymaim_infection_traffic																
62. 20181210_Imminent_Monitor_RAT_infection				✔									✔	✔		
63. 20181227_shade_malspam_infection																
64. 20190104_Nanocore_RAT_infection_traffic				✔									✔	✔		
65. 20190207_cred_stealer_via_FTP_traffic																
66. 20190306_Flawed_Ammyy_traffic	✔			✔				✔			✔					
67. 20190522_Rig_EK_sends_Gandcrab_ransomware																
68. 20190802_Lord_EK_sends_Eris_Ransomware														✔		
69. 20190812_Rig_EK_sends_MeduseHTTP_malware																
70. 20190904_Ursnif_infection_with_Trickbot	✔					✔	✔	✔						✔		
71. 20190913_WSHRAT_infection_traffic				✔				✔	✔							
72. 20200115_RevengeRAT_infection_traffic				✔				✔					✔	✔		
73.20200226_Trickbot_spreads_from_infected_client_to_DC	✔					✔								✔		
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps				✔							✔					
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps				✔							✔					
75. 20200701_pitty_tiger_1hr																
76. 20200701_Valak_infection_with_IcedID								✔		✔		✔		✔		
77.20201229_Emotet_infection_with_Trickbot_and_spambot_activity	✔					✔			✔					✔		✔
78. 20210105_PurpleFox_EK_and_post_infection_traffic																
79. 20210223_lateral_backup_c2_1hr																
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cobalt_Strike	✔			✔				✔						✔		
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	✔			✔				✔						✔		
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike	✔			✔		✔		✔						✔		
83. 20220101_thru_03_server_activity_with_log4j_attempts																
eternalblue_success_unpatched_win7																
85. LM_psexec_smb_dcerpc_epm_svcctl																
86. LM_smbexec_smb_dcerpc_svcctl_epm																
88. mmcexec																
89. 20211215_thru_20_server_activity_with_log4j_attempts																
90. usecase4_spearphishing_EKC2_lateral_move																
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike	✔			✔				✔						✔		

Πίνακας 19. Οι τεχνικές της κατηγορίας Collection στο σύνολο των επιθέσεων

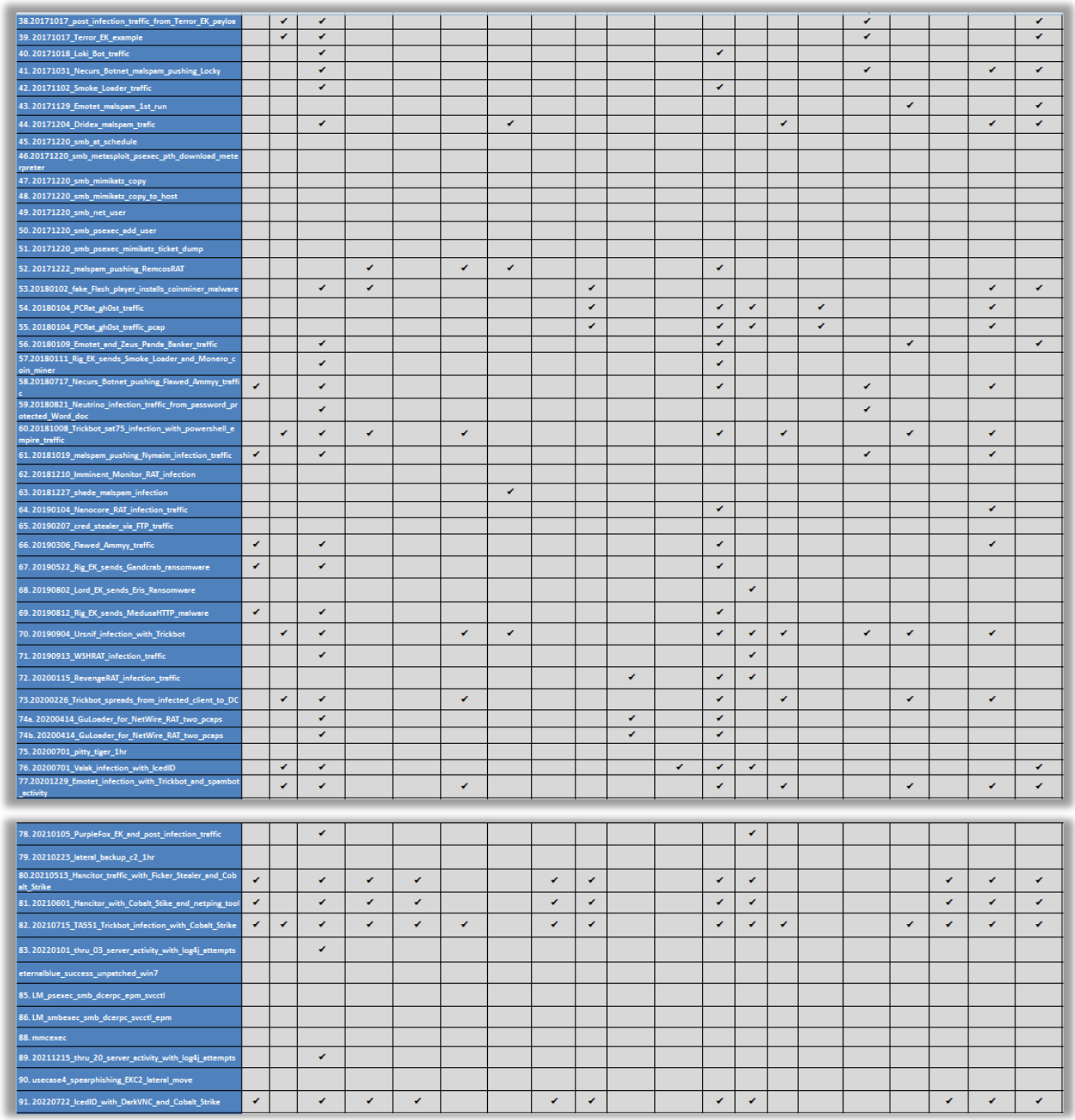
Τα αποτελέσματα συνοπτικά στο γράφημα της Εικόνας 18.



Εικόνα 68. Collection techniques

Την ***T1005:*** *Collection/**Data from Local System*** προτιμούν στις επιθέσεις τους για συλλογή δεδομένων. Τα δεδομένα του συστήματος είναι τα πρώτα που κινδυνεύουν. Ποιες είναι όμως οι προτιμήσεις τους σχετικά με την κατηγορία Command and Control; Αυτό φαίνεται στον πίνακα και στο γράφημα που έπονται.

Pcap Name / Mitre Attack Tactic	Command and Control																			
	T1001	T1008	T1071.001	T1071.004	T1090.001	T1090.002	T1090.003	T1090.004	T1095	T1102.002	T1104	T1105	T1132	T1219	T1568.001	T1568.002	T1571	T1572	T1573.001	T1573.002
1. 20161215_ccnotice.net_malspam_traffic																				
2. 20161216_Locky_malspam_traffic_example			✔													✔			✔	✔
3. 20161222_Cerber_from_malspam_traffic																				
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware																				
5. 20161228_1st_run_Sundown_EK_sends_Chthonic																				
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader																				
7. 20170201_Hancitor_Pony_malspam_traffic			✔									✔								
8. 20170202_Cerber_from_edibes.top			✔																	
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6																				
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6																				
11. 20170221_Hancitor_malspam_traffic												✔								
12. 20170221_ZeusPandaBanker_malspam_traffic			✔									✔								
13. 20170302_Nebula_EK_1st_run									✔			✔								
14. 20170302_Nebula_EK_2nd_run									✔			✔								
15. 20170302_Nebula_EK_3rd_run									✔			✔								
16. 20170313_Kovter_Locky_malspam_traffic			✔																	
17. 20170314_Kovter_malspam_traffic			✔									✔								
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware										✔		✔	✔							
19. 20170330_Dridex_confirmation_letter_Dridex_traffic			✔				✔							✔					✔	✔
20. 20170405_Terror_EK_sends_Andromeda_1st_run			✔									✔				✔				✔
21. 20170405_Terror_EK_sends_Andromeda_2nd_run			✔									✔				✔				✔
22. 20170421_Locky_malspam_traffic			✔																✔	✔
23. 20170429_CVE_2017_0199_attempt_from_horsezangd			✔										✔							
24. 20170516_Jaff_ransomware_malspam_traffic			✔																	
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit							✔													✔
26. 20170601_ZeusPandaBanker_malspam_traffic			✔									✔								
27. 20170612_Loki_Bot_malspam_traffic			✔									✔								
28. 20170612_Trickbot_malspam_traffic		✔	✔			✔						✔		✔			✔		✔	
29. 20170612_Ursnif_malspam_traffic			✔				✔					✔	✔			✔				
30. 20170710_Kovter_Nemucod_malspam_traffic			✔																	
31. 20170724_Trickbot_malspam_traffic		✔	✔			✔						✔		✔			✔		✔	
32. 20170726_Emotet_malspam_traffic																	✔			✔
33. 20170803_Hancitor_malspam_traffic												✔								
34.20170812_Trickbot_infection_from_carriereiserphotography.com		✔	✔			✔						✔		✔			✔		✔	
35. 20170812_Trickbot_infection_from_carriereiter.com.exe		✔	✔			✔						✔		✔			✔		✔	
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu	✔		✔									✔								✔
37. 20171010_Emotet_malspam_traffic																	✔			✔

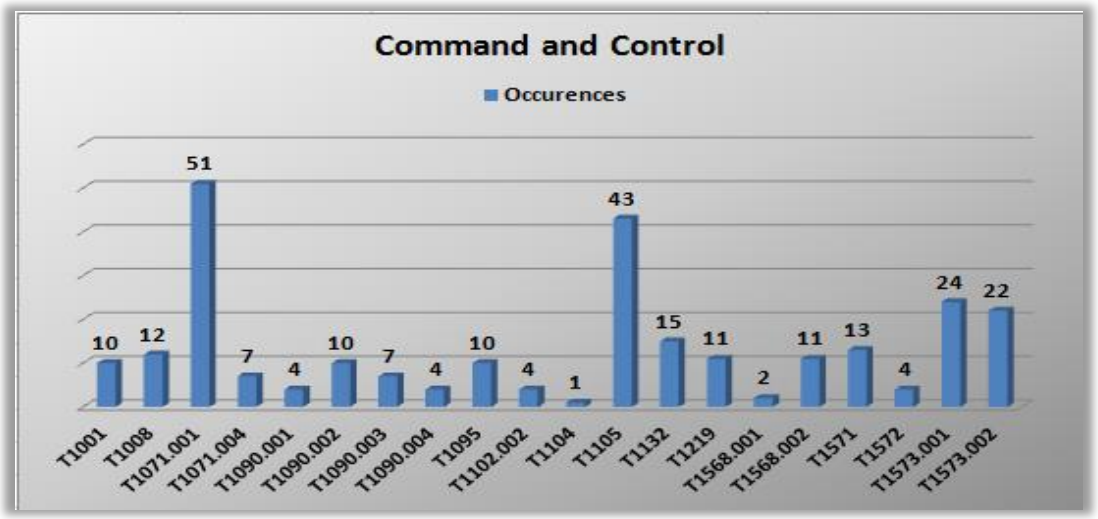


38.20171017_post_infection_traffic_from_Terror_EK_payloa		✔	✔												✔				✔
39. 20171017_Terror_EK_example		✔	✔												✔				✔
40. 20171018_Loki_Bot_traffic			✔									✔							
41. 20171031_Necurs_Botnet_malspam_pushing_Locky			✔												✔			✔	✔
42. 20171102_Smoke_Loader_traffic			✔									✔							
43. 20171129_Emotet_malspam_1st_run																✔			✔
44. 20171204_Dridex_malspam_trafic			✔				✔						✔					✔	✔
45. 20171220_smb_at_schedule																			
46.20171220_smb_metesploit_psexec_pth_download_meterpreter																			
47. 20171220_smb_mimikatz_copy																			
48. 20171220_smb_mimikatz_copy_to_host																			
49. 20171220_smb_net_user																			
50. 20171220_smb_psexec_add_user																			
51. 20171220_smb_psexec_mimikatz_ticket_dump																			
52. 20171222_malspam_pushing_RemcosRAT				✔		✔	✔					✔							
53.20180102_fake_Flash_player_installs_coinminer_malware			✔	✔					✔									✔	✔
54. 20180104_PCRat_gh0st_traffic									✔			✔	✔		✔			✔	
55. 20180104_PCRat_gh0st_traffic_pcap									✔			✔	✔		✔			✔	
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic			✔									✔							✔
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_coin_miner			✔									✔							
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffic	✔		✔									✔				✔		✔	
59.20180821_Neutrino_infection_traffic_from_password_protected_Word_doc			✔													✔			
60.20181008_Trickbot_sat75_infection_with_powershell_empire_traffic		✔	✔	✔		✔						✔		✔			✔	✔	
61. 20181019_malspam_pushing_Nymaim_infection_traffic	✔		✔													✔		✔	
62. 20181210_Imminent_Monitor_RAT_infection																			
63. 20181227_shade_malspam_infection							✔												
64. 20190104_Nanocore_RAT_infection_traffic												✔						✔	
65. 20190207_cred_stealer_via_FTP_traffic																			
66. 20190306_Flawed_Ammyy_traffic	✔		✔									✔						✔	
67. 20190522_Rig_EK_sends_Gandcrab_ransomware	✔		✔									✔							
68. 20190802_Lord_EK_sends_Eris_Ransomware													✔						
69. 20190812_Rig_EK_sends_MedusaHTTP_malware	✔		✔									✔							
70. 20190904_Ursnif_infection_with_Trickbot		✔	✔			✔	✔					✔	✔	✔		✔	✔		✔
71. 20190913_WSHRAT_infection_traffic			✔										✔						
72. 20200115_RevengeRAT_infection_traffic										✔		✔	✔						
73.20200226_Trickbot_spreads_from_infected_client_to_DC		✔	✔			✔						✔		✔			✔		✔
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps			✔							✔		✔							
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps			✔							✔		✔							
75. 20200701_pitty_tiger_1hr																			
76. 20200701_Valak_infection_with_IcedID		✔	✔								✔	✔	✔						✔
77.20201229_Emotet_infection_with_Trickbot_and_spambot_activity		✔	✔			✔						✔		✔			✔	✔	✔

78. 20210105_PurpleFox_EK_and_post_infection_traffic			✔										✔						
79. 20210223_lateral_backup_c2_1hr																			
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cobalt_Strike	✔		✔	✔	✔			✔	✔			✔	✔					✔	✔	✔
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	✔		✔	✔	✔			✔	✔			✔	✔					✔	✔	✔
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike	✔	✔	✔	✔	✔	✔		✔	✔			✔	✔	✔			✔	✔	✔	✔
83. 20220101_thru_03_server_activity_with_log4j_attempts			✔																
eternalblue_success_unpatched_win7																			
85. LM_psexec_smb_dcerpc_epm_svcctl																			
86. LM_smbexec_smb_dcerpc_svcctl_epm																			
88. mmcexec																			
89. 20211215_thru_20_server_activity_with_log4j_attempts			✔																
90. usecase4_speerphishing_EKC2_lateral_move																			
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike	✔		✔	✔	✔			✔	✔			✔	✔					✔	✔	✔

Πίνακας 20. Οι τεχνικές της κατηγορίας Command and Control στο σύνολο των επιθέσεων

Στην περίπτωση αυτή η συνηθέστερη είναι η ***T1071.001:*** *Command and Control/Application Layer Protocol/**Web Protocols***, κυρίως http. Σε πολλές περιπτώσεις οι επιτιθέμενοι μεταφέρουν εργαλεία ή αρχεία σε ένα ήδη παραβιασμένο σύστημα και αυτό γίνεται με χρήση της τεχνικής ***T1105:*** *Command and Control/**Ingress Tool Transfer***



Εικόνα 69. Command and Control techniques

Μία κατηγορία πριν το τέλος είναι η Exfiltration. Ο επόμενος πίνακας δείχνει τις καταγραφές μας για τις τεχνικές.

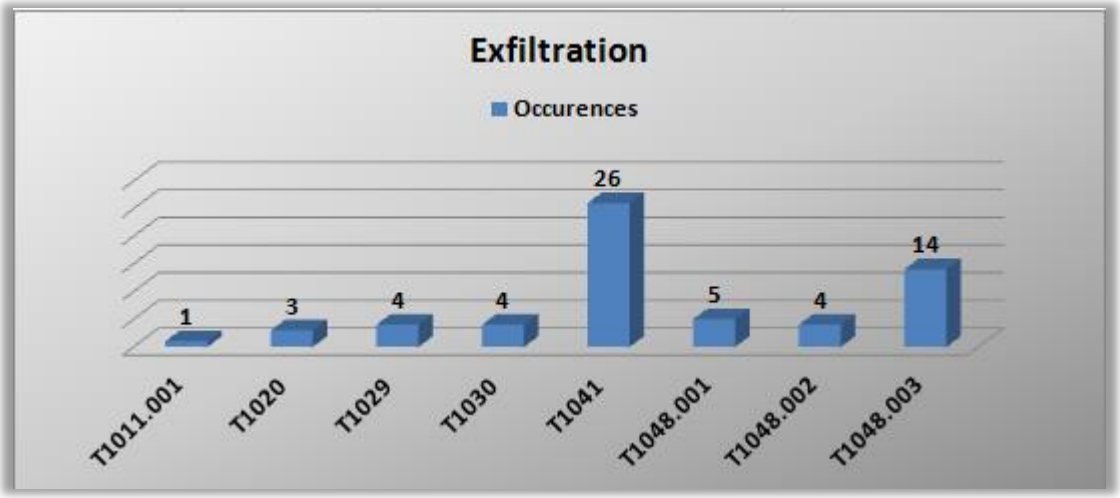
Pcap Name / Mitre Attack Tactic	Exfiltration							
	T1011.001	T1020	T1029	T1030	T1041	T1048.001	T1048.002	T1048.003
1. 20161215_ccnotice.net_malspam_traffic								
2. 20161216_Locky_malspam_traffic_example						✔		
3. 20161222_Cerber_from_malspam_traffic								
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware								
5. 20161228_1st_run_Sundown_EK_sends_Chthonic		✔						
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader		✔						
7. 20170201_Hancitor_Pony_malspam_traffic					✔			
8. 20170202_Cerber_from_adibas.top								
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6								
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6								
11. 20170221_Hancitor_malspam_traffic								
12. 20170221_ZeusPandaBanker_malspam_traffic								✔
13. 20170302_Nebula_EK_1st_run								
14. 20170302_Nebula_EK_2nd_run								
15. 20170302_Nebula_EK_3rd_run								
16. 20170313_Kovter_Locky_malspam_traffic					✔			
17. 20170314_Kovter_malspam_traffic					✔			
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware								
19. 20170330_Dridex_confirmation_letter_Dridex_traffic						✔	✔	✔
20. 20170405_Terror_EK_sends_Andromeda_1st_run							✔	✔
21. 20170405_Terror_EK_sends_Andromeda_2nd_run							✔	✔
22. 20170421_Locky_malspam_traffic						✔		
23. 20170429_CVE_2017_0199_attempt_from_horsezangd					✔			
24. 20170516_Jaff_ransomware_malspam_traffic					✔			
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit								
26. 20170601_ZeusPandaBanker_malspam_traffic								✔
27. 20170612_Loki_Bot_malspam_traffic					✔			
28. 20170612_Trickbot_malspam_traffic					✔			
29. 20170612_Ursnif_malspam_traffic					✔			
30. 20170710_Kovter_Nemucod_malspam_traffic					✔			
31. 20170724_Trickbot_malspam_traffic					✔			
32. 20170726_Emotet_malspam_traffic					✔			
33. 20170803_Hancitor_malspam_traffic								
34.20170812_Trickbot_infection_from_carriereiserphotography.com					✔			
35. 20170812_Trickbot_infection_from_carriereiter.com.exe					✔			
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu								✔
37. 20171010_Emotet_malspam_traffic					✔			

38.20171017_post_infection_traffic_from_Terror_EK_payloa								✔
39. 20171017_Terror_EK_example								✔
40. 20171018_Loki_Bot_traffic					✔			
41. 20171031_Necurs_Botnet_malspam_pushing_Locky						✔		
42. 20171102_Smoke_Loader_traffic								
43. 20171129_Emotet_malspam_1st_run					✔			
44. 20171204_Dridex_malspam_trafic						✔	✔	✔
45. 20171220_smb_at_schedule								
46.20171220_smb_metasploit_psexec_pth_download_meterpreter								
47. 20171220_smb_mimikatz_copy								
48. 20171220_smb_mimikatz_copy_to_host								
49. 20171220_smb_net_user								
50. 20171220_smb_psexec_add_user								
51. 20171220_smb_psexec_mimikatz_ticket_dump								
52. 20171222_malspam_pushing_RemcosRAT								
53.20180102_fake_Flash_player_installs_coinminer_malware	✔	✔						
54. 20180104_PCRat_gh0st_traffic								
55. 20180104_PCRat_gh0st_traffic_pcap								
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic					✔			✔
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_coin_miner								
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffic					✔			
59.20180821_Neutrino_infection_traffic_from_password_protected_Word_doc								
60.20181008_Trickbot_sat75_infection_with_powershell_empire_traffic					✔			
61. 20181019_malspam_pushing_Nymaim_infection_traffic								
62. 20181210_Imminent_Monitor_RAT_infection					✔			
63. 20181227_shade_malspam_infection								
64. 20190104_Nanocore_RAT_infection_traffic								
65. 20190207_cred_stealer_via_FTP_traffic								
66. 20190306_Flawed_Ammyy_traffic					✔			
67. 20190522_Rig_EK_sends_Gandcrab_ransomware								✔
68. 20190802_Lord_EK_sends_Eris_Ransomware								
69. 20190812_Rig_EK_sends_MedusaHTTP_malware								✔
70. 20190904_Ursnif_infection_with_Trickbot					✔			
71. 20190913_WSHRAT_infection_traffic								
72. 20200115_RevengeRAT_infection_traffic								
73.20200226_Trickbot_spreads_from_infected_client_to_DC					✔			
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps								
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps								
75. 20200701_pitty_tiger_1hr								
76. 20200701_Valak_infection_with_IcedID					✔			
77.20201229_Emotet_infection_with_Trickbot_and_spambot_activity					✔			

78. 20210105_PurpleFox_EK_and_post_infection_traffic								
79. 20210223_lateral_backup_c2_1hr								
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cobalt_Strike			✔	✔				
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool			✔	✔				
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike			✔	✔	✔			
83. 20220101_thru_03_server_activity_with_log4j_attempts								✔
eternalblue_success_unpatched_win7								
85. LM_psexec_smb_dcerpc_epm_svcctl								
86. LM_smbexec_smb_dcerpc_svcctl_epm								
88. mmcexec								
89. 20211215_thru_20_server_activity_with_log4j_attempts								✔
90. usecase4_spearphishing_EKC2_lateral_move								
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike			✔	✔				

Πίνακας 21. Οι τεχνικές της κατηγορίας Exfiltration στο σύνολο των επιθέσεων

Η τακτική αυτή αναφέρεται στους τρόπους με τους οποίους οι επιτιθέμενοι «διαρρέουν» τις πληροφορίες ή τα δεδομένα που υποκλέπτουν εκτός συστήματος ή δικτύου. Για τον σκοπό αυτό ξεχωρίζει η τεχνική ***T1041:*** *Exfiltration/**Exfiltration Over C2 Channel***, με αρκετή διαφορά σε εμφανίσεις από την δεύτερη ***T1048.003:*** *Exfiltration/Exfiltration Over Alternative Protocol/**Exfiltration Over Unencrypted Non-C2 Protocol.***



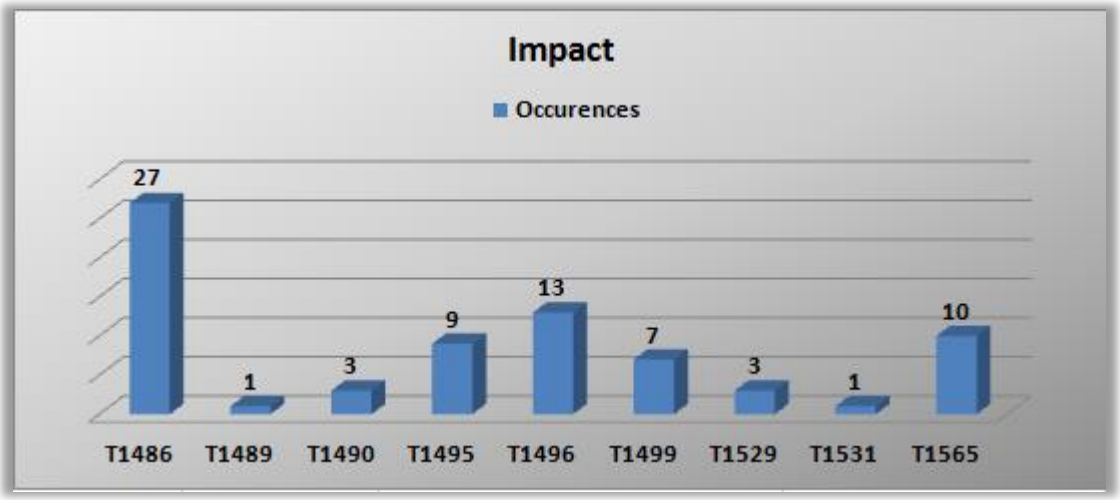
Εικόνα 70. Exfiltration techniques

Pcap Name / Mitre Attack Tactic	Impact								
	T1486	T1489	T1490	T1495	T1496	T1499	T1529	T1531	T1565
1. 20161215_ccnotice.net_malspam_traffic	✔								
2. 20161216_Locky_malspam_traffic_example	✔								
3. 20161222_Cerber_from_malspam_traffic	✔								
4.20161226_pseudoDarkleech_Rig_V_sends_Cerber_ransomware	✔								
5. 20161228_1st_run_Sundown_EK_sends_Chthonic									✔
6.20161230_Sundown_EK_1st_run_sends_Terdot.A_Zloader								✔	
7. 20170201_Hancitor_Pony_malspam_traffic									✔
8. 20170202_Cerber_from_adibas.top	✔								
9.20170215_ElTest_HoeflerText_Chrome_popup_traffic_1_of_6	✔								
10.20170215_ElTest_HoeflerText_Chrome_popup_traffic_2_of_6	✔								
11. 20170221_Hancitor_malspam_traffic	✔								✔
12. 20170221_ZeusPandaBanker_malspam_traffic									✔
13. 20170302_Nebula_EK_1st_run	✔				✔				
14. 20170302_Nebula_EK_2nd_run	✔				✔				
15. 20170302_Nebula_EK_3rd_run	✔				✔				
16. 20170313_Kovter_Locky_malspam_traffic	✔								
17. 20170314_Kovter_malspam_traffic					✔				
18. 20170315_ElTest_Rig_EK_sends_Revenge_ransomware	✔								
19. 20170330_Dridex_confirmation_letter_Dridex_traffic	✔				✔	✔			
20. 20170405_Terror_EK_sends_Andromeda_1st_run					✔				
21. 20170405_Terror_EK_sends_Andromeda_2nd_run					✔				
22. 20170421_Locky_malspam_traffic	✔								
23. 20170429_CVE_2017_0199_attempt_from_horsezangd						✔			✔
24. 20170516_Jaff_ransomware_malspam_traffic	✔								
25.20170518_WannaCry_ransomware_using_EnternalBlue_exploit	✔	✔	✔						
26. 20170601_ZeusPandaBanker_malspam_traffic									✔
27. 20170612_Loki_Bot_malspam_traffic									
28. 20170612_Trickbot_malspam_traffic				✔					
29. 20170612_Ursnif_malspam_traffic									
30. 20170710_Kovter_Nemucod_malspam_traffic					✔				
31. 20170724_Trickbot_malspam_traffic				✔					
32. 20170726_Emotet_malspam_traffic									
33. 20170803_Hancitor_malspam_traffic	✔								✔
34.20170812_Trickbot_infection_from_carriereiserphotography.com				✔					
35. 20170812_Trickbot_infection_from_carriereiter.com.exe				✔					
36. 20170828_Phobos_campaign_Rig_EK_sends_Bunitu	✔				✔	✔			
37. 20171010_Emotet_malspam_traffic									

38.20171017_post_infection_traffic_from_Terror_EK_payloa									
39. 20171017_Terror_EK_example									
40. 20171018_Loki_Bot_traffic									
41. 20171031_Necurs_Botnet_malspam_pushing_Locky	✔								
42. 20171102_Smoke_Loader_traffic									
43. 20171129_Emotet_malspam_1st_run									
44. 20171204_Dridex_malspam_trafic	✔				✔	✔			
45. 20171220_smb_at_schedule									
46.20171220_smb_metasploit_psexec_pth_download_meterpreter									
47. 20171220_smb_mimikatz_copy									
48. 20171220_smb_mimikatz_copy_to_host									
49. 20171220_smb_net_user									
50. 20171220_smb_psexec_add_user									
51. 20171220_smb_psexec_mimikatz_ticket_dump									
52. 20171222_malspam_pushing_RemcosRAT									
53.20180102_fake_Flash_player_installs_coinminer_malware					✔				
54. 20180104_PCRat_gh0st_traffic							✔		
55. 20180104_PCRat_gh0st_traffic_pcap							✔		
56. 20180109_Emotet_and_Zeus_Panda_Banker_traffic									✔
57.20180111_Rig_EK_sends_Smoke_Loader_and_Monero_coin_miner					✔				
58.20180717_Necurs_Botnet_pushing_Flawed_Ammyy_traffic									
59.20180821_Neutrino_infection_traffic_from_password_protected_Word_doc									
60.20181008_Trickbot_sat75_infection_with_powershell_empire_traffic				✔					
61. 20181019_malspam_pushing_Nymaim_infection_traffic	✔								
62. 20181210_Imminent_Monitor_RAT_infection					✔				
63. 20181227_shade_malspam_infection									
64. 20190104_Nanocore_RAT_infection_traffic									
65. 20190207_cred_stealer_via_FTP_traffic									
66. 20190306_Flawed_Ammyy_traffic									
67. 20190522_Rig_EK_sends_Gandcrab_ransomware	✔								
68. 20190802_Lord_EK_sends_Eris_Ransomware	✔		✔						
69. 20190812_Rig_EK_sends_MedusaHTTP_malware	✔					✔			
70. 20190904_Ursnif_infection_with_Trickbot				✔					
71. 20190913_WSHRAT_infection_traffic			✔						
72. 20200115_RevengeRAT_infection_traffic									
73.20200226_Trickbot_spreads_from_infected_client_to_DC				✔					
74a. 20200414_GuLoader_for_NetWire_RAT_two_pcaps									
74b. 20200414_GuLoader_for_NetWire_RAT_two_pcaps									
75. 20200701_pitty_tiger_1hr									
76. 20200701_Valak_infection_with_IcedID									
77.20201229_Emotet_infection_with_Trickbot_and_spambot_activity				✔					
78. 20210105_PurpleFox_EK_and_post_infection_traffic							✔		
79. 20210223_lateral_backup_c2_1hr									
80.20210513_Hancitor_traffic_with_Ficker_Stealer_and_Cobalt_Strike	✔								✔
81. 20210601_Hancitor_with_Cobalt_Stike_and_netping_tool	✔								✔
82. 20210715_TA551_Trickbot_infection_with_Cobalt_Strike				✔					
83. 20220101_thru_03_server_activity_with_log4j_attempts						✔			
eternalblue_success_unpatched_win7									
85. LM_psexec_smb_dcerpc_epm_svcctl									
86. LM_smbexec_smb_dcerpc_svcctl_epm									
88. mmcexec									
89. 20211215_thru_20_server_activity_with_log4j_attempts						✔			
90. usecase4_spearphishing_EKC2_lateral_move									
91. 20220722_IcedID_with_DarkVNC_and_Cobalt_Strike									

Πίνακας 22. Οι τεχνικές της κατηγορίας Impact στο σύνολο των επιθέσεων

Και ολοκληρώνουμε με την τακτική Impact, στην οποία χωρίς αμφισβήτηση πρωταγωνιστεί η τεχνική ***T1486:*** *Impact/**Data Encrypted for Impact***, όπως φαίνεται και στο γράφημα (Εικόνα 71). Το δίχως άλλο αποτελεί νούμερο ένα απειλή στην εποχή μας και δεν είναι άλλη από την κρυπτογράφηση δεδομένων με σκοπό χρηματικά ωφέλη κυρίως.



Εικόνα 71. Impact techniques

Στην ενότητα αυτή παρουσιάσαμε αναλυτικά τα ευρήματα της εργασίας μας και με χρήση πινάκων και γραφημάτων, προσπαθήσαμε να δείξουμε τα βασικά σημεία των αποτελεσμάτων. Στην επόμενη ενότητα αναφέρονται τα κύρια συμπεράσματα.

6

Συμπεράσματα

Η τελευταία ενότητα συνοψίζει τα σημεία κλειδιά της παρούσας διπλωματικής εργασίας.

6.1 Τελικά Suricata ή Zeek;

Όπως προαναφέραμε σκοπός μας ήταν η ποιοτική μελέτη και σύγκριση των δύο IDS και σίγουρα όχι το να αποφανθούμε ποιο είναι καλύτερο. Στα αποτελέσματα της εργασίας μας είδαμε μία ελαφριά υπεροχή του Suricata έναντι του Zeek ως προς την αποτελεσματικότητα. Στο 50% των περιπτώσεων η αποτελεσματικότητα του Suricata αξιολογήθηκε ως *High*, ενώ το Zeek πήρε αντίστοιχη αξιολόγηση στο 40% αυτών. Στον αντίποδα, το Zeek υπερτερεί στις περιπτώσεις που αξιολογήθηκε ως *Medium*. Με άλλα λόγια, δεν υστερούσε καθόλου σε ενδείξεις παραβίασης (IoCs), και αυτό φαίνεται από το γεγονός πως στην αποτελεσματικότητα ως προς τα IoCs, τα δύο IDSs ήταν πολύ κοντά (82% με 80%).

Είδαμε το Suricata να βγάζει περισσότερα alerts και να δείχνει καλύτερη συμπεριφορά και ποικιλομορφία στα alerts απέναντι στην κακόβουλη δικτυακή κίνηση, υπό την έννοια της ανίχνευσής της. Το alert που ξεχώρισε (trojan) υποδηλώνει την έξαρση των λεγόμενων *commodity loaders* (Cisco T. , 2022). Τα τέσσερα πιο ενεργά μέσα στο 2022 ήταν τα Qakbot, Emotet, IcedID και Trickbot, δραστηριότητα των οποίων υπήρχε στο δείγμα μας. Από την άλλη μεριά το Zeek έδωσε μόνο τριών ειδών alerts και τα τρία σχετικά με τα SSL πιστοποιητικά. Το συμπέρασμα στο οποίο οδηγηθήκαμε από τον τύπο του alert, είναι πως εντοπίζονται σε επίπεδο host και σχετίζονται με τα self-signed πιστοποιητικά. Το δεύτερο μεγαλύτερο ποσοστό των alerts ήταν εκείνο που αφορούσε πιστοποιητικά που έχουν λήξει.

Ωστόσο, θα πρέπει να λάβουμε υπόψιν πως το Suricata είναι ένα signature-based IDS. Αυτό σημαίνει πως βασίζεται σε ήδη υπάρχουσες υπογραφές κακόβουλων λογισμικών, τις οποίες ενσωματώνει στους κανόνες του. Το Zeek έχει διαφορετικό τρόπο λειτουργίας και η αξία του φαίνεται περισσότερο σε 0-day επιθέσεις. Εξάλλου, και στην εργασία μας προέκυψαν ευρήματα από το Zeek, τα οποία δεν υπήρχαν στα log files του Suricata. Επομένως, μάλλον ως συμπληρωματικά εργαλεία θα τα χαρακτήριζε κανείς παρά ως ανταγωνιστικά και αυτό είναι και το πόρισμα στο οποίο καταλήγουν και άλλοι συγγραφείς.

Όπως χαρακτηριστικά αναφέρει και ο (Rodfoss, 2011), πριν συγκρίνουμε τα IDSs μεταξύ τους θα πρέπει πρώτα να αποφασίσουμε τον τομέα και τις παραμέτρους που θα αξιολογήσουμε. Μπορεί κανείς να συγκρίνει log files, alerts, ρυθμίσεις, κανόνες, μέθοδο εγκατάστασης, απόδοση

μνήμης και επεξεργαστή... Στο τέλος όμως της ημέρας αυτό που έχει σημασία είναι να τα θέτουμε υπό δοκιμασία, έτσι ώστε να ανακαλύπτουμε τα τρωτά τους σημεία και με αυτό τον τρόπο να τα βελτιώνουμε. Γιατί με αυτό τον τρόπο θα έχουμε καλά και σωστά εργαλεία στα χέρια μας στην προσπάθεια να προστατέψουμε την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα, τόσο των πληροφοριακών συστημάτων όσο και των δικτύων που αυτά σχηματίζουν.

6.2 Η ομάδα των 13

Στο σημείο αυτό θα πρέπει να τονίσουμε πως οι πίνακες που παρουσιάστηκαν στην προηγούμενη ενότητα υπογραμμίζουν τις τεχνικές που σχετίζονται με το συγκεκριμένο δείγμα κακόβουλης δικτυακής κίνησης και αποτελούν μία «δυναμική» αναπαράσταση βασισμένη σε πραγματικές παρατηρήσεις. Αυτό όμως μπορεί να αλλάξει με την πάροδο του χρόνου καθώς τόσο τα λογισμικά, όσο και οι ομάδες που τα υλοποιούν ή τα χρησιμοποιούν εξελίσσονται διαρκώς.

Οι 13 τεχνικές που ξεχώρισαν (μία για κάθε τακτική) είναι:

- Resource Development: T1608.001: **Upload Malware**
- Initial Access: T1566.001: **Spearphishing Attachment /** T1566.002**: Spearphishing Link**
- Execution: T1059.001: **Powershell /** T1059.003**: Windows Command Shell**
- Persistence: T1547.001: **Registry Run Keys-Startup Folder**
- Privilege Escalation: T1547.001: **Registry Run Keys-Startup Folder /** T1543.003: **Windows Service**
- Defense Evasion: T1027: **Obfuscated Files or Information**
- Credential Access: **T1555.003**: **Credentials from Web Browsers**
- Discovery: T1082: **System Information Discovery**
- Lateral Movement: T1021.002: **SMB-Windows Admin Shares** / T1210: **Exploitation of Remote Services**
- Collection: T1005: **Data from Local System**
- Command and Control: T1071.001: **Web Protocols**
- Exfiltration: T1041: **Exfiltration Over C2 Channel**
- Impact : T1486: **Data Encrypted for Impact**

7

Περιορισμοί

Στα πλαίσια της εργασίας υπήρξαν και δυσχέρειες.

- Το γεγονός πως δεν πήραμε καθόλου alerts προερχόμενα από το bzar package ήταν μία από αυτές.
- Μεγαλύτερο δείγμα σημαίνει μεγαλύτερη ακρίβεια στα αποτελέσματα.
- Μεγαλύτερη διάρκεια στην πειραματική διαδικασία σημαίνει πιο πολλά δεδομένα, αρά μεγαλύτερη ακρίβεια στα αποτελέσματα επίσης.

Βιβλιογραφία

- Abdul, W., Abdul, J. F., & Ammar, M. (2022, Αύγουστος 04). Which open-source IDS? Snort, Suricata or Zeek. Association for Computing Machinery. Ανάκτηση Φεβρουάριος 06, 2023, από https://dl.acm.org/doi/abs/10.1016/j.comnet.2022.109116
- Adabi, M. R., Parman, S., & Aulia, W. A. (2022). Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. *217* . Elsevier B. V. Ανάκτηση Φεβρουάριος 06, 2023, από https://www.sciencedirect.com/science/article/pii/S1877050922024243
- Akbanov, M., Vassilakis, V., & Logothetis, M. (2019, Ιανουάριος). WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. Journa of Telecommunications and Information Technology. Ανάκτηση Φεβρουάριος 06, 2023
- Albin, E. (2011, Σεπτέμβριος). A COMPARATIVE ANALYSIS OF THE SNORT AND SURICATA INTRUSION-DETECTION SYSTEMS. Monterey, California. Ανάκτηση Φεβρουάριος 06, 2023, από https://apps.dtic.mil/sti/citations/ADA552115
- Bace, R., & Mell, P. (2001, Νοέμβριος 01). NIST Special Publication on Intrusion Detection Systems. Ανάκτηση από https://www.nist.gov/publications/intrusion-detection-systems
- Cecil, A. (2018). A Summary of Network Traffic Monitoring and Analysis Techniques. Ανάκτηση Φεβρουάριος 06, 2023, από https://www.researchgate.net/publication/228860956_A_Summary_of_Network_Traffic_Monitoring_and_Analysis_Techniques.
- Cisco. (2020). Cisco Annual Internet Report (2018 - 2023). Cisco public. Ανάκτηση Φεβρουάριος 06, 2023, από https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
- Cisco, T. (2022, Δεκέμβριος 14). 2022 Year in Review. Cisco Talos Intelligence . Ανάκτηση Φεβρουάριος 06, 2023, από https://blog.talosintelligence.com/year-in-review/
- Dontje, K. (2022). Quartely Report: Incident Response Trends in Q4 2022. Ανάκτηση Φεβρουάριος 06, 2023, από https://blog.talosintelligence.com/quarterly-report-incident-response-trends-in-q4-2022/
- ENISA. (2022). ENISA THREAT LANDSCAPE 2022. Ανάκτηση Φεβρουάριος 06, 2023, από https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
- Hafizul, A., & Ilir, G. (2022, Οκτώβριος 22). Dynamical analysis of diversity in rule-based open source network intrusion detection systems. Ανάκτηση Φεβρουάριος 06, 2023, από https://link.springer.com/article/10.1007/s10664-021-10046-w
- Hanninen, M. (2019, Δεκέμβριος). Open Source intrusion detection systems evaluation for small and medium-sized enterprise environments. Ανάκτηση Φεβρουάριος 06, 2023, από https://www.theseus.fi/bitstream/handle/10024/265554/Markku%20H%C3%A4nninen%20thesis.pdf?sequence=2

- Hashem, A., Md Tarique, A. J., Abdullah, A., Wael, A., Majid, A., Dhirendra, P., και συν. (2022, Μάρτιος 09). Effectiveness Evaluation of Different IDSs Using Integrated Fuzzy MCDM Model. MPDI. Ανάκτηση Φεβρουάριος 06, 2023, από https://www.mdpi.com/2079-9292/11/6/859
- Huey, C. (2022). Quartely Report: Incident Response Trends in Q3 2022. Cisco Talos. Ανάκτηση Φεβρουάριος 06, 2023, από https://blog.talosintelligence.com/quarterly-report-incident-response-trends-in-q3-2022/
- Johnson, C., Badger, M., Waltermire, D., Snyder, J., & Skorupka, C. (2016, Οκτώβριος). SP 800-150 Guide to Cyber Threat Information Sharing. Ανάκτηση Φεβρουάριος 06, 2023, από https://csrc.nist.gov/publications/detail/sp/800-150/final#pubs-documentation
- Marx, N. (2017, Δεκέμβριος 20). An Introduction to SMB for Network Security Analysts. Ανάκτηση Φεβρουάριος 06, 2023, από https://github.com/401trg/detections/blob/master/pdfs/20171220_An-Introduction-to-SMB-for-Network-Security-Analysts.pdf
- Neha, S. V., Kavita, Gaurav, A., & Saurabh, S. (2021). Performance Study of Snort and Suricata for Intrusion Detection System. IOP Publishing Ltd. Ανάκτηση Φεβρουάριος 06, 2023, από https://www.researchgate.net/publication/350081396_Performance_Study_of_Snort_and_Suricata_for_Intrusion_Detection_System
- NIST. (2011, Μάρτιος). NIST SP 800-39 - Managing Information Security Risk. Ανάκτηση Φεβρουάριος 06, 2023
- Pihelgas, M. (2012). A Comparative Analysis of open-source intrusion detection system. Tallinn University of Technology. Ανάκτηση Φεβρουάριος Δευτέρα, 2023, από https://www.semanticscholar.org/paper/A-COMPARATIVE-ANALYSIS-OF-OPEN-SOURCE-INTRUSION/b477ff3b9b52914eb095483603093b7d2f2dbd59
- Prenosil, V., Hammoudeh, M., Ghafir, I., & Svoboda, J. (2016). A Survey on Network Security Monitoring Systems. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. ResearchGate.
- Qinwen, H., Se-Young, Y., Asghar, M. R., & Muhammad, A. R. (2020, Απρίλιος). Analysing Performance Issues of Open-Source Intrusion Detection Systems in High-speed Networks. Ανάκτηση Φεβρουάριος 06, 2023, από https://dl.acm.org/doi/abs/10.1016/j.jisa.2019.102426
- Rodfoss, J. T. (2011, Μάϊος 24). Comparison of Open Source Network Intrusion Detection Systems. University of Oslo. Ανάκτηση Φεβρουάριος 06, 2023, από https://www.duo.uio.no/bitstream/handle/10852/8951/1/Rodfoss.pdf
- Scarfone, K., & Mell, P. (2007, Φεβρουάριος). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST - National Institute of Standards and Technology. Ανάκτηση Φεβρουάριος 06, 2023, από https://csrc.nist.gov/publications/detail/sp/800-94/final#pubs-documentation
- Μέμτσας, Δ. (2020, Νοέμβριος). Ανίχνευση Κακόβουλης Δραστηριότητας βασισμένη στα αρχεία καταγραφής των MS Windows 10 με εφαρμογή του πλαισίου MITRE ATT&CK. Παν/μιο Αιγαίου - Πολυτεχνική Σχολή - Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων. Ανάκτηση Φεβρουάριος 06, 2023, από http://hdl.handle.net/11610/21466

- Μουζενίδης, Π. (2022, Ιούνιος). Ανάπτυξη και Συγκριτική μελέτη Συστημάτων Ανίχνευσης Εισβολών με την χρήση Τεχνητής Νοημοσύνης. Θεσσαλονίκη: Αριστοτέλειο Παν/μιο Θεσσαλονίκης. Ανάκτηση Φεβρουάριος 06, 2023, από https://ikee.lib.auth.gr/record/342366?ln=en
- Παπαμαρτζιβάνος, Δ. (2019, Ιούνιος). Προηγμένες μέθοδοι μηχανικής μάθησης στην ανίχνευση δικτυακών επιθέσεων. Σάμος: Πανεπιστήμιο Αιγαίου - Πολυτεχνική Σχολή - Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων. Ανάκτηση Φεβρουάριος 06, 2023, από http://hdl.handle.net/10442/hedi/45893
- Παππάς, Σ. (2021, Ιούνιος 26). Κυβερνοεπιθέσεις και πρακτικές διασφάλισης της υποδομής ενός Πληροφοριακού Συστήματος. Σάμος: Παν/μιο Αιγαίου - Πολυτεχνική Σχολή - Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων. Ανάκτηση Φεβρουάριος 06, 2023, από http://hdl.handle.net/11610/23064

Παράρτημα Ι – Πηγές pcap αρχείων

• https://github.com/sbousseaden/PCAP-ATTACK
• https://github.com/tatsui-geek/malware-traffic-analysis.net
• https://github.com/elcabezzonn/Pcaps
• https://github.com/chrissanders/packets
• https://github.com/jasklabs/blackhat2017/tree/master/datasets
• https://github.com/401trg/detections/tree/master/pcaps
• https://www.malware-traffic-analysis.net/training/exporting-objects.html
• https://www.activecountermeasures.com/category/malware-of-the-day/

Πίνακας 23. Οι πηγές προέλευσης των pcap files

Παράρτημα ΙΙ – MITRE ATT&CK TACTICS & TECHNIQUES

Στο σημείο αυτό παραθέτουμε τις τακτικές και τεχνικές που εντοπίστηκαν στο σύνολο του δείγματος επιθέσεων.

Mitre Tactics

1. Reconnaissance

2. Resource Development

T1583.004: Resource Development/Acquire Infrastructure/Server

T1584.004: Resource Development/Compromise Infrastructure/Server

T1583.005: Resource Development/Acquire Infrastructure/Botnet

T1584.005: Resource Development/Compromise Infrastructure/Botnet

T1583.006 : Resource Development/Acquire Infrastructure/Web Services

T1587.001: Resource Development/Develop Capabilities/Malware

T1588.001: Resource Development/Obtain Capabilities/Malware (RaaS)

T1587.003: Resource Development/Develop Capabilities/Digital Certificates (self-signed)

T1588.004: Resource Development/Obtain Capabilities/ Digital Certificates (expired & unable to get local issuer cert)

T1587.004: Resource Development/Develop Capabilities/Exploits

T1588.005: Resource Development/Obtain Capabilities/Exploits (RaaS)

T1608.001: Resource Development/Stage Capabilities/Upload Malware

T1608.002: Resource Development/Stage Capabilities/Upload Tool

T1608.003: Resource Development/Stage Capabilities/Install Digital Certificates

T1608.004: Resource Development/Stage Capabilities/Drive-by Target

T1608.005: Resource Development/Stage Capabilities/Link Target

T1608.006: Resource Development/Stage Capabilities/SEO Poisoning

3. Initial Access

T1078.002: Initial Access/Valid Accounts/Domain Accounts

T1078.003: Initial Access/Valid Accounts/Local Accounts

T1091: Initial Access/Replication Through Removable Media

T1133: Initial Access/External Remote Services

T1189: Initial Access/Drive-by Compromise

T1566.001: Initial Access/Phishing/Spearphishing Attachment

T1566.002: Initial Access/Phishing/Spearphishing Link

4. Execution

T1047: Execution/Windows Management Instrumentation

T1053.002: Execution/Scheduled Task-Job/At

T1053.005: Execution/Scheduled Task-Job/Scheduled Task

T1059.001: Execution/Command and Scripting Interpreter/Powershell

T1059.003: Execution/Command and Scripting Interpreter/Windows Command Shell

T1059.005: Execution/Command and Scripting Interpreter/Visual Basic

T1059.007: Execution/Command and Scripting Interpreter/Javascript

T1059.006: Execution/ Command and Scripting Interpreter/Python

T1106: Execution/Native API

T1129: Execution/Shared Modules

T1203: Execution/Exploitation for Client Execution

T1204.001: Execution/User Execution/Malicious Link

T1204.002: Execution/User Execution/Malicious File

T1204.003: Execution/User Execution/Malicious Image

T1559.001: Execution/Inter-Process Communication/Component Object Model

T1559.002: Execution/Inter-Process Communication/Dynamic Data Exchange

T1569.002: Execution/System Services/Service Execution

5. Persistence

T1037.001: Persistence/Boot or Logon Initialization Scripts/Logon Script (Windows)

T1053.002: Persistence /Scheduled Task-Job/At

T1053.005: Persistence/Scheduled Task-Job/Scheduled Task

T1078.002: Persistence/Valid Accounts/Domain Accounts

T1078.003: Persistence /Valid Accounts/Local Accounts

T1098: Persistence/Account Manipulation

T1136.002: Persistence/Create Account/Domain Account

T1137.001: Persistence/Office Application Startup/Office Template Macros

T1137.006: Persistence/Office Application Startup/Add-ins

T1176: Persistence/Browser Extensions

T1197: Persistence/BITS Jobs

T1542.003: Persistence/Pre-OS Boot /Bootkit

T1543.003: Persistence/Create of Modify System Process/Windows Service

T1546.012: Persistence/Event Triggered Execution/Image File Execution Options Injection

T1546.015: Persistence/Event Triggered Execution/Component Object Model Hijacking

T1546.016: Persistence/Event Triggered Execution/Installer Packages

T1547.001: Persistence/Boot or Logon Autostart Execution/Registry Run Keys-Startup Folder

T1547.005: Persistence/ Boot or Logon Autostart Execution/Security Support Provider

T1574.002: Persistence/Hijack Execution Flow/DLL Side-Loading

6. Privilege Escalation

T1037.001: Privilege Escalation /Boot or Logon Initialization Scripts/Logon Script (Windows)

T1053.002: Privilege Escalation /Scheduled Task-Job/At

T1053.005: Privilege Escalation/ Scheduled Task-Job/Scheduled Task

T1055.001: Privilege Escalation/Process Injection/Dynamic-link Library Injection

T1055.002: Privilege Escalation/Process Injection/Portable Executable Injection

T1055.004: Privilege Escalation/Process Injection/Asynchronous Procedure Call

T1055.005: Privilege Escalation/Process Injection/Thread Local Storage

T1055.012: Privilege Escalation/Process Injection/Process Hollowing

T1068: Privilege Escalation/Exploitation for Privilege Escalation

T1078.002: Privilege Escalation/Valid Accounts/Domain Accounts

T1078.003: Privilege Escalation/Valid Accounts/Local Accounts

T1134.001: Privilege Escalation/Access Token Manipulation/Token Impersonation-Theft

T1134.003: Privilege Escalation/Access Token Manipulation/Make and Impersonate Token

T1134.004: Privilege Escalation/Access Token Manipulation/Parent PID Spoofing

T1134.005: Privilege Escalation/Access Token Manipulation/SID-History Injection

T1543.003: Privilege Escalation/Create or Modify System Process/Windows Service

T1546.012: Privilege Escalation /Event Triggered Execution/Image File Execution Options Injection

T1546.013: Privilege Escalation/Event Triggered Execution /Powershell Profile

T1546.015: Privilege Escalation/Event Triggered Execution/Component Object Model Hijacking

T1546.016: Privilege Escalation /Event Triggered Execution/Installer Packages

T1547.001: Privilege Escalation/Boot or Logon Autostart Execution/Registry Run Keys-Startup Folder

T1547.005: Privilege Escalation/ Boot or Logon Autostart Execution/Security Support Provider

T1548.002: Privilege Escalation/Abuse Elevation Control Mechanism/Bypass User Account Control

T1548.003: Privilege Escalation/Abuse Elevation Control Mechanism/Sudo and Sudo Caching

T1574.002: Privilege Escalation/Hijack Execution Flow/DLL Side-Loading

7. Defense Evasion

T1014: Defense Evasion/Rootkit

T1027: Defense Evasion/Obfuscated Files or Information (.002: Emotet, IcedID, Lokibot, Trickbot, Valak)(.003:IcedID, TA551, PurleFox)

T1036.004: Defense Evasion/Masquerading/Masquerade Task or Service (Nebula, Lokibot)

T1036.005: Defense Evasion/Masquerading/Match Legitimate Name or Location

T1055.001: Defense Evasion/Process Injection/Dynamic-link Library Injection

T1055.002: Defense Evasion/ Process Injection /Portable Executable Injection

T1055.004: Defense Evasion /Process Injection/Asynchronous Procedure Call

T1055.005: Defense Evasion /Process Injection/Thread Local Storage

T1055.012: Defense Evasion/Process Injection/Process Hollowing

T1070.001: Defense Evasion/Indicator Removal/ Clear Windows Event Logs

T1070.004: Defense Evasion/Indicator Removal/ File Deletion

T1070.006: Defense Evasion/Indicator Removal/ Timestomp

T1078.002: Defense Evasion/Valid Accounts/Domain Accounts

T1078.003: Defense Evasion/Valid Accounts/Local Accounts

T1112: Defense Evasion/Modify Registry

T1134.001: Defense Evasion/Access Token Manipulation/Token Impersonation-Theft

T1134.003: Defense Evasion/Access Token Manipulation/Make and Impersonate Token

T1134.004: Defense Evasion/Access Token Manipulation/Parent PID Spoofing

T1134.005: Defense Evasion/Access Token Manipulation/SID-History Injection

T1140: Defense Evasion/Deobfuscate-Decode Files or Information

T1197: Defense Evasion/BITS Jobs

T1202: Defense Evasion/Indirect Command Execution

T1207: Defense Evasion/Rogue Domain Controller

T1218.005: Defense Evasion/System Binary Proxy Execution/Mshta

T1218.007: Defense Evasion/ System Binary Proxy Execution/Msiexec

T1218.010: Defense Evasion/System Binary Proxy Execution/Regsvr32

T1218.011: Defense Evasion/System Binary Proxy Execution/Rundll32

T1218.012: Defense Evasion/System Binary Proxy Execution/Verclsid

T1497.001: Defense Evasion/Virtualization-Sandbox Evasion/System Checks

T1497.002: Defense Evasion/Virtualization-Sandbox Evasion/User Activity Based Checks

T1497.003: Defense Evasion/Virtualization-Sandbox Evasion/Time Based Evasion

T1542.003: Defense Evasion/Pre-OS Boot/Bootkit

T1548.002: Defense Evasion/Abuse Elevation Control Mechanism/Bypass User Account Control

T1548.003: Defense Evasion/Abuse Elevation Control Mechanism/Sudo and Sudo Caching

T1550.002: Defense Evasion/Use Alternate Authentication Material/Pass the Hash

T1550.003: Defense Evasion/Use Alternate Authentication Material/Pass the Ticket

T1553.002: Defense Evasion/Subvert Trust Controls/Code Singing

T1553.005: Defense Evasion/ Subvert Trust Controls/Mark-of-the-Web-Bypass
T1562.001: Defense Evasion/Impair Defenses/Disable or Modify Tools
T1562.004: Defense Evasion/Impair Defenses/Disable or Modify System Firewall
T1562.009: Defense Evasion/Impair Defenses/Safe Mode Boot
T1564.001: Defense Evasion/Hide Artifacts/Hidden Files and Directories
T1564.003: Defense Evasion/Hide Artifacts/Hidden Window
T1564.004: Defense Evasion/Hide Artifacts/NTFS File Attributes
T1564.010: Defense Evasion/Hide Artifacts/Process Argument Spoofing
T1574.002: Defense Evasion/Hijack Execution Flow/DLL Side-Loading
T1620: Defense Evasion/Reflective Code Loading
T1622: Defense Evasion/Debugger Evasion

8. Credential Access

T1003: Credential Access/OS Credential Dumping
T1040: Credential Access/Network Sniffing
T1056.001: Credential Access/Keylogging
T1056.004: Credential Access/Input Capture/Credential API Hooking
T1110.001: Credential Access/Brute Force/Password Guessing
T1110.003: Credential Access/Brute Force/Password Spraying
T1110.004: Credential Access/Brute Force/Credential Stuffing
T1539: Credential Access/Steal Web Session Cookie
T1552.001: Credential Access/Unsecured Credentials/Credentials in Files
T1552.002: Credential Access/Unsecured Credentials/Credentials in Registry
T1552.004: Credential Access/Unsecured Credentials/Private Keys
T1555.003: Credential Access/Credentials from Password Stores/Credentials from Web Browsers
T1555.004: Credential Access/ Credentials from Password Stores/Windows Credential Manager
T1555.005: Credential Access/Credentials from Password Stores/Password Managers
T1557: Credential Access/Adversary-in-the-Middle
T1649: Credential Access/Steal or Forge Authentication Certificates

9. Discovery

T1007: Discovery/System Service Discovery
T1012: Discovery/Query Registry
T1016: Discovery/System Network Configuration Discovery
T1018: Discovery/Remote System Discovery
T1033: Discovery/System Owner-User Discovery

T1040: Discovery/Network Sniffing
T1046: Discovery/Network Service Discovery
T1057: Discovery/Process Discovery
T1069: Discovery/Permission Groups Discovery
T1082: Discovery/System Information Discovery
T1083: Discovery/File and Directory Discovery
T1087.001: Discovery/Account Discovery/Local Account
T1087.002: Discovery/Account Discovery/Domain Account
T1087.003: Discovery/Account Discovery/Email Account
T1120: Discovery/Peripheral Device Discovery
T1124: Discovery/System Time Discovery
T1135: Discovery/Network Share Discovery
T1482: Discovery/Domain Trust Discovery
T1497.001: Discovery/Virtualization-Sandbox Evasion/System Checks
T1497.002: Discovery /Virtualization-Sandbox Evasion/User Activity Based Checks
T1497.003: Discovery/Virtualization-Sandbox Evasion/Time Based Evasion
T1518.001: Discovery/Software Discovery/Security Software Discovery
T1614: Discovery/System Location Discovery
T1614.001: Discovery/System Location Discovery/System Language Discovery
T1622: Discovery/Debugger Evasion

10. Lateral Movement

T1021.001: Lateral Movement/Remote Services/Remote Desktop Protocol
T1021.002: Lateral Movement/Remote Services/SMB-Windows Admin Shares
T1021.003: Lateral Movement/Remote Services/Distributed Component Object Model
T1021.004: Lateral Movement/ Remote Services/SSH
T1021.005: Lateral Movement/ Remote Services/VNC
T1021.006: Lateral Movement/ Remote Services/Windows Remote Management
T1080: Lateral Movement/Taint Shared Content
T1091: Lateral Movement/Replication Through Removable Media
T1210: Lateral Movement/Exploitation of Remote Services
T1550.002: Lateral Movement/Use Alternate Authentication Material/Pass the Hash
T1550.003: Lateral Movement /Use Alternate Authentication Material/Pass the Ticket
T1563.001: Lateral Movement/Remote Service Session Hijacking/SSH Hijacking
T1563.002: Lateral Movement/Remote Service Session Hijacking/RDP Hijacking
T1570: Lateral Movement/Lateral Tool Transfer

11. Collection

T1005: Collection/Data from Local System

T1025: Collection/Data from Removable Media

T1039: Collection/Data from Network Shared Drive

T1056.001: Collection/Input Capture/Keylogging

T1056.002: Collection/Input Capture/GUI Input Capture

T1056.004: Collection/Input Capture/Credential API Hooking

T1074.001: Collection/Data Staged/Local Data Staging

T1113: Collection/Screen Capture

T1114.001: Collection/Email Collection/Local Email Collection

T1114.002: Collection/Email Collection/Remote Email Collection

T1115: Collection/Clipboard Data

T1119: Collection/Automated Collection

T1123: Collection/Audio Capture

T1125: Collection/Video Capture

T1185: Collection/Browser Session Hijacking

T1557: Collection/Adversary-in-the-Middle

T1560: Collection/Archive Collected Data

12. Command and Control

T1001: Command and Control/Data Obfuscation

T1008: Command and Control/Fallback Channels

T1071.001: Command and Control/Application Layer Protocol/Web Protocols

T1071.004: Command and Control/Application Layer Protocol/DNS

T1090.001: Command and Control/Proxy/Internal Proxy

T1090.002: Command and Control/Proxy/External Proxy

T1090.003: Command and Control/Proxy/Multi-hop Proxy

T1090.004: Command and Control/Proxy/Domain Fronting

T1095: Command and Control/Non Application Layer Protocol

T1102.002: Command and Control/Web Service/Bidirectional Communication (Revenge RAT)

T1104: Command and Control/Multi-Stage Channels

T1105: Command and Control/Ingress Tool Transfer (Hancitor, Zeus Panda, Nebula, Revenge RAT)

T1132.001: Command and Control/Data Encoding/Standard Encoding (Revenge RAT)

T1219: Command and Control/Remote Access Software

T1568.001: Command and Control/Dynamic Resolution/Fast Flux DNS

T1568.002: Command and Control/Dynamic Resolution/Domain Generation Algorithms

T1571: Command and Control/Non-Standard Port

T1572: Command and Control/Protocol Tunneling

T1573.001: Command and Control/Encrypted Channel/Symmetric Cryptography

T1573.002: Command and Control/Encrypted Channel/Asymmetric Cryptography

13. Exfiltration

T1011.001: Exfiltration/Exfiltration Over Other Network Medium/Exfiltration Over Bluetooth

T1020: Exfiltration/Automated Exfiltration

T1029: Exfiltration/Scheduled Transfer

T1030: Exfiltration/Data Transfer Size Limits

T1041: Exfiltration/Exfiltration Over C2 Channel

T1048.001: Exfiltration/Exfiltration Over Alternative Protocol/Exfiltration Over Symmetric Encrypted Non-C2 Protocol

T1048.002: Exfiltration/Exfiltration Over Alternative Protocol/Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

T1048.003: Exfiltration/Exfiltration Over Alternative Protocol/Exfiltration Over Unencrypted Non-C2 Protocol

14. Impact

T1486: Impact/Data Encrypted for Impact

T1489: Impact/Service Stop

T1490: Impact/Inhibit System Recovery

T1495: Impact/Firmware Corruption

T1496: Impact/Resource Hijacking

T1499: Impact/Endpoint Denial of Service

T1529: Impact/System Shutdown-Reboot

T1531: Impact/Account Access Removal

T1565: Impact/Data Manipulation