Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών «Προηγμένα Συστήματα Πληροφορικής»

Τίτλος Διατριβής	**Χρήση διαμοιρασμένων πληροφοριών για τον εντοπισμό άγνωστων κυβερνοαπειλών (Active Cyber Defence: Cyber Threat Intelligence)**
Ονοματεπώνυμο Φοιτητή	**Αλέξιος Πετρόπουλος**
Πατρώνυμο	**Γεώργιος**
Αριθμός Μητρώου	**ΜΠΣΠ16026**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Οκτώβριος 2019**

Τριμελής Εξεταστική Επιτροπή

Παναγιώτης Κοτζανικολάου	Κωνσταντίνος Πατσάκης	Μιχαήλ Ψαράκης
Επίκουρος Καθηγητής	Επίκουρος Καθηγητής	Επίκουρος Καθηγητής

Περίληψη

Σκοπός της παρούσας εργασίας είναι η μελέτη μηχανισμών διαμοιρασμού πληροφοριών (Cyber Threat Intelligence) με σκοπό τον εντοπισμό απειλών και την ενεργή κυβερνοάμυνα (Active Cyber Defence). Στο πλαίσιο της εργασίας πραγματοποιείται μελέτη γύρω από τους τύπους των επιθέσεων, των τρόπων με τους οποίους εφαρμόζεται η ενεργή κυβερνοάμυνα, καθώς και των μηχανισμών για την ασφάλεια της υποδομής. Παράλληλα, γίνεται μελέτη και ανάλυση του εργαλείου MISP, το οποίο αποτελεί μια πλατφόρμα ανταλλαγής πληροφοριών για κακόβουλα λογισμικά και η συνεργασία του με το εργαλείο LOKI. Η πλατφόρμα αυτή αποτελεί ένα μηχανισμό για την εφαρμογή της ενεργής κυβερνοάμυνας. Το βασικό συμπέρασμα είναι ότι η ενεργή κυβερνοάμυνα, παρόλο που δεν μπορεί να εγγυηθεί την απόλυτη προστασία από επιθέσεις μηδενικών ημερών (zero-day attacks) μπορεί να αυξήσει σε σημαντικό βαθμό το επίπεδο ασφάλειας των συστημάτων. Επιπλέον, είναι σημαντικό να αναπτυχθούν πολιτικές ασφαλείας, οι οποίες θα πρέπει να εφαρμόζονται από όλους τους χρήστες μια υποδομής, δημιουργώντας τους παράλληλα το αίσθημα της ευθύνης.

Λέξεις κλειδιά: κυβερνοάμυνα, κυβερνοασφάλεια, ενεργή κυβερνοασφάλεια, MISP, LOKI

Abstract

The aim of this thesis is to study how existing Cyber Threat Intelligence mechanisms can be utilized for the identification of novel threats in the context of Active Cyber Defence. We a study the various existing types of attack, of the active cyber-defence implementations, as well as of existing infrastructure security mechanisms. In addition we study the MISP tool, which is an information exchange platform for malware, as well as its integration with the LOKI tool, that can provide an effective mechanism for active cyber-defence. The basic conclusion is that although active cyber defence cannot guarantee the absolute protection from zero-day attacks, it can significantly increase the security level. In addition to this, it is important to develop and implement proper security policies, that will enhance security awareness and users' responsibility.

Keywords: cyber security, active cyber-security, MISP, LOKI

Περιεχόμενα

1. Εισαγωγή

Το σημερινό απειλητικό περιβάλλον στον κυβερνοχώρο θέτει μεγαλύτερη πρόκληση από ποτέ. Τα τελευταία χρόνια η αύξηση των εξειδικευμένων, στοχευμένων κυβερνοεπιθέσεων εναντίον κυβερνήσεων και επιχειρήσεων υπογραμμίζει την ανάγκη βελτίωσης της άμυνας. Οι οργανισμοί πρέπει να προστατεύονται από τους επιτιθέμενους, οι οποίοι διερευνούν επιμελώς τους στόχους τους, αναλύουν τις αδυναμίες τους και χρησιμοποιούν αυτές τις πληροφορίες για να προσαρμόσουν τις επιθέσεις τους (Thomlinson, 2015).

Έτσι αντικείμενο της παρούσας εργασίας είναι η κυβερνοασφάλεια και οι τρόποι με τους οποίους μπορεί να επιτευχθεί. Σκοπός της εργασίας είναι να δείξει αν οι υφιστάμενοι μηχανισμοί γύρω από την ασφάλεια και την προστασία από τις απειλές και τους εισβολείς είναι επαρκείς.

Ένας από τους στόχους της εργασίας αποτελεί η κατανόηση όλων των τύπων των επιθέσεων που μπορούν να πραγματοποιηθούν στα πλαίσια του κυβερνοχώρου. Επίσης, μέσα από αυτή τη μελέτη στοχεύετε να εντοπιστούν οι τρόποι με τους οποίους μπορεί να ενισχυθεί η ασφάλεια και προστασία στον κυβερνοχώρο μέσω της ενεργής κυβερνοάμυνας (Active Cyber Defence) και την ασφάλεια της υποδομής (Security the infrastructure). Ιδιαίτερη σημασία στα πλαίσια της ανάλυσης των μηχανισμός της ενεργής κυβερνοάμυνας δίνεται στα πλαίσια ανταλλαγής πληροφοριών και στο εργαλείο MISP.

Η εργασία υλοποιείται μέσω της ανασκόπησης σε βιβλιογραφικές και διαδικτυακές πηγές και διαρθρώνεται σε πέντε κύρια κεφάλαια, το πρώτο κεφάλαιο αφορά την κυβερνοάμυνα, το δεύτερο κεφάλαιο την ασφάλεια της υποδομής, το τρίτο κεφάλαιο περιλαμβάνει τις απόψεις σχετικά με τα εργαλεία και τους τρόπους ασφάλειας και άμυνας, το τέταρτο κεφάλαιο αφοράς τον τρόπο με τον οποίο ενισχύεται η ασφάλεια μέσω της ανταλλαγής πληροφοριών και των δεικτών και το πέμπτο κεφάλαιο περιλαμβάνει την καταγραφή των συμβάντων μέσω της πλατφόρμας MISP.

Αναλυτικότερα, εισαγωγικά στο πρώτο κεφάλαιο γίνεται μια πρώτη γνωριμία με το εργαλείο MISP ως προς το τι είναι, το σκοπό του και τις δυνατότητες του. Στη συνέχεια ορίζονται οι έννοιες κυβερνοάμυνα και απειλή νοημοσύνης (ή απειλή της πληροφορίας). Επίσης, γίνεται μια σύντομη περιγραφή στους συνηθέστερους τύπους επιθέσεων, δηλαδή τα κακόβουλα λογισμικά, την εκμετάλλευση της μηδενικής ημέρας, το ηλεκτρονικό ψάρεμα, τους ιούς, τις εγχύσεις SQL, τις επιθέσεις μεταξύ των ιστότοπων (XSS) και τις

προηγμένες απειλές (APT). Παράλληλα, γίνεται αναφορά σε δύο γνωστές ιστορικές εγκληματικές επιθέσεις του κυβερνοχώρους, το Stuxnet και το Zeus. Στο τέλος του πρώτου κεφαλαίου παρουσιάζονται οι τρόποι με τους οποίους μπορεί να εφαρμοστεί η ενεργή κυβερνοάμυνα μέσω του ελέγχου τρωτότητας, του ελέγχου των κανόνων και των πολιτικών ασφαλείας, τα Honeypots, τα πλαίσια ανταλλαγής πληροφοριών, την αντιμετώπιση των περιστατικών και το συνδυασμό των μεγάλων δεδομένων με την τεχνητή νοημοσύνη για την ενίσχυση της ασφάλειας.

Στο δεύτερο κεφάλαιο παρουσιάζονται οι τρόποι με τους οποίους μπορεί να ενισχυθεί η ασφάλεια της υποδομής. Οι τρόποι αυτοί περιλαμβάνουν τα τείχη προστασίας, τα συστήματα ανίχνευσης εισβολών (IDS), τα συστήματα πρόληψης εισβολών (IPS), τα λογισμικά προστασία από ιούς και κακόβουλα λογισμικά, τα εικονικά ιδιωτικά δίκτυα (VPN), την κρυπτογράφηση των δεδομένων και τις ταξινομίες και την ευαισθητοποίηση των χρηστών γύρω από την εφαρμογή της ασφάλειας.

Στο τρίτο κεφάλαιο παρουσιάζονται οι απόψεις της διαθέσιμης βιβλιογραφίας και δικτυογραφίας σχετικά με το κατά πόσο όλες οι αυτές οι μέθοδοι και τα εργαλεία που μελετήθηκαν γύρω από την ασφάλεια και την προστασία από τις απειλές είναι αρκετά αποτελεσματικά.

Στο τέταρτο κεφάλαιο παρουσιάζεται π τρόπος με τον οποίο ενισχύεται η ασφάλεια μέσω της ανταλλαγής πληροφοριών και των δεικτών με τη χρήση των πλαισίων ανταλλαγής πληροφοριών. Για την καλύτερη κατανόηση η αναφορά σε αυτούς τους τρόπους γίνεται με βάση τη δημοφιλή πλατφόρμα ανταλλαγής πληροφοριών για απειλές, MISP.

Στο πέμπτο και τελευταίο κεφάλαιο παρουσιάζεται ο τρόπος με τον οποίο καταγράφεται ένα συμβάν (event) από κάποια απειλή ή ένα κακόβουλο λογισμικό στο MISP. Πραγματοποιήσαμε ανίχνευση απειλών-κακόβουλων ευρημάτων (σε συνέχεια εκτέλεσης σκαναρίσματος του συστήματος) από το εργαλείο LOKI. Επίσης, έγινε εισαγωγή και έρευνα επί των στοιχείων που συλλέχθηκαν από το τελευταίο scan στα εργαλεία ανοικτού κώδικα.

Η εργασία ολοκληρώνεται με την αποτύπωση των συμπερασμάτων που προέκυψαν από την ολοκλήρωση της μελέτης που πραγματοποιήθηκε.

1.1 Κυβερνοάμυνα (Cyber Defence)

Αντικείμενο της διατριβής αποτελεί η κυβερνοάμυνα (Cyber Defence). Η κυβερνοάμυνα (Cyber Defence) είναι ένας αμυντικός μηχανισμός δικτύου ηλεκτρονικών υπολογιστών ο οποίος περιλαμβάνει την ανταπόκριση στις δράσεις και την προστασία της υποδομής και τη διασφάλιση πληροφοριών για οργανώσεις, κυβερνητικές οντότητες και άλλα πιθανά δίκτυα (Galinec et al., 2017). Από την άλλη, η ενεργή κυβερνοάμυνα (Active Cyber Defence - ACD) είναι μια ιδέα που βασίζεται στα εργαλεία απόσπασης, όχι μόνο για τον εντοπισμό και τον τερματισμό των επιθέσεων στον κυβερνοχώρο καθώς συμβαίνουν, αλλά και για τη λήψη επιθετικών μέτρων για την ελαχιστοποίηση των δυνατοτήτων των εισβολέων (Dewar, 2017).

Έτσι, ο βασικός προβληματισμός που προκύπτει στην παρούσα διατριβή είναι ο τρόπος με τον οποίο μπορεί να επιτευχθεί η κυβερνοάμυνα και πως μπορεί να συνεισφέρει η ενεργή κυβερνοάμυνα στην ασφάλεια και την προστασία των οργανισμών από του επιτιθέμενους. Για ποιο λόγο είναι απαραίτητη η ασφάλεια της υποδομής και με ποιους τρόπους μπορεί να επιτευχθεί. Σύμφωνα με αυτό, ένας ακόμη προβληματισμός που προκύπτει είναι ποιοι τρόποι και ποια μέσα χρησιμοποιούν οι επιτιθέμενοι για να έχουν πρόσβαση σε πληροφορίες και συστήματα.

Με βάση τους παραπάνω προβληματισμούς γεννιέται το ερώτημα αν οι τεχνολογικές λύσεις κυβερνοάμυνας και της ενεργής κυβερνοάμυνας είναι αρκετές για να διασφαλιστεί η προστασία των δεδομένων και των συστημάτων από τους επιτιθέμενους και ποιο ρόλο διαδραματίζει η γνώση και η συνειδητοποίηση όλων των συμμετεχόντων που έχουν πρόσβαση σε πληροφορίες, δεδομένα και συστήματα.

Τέλος, κάθε τεχνολογία ασφαλείας προσφέρει διαφορετικές υπηρεσίες και καλύπτει χαρακτηριστικά, όμως το ερώτημα είναι τι καλύπτει η κάθε τεχνολογία, σε ποιες περιπτώσεις είναι συμπληρωματικές μεταξύ τους και σε ποια σημεία δημιουργούνται αλληλοκαλύψεις.

1.2 Στόχος της διατριβής

Ο βασικός σκοπός σε αυτή τη διατριβή είναι να δείξει αν οι υφιστάμενοι μηχανισμοί γύρω από την ασφάλεια και την προστασία από τις απειλές και τους εισβολείς είναι επαρκείς. Έτσι, μέσα από την εργασία αυτή στοχεύετε να παρουσιαστούν και να κατανοηθούν όλοι οι τρόποι με τους οποίους μπορεί να επιχειρηθεί από έναν επιτιθέμενο να αποκτήσει πρόσβαση σε πληροφορίες και δεδομένα ή σε συστήματα.

Αυτό θα βοηθήσει στην κατανόηση και τον ρόλο που διαδραματίζουν οι μηχανισμοί ασφαλείας και προστασίας στον κυβερνοχώρο μέσω της ενεργής κυβερνοαάμυνας, γεγονός που αποτελεί και το σημαντικότερο στόχο της διατριβής.

1.3 Δομή της διατριβής

Σε αυτή την ενότητα προσδιορίζεται η δομή της διατριβής και εξηγείται τι περιλαμβάνει το κάθε κεφάλαιο, ώστε να γίνει ποιο κατανοητό το περιεχόμενο που περιλαμβάνει η εργασία. Η εργασία δομείται σε πέντε κεφάλαια τα οποία περιγράφονται στις ακόλουθες παραγράφους.

Το Κεφάλαιο 1 ξεκινάει με μια γενική εισαγωγή γύρω από τους βασικούς προβληματισμούς, τους στόχους και της δομή της διατριβής. Στη συνέχεια του κεφαλαίου πραγματοποιείται παρουσίαση και ανάλυση της κυβερνοάμυνας. Αναλυτικότερα, εισαγωγικά γίνεται μια πρώτη γνωριμία με το εργαλείο MISP ως προς το τι είναι, το σκοπό του και τις δυνατότητες του. Στη συνέχεια ορίζονται οι έννοιες κυβερνοάμυνα και απειλή νοημοσύνης (ή απειλή της πληροφορίας). Επίσης, γίνεται μια σύντομη περιγραφή στους συνηθέστερους τύπους επιθέσεων, δηλαδή τα κακόβουλα λογισμικά, την εκμετάλλευση της μηδενικής ημέρας, το ηλεκτρονικό ψάρεμα, τους ιούς, τις εγχύσεις SQL, τις επιθέσεις μεταξύ των ιστότοπων (XSS) και τις προηγμένες απειλές (APT). Παράλληλα, γίνεται αναφορά σε δύο γνωστές ιστορικές εγκληματικές επιθέσεις του κυβερνοχώρους, το Stuxnet και το Zeus. Στο τέλος του πρώτου κεφαλαίου παρουσιάζονται οι τρόποι με τους οποίους μπορεί να εφαρμοστεί η ενεργή κυβερνοάμυνα μέσω του ελέγχου τρωτότητας, του ελέγχου των κανόνων και των πολιτικών ασφαλείας, τα Honeypots, τα πλαίσια ανταλλαγής πληροφοριών, την αντιμετώπιση των περιστατικών και το συνδυασμό των μεγάλων δεδομένων με την τεχνητή νοημοσύνη για την ενίσχυση της ασφάλειας. Επίσης, γίνεται αναφορά στο εργαλείο LOKI.

Στο Κεφάλαιο 2 παρουσιάζονται οι τρόποι με τους οποίους μπορεί να ενισχυθεί η ασφάλεια της υποδομής. Οι τρόποι αυτοί περιλαμβάνουν τα τείχη προστασίας, τα συστήματα ανίχνευσης εισβολών (IDS), τα συστήματα πρόληψης εισβολών (IPS), τα λογισμικά προστασία από ιούς και κακόβουλα λογισμικά, τα εικονικά ιδιωτικά δίκτυα (VPN), την κρυπτογράφηση των δεδομένων και τις ταξινομίες και την ευαισθητοποίηση των χρηστών γύρω από την εφαρμογή της ασφάλειας.

Στο Κεφάλαιο 3 παρουσιάζονται οι απόψεις της διαθέσιμης βιβλιογραφίας και δικτυογραφίας σχετικά με το κατά πόσο όλες οι αυτές οι μέθοδοι και τα εργαλεία που μελετήθηκαν γύρω από την ασφάλεια και την προστασία από τις απειλές είναι αρκετά αποτελεσματικά. Ορίζονται επίσης ορίσετε κάποια χαρακτηριστικά και υπηρεσίες που προσφέρει η κάθε τεχνολογία ασφαλείας και προσδιορίζεται τι καλύπτει η κάθε τεχνολογία, σε ποια σημεία είναι συμπληρωματικές μεταξύ τους, καθώς και που εντοπίζονται αλληλοκαλύψεις.

Στο Κεφάλαιο 4 κεφάλαιο παρουσιάζεται ο τρόπος με τον οποίο ενισχύεται η ασφάλεια μέσω της ανταλλαγής πληροφοριών και των δεικτών με τη χρήση των πλαισίων ανταλλαγής πληροφοριών. Για την καλύτερη κατανόηση η αναφορά σε αυτούς τους τρόπους γίνεται με βάση τη δημοφιλή πλατφόρμα ανταλλαγής πληροφοριών για απειλές, MISP.

Στο Κεφάλαιο 5 παρουσιάζεται ο τρόπος με τον οποίο καταγράφεται ένα συμβάν (event) από μια απειλή ή ένα κακόβουλο λογισμικό στο εργαλείο MISP.

Στις ακόλουθες ενότητες αυτού του κεφαλαίου γίνεται μια πρώτη προσέγγιση του εργαλείου MISP το οποίο αποτελεί μια πλατφόρμα κοινής χρήσης απειλών και αποτελεί ένα από τις μηχανισμούς της ενεργής κυβερνοάμυνας. Για την καλύτερη κατανόηση στον οποίο μπορεί να συνεισφέρει η ενεργή κυβερνάμυνα περιγράφονται οι τύποι των πιθανών επιθέσεων και στη συνέχεια περιγράφονται οι μηχανισμοί της. Επίσης, στην εργασία χρησιμοποιήσαμε το εργαλείο LOKI και μέσω της πλατφόρμας Virustotal αναλύσαμε ένα αρχείο, χρησιμοποιώντας το όνομα του ή το μοναδικό αριθμό κατακερματισμού του (hash), πραγματοποιώντας δυναμική ανάλυση.

1.4 Τι είναι η προληπτική κυβερνοάμυνα (cyber defence)

Η ασφάλεια στον κυβερνοχώρο (cyber security) είναι ένα σημαντικό και πολύ επίκαιρο ζήτημα ασφάλειας. Περιλαμβάνει μια σειρά τεχνικών και εφαρμογών για την εξασφάλιση των ψηφιακών δικτύων και των υποδομών, καθώς και τα συστήματα που εξαρτώνται από αυτά (Dewar, 2017). Η κυβερνοασφάλεια (Cyber Security) είναι η διακυβέρνηση, η ανάπτυξη, η διαχείριση και η χρήση της ασφάλειας των πληροφοριών, της ασφάλειας της τεχνολογίας της πληροφορίας και των εργαλείων και τεχνικών ασφάλειας της πληροφορικής για την τήρηση της κανονιστικής συμμόρφωσης, την υπεράσπιση των περιουσιακών στοιχείων και τη συρρίκνωση των περιουσιακών στοιχείων των αντιπάλων (Galinec et al., 2017).

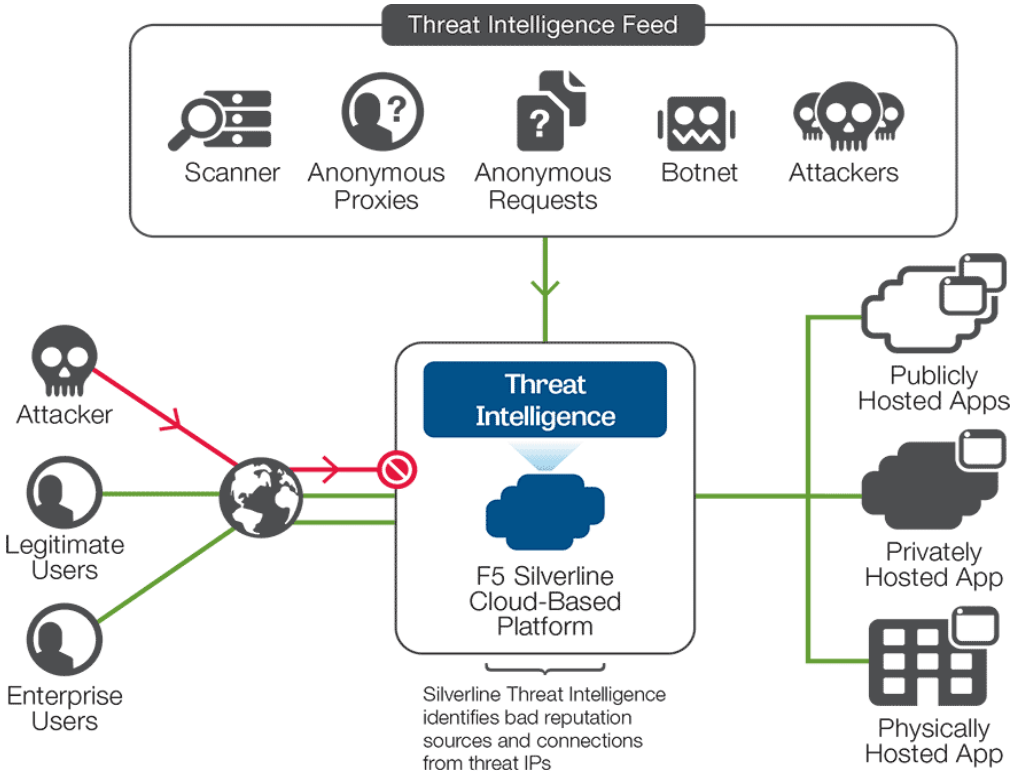
Η κυβερνοάμυνα (cyber defence) είναι ένας αμυντικός μηχανισμός δικτύου ηλεκτρονικών υπολογιστών ο οποίος περιλαμβάνει την ανταπόκριση στις δράσεις και την προστασία της υποδομής ζωτικής σημασίας και τη διασφάλιση πληροφοριών για οργανισμούς, κυβερνητικές οντότητες και άλλα πιθανά δίκτυα (Galinec et al., 2017).
Ουσιαστικά, η κυβερνοάμυνα παρέχει την απαιτούμενη ασφάλεια για να τρέξει τις διαδικασίες και τις δραστηριότητες, χωρίς να ανησυχεί για τις απειλές. Βοηθά στην ενίσχυση των δυνατοτήτων και των πηγών ασφάλειας. Η κυβερνοάμυνα βοηθά επίσης στη βελτίωση της αποτελεσματικότητας των πόρων ασφαλείας και των εξόδων ασφαλείας, ειδικά σε κρίσιμες τοποθεσίες.

1.5 Συλλογή και κατανόηση των κυβερνοαπειλών με την χρήση τεχνικών υψηλής νοημοσύνης (Cyber Threat Intelligence)

Η νοημοσύνη (intelligence) ορίζεται τακτικά ως πληροφορία που μπορεί να χρησιμοποιηθεί για την αλλαγή των αποτελεσμάτων. Αξίζει να σκεφτεί κανείς την παραδοσιακή νοημοσύνη πριν διευκρινιστεί ο όρος της κατανόησης των κυβερνοαπειλών με χρήση τεχνικών νοημοσύνης, καθώς με πολλούς τρόπους η τελευταία είναι απλώς η παραδοσιακή νοημοσύνη που εφαρμόζεται στις απειλές του κυβερνοχώρου. Μια καλή επεξήγηση του όρου που αναγράφεται στον τίτλο ε είναι η διαδικασία της μετακίνησης θεμάτων από άγνωστα σε γνωστά με την ανακάλυψη της ύπαρξης, όπου η απειλή είναι κατανοητή και μετριασμένη (Chismon & Ruks, 2015).
Στην απλούστερη μορφή της είναι η διαδικασία κατανόησης των απειλών για έναν οργανισμό με βάση τα διαθέσιμα σημεία δεδομένων. Αλλά ξεπερνά την απλή συλλογή σημείων δεδομένων. Πρέπει επίσης να υπάρχει κατανόηση του τρόπου με τον οποίο τα δεδομένα σχετίζονται με τον οργανισμό. Οι ομάδες πρέπει να συνδυάζουν τα σημεία δεδομένων με τις πληροφορίες για τον προσδιορισμό σχετικών απειλών για τον οργανισμό (Bromiley, 2016).
Το 2013 ο αναλυτής Rob McMilan της Gartner όρισε την κατανόηση κυβερνοαπειλών με τη χρήση νοημοσύνης ως τη γνώση που βασίζεται σε τεκμήρια, συμπεριλαμβανομένων πλαισίων, μηχανισμών, δεικτών (indicators), επιπτώσεων και συμβουλών, σχετικά με κάποια υπάρχουσα ή αναδυόμενη απειλή για περιουσιακά στοιχεία που μπορούν να χρησιμοποιηθούν για την ενημέρωση των αποφάσεων σχετικά με την ανταπόκριση του ατόμου στην εν λόγω απειλή.

Για την βαθύτερη κατανόηση των κυβερνοαπειλών καθορίζονται οι οικογένειες ομάδων δεικτών (IOCs – Indicators of Compromise). Ένας δείκτης είναι μια πληροφορία που σχετίζεται με ένα κακόβουλο συμβάν. Για παράδειγμα, ένας αναλυτής μπορεί να αντλήσει ένα δείκτη από κάποιο δείγμα κακόβουλου λογισμικού που βρίσκεται όταν απαντά σε ένα περιστατικό. Ένας δείκτης μπορεί να μην είναι απαραίτητα κακόβουλος, αλλά να σχετίζεται με τη χρήση ενός νόμιμου συστήματος, πόρου ή τεχνολογίας από έναν χρήστη («ηθοποιό») για την επίτευξη των στόχων του.

Οι Mavroeidis και Bromander (2017) κάνουν αναφορά για δύο μοντέλα που σχετίζονται με την ωριμότητα ανίχνευσης απειλών και την ανίχνευσή τους στον κυβερνοχώρο, αντίστοιχα. Τα δύο μοντέλα επικαλύπτονται αλλά το καθένα μπορεί να ικανοποιήσει διαφορετικές ανάγκες.



Όπως αναφέρθηκε και παραπάνω οι δείκτες νοημοσύνης καθορίζονται σε τέσσερις (4) κατηγορίες. Τους κακόβολους δείκτες (malicious indicators), τους δείκτες ύποπτων ενδείξεων (suspicious indicators), τους δείκτες μικρού ρίσκου για ένα περιβάλλον (low risk indicators) και τέλος τους δείκτες εκείνους για τους οποίους δεν έχει ανιχνευτεί καμία υποψία ρίσκου (legitimate indicator values).

Μέχρι στιγμής γίνεται συνεχώς αναφορά για τις απειλές στον κυβερνοχώρο και πόσο σημαντική είναι προστασία από αυτές. Έτσι, στην επόμενη ενότητα περιγράφουν οι τύποι των επιθέσεων που μπορεί να πραγματοποιηθούν στον κυβερνοχώρο.

1.6 Τύποι επιθέσεων (Types of attacks)

Σε αυτή την ενότητα γίνεται μια σύντομη περιγραφή των πιο συνηθισμένων τύπων επιθέσεων στον κυβερνοχώρο. Οι τύποι αυτοί περιλαμβάνουν τα κακόβουλα λογισμικά, τις μηδενικές ημέρες, το ηλεκτρονικό ψάρεμα, τους ιούς, τις εγχύσεις SQL, τις επιθέσεις μεταξύ των ιστότοπων (XSS) και τις προηγμένες απειλές (APT).

1.6.1 Κακόβουλο Λογισμικό (Malware)

Το κακόβουλο λογισμικό είναι ένας γενικός όρος που περιλαμβάνει κακόβουλο περιεχόμενο. Παράδειγμα κακόβουλου λογισμικού είναι αυτό που περιλαμβάνει ιούς, όπως trojans, spywares και άλλους επεμβατικούς κώδικες (Christodorescu et al., 2005). Τα κακόβουλα λογισμικά σχεδιάζονται για να βλάψουν τα συστήματα ηλεκτρονικών υπολογιστών χωρίς τη γνώση του ιδιοκτήτη χρησιμοποιώντας το ίδιο το σύστημα. Τα περισσότερα προγράμματα κακόβουλου λογισμικού είναι μεγάλα και σύνθετα και κανείς δεν μπορεί να καταλάβει κάθε λεπτομέρεια (Verma et al., 2013).

Ο στόχος του δημιουργού ενός κακόβουλου λογισμικού είναι να τροποποιήσει ή να μορφοποιήσει κακόβουλο λογισμικό για να αποφύγει την ανίχνευση από έναν ανιχνευτή κακόβουλου λογισμικού (malware detector) (Nachenberg, 1997; Christodorescu et al., 2005).

1.6.2 Εκμετάλλευση μηδενικής ημέρας (Zero Day Exploit)

Όταν υπάρχει κάποιο κενό ασφαλείας σε ένα λογισμικό, το οποίο δεν το γνωρίζει ο κατασκευαστής του, αναφέρεται ως ευαισθησία μηδενικής ημέρας (Zero Day Susceptibility). Στη συνέχεια, αυτή η ευαισθησία, δηλαδή το κενό ασφαλείας, χρησιμοποιείται από έναν εισβολέα (hacker) πριν προλάβει ο κατασκευαστής του να το εντοπίσει και να το διορθώσει. Αυτή η επίθεση ονομάζεται εκμετάλλευση της μηδενικής ημέρας (Vaisla & Saini, 2014). Το Zero Day προέρχεται από το γεγονός ότι ορισμένες ευπάθειες δεν είναι γνωστές μέχρι να ανακαλυφθούν και να δημοσιευτούν, δηλαδή υπάρχουν μηδέν ημέρες από τη δημοσίευση τους (ISACA, 2017).

1.6.3 Ηλεκτρονικό Ψάρεμα (Phishing)

Το ηλεκτρονικό ψάρεμα (phishing) γίνεται όλο και πιο απειλητικό για την ασφάλεια του Διαδικτύου σε όλους. Το ηλεκτρονικό ψάρεμα είναι ένα από τα πιο οργανωμένα εγκλήματα του 21ου αιώνα (Vayansky & Kumar, 2018). Οι περισσότεροι άνθρωποι θα έχουν κάποια προσωπική εμπειρία ηλεκτρονικού ψαρέματος επειδή, κάποια στιγμή, έλαβε ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι προέρχονται από τις τράπεζες και ενθαρρύνουν να συνδεθούν σε φαινομενικά πειστικές αλλά ψευδείς ιστοσελίδες για να δηλώσουν τα στοιχεία τους (Wall, 2018).

Στο ηλεκτρονικό ψάρεμα, οι επιτιθέμενοι χρησιμοποιούν μια αυτοματοποιημένη μορφή κοινωνικής μηχανικής (social engineering) στο Διαδίκτυο για να εξαγάγουν παραπλανητικά ευαίσθητες πληροφορίες από επιχειρήσεις και ιδιώτες, συχνά με την παραποίηση νόμιμων διαδικτυακών τόπων (Suman et al., 2014). Η κοινωνική μηχανική είναι η διαδικασία με την οποία ένα άτομο προσπαθεί να αποσπάσει πληροφορίες από ένα άλλο μέσω της χειραγώγησης. Πρόκειται για μια διαδικασία εξαπάτησης των ατόμων να αποκαλύψουν πρόσβαση ή εμπιστευτικές πληροφορίες, είμαι μια τεχνική πειθούς (Hasan et al., 2010).

Ο όρος ηλεκτρονικό ψάρεμα είναι ένας γενικός όρος και αφορά τη δημιουργία και τη χρήση ηλεκτρονικών μηνυμάτων (e-mails) και διαδικτυακών τόπων, που έχουν σχεδιαστεί από τους επιτιθέμενους για να φαίνεται ότι προέρχονται από γνωστές, νόμιμες και αξιόπιστες επιχειρήσεις, σε μια προσπάθεια να συγκεντρωθούν ευαίσθητες πληροφορίες.

Η ροή πληροφοριών σε μια επίθεση ηλεκτρονικού ψαρέματος είναι (Suman et al., 2014):

1. Από τον επιτιθέμενο «ψαρά» (“phisher”) αποστέλλεται ένα περιγραφικό μήνυμα στο χρήστη.
2. Ένας χρήστης παρέχει εμπιστευτικές πληροφορίες σε ένα διακομιστή ηλεκτρονικού ψαρέματος (phishing server).
3. Ο επιτιθέμενος αποκτά τις εμπιστευτικές πληροφορίες από το διακομιστή.
4. Οι εμπιστευτικές πληροφορίες χρησιμοποιούνται για την παραποίηση του χρήστη.
5. Ο επιτιθέμενος αποκτά παράνομο νομισματικό όφελος.

1.6.4 Viruses/Trojan

Η ιστορία του Δούρειου Ίππου (Trojan Horse), φημισμένη από τον ελληνικό επικό ποιητή Όμηρο στην Οδύσσεια. Ήταν ένα από τα πιο έξυπνα τεχνικά κόλπα στην ιστορία του ανθρώπινου είδους. Ο Edwards τον ονόμασε έτσι μετά την τεχνική κοινωνικής μηχανικής που χρησιμοποιούσαν οι Έλληνες. Αυτή η επίθεση είναι η πιο ισχυρή επίθεση, καθώς κανένα υλικό ή λογισμικό δεν μπορεί να την αποτρέψει (Hasan et al., 2010).

Η Kaspersky[1] ορίζει το Trojan Horse ή Trojan ως ένα τύπο κακόβουλου λογισμικού που συχνά συγκαλύπτεται ως νόμιμο λογισμικό. Οι Trojans μπορούν να χρησιμοποιηθούν από τους κυβερνοκλέφτες (cyber thieves) και τους απιτηθέμενους (hackers) που προσπαθούν να αποκτήσουν πρόσβαση στα συστήματα των χρηστών. Οι χρήστες συνήθως εξαπατούνται από κάποια μορφή κοινωνικής μηχανικής για τη φόρτωση και την εκτέλεση των Trojans στα συστήματά τους. Μόλις ενεργοποιηθούν, οι Trojans μπορούν να επιτρέψουν στους επιτιθέμενους να σας κατασκοπεύσουν, να κλέψουν τα ευαίσθητα δεδομένα και να αποκτήσουν πρόσβαση στην πίσω πόρτα (backdoor) του συστήματος. Αυτές οι ενέργειες μπορούν να περιλαμβάνουν τη διαγραφή, τον αποκλεισμό, την τροποποίηση και την αντιγραφή των δεδομένων και παράλληλα τη διαταραχή της απόδοσης των υπολογιστών ή των δικτύων των υπολογιστών.

Οι ιοί (viruses) είναι εκτελέσιμα προγράμματα κώδικα που έχουν μοναδική δυνατότητα αναπαραγωγής τους στο σύστημα του υπολογιστή και εξαπλώνονται γρήγορα από τον έναν υπολογιστή στον άλλο επηρεάζοντας τα αρχεία, τα έγγραφα και τα προγράμματα για να αλλάξουν την κανονική τους λειτουργία (Wanjala & Jacob, 2017).

1.6.5 Εγχύσεις SQL (SQL Injections)

Σήμερα, οι περισσότερες εφαρμογές του διαδικτύου χρησιμοποιούν σχεδιασμό τριών επιπέδων, δηλαδή μια παρουσίαση, μια επεξεργασία και μια βάση δεδομένων. Το επίπεδο παρουσίασης είναι η διεπαφή ιστού HTTP, το επίπεδο εφαρμογής υλοποιεί τη λειτουργικότητα του λογισμικού και η βάση δεδομένων διατηρεί τα δεδομένα δομημένα και απαντά σε αιτήματα από το επίπεδο εφαρμογής (Carstoiu & Carstoiu, 2010). Αξίζει να σημειωθεί ότι μεγάλες εταιρείες που αναπτύσσουν συστήματα διαχείρισης βάσεων δεδομένων βασισμένα σε SQL βασίζονται σε μεγάλο βαθμό στο υλικό για να εξασφαλίσουν την επιθυμητή απόδοση (Carstoiu et al., 2010).

[1] Kaspersky ,www.kaspersky.com

Η SQL Injection (έγχυση) είναι ένας τύπος επίθεσης κατά την οποία ο εισβολέας προσθέτει κώδικα «Δομημένης Γλώσσας Ερωτήματος» (“Structured Query Language” - SQL) σε ένα πλαίσιο εισαγωγής φόρμας ιστού για να αποκτήσει πρόσβαση ή να κάνει αλλαγές στα δεδομένα.

Η ευπάθεια SQL injection επιτρέπει σε έναν εισβολέα να εκτελεί εντολές απευθείας σε μια υποκείμενη βάση δεδομένων μιας εφαρμογής ιστού και να καταστρέφει τη λειτουργικότητα ή την εμπιστευτικότητα (Tajpour et al., 2011).

Οι Bizimana και Belkhouja (2017) αναφέρουν ότι η SQL Injection είναι ένας μηχανισμός επίθεσης στο διαδίκτυο στον οποίο μια κακόβουλη δήλωση SQL εισάγεται μέσω του τομέα δεδομένων εισόδου από τον πελάτη (client) στην εφαρμογή των δεδομένων.

1.6.6 XSS

Οι επιθέσεις μεταξύ των ιστότοπων (“Cross Site Scripting” - XSS) είναι εκείνες οι επιθέσεις στις εφαρμογές στις οποίες ένας εισβολέας παίρνει τον έλεγχο του προγράμματος περιήγησης (browser) ενός χρήστη για να εκτελέσει ένα κακόβουλο σενάριο (script), συνήθως ένα κώδικα HTML και JavaScript, μέσα στο κείμενο της της εφαρμογής του ιστού. Ως αποτέλεσμα, και αν ο ενσωματωμένος κώδικας εκτελεστεί με επιτυχία, ο εισβολέας μπορεί στη συνέχεια να έχει πρόσβαση, παθητικά ή ενεργά, σε κάθε ευαίσθητο πόρο του προγράμματος περιήγησης που σχετίζεται με την εφαρμογή του ιστού, όπως cookies, αναγνωριστικά περιόδου σύνδεσης (session IDs) και άλλα (Garcia-Alfaro & Navarro-Arribas, 2009).

1.6.7 APT

Οι προηγμένες απειλές (“Advanced Persistent Threat” – APT) είναι μια κατηγορία εγκληματικότητας στον κυβερνοχώρο που απευθύνεται σε επιχειρηματικούς και πολιτικούς στόχους. Οι APT απαιτούν υψηλό βαθμό μυστικότητας για παρατεταμένη διάρκεια λειτουργίας, προκειμένου να είναι επιτυχείς. Οι στόχοι επίθεσης συνήθως υπερβαίνουν το άμεσο οικονομικό όφελος και τα συμβιβασμένα συστήματα εξακολουθούν να λειτουργούν ακόμη και μετά την παραβίαση βασικών συστημάτων και την επίτευξη των αρχικών στόχων (Ghafir & Prenosil, 2014).

Ένα APT είναι ένας τύπος στοχοθετημένης επίθεσης. Οι στοχευμένες επιθέσεις χρησιμοποιούν μια μεγάλη ποικιλία τεχνικών, συμπεριλαμβανομένων των λήψεων με κίνηση από το κινητό, των SQL injection, των κακόβουλων λογισμικών (malware), των

λογισμικών υποκλοπής (spyware), του ηλεκτρονικού ψαρέματος (phishing) και του ανεπιθύμητου περιεχομένου (spam) και άλλα. Τα APT μπορούν και συχνά χρησιμοποιούν πολλές από αυτές τις ίδιες τεχνικές (Symantec, 2011).

Για να γίνουν πιο κατανοητοί οι τύποι όλων αυτών των επιθέσεων στην επόμενη ενότητα γίνονται αναφορά σε δύο ιστορικά παραδείγματα εγκληματικών ενεργειών στων κυβερνοχώρο.

1.7 Τι είναι το εργαλείο MISP

Η πλατφόρμα κοινής χρήσης απειλών MISP[2] ("Malware Information Sharing Platform") (www.misp-project.org) είναι ένα δωρεάν λογισμικό ανοιχτού κώδικα (open source) που βοηθά στην ανταλλαγή πληροφοριών σχετικά με την απειλή των πληροφοριών, συμπεριλαμβανομένων των δεικτών ασφάλειας στον κυβερνοχώρο. Ουσιαστικά, πρόκειται για μια πλατφόρμα με πληροφορίες απειλών για τη συγκέντρωση, την ανταλλαγή, την αποθήκευση και τη συσχέτιση των δεικτών συμβιβασμού στοχοθετημένων επιθέσεων, την απειλή νοημοσύνης (threat intelligence), πληροφοριών για οικονομικές απάτες, πληροφοριών για τρωτότητα ή ακόμη και για την καταπολέμηση της τρομοκρατίας.

Εικόνα 1: Λογότυπο MISP

Το MISP αναπτύσσεται ως ελεύθερο λογισμικό από μια ομάδα προγραμματιστών από το CIRCL[3], αλλά και από τη βελγική άμυνα (Belgian Defence) και το NATO/NCIRC ("Computer Response Capability Capability").

[2] MISP, https://www.misp-project.org/

[3] CIRC, https://www.circl.lu/services/misp-malware-information-sharing-platform/

1.7.1 Ποιος είναι ο σκοπός του MISP

Το MISP επιτρέπει στους οργανισμούς να ανταλλάσσουν πληροφορίες σχετικά με το κακόβουλο λογισμικό και τους δείκτες. Οι χρήστες του MISP μπορούν να επωφεληθούν από τις συνεργατικές γνώσεις σχετικά με υπάρχοντα κακόβουλα προγράμματα ή απειλές. Έτσι σκοπός του MISP είναι να συμβάλει στη βελτίωση των αντιμέτρων που χρησιμοποιούνται κατά των στοχοθετημένων επιθέσεων και της δημιουργίας προληπτικών ενεργειών και ανίχνευσης[4].

Οι στόχοι της πλατφόρμας MISP είναι να διευκολύνει την αποθήκευση τεχνικών και μη τεχνικών πληροφοριών σχετικά με το κακόβουλο λογισμικό και τις επιθέσεις, να δημιουργήσει αυτόματα τις σχέσεις μεταξύ κακόβουλου λογισμικού και των χαρακτηριστικών του, παράλληλα να αποθηκεύει τα δεδομένα με δομημένη μορφή, ώστε να επιτρέπεται η αυτοματοποιημένη χρήση της βάσης δεδομένων για την τροφοδοσία συστημάτων ανίχνευσης (detection systems) ή εγκληματολογικών εργαλείων (forensic tools).

Παράλληλα, στόχο του MISP αποτελεί η δημιουργία κανόνων για το σύστημα ανίχνευσης εισβολής στο δίκτυο (“Network Intrusion Detection System ” - NIDS) που μπορούν να εισαχθούν σε συστήματα IDS, όπως για παράδειγμα οι διευθύνσεις IP, ονόματα τομέων (domain names), χτύπημα κακόβουλων αρχείων (malicious files), μοτίβο στη μνήμη (pattern in memory) και άλλα.

1.7.2 Τι δυνατότητες έχει το MISP

Με το εργαλείο MISP δίνεται η δυνατότητα να δημιουργηθεί μια πλατφόρμα αξιόπιστων πληροφοριών από αξιόπιστους συνεργάτες και μπορεί να γίνει ο διαμοιρασμός των χαρακτηριστικών κακόβουλου λογισμικού και απειλών με άλλα μέρη και άλλες ομάδες εμπιστοσύνης.

Κάθε συμμετέχον μέλος στο MISP μπορεί να παράγει, να ενισχύει ή να καταναλώνει πληροφορίες και να παρέχει πληροφορίες σχετικά με πληροφορίες που παράγονται από άλλους. Τεμάχια πληροφοριών μπορούν να μεταφερθούν κατά μήκος πολλαπλών κόμβων μεταξύ εταίρων. Έτσι, η ποιότητα των δεδομένων και η εμπιστοσύνη της πηγής δεδομένων δεν είναι πάντα βέβαιη. Για να παράσχουν ένα μέτρο αξιοπιστίας και αξιοπιστίας στους προμηθευτές δεδομένων, εφαρμόζονται ορισμένα μοντέλα

[4]CIRC, https://www.circl.lu/services/misp-malware-information-sharing-platform/

αλληλεπίδρασης δεδομένων, όπως οι ταξινομίες. Περισσότερα στοιχεία σχετικά με τις ταξινομίες δίνονται στη συνέχεια.

Παράλληλα, δίνει τη δυνατότητα στο χρήστη να αποθηκεύσει τις πληροφορίες του από άλλες περιπτώσεις τοπικά, έτσι ώστε να εξασφαλιστεί η εμπιστευτικότητα των ερωτημάτων. Υπάρχουν τέσσερις επιλογές σχετικά με τη διανομή και το διαμοιρασμό συμβάντων και τα αντίστοιχα χαρακτηριστικά τους, αυτές οι επιλογές περιλαμβάνουν μόνο τον οργανισμό, μόνο την κοινότητα, τις συνδεδεμένες κοινότητες ή και όλες τις κοινότητες.

Τα δεδομένα που αποθηκεύονται είναι άμεσα διαθέσιμα στους συναδέλφους και στους συνεργάτες, αποθηκεύοντας το αναγνωριστικό συμβάντος (Event IS) στο σύστημα έκδοσης ή με ενημέρωση από τις υπογεγραμμένες και κρυπτογραφημένες ειδοποιήσεις ηλεκτρονικού ταχυδρομείου.

Επίσης, τα δεδομένα που αποθηκεύονται στο MISP μπορούν να συνεργαστούν με την ανταλλαγή δεδομένων από άλλες πλατφόρμες. Συγκεκριμένα επιτρέπει την αυτόματη εισαγωγή των δεδομένων στα συστήματα ανίχνευσης με αποτέλεσμα την καλύτερη και ταχύτερη ανίχνευση των εισβολών.

Όταν προστεθούν νέα δεδομένα, το MISP θα παρουσιάσει αμέσως σχέσεις με άλλα σχετικά στοιχεία και δείκτες. Αυτό έχει ως αποτέλεσμα πιο αποτελεσματική ανάλυση, αλλά επιτρέπει επίσης μια καλύτερη εικόνα για τις τακτικές, τις τεχνικές και τις διαδικασίες, των σχετικών εκστρατειών και της ανάθεσης.

Η λειτουργία συζήτησης θα επιτρέψει επίσης συνομιλίες μεταξύ πολλαπλών αναλυτών.

Περισσότερες λεπτομέρειες σχετικά με το εργαλείο MISP και τις δυνατότητες του θα δοθούν στα τελευταία κεφάλαια αφού εξηγηθούν οι έννοιες γύρω από την κυβερνοάμυνα, ώστε να γίνει πιο κατανοητή η λειτουργία του.

1.8 Ιστορικό εγκλημάτιών στον κυβερνοχώρο

Στην ενότητα αυτή αναφέρονται δύο από τις σημαντικότερες εγκληματικές ενέργειες που συνέβησαν στην ιστορία του κυβερνοχώρου. Συγκεκριμένη γίνεται αναφορά στα κακόβουλα λογισμικά Stuxnet και Zeus (ή Zbot).

1.8.1 Stuxnet

Το Stuxnet ήταν ένα κακόβουλο λογισμικό (malware) που ανακαλύφθηκε για πρώτη φορά το 2010 σε έναν ιρανικό υπολογιστή. Σχεδιάστηκε ειδικά για να σαμποτάρει φυγοκεντρητές (centrifuges) στην ιρανική πυρηνική εγκατάσταση του Natanz.

Η ανακάλυψη του Stuxnet αύξησε την ευαισθητοποίηση σχετικά με θέματα ασφάλειας του κυβερνοχώρου για κρίσιμες υποδομές σε όλο τον κόσμο (Baezner & Robin, 2018).

Σύμφωνα με την τεχνική έκθεση της Symantec "W32.Stuxnet Dossier" (2011) ένα από τα κύρια στοιχεία που έκανε το Stuxnet να ξεχωρίσει είναι η διαφορά μεταξύ του σταγονόμετρου (dropper) και του ωφέλιμου φορτίου (payload). Το dropper στόχευε στο λειτουργικό σύστημα Microsoft Windows, ενώ το payload στόχευε τα βιομηχανικά συστήματα ελέγχου (Industrial Control Systems - ICS). Σε αντίθεση με τα περισσότερα κακόβουλα προγράμματα, το Stuxnet δεν έβλαψε το σύστημα που στόχευσε το dropper, ενώ το payload στοχεύει και καταστρέφει άλλο τύπο συστήματος. Η πολυπλοκότητα αυτού του κακόβουλου λογισμικού περιελάμβανε εκμεταλλεύσεις μηδενικών ημερών, των ριζικών πακέτων (rootkit) των Windows, των προγραμματιζόμενων ριζικών πακέτων λογικών ελεγκτών, τις τεχνικές αποφυγής των ιών, σύνθετη διαδικασία έγχυσης (injection) και κώδικα αγκίστρωσης (hooking code), ρουτίνες μόλυνση του δικτύου, ενημερώσεις και μια διασύνδεση εντολών και ελέγχου (command and control, C&C).

Το Stuxnet χρησιμοποίησε διάφορες μεθόδους για την αυτοδιάθεση του, συμπεριλαμβανομένων πολλών εκμεταλλεύσεων, όπως αυτοαναδιπλασιασμό μέσω αφαιρούμενων δίσκων, διάδοση στο τοπικό δίκτυο (LAN), διάδοση μέσω SMB (πρωτόκολλο δικτυού του επιπέδου εφαρμογής για την κοινή πρόσβαση αρχείων, εκτυπωτών και άλλων σειριακών θυρών) και την αντιγραφή και την αποστολή σε απομακρυσμένους υπολογιστές μέσω κοινόχρηστων δικτύων και απομακρυσμένων υπολογιστών που εκτελούν WinCC DB server.

Κατά τη μόλυνση, η Stuxnet ανιχνεύει ένα συγκεκριμένο αρχείο SCADA, δηλαδή το PLC της Siemens. Εάν δεν εντοπίσει το συγκεκριμένο PLC που υπάρχει στο σύστημα, δεν βλάπτει το σύστημα. Ωστόσο, όταν ταιριάζει το αρχείο, το payload κακόβουλου λογισμικού θα εμφανιστεί. Ουσιαστικά, το Stuxnet κατασκόπευε πρώτα τις λειτουργίες του συστήματος και τη συλλογή των πληροφοριών. Στη συνέχεια, χρησιμοποιούσε τις συγκεντρωμένες πληροφορίες για να πάρει τον έλεγχο του PLC που ελέγχει τους φυγοκεντρητές, κάνοντάς τους να δυσλειτουργούν αλλάζοντας ελαφρώς την ταχύτητα των λειτουργιών, έτσι ώστε να αποτύχουν. Το κακόβουλο λογισμικό διεξήχθη ως επίθεση, παρέχοντας ψεύτικα δεδομένα στους εξωτερικούς ελεγκτές, εξασφαλίζοντας λανθασμένες μετρήσεις και αποφεύγοντας την ανίχνευση του σαμποτάζ. Ένα από τα χαρακτηριστικά που κάνει το Stuxnet ενδιαφέρον στο πλαίσιο της κυβερνητικής κατασκοπείας είναι η στρατηγική της επίθεσης.

Η επίθεση ήταν πράγματι στοχοθετημένη, αλλά οι επιτιθέμενοι διέδιδαν το κακόβουλο λογισμικό στο διαδίκτυο και ήλπιζαν ότι θα φθάσουν τελικά στο στόχο και θα το ενεργοποιήσουν (Wangen, 2015).

1.8.2 Zeus

Το Zeus, επίσης γνωστός ως Zbot, είναι ένα πακέτο κακόβουλου λογισμικού το οποίο είναι άμεσα διαθέσιμο προς πώληση και επίσης διατίθεται σε υπόγεια φόρουμ. Το πακέτο περιέχει έναν οικοδόμο που μπορεί να δημιουργήσει ένα εκτελέσιμο αρχείο bot και αρχεία διακομιστή Web (PHP, εικόνες, SQL πρότυπα) για χρήση ως διακομιστής εντολών και ελέγχου (C&C). Ενώ το Zeus είναι μια γενική πίσω πόρτα που επιτρέπει τον πλήρη έλεγχο από έναν μη εξουσιοδοτημένο απομακρυσμένο χρήστη, η κύρια λειτουργία του είναι το οικονομικό κέρδος κλέβοντας διαπιστευτήρια στο διαδίκτυο, όπως FTP, ηλεκτρονικό ταχυδρομείο, διαδικτυακή τραπεζική (online banking) και άλλους ηλεκτρονικούς κωδικούς πρόσβασης (Falliere & Chien, 2009).

Το Zeus υπήρξε τουλάχιστον από το 2007, αλλά με την πάροδο του χρόνου μέχρι το 2009 εξελίχθηκε. Πιθανότατα προέρχεται από τη Ρωσία ή από ρωσόφωνες χώρες, η άποψη αυτή στηρίζεται στο γεγονός ότι αρχικά βοηθητικά αρχεία και άλλα αρχεία στο πακέτο είχαν γραφτεί στα ρωσικά. Από το 2007 μέχρι το 2009 η ενημέρωση του πακέτου ήταν συνεχής, και είχε κερδίσει τη φήμη του στα υπόγεια φόρουμ ως ένα επιτυχημένο μέσο για την απόκτηση διαδικτυακών διαπιστευτηρίων. Το Zeus είναι ένα πακέτο botnet που μπορεί να αγοραστεί για μόλις 700 δολάρια και μπορεί επίσης να βρεθεί ελεύθερα (Falliere & Chien, 2009).

Το ερώτημα που προκύπτει από τον προσδιορισμό όλων αυτών των διαφορετικών τύπων επιθέσεων είναι με ποιο τρόπο μπορεί κανείς να προστατευτεί από όλες αυτές τις περιπτώσεις και πως μπορεί να αμυνθεί σε μια επίθεση. Για να απαντηθεί αυτό το ερώτημα στην ακόλουθη ενότητα περιγράφεται η ενεργή κυνβερνοάμυνα και τρόποι με τους οποίους μπορεί να εφαρμοστεί.

1.9 Ενεργή κυβερνοάμυνα (Active Cyber Defence)

Η ενεργή κυβερνοάμυνα (“Active Cyber Defence” - ACD) είναι ένας τρόπος που υιοθετείται από διάφορους διεθνείς παράγοντες. Η ACD είναι μια ιδέα που βασίζεται στην ανάπτυξη εργαλείων όχι μόνο για τον εντοπισμό και τον τερματισμό των συμπτωμάτων του κυβερνοχώρου καθώς συμβαίνουν, αλλά και για τη λήψη επιθετικών μέτρων για την ελαχιστοποίηση των δυνατοτήτων των εισβολέων. Αυτό μπορεί να

επιτευχθεί μέσω μιας ποικιλίας τεχνικών λύσεων, όπως η ανάπτυξη κραδασμών (deploying decoys) ή η επίθεση (hacking) των δικτύων των επιτιθέμενων για την εξουδετέρωση των προσπαθειών τους (Dewar, 2017).

Παρά την ύπαρξη αυτών των εργαλείων και παρά την επικράτηση στα μέσα μαζικής ενημέρωσης και στις εθνικές και διεθνείς οργανωτικές δηλώσεις, η ACD στερείται εννοιολογικού ορισμού (Dewar, 2017; Galinec et al., 2017).

Το Υπουργείο Άμυνας ("Department of Defence" - DoD) των Ηνωμένων Πολιτειών (US) (2011) όρισε το ACD ως συγχρονισμένη, η οποία σε πραγματικό χρόνο καλύπτει, ανιχνεύει, αναλύει και μετριάζει τις απειλές και τα τρωτά σημεία.

Η ενεργή κυβερνοάμυνα περιλαμβάνει τον έλεγχο τρωτότητας, τον έλεγχο των κανόνων και πολιτικών ασφαλείας, τα εργαλεία honeypots, τα πλαίσια ανταλλαγής πληροφοριών, την αντιμετώπιση περιστατικών και τα μεγάλα δεδομένα σε συνδυασμό με την τεχνητή νοημοσύνη. Όλοι αυτοί οι μηχανισμοί αναλύονται στις ακόλουθες υποενότητες.

1.9.1 Έλεγχος Τρωτότητας (Penetration Testing)

Ο έλεγχος τρωτότητας (Penetration Testing) είναι μια ολοκληρωμένη μέθοδος για τη δοκιμή της πλήρους, ολοκληρωμένης, λειτουργικής και αξιόπιστης βάσης υπολογιστών που αποτελείται από υλικό, λογισμικό και άτομα (McGraw, 2004). Η διαδικασία περιλαμβάνει μια ενεργή ανάλυση του συστήματος για τυχόν αδυναμίες, συμπεριλαμβανομένης της κακής ή ακατάλληλης διαμόρφωσης του συστήματος, ελαττωμάτων υλικού και λογισμικού και λειτουργικών αδυναμιών στη διαδικασία ή τεχνικών αντιμέτρων (Bacudio et al., 2011).

Με πιο απλά λόγια ο έλεγχος τρωτότητας είναι ένας τύπος δοκιμών ασφαλείας που χρησιμοποιείται για τη δοκιμή της ασφάλειας μιας εφαρμογής. Διεξάγεται για να εντοπίσει τον κίνδυνο ασφαλείας που μπορεί να υπάρχει στο σύστημα. Εάν ένα σύστημα δεν είναι ασφαλές, τότε οποιοσδήποτε εισβολέας μπορεί να διακόψει ή να λάβει εξουσιοδοτημένη πρόσβαση στο σύστημα. Ο κίνδυνος ασφαλείας είναι συνήθως ένα τυχαίο λάθος που εμφανίζεται κατά την ανάπτυξη και εφαρμογή του λογισμικού (Tutorial Point, 2018).

Οι έλεγχοι τρωτότητας συνήθως εκτελούνται χρησιμοποιώντας μη αυτόματες ή αυτοματοποιημένες τεχνολογίες ή και τις δύο μαζί για τη συστηματική καταστολή των διακομιστών, των τελικών σημείων, των εφαρμογών ιστού, των ασύρματων δικτύων, των συσκευών δικτύου, των κινητών συσκευών και άλλων πιθανών σημείων έκθεσης (Bacudio et al., 2011).

1.9.2 Έλεγχος κανόνων & πολιτικές (Rules auditing & policies)

Η ανάπτυξη πολιτικών ασφάλειας εταιρικών πληροφοριών (“Information Security Policies” - ISP) αποτελεί βασική πηγή των πρακτικών διαχείρισης για την ασφάλεια του συστήματος πληροφοριών (“Information System Security” - ISS) (Chan et al., 2005). Ένας ISP μπορεί να οριστεί ευρέως ως δηλώσεις από έναν οργανισμό που παρέχει καθοδήγηση σχετικά με τις ευθύνες, τους κανόνες και τις κατευθυντήριες γραμμές που σχετίζονται με το ISS, οι οποίες καθορίζουν τον τρόπο με τον οποίο χρησιμοποιούνται σωστά και με ασφαλή τρόπο οι πόροι του συστήματος πληροφοριών (D’Arcy et al., 2009).

1.9.3 Honeypots

Το 2002, ο Spitzner καθόρισε το honeypot ως έναν πόρο ασφαλείας, του οποίου η αξία έγκειται στην ανίχνευση, επίθεση ή συμβιβασμό. Επιπλέον, τα honeypots δεν παρέχουν καμία λύση σε κανένα πρόβλημα, ούτε διορθώνουν τίποτα, είναι απλά ένα εργαλείο. Εξαρτάται από τον χρήστη πώς και με ποιο τρόπο θα το χρησιμοποιήσει αυτό το εργαλείο είτε για καλό είτε για κακό.

Υπάρχουν δύο τύποι honeypots, τα ερευνητικά (research) τα οποία αναλύουν τα περιστατικά για να εντοπίσουν τους δράστες και να μελετήσουν μεθόδους και εργαλεία επίθεσης και της παραγωγής (production), τα οποία εντοπίζουν κακόβουλη δραστηριότητα και παράγουν ειδοποιήσεις αλλά πραγματοποιούν περιορισμένες αναλύσεις για την απόδοση.

Ως τεχνική, τα honeypots έχουν το πλεονέκτημα ότι μπορούν να αναπτυχθούν σε μια ποικιλία περιβαλλόντων και καταστάσεων δικτύου τόσο με προληπτικό όσο και με αντιδραστικό τρόπο. Δηλαδή, όχι μόνο μπορούν να αναπτυχθούν πριν από ένα περιστατικό, προκειμένου να προστατευθούν γνήσια δεδομένα και περιουσιακά στοιχεία από τη διείσδυση ή τη διαφθορά, τα honeypots μπορούν να αναπτυχθούν μόλις συμβεί ένα περιστατικό επίθεσης (Dewar, 2017).

1.9.4 Πλαίσια ανταλλαγής πληροφοριών

Έχει υπογραμμιστεί σε διάφορες διεθνείς εκθέσεις ότι η ανταλλαγή πληροφοριών σχετικά με τις απειλές για την ασφάλεια στον κυβερνοχώρο έχει γίνει ιδιαίτερα κρίσιμη, ενισχύοντας την ανάγκη για περισσότερη διασυνοριακή συνεργασία, άτομα και οργανισμούς. Η ανταλλαγή πληροφοριών (information sharing) αποτελεί βασικό παράγοντα για τη βελτίωση της ασφάλειας, αλλά απαιτείται συνεπής προσέγγιση

(ENISA, 2015). Η ανταλλαγή πληροφοριών περιγράφει ένα μέσο διαβίβασης πληροφοριών ή εμπειρίας από ένα αξιόπιστο μέρος σε ένα άλλο (Goodwin & Nicholas, 2015).

Όλες οι πρωτοβουλίες ανταλλαγής πληροφοριών έχουν τον κοινό στόχο να βελτιώσουν την πρόληψη, την ανίχνευση, την πρόβλεψη, την ανταπόκριση και την ανάκαμψη περιστατικών στον κυβερνοχώρο. Η ανταλλαγή δεδομένων μπορεί να γίνει για να επιτευχθούν διαφορετικοί στόχοι, όπως καλύτερες καινοτομίες στον τομέα της πληροφορικής και μεθοδολογίες χειρισμού περιστατικών μεταξύ των εταίρων που μοιράζονται, καθώς και βελτίωση της ασφάλειας των εργαλείων παρακολούθησης δικτύου και συστήματος (CIRCL, 2016).

Στις πλατφόρμες ανταλλαγής πληροφοριών κάθε κομμάτι δεδομένων μπορεί να μοιραστεί. Ωστόσο, οι πιο συνηθισμένοι τύποι κοινών δεδομένων είναι αναφορές συμβάντων ή ειδοποιήσεων ασφαλείας, δείκτες συμβιβασμού ("Indicators of Compromise" - IoC), ανεπεξέργαστα δεδομένα και εργαλεία. Τα ακατέργαστα δεδομένα συνήθως ανταλλάσσονται μεταξύ των συστημάτων ανίχνευσης εισβολής. Τα δεδομένα συμβάντων (events) συνήθως περιέχουν όλες τις πληροφορίες που σχετίζονται με ένα περιστατικό ασφάλειας, συμπεριλαμβανομένων ευαίσθητων πληροφοριών, οι οποίες δεν μπορούν να μοιραστούν εύκολα. Τα συμβάντα ασφαλείας περιλαμβάνουν μη ευαίσθητα μεταδεδομένα που σχετίζονται με ένα περιστατικά. Οι δείκτες συμβιβασμού είναι αντικείμενα που βρέθηκαν σε ένα σύστημα ή στην κυκλοφορία δικτύου που δείχνουν μια εισβολή. Οι δείκτες συμβιβασμού και τα συμβάντα είναι συχνά εναλλάξιμα. Τέλος, τα εργαλεία ενδέχεται επίσης να αποτελούν αντικείμενο κοινής χρήσης, αλλά αυτά συνήθως δεν περιέχουν πληροφορίες εκτός από τους πηγαίους κώδικες ή τα δυαδικά αρχεία (Stupka et al., 2017).

Υπάρχουν πολλές πλατφόρμες ανταλλαγής πληροφοριών, ένας κατάλογος πλατφορμών παρέχεται από τον ENISA (2014). Μία από τις πιο γνωστές πλατφόρμες ανταλλαγής πληροφοριών είναι το MISP, το οποίο περιγράφεται στην αρχή αυτής της εργασίας και επικεντρώνεται στην ανταλλαγή δεικτών συμβιβασμού που προέρχονται από κακόβουλο λογισμικό.

1.9.5 Αντιμετώπιση περιστατικών (Incident response)

Η αντιμετώπιση περιστατικών ("Incident response" - IR) είναι μια διαδικασία αντιμετώπισης και διαχείρισης ενός περιστατικού, όπως για παράδειγμα, επιθέσεις στο κυβερνοχώρο (Kasperky Lab, 2018).

Κατά την εκτέλεση επιθέσεων στον κυβερνοχώρο, ο εισβολέας ακολουθεί μια δομημένη σειρά ενεργειών. Ένα από τα μοντέλα που περιγράφουν αυτό το σύνολο ενεργειών είναι το μοντέλο αλυσίδας θανάτου (kill chain). Μια ομάδα ασφάλειας γνωρίζοντας την αλυσίδα ενεργειών, δηλαδή τις ενέργειες ενός εισβολέα στον κυβερνοχώρο μπορεί να δημιουργήσει μια αμυντική στρατηγική κατά των απειλών στον κυβερνοχώρο. Για να αντιμετωπιστεί επιτυχώς μια απειλή, η ομάδα ασφάλειας πρέπει να βασίσει την αμυντική στρατηγική σε πληροφορίες σχετικά με την ακολουθία των ενεργειών του εισβολέα (Kasperky Lab, 2018).

Οι κύριοι στόχοι της αντιμετώπισης περιστατικών είναι να ελαχιστοποιηθεί η ζημιά από την επίθεση, να ελαχιστοποιηθεί ο χρόνος ανάκτησης από την επίθεση και να δημιουργηθούν οδηγίες και αμυντικά μέτρα, τα οποία θα εμποδίσουν τέτοιες επιθέσεις στο μέλλον.

Η διαδικασία αντιμετώπισης περιστατικών αρχίζει με τη διερεύνηση του συμβάντος ασφαλείας. Όταν η ομάδα ασφάλειας διερευνά ένα περιστατικό, πρέπει να καθορίσει τον φορέα της επίθεσης, δηλαδή τα μέσα με τα οποία ο εισβολέας για να παραδώσει το ωφέλιμο φορτίο, το φορτίο και την εκμετάλλευση, δηλαδή, το κακόβουλο λογισμικό και άλλα εργαλεία που χρησιμοποιεί ο εισβολέας, το στόχος της επίθεσης, δηλαδή, τα δίκτυα, τα συστήματα και τα δεδομένα που επηρεάζονται από την επίθεση, τις ζημιές που προκλήθηκαν, δηλαδή το μέγεθος της βλάβης και της φήμης που προκάλεσε η επίθεση, την κατάσταση της επίθεσης, δηλαδή το σημερινό στάδιο του κύκλου ζωής της επίθεσης, αν ο επιτιθέμενος ήταν σε θέση να εκτελέσει ενέργειες για την επίτευξη στόχων και αν ο επιτιθέμενος έφτανε στους στόχους επίθεσης, και τέλος το χρονοδιάγραμμα επίθεσης, δηλαδή, όταν η επίθεση ξεκίνησε και έληξε, όταν εντοπίστηκε και όταν η ομάδα ασφαλείας μπόρεσε να αντιδράσει στην επίθεση (Kasperky Lab, 2018).

Όταν ολοκληρωθεί η έρευνα, η ομάδα ασφάλειας πρέπει να χρησιμοποιήσει τις πληροφορίες που έχει λάβει για να ανακτήσει τα στοχευμένα συστήματα και να ενημερώσει τις πολιτικές ασφαλείας και το σχέδιο αντιμετώπισης απειλών (IR plan). Η διαδικασία αντιμετώπισης περιστατικών περιλαμβάνει την προετοιμασία, την ταυτοποίηση, τον περιορισμό, την εξάλειψη, την ανάκτηση και τα διδάγματα (Kasperky Lab, 2018).

1.9.6 Μεγάλα δεδομένα & Τεχνητή νοημοσύνη

Ως ένας από τους πιο καινούριους όρους στην αγορά σήμερα, δεν υπάρχει συναίνεση ως προς τον τρόπο καθορισμού μεγάλων δεδομένων (big data). Ο όρος χρησιμοποιείται συχνά συνώνυμα με την έννοια Business Intelligence (BI) και την εξόρυξη δεδομένων (data mining). Είναι αλήθεια ότι και οι τρεις όροι αφορούν την ανάλυση δεδομένων και, σε πολλές περιπτώσεις, τα προηγμένα αναλυτικά στοιχεία. Όμως, η έννοια των μεγάλων δεδομένων είναι διαφορετική από τις δύο άλλες όταν οι όγκοι δεδομένων, ο αριθμός των συναλλαγών και ο αριθμός των πηγών δεδομένων είναι τόσο μεγάλος και πολύπλοκος που απαιτούν ειδικές μεθόδους και τεχνολογίες για να αντλήσουν πληροφορίες από δεδομένα (Su, 2017).

Τα μεγάλα δεδομένα αναφέρονται σε μεγάλα σύνολα σύνθετων δεδομένων, δομημένων και μη δομημένων, των οποίων οι παραδοσιακές τεχνικές επεξεργασίας και οι αλγόριθμοι δεν είναι σε θέση να λειτουργήσουν (Taylor-Sakyi, 2016). Αναλυτικότερα, τα μεγάλα δεδομένα αποτελούν μια μεθοδολογία ανάλυσης δεδομένων που επιτρέπει την πρόσφατη πρόοδο σε τεχνολογίες που υποστηρίζουν τη συλλογή, την αποθήκευση και την ανάλυση δεδομένων υψηλής ταχύτητας. Οι πηγές δεδομένων επεκτείνονται πέρα από την παραδοσιακή εταιρική βάση δεδομένων, ώστε να συμπεριλαμβάνουν τα μηνύματα ηλεκτρονικού ταχυδρομείου, τις εξόδους των κινητών συσκευών και τα δεδομένα που παράγονται από τους αισθητήρες, όπου τα δεδομένα δεν περιορίζονται πλέον σε δομημένες εγγραφές βάσεων δεδομένων, αλλά σε μη δομημένα δεδομένα χωρίς τυπική μορφοποίηση (Villars, Olofson & Eastwood, 2011).

Γενικά, τα μεγάλα δεδομένα μπορούν να εφαρμοστούν για την ανίχνευση απάτης σε πραγματικό χρόνο, την ανταγωνιστική ανάλυση, τη βελτιστοποίηση του τηλεφωνικού κέντρου, την έξυπνη διαχείριση κυκλοφορίας και διαχείριση έξυπνων δικτύων ηλεκτρικής ενέργειας, για να αναφέρουμε μόνο μερικές εφαρμογές. Με τα σωστά αναλυτικά στοιχεία, τα μεγάλα δεδομένα μπορούν να αποδώσουν πλουσιότερη εικόνα αφού αντλούν από πολλαπλές πηγές και συναλλαγές για να αποκαλύψουν κρυμμένα μοτίβα και σχέσεις (Ingram Micro, 2017).

Τα μεγάλα δεδομένα μπορούν να χρησιμοποιηθούν αποτελεσματικά στους διάφορους τομείς της τεχνολογία της πληροφορίας, προκειμένου να βελτιωθεί η ασφάλεια και η αντιμετώπιση προβλημάτων αναλύοντας τα πρότυπα στα υπάρχοντα αρχεία καταγραφής (Ularu, 2012).

Οι τεχνικές που χρησιμοποιούνται για την ανίχνευση απάτης εμπίπτουν σε δύο βασικές κατηγορίες: στατιστικές τεχνικές και τεχνητή νοημοσύνη (Artificial intelligence) (Bajpai et al., 2018).

Παραδείγματα τεχνικών ανάλυσης στατιστικών δεδομένων είναι:

1. Τεχνικές προεπεξεργασίας δεδομένων για ανίχνευση, επικύρωση, διόρθωση σφαλμάτων και συμπλήρωση ελλιπών ή λανθασμένων δεδομένων.
2. Υπολογισμός διαφόρων στατιστικών παραμέτρων, όπως μέσοι όροι, πεντάδες, μετρήσεις απόδοσης, κατανομές πιθανοτήτων και άλλα.
3. Μοντέλα και κατανομές πιθανοτήτων διαφόρων επιχειρηματικών δραστηριοτήτων είτε από πλευράς διαφόρων παραμέτρων είτε από κατανομές πιθανοτήτων.
4. Υπολογισμός προφίλ χρηστών.
5. Ανάλυση χρονικών σειρών δεδομένων που εξαρτώνται από το χρόνο.
6. Ομαδοποίηση και ταξινόμηση για την εύρεση σχεδίων και συσχετισμών μεταξύ ομάδων δεδομένων.
7. Αντιστοίχιση αλγορίθμων για την ανίχνευση ανωμαλιών στη συμπεριφορά των συναλλαγών ή των χρηστών σε σύγκριση με προγενέστερα γνωστά μοντέλα και προφίλ. Απαιτούνται επίσης τεχνικές για την εξάλειψη των ψευδών συναγερμών, την εκτίμηση των κινδύνων και την πρόβλεψη του μέλλοντος των τρεχουσών συναλλαγών ή των χρηστών. Η διαχείριση της απάτης είναι μια δραστηριότητα που βασίζεται στη γνώση.

Οι κύριες τεχνικές τεχνητής νοημοσύνης (Artificial Intelligence) που χρησιμοποιούνται για τη διαχείριση της απάτης περιλαμβάνουν (Bajpai et al., 2018):

1. Εξόρυξη δεδομένων για την ταξινόμηση, τη σύμπλεξη και την ταξινόμηση των δεδομένων και την εύρεση αυτόματων συσχετίσεων και κανόνων στα δεδομένα που μπορεί να σημαίνουν ενδιαφέροντα πρότυπα, συμπεριλαμβανομένων εκείνων που σχετίζονται με την απάτη.
2. Συστήματα εμπειρογνωμόνων για την κωδικοποίηση εμπειρογνωμοσύνης για την ανίχνευση της απάτης με τη μορφή κανόνων.
3. Αναγνώριση μοτίβων για την ανίχνευση κατά προσέγγιση κατηγοριών, συμπλεγμάτων ή μοτίβων ύποπτης συμπεριφοράς είτε αυτόματα (χωρίς επιτήρηση) είτε για να ταιριάζει με τις δεδομένες εισόδους.
4. Τεχνικές μηχανικής μάθησης για την αυτόματη αναγνώριση των χαρακτηριστικών της απάτης.

5. Νευρωνικά δίκτυα που μπορούν να μάθουν ύποπτα μοτίβα από δείγματα και να χρησιμοποιηθούν αργότερα για να τα ανιχνεύσουν.

Προκειμένου να αντιμετωπιστούν οι προκλήσεις γύρω από την ασφάλεια, ο τομέας της πληροφορικής στον κυβερνοχώρο θεωρεί ότι η εφαρμογή τεχνικών τεχνητής νοημοσύνης (Artificial intelligence) και μηχανικής μάθησης (Machine Learning) μπορεί να αντιληφθεί, να αιτιολογήσει, να μάθει και να ενεργήσει με έξυπνο τρόπο ενάντια σε προηγμένες επιθέσεις στον κυβερνοχώρο. Κατά τη διάρκεια των τελευταίων ετών, οι ερευνητές έλαβαν υπόψη τις διάφορες τεχνικές τεχνητής νοημοσύνης, προκειμένου να παράσχουν στους επαγγελματίες της ασφάλειας ένα μέσο αναγνώρισης των δεικτών του κυβερνοθεραπευτηρίου (Conti et al., 2018).

Στο επόμενο κεφάλαιο αναλύονται οι τρόποι με τους οποίους μπορεί κανείς να προστατευτεί φροντίζοντας την ασφάλεια της υποδομής των εγκαταστάσεων του. Η υποδομή περιλαμβάνει τις συσκευές, τα δίκτυα και τα άτομα.

1.10 Το εργαλείο LOKI IOC Scanner

Το LOKI είναι ένας ελεύθερος και απλός σαρωτής IOC, ένας πλήρης ανασυντάκτης των κύριων ενοτήτων ανάλυσης του πλήρως εξοπλισμένου APT Scanner THOR. Αυτοί οι δείκτες μπορούν να προέρχονται από δημοσιευμένες εκθέσεις περιστατικών, εγκληματολογικές αναλύσεις ή συλλογές δειγμάτων κακόβουλου λογισμικού στο εργαστήριό μας. Το LOKI προσφέρει έναν απλό τρόπο ανίχνευσης των συστημάτων σας για γνωστά ΔΟΕ.

* Η ΔΟΕ σημαίνει "Δείκτες Συμβιβασμού".

Υποστηρίζει αυτούς τους διάφορους τύπους δεικτών(indicators):

- MD5 / SHA1 / SHA256 hashes
- Κανόνες Yara (ισχύουν για δεδομένα αρχείων και μνήμη διαδικασιών)
- Δείκτης σκληρού δείκτη Αρχεία με βάση την Κανονική έκφραση (π.χ. \\ pwdump \ .exe)
- Χαρακτηριστικά μαλακών ενδείξεων με βάση τις Κανονικές εκφράσεις (π.χ. Windows \\ [\ w] \ .exe)

Το LOKI διαθέτει κάποιους από τους πιο αποτελεσματικούς κανόνες που δανείστηκαν από τα σύνολα κανόνων του διάσημου σαρωτή THOR APT. Αποφάσισαν να ενσωματώσουν πολλούς κανόνες webshell, καθώς ακόμη και οι καλύτεροι μηχανισμοί Antivirus δεν ανιχνεύουν τα περισσότερα από αυτά.

Η βάση δεδομένων υπογραφής της ΔΟΕ δεν είναι κρυπτογραφημένη ή αποθηκευμένη σε ιδιόκτητο σχήμα. Μπορούμε να επεξεργαστούμε τη βάση δεδομένων υπογραφής και να προσθέσουμε τα δικά μας ΔΟΕ. Επίσης, οι εισβολείς μπορούν επίσης να έχουν πρόσβαση σε αυτούς τους κανόνες στα συστήματα προορισμού, αν χρησιμοποιήσουμε το σαρωτή και αφήσουμε το πακέτο σε ένα συμβιβασμένο σύστημα.

1.10.1 Η χρησιμότητα του LOKI

Μπορούμε εύκολα να προσθέσουμε το δικό σας δειγματοληπτικό δείγμα, τα χαρακτηριστικά του ονόματος αρχείου και τους κανόνες Yara στα δίκτυα κανόνων που ομαδοποιήσαμε μαζί του.

Η πιο συνηθισμένη περίπτωση χρήσης είναι το σενάριο Triage ή APT Scan, στο οποίο σαρώσαμε όλες τις μηχανές μας για να εντοπίσουμε απειλές που δεν ανιχνεύθηκαν από τα Antivirus. Μπορούμε να χρησιμοποιήσουμε το LOKI σαν οποιοδήποτε άλλο λογισμικό χρησιμοποιώντας τη μέθοδο που προτιμάμε ή να το χρησιμοποιήσουμε σ' ένα μερίδιο δικτύου. Το LOKI μπορεί να ξεκινήσει μέσω προγραμματισμένης εργασίας (GPO). Μπορείτε να το εκτελέσουμε απλά χρησιμοποιώντας τη διαδρομή UNC "\\ system \ share \ loki.exe".

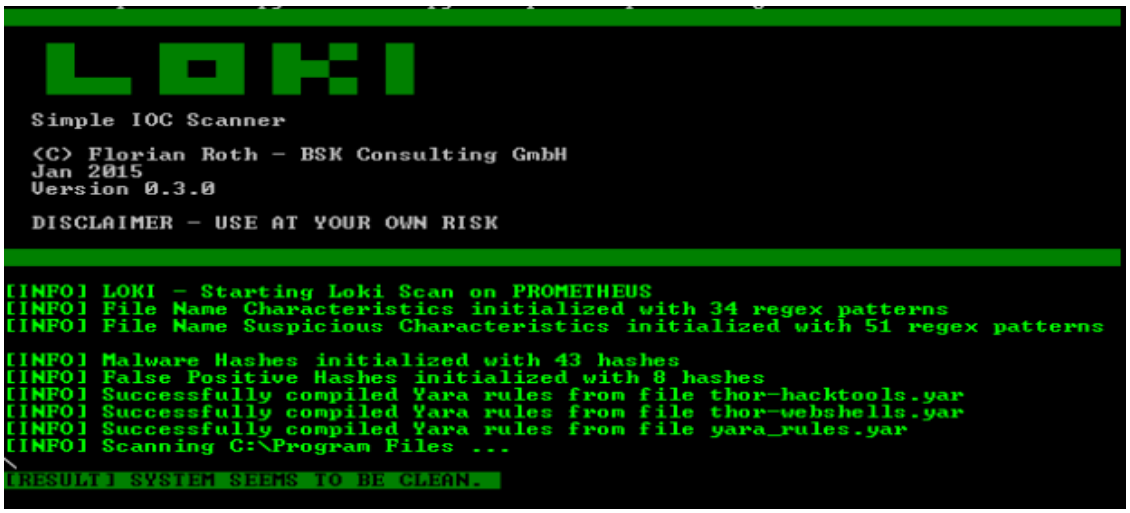
Ένα άλλο σενάριο είναι η χρήση σε ένα ιατροδικαστικό εργαστήριο. Σάρωση εικόνων με LOKI για τον εντοπισμό γνωστών απειλών χρησιμοποιώντας τους ορισμούς του IOC.

Προσθέτουμε γρήγορα τις ΔΟΕ που προέρχονται από σημαντικές αναφορές απειλών στα σύνολα κανόνων μας (π.χ. Regin, Skeleton Key). Χρησιμοποιούμε το LOKI για να ελέγξουμε την ακεραιότητα των συστημάτων σας γρήγορα και στοχευμένα. Επίσης, το LOKI διαθέτει μια απλή έξοδο αρχείου καταγραφής στη μορφή που δημιουργήθηκε από τους δαίμονες syslog.

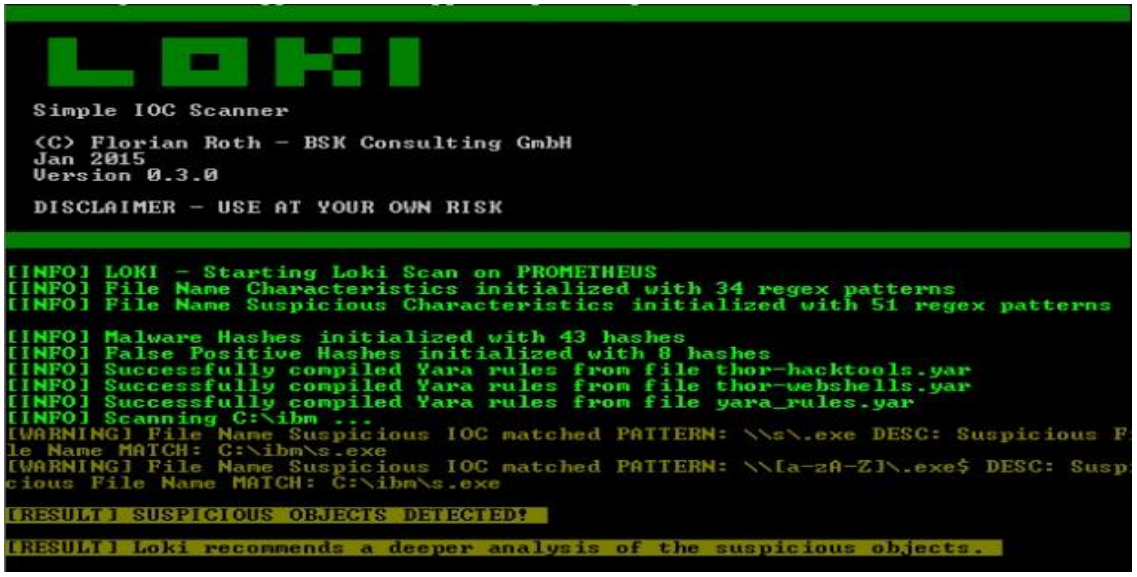
Στο τέλος της σάρωσης, το LOKI παράγει ένα αποτέλεσμα.

Αυτό το αποτέλεσμα μπορεί να είναι:

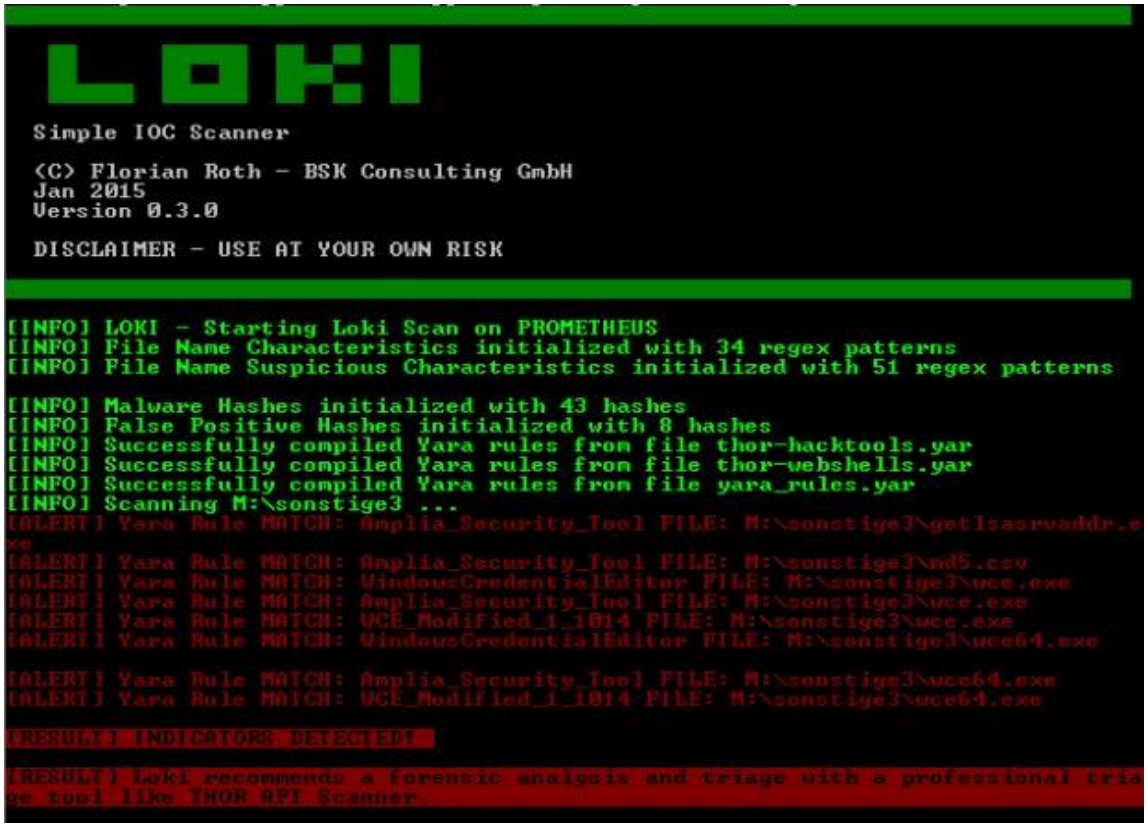
1. Το σύστημα φαίνεται να είναι καθαρό!



2. Εντοπίστηκαν ύποπτα αντικείμενα!



3. Εντοπίστηκαν δείκτες!



Στο παρακάτω πίνακα συγκρίνουμε το LOKI με άλλα εργαλεία

	LOKI	SPARK Core	SPARK	THOR
Type	Free / Open Source	Free / Registration Required	Enterprise Product	Enterprise Product
Main Use Case	Preventive Scanning / Triage	Preventive Scanning / Triage	Preventive Scanning / Triage	Incident Response / Live Forensics
Platform	Windows (precompiled), Linux / macOS (source with dependencies)	Windows, Linux, macOS	Windows, Linux, macOS	Windows
Size (Binaries)	8 MB	9 MB	9 MB	16 MB
Language	Python	Go	Go	Python
Modules	3	5	9	26
Bundled Signatures	Open Source (~3000 YARA rules)	Open Source (~3000 YARA rules)	THOR's Signature Set (~9000 YARA rules)	THOR's Signature Set (~9000 YARA rules)
Support and Testing	Github README & Issues, Travis-CI	Manual & Github Issues, Internal CI	Manual & Support Portal, Internal CI	Manual & Support Portal, Internal CI
Special Extras	Levenshtein check PESieve check Double Pulsar check	JSON output SYSLOG (tcp/udp/ssl) Scan Throttling	JSON output SYSLOG (tcp/udp/ssl) Scan Throttling	... a lot, see comparison

Αναλυτικότερος πίνακας σύγκρισης χαρακτηριστικών

Χαρακτηριστικό	Περιγραφή	LOKI	SPARK Core	THOR
Προσαρμοσμένο αρχείο Hashes	Εντοπίστε εργαλεία κακόβουλου λογισμικού ή hack βάσει προσαρμοσμένων κατακερματισμών αρχείων. MD5 / SHA1 / SHA256	✓	✓	✓
Προσαρμοσμένοι κανόνες Yara	Εντοπίστε εργαλεία κακόβουλου λογισμικού ή hack με βάση υπογραφές YARA (σάρωση μνήμης αρχείων και διαδικασιών)	✓	✓	✓
Ανάλυση συμβάντων	Εντοπίστε τη δραστηριότητα του εισβολέα και τα ίχνη της χρήσης του εργαλείου hack στα Windows Eventslogs (συμπεριλαμβανομένων SysInternals Sysmon, Windows Defender, Applocker, PowerShell και άλλα)			✓
Ανάλυση μητρώου	Εντοπίστε τυπικά κλειδιά που χρησιμοποιούνται στις ομάδες APT για να διατηρήσετε την επιμονή στο σύστημα			✓
Αντίσταση Ανάλυσης	Επεξεργάζεται όλα τα στοιχεία autoruns, plugins, καταχωρημένους οδηγούς, καταναλωτές WMI, παρόχους LSA και εφαρμόζει τη βάση δεδομένων της ΔΟΕ		✓	
WMI Persistence	Αναλύει τα αρχεία OBJECTS.DATA, καταγράφει καταχωρημένα στοιχεία και προειδοποιεί για ύποπτα			✓
Προφίλ Κατάλογοι	Ελέγχει την ανίχνευση παρατυπιών στους καταλόγους προφίλ χρηστών			✓

Ανάλυση διαδικασιών	Ανάλυση των τρεχουσών διαδικασιών που εκτελούνται για παράξενα ορισμούς άγκιστρων / αρχείων χειρισμών / Mutex, συνδέσεις δικτύου, σειρές μνήμης, καταλόγους εργασίας	✓	✓	✓
Rootkit Έλεγχος	Μερικοί έλεγχοι για τα rootkits που χρησιμοποιούν Named Pipes ή επικοινωνούν μέσω των χειριστηρίων Device IO			✓
Εξαγωγή TXT	Αρχείο καταγραφής απλού κειμένου όλων των συμβάντων που αναφέρθηκαν από το THOR	✓	✓	✓
Εξαγωγή HTML	Δομημένη αναφορά HTML για όλα τα συμβάντα που αναφέρθηκαν από το THOR	✓	✓	✓
Εξαγωγή Syslog	Εξαγωγή Syslog των συμβάντων που δημιουργούνται από το THOR. Αυτή η επιλογή εξαγωγής είναι πλήρως ευέλικτη. Μπορείτε να ορίσετε διαφορετικές θύρες προορισμού, πολλαπλά συστήματα προορισμού, να χρησιμοποιήσετε UDP ή TCP και να επιλέξετε μεταξύ διαφορετικών μορφών	✓	✓	✓
Μορφή εξόδου JSON	Στείλτε JSON μέσω UDP / TCP σε ένα απομακρυσμένο σύστημα ή γράψτε ένα τοπικό αρχείο σε μορφή JSON		✓	
Μορφή μηνύματος CEF	Το Syslog στέλνει μηνύματα σε μορφή Arcsight CEF για να λαμβάνει προειδοποιήσεις και ειδοποιήσεις στα συστήματα SIEM της Arcsight			✓

Έλεγχος ευπάθειας	Ένας βασικός έλεγχος ευπάθειας στις πιο κοινές ευπάθειες που επιτρέπουν την πλευρική μετακίνηση (λάθος διαμόρφωση Tomcat, HP Data Protector, ελλείποντα patches)			✓
Αναφορά σφάλματος των Windows (WER)	Αυτός ο έλεγχος εξάγει σχετικές πληροφορίες από αναφορές σφαλμάτων των Windows (αναφορές του Dr. Watson) για τον εντοπισμό συνθηκών που προκλήθηκαν από εκμεταλλεύσεις που στοχεύουν γνωστά ευπάθειες CVE σε προγράμματα περιήγησης, plugins για προγράμματα περιήγησης και άλλο λογισμικό			✓
Ανάλυση συστήματος αρχείων	Ανάλυση του συστήματος αρχείων με υπογραφές για τον προσδιορισμό των συνόλων εργαλείων του εισβολέα, των κοινών τροποποιήσεων των κερκόπορτων, των αρχείων ένδειξης κατακερματισμού ή κωδικού πρόσβασης, των εκτεταμένων εκτελέσιμων αρχείων και πολλά άλλα	✓	✓	✓
Έλεγχος ακεραιότητας αρχείων συστήματος	Ελέγχει την ακεραιότητα των πιο συνηθισμένων αρχείων συστήματος χρησιμοποιώντας τους κανόνες YARA	✓	✓	✓

2.Ασφάλεια υποδομής (Security the infrastructure)

Η ανάγκη για υποδομή ασφάλειας στον κυβερνοχώρο για την προστασία της εξελισσόμενης υποδομής στη σύγχρονη κοινωνία της πληροφορίας είναι γεγονός. Η υποδομή της τεχνολογίας των πληροφοριών και της επικοινωνίας είναι το νήμα μέσω του οποίου συνδέονται όλες οι κρίσιμες εθνικές υποδομές. Η ύπαρξη μιας αξιόπιστης υποδομής για την ασφάλεια στον κυβερνοχώρο αποτελεί προϋπόθεση για την ανάληψη όλων των πρωτοβουλιών ηλεκτρονικής διακυβέρνησης και ηλεκτρονικού εμπορίου παγκοσμίως (Chaturvedi et al., 2009).

Σε αυτό το κεφάλαιο γίνεται προσπάθεια να παρουσιαστούν οι προϋποθέσεις για την ασφάλεια μιας τέτοιας υποδομής. Οι τρόποι με τους οποίους μπορεί να προστατευτεί η υποδομή, και οι οποίοι περιγράφονται στις ακόλουθες υποενότητες, περιλαμβάνουν τα τείχη προστασίας, τα συστήματα ανίχνευσης εισβολών (IDS), τα συστήματα πρόληψης εισβολών (IPS), τα λογισμικά για την προστασία από ιούς και κακόβουλα λογισμικά, τα εικονικά ιδιωτικά δίκτυα (VPN), την κρυπτογράφηση των δεδομένων και τις ταξινομίες και την ευαισθητοποίηση των χρηστών γύρω από την εφαρμογή της ασφάλειας.

2.1.1 Τείχη προστασίας (Firewalls)

Λόγω της αυξανόμενης απειλής των επιθέσεων δικτύου, το τείχος προστασίας (firewall) έχει καταστεί από τα πιο σημαντικά στοιχεία για την εξασφάλιση των δεδομένων από τις μη εξουσιοδοτημένες επιθέσεις στο δίκτυο (Salaria & Madaan, 2014). Το τείχος προστασίας αναφέρεται στην προστασία ενός δικτύου ή ενός υπολογιστή αποκλείοντας ορισμένες περιπτώσεις κίνησης στο δίκτυο. Δηλαδή, δημιουργεί ένα εμπόδιο μεταξύ του αξιόπιστου και του μη αξιόπιστου δικτύου, προστατεύει τις εμπιστευτικές πληροφορίες και από μη ηθική χρήση. Ο κύριος ρόλος της του τείχους προστασίας είναι η ασφάλεια από μη εξουσιοδοτημένη πρόσβαση στο δίκτυο (Imran et al., 2015).

Ειδικότερα, ένα τείχος προστασίας είναι ένα σύστημα ασφαλείας δικτύου που βασίζεται σε λογισμικό ή υλικό, το οποίο ελέγχει την εισερχόμενη και εξερχόμενη κυκλοφορία του δικτύου, αναλύοντας τα πακέτα δεδομένων και προσδιορίζοντας εάν θα πρέπει να επιτρέπεται ή όχι, βάσει του εφαρμοζόμενου κανόνα. Ο στόχος του είναι ιδανικά να φιλτράρει την ανεπιθύμητη κίνηση του δικτύου που προέρχεται από το ασφαλές δίκτυο ή πηγαίνει στο ασφαλές δίκτυο. Η απόφαση φιλτραρίσματος βασίζεται στην πολιτική (policy) του τείχους προστασίας.

Η πολιτική είναι σύνολο κανόνων ταξινόμησης που καθορίζονται σύμφωνα με προκαθορισμένες απαιτήσεις πολιτικής ασφαλείας (Salaria & Madaan, 2014).

Τα τείχη προστασίας χρησιμοποιούνται για πολλές μορφές επιθέσεων, όπως από Trojan των κοινωνικών μηχανών, μη κατοχυρωμένο λογισμικό (unpatched software), επιθέσεις ηλεκτρονικού ψαρέματος, σκουλήκια (worms) που μετακινούνται μέσω του διαδικτύου και προηγμένες απειλές (APT) (Imran et al., 2015).

Τα τείχη προστασίας ποικίλλουν από απλά μηχανήματα που έχουν σχεδιαστεί για να χρησιμοποιηθούν και να εγκατασταθούν από κάποιον ανειδίκευτο στη ασφάλεια του δικτύου και σε πολύπλοκες εγκαταστάσεις πολλαπλών μηχανημάτων που χρησιμοποιούνται σε μεγάλους οργανισμούς (Ingham & Forrest, 1994). Διαφορετικά τείχη προστασίας έχουν διαφορετικές μεθόδους ελέγχου των πακέτων για αποδοχή ή απόρριψη (Hazari, 2000).

Τα τείχη προστασίας διαχωρίζονται σε διάφορους τύπους όπως το φιλτράρισμα πακέτων (packet filtering), βαθιά επιθεώρηση πακέτων (deep packet inspection), τείχη προστασία μεσολάβησης (proxy firewalls) ή τείχη προστασίας επιπέδου εφαρμογής (application layer firewalls), μετάφραση διεύθυνσης δικτύου (Network Address Translation - NAT) Στη συνέχεια, περιγράφονται οι διάφοροι τύποι αυτοί.

2.1.1.1 Φιλτράρισμα πακέτων (Packet Filtering)

Η πιο κοινή μέθοδος τείχους προστασίας είναι γνωστή ως φιλτράρισμα πακέτων. Στο διαδίκτυο, το φιλτράρισμα πακέτων είναι η διαδικασία διέλευσης ή αποκλεισμού πακέτων σε μια διεπαφή δικτύου που βασίζεται σε διευθύνσεις προέλευσης και προορισμού, θύρες ή πρωτόκολλα. Η διαδικασία χρησιμοποιείται σε συνδυασμό με τη μετάφραση διεύθυνσης δικτύου (NAT). Το φιλτράρισμα πακέτων αποτελεί συχνά μέρος ενός προγράμματος τείχους προστασίας για την προστασία ενός τοπικού δικτύου από ανεπιθύμητη διείσδυση (Rouse, 2005).

Όταν ένα τείχος προστασία φιλτραρίσματος πακέτων δέχεται ένα πακέτο από το διαδίκτυο, ελέγχει τις πληροφορίες που διατηρούνται στη διεύθυνση IP στην κεφαλίδα του πακέτου και το ελέγχει με βάση έναν πίνακα κανόνων ελέγχου πρόσβασης για να καθορίσει εάν το πακέτο είναι αποδεκτό ή όχι. Στην περίπτωση αυτή, ένα σύνολο κανόνων καθορίζονται από τον διαχειριστή του τείχους προστασίας. Αυτοί οι κανόνες ενδέχεται να καθορίζουν συγκεκριμένες ενέργειες όταν εντοπίζεται μια συγκεκριμένη διεύθυνση IP ή ένας αριθμός θύρας προέλευσης ή προορισμού (Hazari, 2000).

2.1.1.2 Βαθιά επιθεώρηση πακέτων (Deep Packet Inspection - DPI)

Μια άλλη μέθοδος που χρησιμοποιείται από τα τείχη προστασίας είναι γνωστή ως βαθιά επιθεώρηση πακέτων (deep packet inspection). Η βαθιά επιθεώρηση πακέτων είναι μια μορφή φιλτραρίσματος πακέτων με υπερβολικό έλεγχο. Εξετάζει όχι μόνο τις κεφαλίδες του πακέτου, αλλά και τα περιεχόμενα, για να καθορίσει περισσότερα για το πακέτο και όχι μόνο για τις πηγές και τις πληροφορίες προορισμού (Rouse & Scarpati, 2017).

Η μέθοδος αυτή εξασφαλίζει ότι ο δηλωμένος υπολογιστής προορισμού έχει ζητήσει προηγουμένως την τρέχουσα επικοινωνία. Αυτό απέχει από την εξασφάλιση ότι όλες οι επικοινωνίες ξεκινούν από τον υπολογιστή παραλήπτη και πραγματοποιούνται μόνο με πηγές που είναι γνωστές και αξιόπιστες από προηγούμενες αλληλεπιδράσεις. Εκτός από την αυστηρότερη παρακολούθηση των πακέτων, αυτά τα τείχη ασφαλείας επίσης κλείνουν τις θύρες έως ότου ζητηθεί σύνδεση με τη συγκεκριμένη θύρα. Αυτό επιτρέπει ένα πρόσθετο επίπεδο προστασίας από την απειλή της σάρωσης θύρας (Hazari, 2000).

Η βαθιά επιθεώρηση πακέτων είναι μια μορφή φιλτραρίσματος πακέτων που συνήθως εκτελείται ως συνάρτηση του τείχους προστασίας. Εφαρμόζεται στο στρώμα εφαρμογής. Η βαθιά επιθεώρηση πακέτων αξιολογεί τα περιεχόμενα ενός πακέτου που διέρχεται από ένα σημείο ελέγχου. Χρησιμοποιώντας κανόνες που εκχωρείται από τον διαχειριστή του συστήματος, τον πάροχο υπηρεσιών διαδικτύου ή από τον διαχειριστή δικτύου ή συστημάτων, η βαθιά επιθεώρηση πακέτων καθορίζει τι πρέπει να γίνει με αυτά τα πακέτα σε πραγματικό χρόνο (Brook, 2018).

Ακόμη, η βαθιά επιθεώρηση πακέτων είναι σε θέση να ελέγξει το περιεχόμενο αυτών των πακέτων και στη συνέχεια να υπολογίσει από πού προήλθε, όπως η υπηρεσία ή η εφαρμογή που το έστειλε. Επιπλέον, μπορεί να λειτουργήσει με φίλτρα, προκειμένου να εντοπίσει και να ανακατευθύνει την κυκλοφορία δικτύου από μια ηλεκτρονική υπηρεσία, όπως Twitter ή Facebook, ή από μια συγκεκριμένη διεύθυνση IP (Brook, 2018).

2.1.1.3 Τείχη προστασία μεσολάβησης (proxy firewalls)

Ένα από τα είδη τείχους προστασίας είναι τα τείχη προστασία μεσολάβησης (Proxy Firewalls). Ένα τείχος προστασίας μεσολάβησης είναι ένα σύστημα ασφαλείας δικτύου που προστατεύει τους πόρους δικτύου φιλτράροντας μηνύματα στο επίπεδο εφαρμογής (application layer). Ένα τείχος προστασίας μεσολάβησης μπορεί επίσης να ονομάζεται τείχος προστασίας εφαρμογών (application firewall) ή τείχος προστασίας πύλης (gateway firewall) (Rouse & Shea, 2014).

Τα τείχη προστασίας μεσολάβησης θεωρούνται ως ο πιο ασφαλής τύπος τείχους προστασίας επειδή εμποδίζουν την άμεση επαφή του δικτύου με άλλα συστήματα (Rouse & Shea, 2014; BullGuard, 2019), αλλά αυτό συμβαίνει σε βάρος της ταχύτητας και της λειτουργικότητας, καθώς μπορεί να περιορίσει τις εφαρμογές που μπορεί να υποστηρίξει το δίκτυό σας (BullGuard, 2019).

Ένα τείχος προστασίας μεσολάβησης, όπως υποδεικνύει ο ίδιος ο όρος, είναι μια ολοκληρωμένη στρατηγική για την προστασία ενός χρήστη από κακόβουλο περιεχόμενο μέσω τείχους προστασίας, ενώ ταυτόχρονα κρύβει την πραγματική διεύθυνση IP του χρήστη και την τοποθεσία του ως διακομιστή μεσολάβησης (Proxy Firewall, 2018).

Η ενισχυμένη ασφάλεια ενός τείχους προστασίας διακομιστή μεσολάβησης είναι επειδή, αντίθετα με άλλους τύπους τείχους προστασίας, τα πακέτα πληροφοριών δεν περνούν μέσω ενός διακομιστή μεσολάβησης. Αντίθετα, ο διακομιστής μεσολάβησης λειτουργεί ως ενδιάμεσος - οι υπολογιστές πραγματοποιούν σύνδεση με το διακομιστή μεσολάβησης, ο οποίος στη συνέχεια εκκινεί μια νέα σύνδεση δικτύου βάσει της αίτησης. Ουσιαστικά έναν καθρέφτη της μεταφοράς πληροφοριών. Αυτό αποτρέπει τις άμεσες συνδέσεις και τη μεταφορά πακέτων μεταξύ των δύο πλευρών του τείχους προστασίας, γεγονός που δυσκολεύει τους εισβολείς να ανακαλύψουν πού βρίσκεται η τοποθεσία του δικτύου από πληροφορίες πακέτων (Hazari, 2000).

Με ποιο απλά λόγια, ένας διακομιστής μεσολάβησης τείχους προστασίας παρέχει πρόσβαση στο διαδίκτυο σε υπολογιστές σε ένα δίκτυο, αλλά χρησιμοποιείται ως επί το πλείστον για την παροχή ασφάλειας ελέγχοντας τις πληροφορίες που εισέρχονται και εξέρχονται από το δίκτυο. Οι διακομιστές μεσολάβησης του διακομιστή μεσολάβησης τείχους προστασίας, τα αρχεία cache, τα αρχεία καταγραφής και τα ερωτήματα ελέγχου που προέρχονται από έναν υπολογιστή-πελάτη για να διατηρούν το δίκτυο ασφαλή και χωρίς εισβολείς και ιούς.

2.1.1.4 Μετάφραση διεύθυνσης δικτύου (Network Address Translation - NAT)

Για να έχει κανείς πρόσβαση στο διαδίκτυο, απαιτείται μια δημόσια διεύθυνση IP, αλλά καθώς χρησιμοποιεί ιδιωτική διεύθυνση IP στο ιδιωτικό του δίκτυο, απαιτείται η μετάφραση ιδιωτικής διεύθυνσης IP σε δημόσια διεύθυνση IP. Η μετάφραση διεύθυνσης δικτύου (Network Address Translation - NAT) είναι μια διαδικασία στην οποία μία ή περισσότερες τοπικές διευθύνσεις IP μεταφράζονται σε μία ή περισσότερες παγκόσμιες διευθύνσεις IP και αντίστροφα, προκειμένου να παρέχουν πρόσβαση στο διαδίκτυο

στους τοπικούς κεντρικούς υπολογιστές. Η NAT λειτουργεί γενικά σε δρομολογητή ή τείχος προστασίας (Tyson, 2019).

Η NAT χρησιμεύει ως τείχος προστασίας διατηρώντας τις ατομικές διευθύνσεις IP κρυμμένες από τον έξω κόσμο. Παρόμοια με διακομιστή μεσολάβησης, η NAT λειτουργεί ως ενδιάμεσος μεταξύ μιας ομάδας υπολογιστών και του διαδικτύου. Το NAT επιτρέπει σε έναν οργανισμό να παρουσιάζεται στο διαδίκτυο με μία διεύθυνση. Το NAT μετατρέπει τη διεύθυνση κάθε υπολογιστή και συσκευής σε τοπικό δίκτυο LAN σε μία διεύθυνση IP για το διαδίκτυο και αντίστροφα. Ως αποτέλεσμα, οι χρήστες που ανιχνεύουν το διαδίκτυο για διευθύνσεις δεν μπορούν να προσδιορίσουν τους υπολογιστές στο δίκτυο ή να εντοπίσουν λεπτομέρειες σχετικά με την τοποθεσία, τη διεύθυνση IP και άλλα. Η λογική είναι ότι αν οι επιτιθέμενοι δεν μπορούν να εντοπίσουν κάποιον δεν μπορούν και να τον βλάψουν (Hazari, 2000).

2.1.2 IDS/IPS

Μια εισβολή (Intrusion) ορίζεται ως κάθε σειρά ενεργειών που επιχειρούν να θέσουν σε κίνδυνο την αγανάκτηση, την εμπιστευτικότητα ή τη διαθεσιμότητα ενός πόρου. Συνεπώς, απαιτείται ανίχνευση εισβολής (Intrusion Detection) ως πρόσθετος τοίχος για την προστασία των συστημάτων. Η ανίχνευση εισβολών είναι χρήσιμη όχι μόνο για την ανίχνευση επιτυχών εισβολών, αλλά παρέχει επίσης σημαντικές πληροφορίες για έγκαιρα μέτρα αντιμετώπισης (Gurusamy & Hirani, 2018).

Ως Σύστημα Ανίχνευσης Εισβολών (“Intrusion Detection System” - IDS) ορίζεται μια συσκευή ή εφαρμογή λογισμικού που παρακολουθεί τις δραστηριότητες του δικτύου ή του συστήματος και διαπιστώνει την ύπαρξη κακόβουλων ενεργειών. Το IDS είναι μια εξέλιξη που ενισχύει την ασφάλεια του δικτύου και διασφαλίζει τα δεδομένα του οργανισμού. Το IDS βοηθά τον διαχειριστή δικτύου να ανιχνεύει οποιαδήποτε κακόβουλη δραστηριότητα στο δίκτυο και ειδοποιεί τον διαχειριστή να εξασφαλίσει τα δεδομένα, λαμβάνοντας τα κατάλληλα μέτρα ενάντια στις επιθέσεις αυτές (Tiwari et al., 2017). Ουσιαστικά, το IDS είναι ένα σύστημα ασφαλείας, το οποίο λειτουργεί ως στρώμα προστασίας σε μια υποδομή.

Τα IDS φιλτράρουν κάθε ύποπτη ή ανώμαλη δραστηριότητα στο δίκτυο. Αυτά τα συστήματα ανίχνευσης είναι πολύτιμα με τέτοιο τρόπο ώστε να επιδιώκουν να ανιχνεύσουν τα αρχικά στάδια μιας επίθεσης και στη συνέχεια να βοηθήσουν στην προστασία από τα επόμενα στάδια της επίθεσης. Επίσης, αυτά τα συστήματα επιδιώκουν να ανιχνεύσουν προειδοποιητικές ενδείξεις ύποπτων δραστηριοτήτων ή μοτίβων

συμπεριφοράς, είτε από έναν χρήστη, από μια εφαρμογή είτε από ένα κομμάτι κακόβουλου κώδικα, γεγονός που τα τείχη προστασίας ή άλλα εργαλεία προστασίας μπορεί να χάσουν ή να αγνοήσουν (Jang-Jaccard & Nepal, 2014).

Οι κύριες λειτουργίες των συστημάτων πρόληψης εισβολής ("Intrusion Prevention Systems" - IPS) είναι να εντοπίσουν κακόβουλη δραστηριότητα, να καταγράψουν πληροφορίες σχετικά με αυτή τη δραστηριότητα, να επιχειρήσουν να την εμποδίσουν να σταματήσουν και να την αναφέρουν. Τα IPS αναπτύχθηκαν για να επιλύσουν αμφισημίες στην παθητική παρακολούθηση του δικτύου τοποθετώντας τα συστήματα ανίχνευσης σε σειρά. Με βελτιωμένες τεχνολογίες τείχους προστασίας, η IPS μπορεί να εκτελέσει αποφάσεις ελέγχου πρόσβασης βάσει του περιεχομένου της εφαρμογής, αντί της διεύθυνσης IP ή των θυρών, όπως στα παραδοσιακά τείχη προστασίας (Panda & Patra, 2013).

Τα τείχη προστασίας λειτουργούν όπως τα IPS, όμως τα IPS επικεντρώνονται στην πρόληψη των επιθέσεων σε στρώματα στα οποία τα περισσότερα τείχη προστασίας δεν είναι σε θέση να αποκρυπτογραφήσουν, τουλάχιστον όχι ακόμη. Υπάρχουν πολλοί τύποι IPS που δρουν σε πολλές περιοχές, αυτοί οι τύποι είναι ενσωματωμένοι σε IDS δικτύου, σε εφαρμογές που βασίζονται σε τείχη προστασίας και IDS και σε παραπλανητικές εφαρμογές. Συνήθως, ένα IPS είναι σχεδιασμένο έτσι ώστε να λειτουργεί εντελώς αόρατα σε ένα δίκτυο. Τα προϊόντα IPS δεν απαιτούν τυπικά διεύθυνση IP στο προστατευμένο δίκτυο, αλλά ενδέχεται να ανταποκρίνονται άμεσα σε οποιαδήποτε κίνηση με διάφορους τρόπους (Abdelkarim & Nasereddin, 2011).

Όπως αναφέρθηκε προηγουμένως, τα προϊόντα IPS έχουν τη δυνατότητα να εφαρμόζουν κανόνες τείχους προστασίας, αλλά δεν αποτελούν τη βασική λειτουργία του IPS. Επίσης, το IPS προσφέρει βαθύτερη παρακολούθηση και σε λειτουργίες δικτύου όπως κακές συνδέσεις, ακατάλληλο περιεχόμενο και πολλές άλλες λειτουργίες δικτύου και εφαρμογών.

Ο συνδυασμός των τεχνολογιών IPS, IDS και Firewall θα προσφέρει μια ισχυρή γραμμή άμυνας για την προστασία των συστημάτων από οποιαδήποτε επίθεση, όπως για παράδειγμα το firewall ως πρώτη γραμμή άμυνας που συνδέεται με τη δεύτερη IDS γραμμή άμυνας και η πρώτη και η δεύτερη γραμμή συνδέονται με την τρίτη γραμμή IPS. Επομένως, ένα IDS είναι ένα λογισμικό που αυτοματοποιεί τη διαδικασία ανίχνευσης εισβολής, ενώ ένα IPS είναι ένα λογισμικό που έχει όλες τις δυνατότητες ενός

συστήματος ανίχνευσης εισβολής (IDS) και μπορεί επίσης να επιχειρήσει να σταματήσει πιθανά περιστατικά.

Υπάρχουν τέσσερις διαφορετικοί τύποι συστημάτων ανίχνευσης εισβολής (IDS), συγκεκριμένα υπάρχουν τα συστήματα που βασίζονται στο δίκτυο, στον κεντρικό υπολογιστή, σε εικονική μηχανή (virtual machine) και περιμετρικά συστήματα ανίχνευσης εισβολών. Στη συνέχεια, περιγράφονται αυτοί οι διαφορετικοί τύποι IDS.

2.1.2.1 Σύστημα ανίχνευσης εισβολής δικτύου (NIDS)

Το σύστημα ανίχνευσης εισβολής δικτύου ("Network IDS" - NIDS) αποτελεί μια ανεξάρτητη πλατφόρμα που εντοπίζει εισβολές εξετάζοντας την κυκλοφορία δικτύου και παρακολουθεί πολλούς κεντρικούς υπολογιστές (Yada, 2018). Πιο συγκεκριμένα, ένα NIDS που υπάρχει σε έναν υπολογιστή ή είναι συνδεδεμένο σε μια συσκευή σε ένα τμήμα του δικτύου ενός οργανισμού και παρακολουθεί την κυκλοφορία δικτύου σε αυτό το τμήμα δικτύου, αναζητώντας συνεχείς επιθέσεις.

Σε ένα δίκτυο για τη διατήρηση της ασφάλειας στα αρχεία χρησιμοποιούνται πολλοί διάφοροι αλγόριθμοι. Όταν προκύψει μια κατάσταση που το NIDS προγραμματίζεται να γνωρίζει μια επίθεση, απαντά με την αποστολή ειδοποιήσεων σε διαχειριστές. Το NIDS αναζητά μοτίβα επίθεσης μέσα σε μια κυκλοφορία δικτύου, όπως μεγάλες συλλογές σχετικών στοιχείων που είναι συγκεκριμένου τύπου που θα μπορούσαν να καθορίσουν ότι μια επίθεση άρνησης υπηρεσίας είναι σε εξέλιξη ή αναζητά την ανταλλαγή μιας σειράς σχετικών πακέτων με ένα συγκεκριμένο μοτίβο, το οποίο θα μπορούσε να δείξει ότι βρίσκεται σε εξέλιξη μια σάρωση θύρας (Tiwari et al., 2017).

2.1.2.2 Σύστημα ανίχνευσης εισβολής βασισμένο σε κεντρικό υπολογιστή (HIDS)

Ένα σύστημα ανίχνευσης εισβολής βασισμένο σε κεντρικό υπολογιστή ("Host-based IDS" - HIDS) αποτελείται από έναν πράκτορα σε έναν κεντρικό υπολογιστή που προσδιορίζει εισβολές από την ανάλυση των κλήσεων συστήματος, αρχεία καταγραφής εφαρμογής, τροποποιήσεις του συστήματος αρχείων (όπως, δυαδικά αρχεία, αρχεία κωδικών πρόσβασης, βάσεις δεδομένων, λίστες ελέγχου πρόσβασης, και άλλα) και άλλες δραστηριότητες υποδοχής (Yada, 2018).

Αναλυτικότερα, ένα HIDS τοποθετείται σε έναν συγκεκριμένο υπολογιστή ή διακομιστή, γνωστό ως κεντρικό υπολογιστή, και παρακολουθεί τη δραστηριότητα μόνο σε αυτό το σύστημα. Τα HIDS μπορούν να χωριστούν σε δύο κατηγορίες: τεχνικές ανίχνευσης που βασίζονται σε υπογραφή (δηλαδή ανίχνευση κακής χρήσης) και βασισμένες σε

ανωμαλία. Το HIDS παρακολουθεί την κατάσταση των βασικών αρχείων συστήματος και εντοπίζει πότε ένας εισβολέας δημιουργεί, τροποποιεί ή διαγράφει τα αρχεία που παρακολουθούνται. Στη συνέχεια, το HIDS ενεργοποιεί μια ειδοποίηση όταν εμφανιστεί μια αλλαγή όπως να αλλάζουν τα χαρακτηριστικά αρχείων, να δημιουργούνται νέα αρχεία ή να διαγράφονται υπάρχοντα αρχεία. Η κύρια διαφορά μεταξύ του NIDS και του HIDS είναι ότι το NIDS μπορεί να αποκτήσει πρόσβαση σε πληροφορίες που είναι κρυπτογραφημένες όταν ταξιδεύουν μέσω του δικτύου (Tiwari et al., 2017).

2.1.2.3 Περιμετρικό σύστημα ανίχνευσης εισβολής (PIDS)

Ένα περιμετρικό σύστημα ανίχνευσης εισβολής (“Perimeter IDS” - PIDS) εντοπίζει τη θέση των προσπαθειών εισβολής σε περιμετρικές περιφράξεις κρίσιμων υποδομών. Χρησιμοποιώντας ηλεκτρονικά ή πιο προηγμένη τεχνολογία καλωδίων οπτικών ινών προσαρμοσμένη στον περιμετρικό φράκτη, το PIDS ανιχνεύει διαταραχές στο φράχτη και εάν ανιχνευθεί μια εισβολή και θεωρηθεί από το σύστημα ως απόπειρα εισβολής, ενεργοποιείται συναγερμός (Yada, 2018).

Τα PIDS είναι συστήματα χρησιμοποιούνται σε εξωτερικό περιβάλλον για την ανίχνευση της παρουσίας ενός εισβολέα που επιχειρεί να παραβιάσει μια περίμετρο. Η υιοθέτηση της τεχνολογίας Κατανεμημένης Ακουστικής Αίσθησης (“Distributed Acoustic Sensing” - DAS) των οπτικών ινών αναπτύσσεται ραγδαία ως μέρος των στρατηγικών PIDS για πολλές εταιρείες σε ένα φάσμα βιομηχανιών και μπορεί να χρησιμοποιηθεί σε όλες τις περιπτώσεις PIDS (Bandweaver, 2018).

2.1.2.4 Σύστημα ανίχνευσης εισβολών βασισμένο σε εικονική μηχανή (VMIDS)

Ένα σύστημα ανίχνευσης εισβολών βασισμένο σε εικονική μηχανή (“Virtual Machine-based IDS” - VMIDS) ανιχνεύει εισβολές χρησιμοποιώντας παρακολούθηση εικονικής μηχανής. Αυτός είναι ο πιο πρόσφατος τύπος και είναι ακόμα υπό ανάπτυξη. Δεν υπάρχει ανάγκη για ένα ξεχωριστό σύστημα ανίχνευσης εισβολών, αφού χρησιμοποιώντας αυτό, μπορεί κανείς να παρακολούθησει τις συνολικές δραστηριότητες (Yada, 2018).

2.1.2.5 AlienVault

Η AlienVault (www.alienvault.com) είναι μια εταιρία που παράγει προγράμματα για ανίχνευση των απειλών και την αντιμετώπιση τους. Η ενοποιημένη πλατφόρμα USM (Unified Security Managment) συνδυάζει τις βασικές δυνατότητες ασφαλείας και τις εξειδικευμένες πληροφορίες απειλών. Οι πληροφορίες αυτές ενημερώνονται κάθε 30 λεπτά με δεδομένα από την ανοιχτή κοινότητα πληροφοριών για απειλές OTX (Open Threat Exchange), η οποία επιτρέπει την συνεργατική άμυνα και έχει αναλυθεί και ταξινομηθεί από την ομάδα του εργαστηρίου AlienVault.

Το USM της AlienVault έχει αναπτυχθεί έτσι ώστε να ανταποκρίνεται στις προκλήσεις της σημερινής δυναμικής Υπηρεσίας Παροχής Υπηρεσιών Ασφαλείας ("Managed Security Service Provider" - MSSP). Ένας MSSP είναι ένας πάροχος υπηρεσιών πληροφορικής ο οποίος παρέχει σε έναν οργανισμό κάποια ποσότητα παρακολούθησης και διαχείρισης στον κυβερνοχώρο, η οποία μπορεί να περιλαμβάνει αποκλεισμό από ιούς και ανεπιθύμητα μηνύματα, ανίχνευση εισβολών, διαχείριση τείχους προστασίας και διαχείριση εικονικού ιδιωτικού δικτύου (VPN). Ένα MSSP μπορεί επίσης να χειριστεί αλλαγές συστήματος, τροποποιήσεις και αναβαθμίσεις. Επομένως, το USM της AllienVault είναι μια λύση για τις MSSP για να δημιουργήσουν διαχειριζόμενες υπηρεσίας ασφάλειας και συμμόρφωσης (όπως, το GDPR).

Το USM η οποία λειτουργεί και φιλοξενείται σε ένα υπολογιστικό νέφος (cloud computing, έτσι μειώνεται σημαντικά το κόστος και το βάρος της εγκατάστασης, της διαχείρισης και της συντήρησης υλικού. Παρόλα αυτά μπορεί να εγκατασταθεί και να λειτουργήσει και στις εγκαταστάσεις του χρήστη. Το λογισμικό USM συγχωνεύει όλα τα απαραίτητα εργαλεία σε μια ενιαία τοποθεσία και τα διασυνδέει με την πιο πρόσφατη απειλή, σε πραγματικό χρόνο. Τροφοδοτείται επίσης από μία από τις μεγαλύτερες ανταλλαγές ανοιχτών απειλών που προέρχονται από πλήθος, ώστε να παρέχουν μια αξιόπιστη λύση για την αντιμετώπιση των περιστατικών, τη συμμόρφωση και την ανίχνευση απειλών.

2.1.3 Προστασία από ιούς (Antivirus)

Η προστασία από ιούς (antivirus) είναι ένας αλγόριθμος ή ένα σύνολο αλγορίθμων που αναγνωρίζει με μοναδικό τρόπο έναν συγκεκριμένο ιό. Τα antivirus είναι προγράμματα ειδικά σχεδιασμένα για να αντιμετωπίζουν τις προκλήσεις που προκαλούνται από ιούς, καθώς προστατεύουν τα συστήματα υπολογιστών από επιθέσεις από ιούς. Επομένως, τα

antivirus σαρώνουν τον υπολογιστή χρησιμοποιώντας ορισμένα συγκεκριμένα μοτίβα ενδεικτικά γνωστών ιών. Για να παραμείνουν σε ισχύ, πρέπει οι προγραμματιστές αυτών των antivirus να ενημερώσουν τις βάσεις δεδομένων τους κάθε φορά που προκύπτουν νέα στοιχεία για ιούς (Wanjala & Jacob, 2017).

Ένα από τα βασικά χαρακτηριστικά των Antivirus είναι η ανίχνευση ιών, η οποία γίνεται στο παρασκήνιο, και το σαρωμένο αρχείο ή το πρόγραμμα θα ανοίξει μόνο όταν το πρόγραμμα προστασίας από ιούς έχει τελειώσει την πλήρη σάρωση του συστήματος. Τα περισσότερα προγράμματα προστασίας από ιούς διαθέτουν δυνατότητα σάρωσης σε πραγματικό χρόνο, η οποία επιτρέπει την ταχεία ανίχνευση παρουσίας κακόβουλων αρχείων στον υπολογιστή. Επίσης, ένα antivirus αποκλείει τα κακόβουλα αρχεία δέσμης ενεργειών και εμποδίζει την εκτέλεσή τους, επειδή θέτουν τον υπολογιστή σε κίνδυνο να μολυνθεί από κακόβουλο λογισμικό (Rijnetu, 2017).

Η ευρετική (heuristic) ανάλυση είναι μια μέθοδος που χρησιμοποιείται σε πολλά προγράμματα antivirus για υπολογιστές και έχει σχεδιαστεί για τον εντοπισμό γνωστών ιών υπολογιστών, καθώς και νέων παραλλαγών ιών. Έτσι ένα antivirus μια βάση δεδομένων η οποία περιλαμβάνει γνωστά κακόβουλα λογισμικά και συγκρίνει κάθε σαρωμένο αρχείο με τα περιεχόμενα της βάσης δεδομένων (Rijnetu, 2017).

Αξίζει να σημειωθεί ότι η αφαίρεση κακόβουλου λογισμικού είναι σημαντική επειδή υπάρχουν πολλοί τύποι κακόβουλου λογισμικού που μπορεί να βλάψουν τον υπολογιστή σας. Ωστόσο, πολλά antivirus ενδέχεται να περιορίζονται μόνο στην ανίχνευση και αποκλεισμό κακόβουλου λογισμικού, αλλά δεν θα είναι δυνατή η κατάργησή του από τον μολυσμένο υπολογιστή.

*2.1.4 Λογισμικό προστασίας από κακόβουλο λογισμικό (**Antimalware Software**)*

Οι δυνατότητες του λογισμικού προστασίας από κακόβουλο λογισμικό (antimalware software) μπορούν να καλύψουν ευρύτερες λύσεις λογισμικού και εστιάζουν περισσότερο σε προηγμένες μορφές απειλών κακόβουλου λογισμικού, όπως το κακόβουλο λογισμικό των μηδενικών ημερών και είναι άγνωστα από τα προϊόντα προστασίας από ιούς (antivirus) (Rijnetu, 2017).

Η διαφορά μεταξύ του antivirus και του antimalware είναι ότι το antivirus επικεντρώνεται στην πρόληψη, προστατεύοντας ένα μηχάνημα σταματώντας το να μολυνθεί στην πρώτη φάση, ενώ το Antimalware έχει ως στόχο να εξαλείψει και να καταστρέψει κακόβουλα λογισμικά που έχουν ήδη ληφθεί και ενεργοποιηθεί (Hopping, 2018).

2.1.5 VPN

Το Εικονικό Ιδιωτικό Δίκτυο (“Virtual Private Network” - VPN) είναι μια τεχνολογία που παρέχει ασφαλή επικοινωνία για δεδομένα, καθώς διέρχεται μέσω ανασφαλών περιοχών της υποδομής τεχνολογίας πληροφοριών. Με την παραγωγική ανάπτυξη του διαδικτύου, οι επιχειρήσεις σήμερα εφαρμόζουν σήραγγες VPN χρησιμοποιώντας διαφορετικά πρωτόκολλα που εγγυώνται την αυθεντικότητα των δεδομένων και την ασφάλεια μεταξύ πολλαπλών τοποθεσιών που συνδέονται με τη δημόσια τηλεπικοινωνιακή υποδομή. Το VPN παρέχει εναλλακτική λύση για τη δημιουργία επικοινωνίας μεταξύ τοποθεσιών (Narayan et al., 2009).

Τα πρωτόκολλα που χρησιμοποιούνται περισσότερο σε δίκτυα VPN είναι το πρωτόκολλο ασφαλείας του διαδικτύου (“Internet Protocol Security” - IPsec), το πρωτόκολλο σήραγγας από σημείο σε σημείο (“Point-to-Point Tunneling Protocol” - PPTP) και η ασφάλεια του επιπέδου υποδοχής (“Secure Socket Layer” - SSL).

Το πρωτόκολλο IPSec είναι ένα πρωτόκολλο ασφαλείας που χρησιμεύει για την εξασφάλιση πληροφοριών σε περίπτωση ανταλλαγής τους μέσω του διαδικτύου. Αυτό συμβαίνει εάν υπάρχει σύνδεση μεταξύ ιδιωτικής IP και δημόσιας IP. Αυτό το πρωτόκολλο θα ανταλλάξει τα πακέτα στο επίπεδο IP με ασφάλεια. Παρέχει δύο τύπους επιλογών κρυπτογράφησης, μεταφοράς (transport) και σήραγγας (tunnel). Η λειτουργία μεταφοράς θα κρυπτογραφήσει το τμήμα δεδομένων χωρίς να αλλάξει η κεφαλίδα πακέτων. Ο αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση δεδομένων είναι ένας συμμετρικός αλγόριθμος κρυπτογραφίας. Αυτό το πρωτόκολλο επικυρώνει και κρυπτογραφεί κάθε πακέτο από μια συνεδρία μετάδοσης δεδομένων. Επίσης, μπορεί να δημιουργήσει κλειδιά μεταξύ του αποστολέα και του παραλήπτη την πρώτη φορά που είναι ενεργοποιημένη και μπορεί να διαπραγματευτεί τα κρυπτογραφικά κλειδιά που θα χρησιμοποιηθούν κατά τη διάρκεια της περιόδου σύνδεσης. Το πρωτόκολλο αυτό χρησιμεύει για την προστασία της ροής δεδομένων από υπολογιστή σε υπολογιστή, από δίκτυο σε δίκτυο και από δίκτυο σε κεντρικό υπολογιστή (Haryanto et al., 2017).

Το PPTP αναπτύχθηκε από μια κοινοπραξία προμηθευτών της Microsoft, και είναι ένα πρωτόκολλο OSI Layer 2. Το PPTP είναι μια επέκταση του πρωτοκόλλου σημείου προς σημείο (PPP) και η δημοτικότητά του αποδίδεται στην ευκολία με την οποία μπορεί να διαμορφωθεί. Η ασφαλής επικοινωνία που δημιουργείται χρησιμοποιώντας αυτό το πρωτόκολλο συνήθως περιλαμβάνει τρία στάδια. όπου το καθένα πρέπει να ολοκληρωθεί πριν από το επόμενο. Πρώτον, ένα πρόγραμμα-πελάτης (client) PPTP χρησιμοποιεί μια

σύνδεση τύπου PPP για να δημιουργήσει μια σύνδεση μέσω του δικτύου μεταφοράς από την πηγή στον προορισμό. Μόλις γίνει αυτό, το πρωτόκολλο PPTP δημιουργεί μια σύνδεση ελέγχου από τον πελάτη στο διακομιστή (server) PPTP. Αυτή η σύνδεση χρησιμοποιεί το TCP για τη δημιουργία σύνδεσης. Και τέλος, το πρωτόκολλο PPTP δημιουργεί IP διαγράμματα δεδομένων (datagrams) που περιέχουν κρυπτογραφημένα πακέτα PPP τα οποία μεταφέρονται μέσω της σήραγγας (Narayan et al., 2009).

Το SSL είναι μια τεχνολογία VPN που χρησιμοποιείται συνήθως με προγράμματα περιήγησης για να παρέχει στους χρήστες μια απρόσκοπτη ασφαλή σύνδεση. Ωστόσο, το SSL μπορεί επίσης να χρησιμοποιηθεί για τη δημιουργία σηράγγων VPN. Προστατεύει τα δεδομένα χρησιμοποιώντας κρυπτογράφηση για να εξασφαλίσει την ακεραιότητα (Narayan et al., 2009).

2.1.6 Κρυπτογράφηση δεδομένων – ταξινομήσεις

Η χειρότερη περίπτωση μιας επίθεσης μέσα στην επικοινωνία είναι ο πλήρης έλεγχος του συστήματος κρυπτογράφησης από παράνομους χρήστες. Αυτό συμβαίνει με την πρόσβαση στον αλγόριθμο κρυπτογράφησης για την αποκρυπτογράφηση των δεδομένων και την πρόσβαση σε ευαίσθητες πληροφορίες (Bazli et al., 2014). Η κρυπτογραφία είναι μια τεχνική για την επίτευξη ασφάλειας για τις επικοινωνίες με την κωδικοποίηση μηνυμάτων απλού κειμένου ώστε να είναι δυσανάγνωστη. Η κρυπτογράφηση (encryption) είναι ένα χρήσιμο εργαλείο για την προστασία της εμπιστευτικότητας και της ακεραιότητας των πληροφοριών. Είναι απλά μια τεχνική για την απόκρυψη της πραγματικής σημασίας των πληροφοριών από μη εξουσιοδοτημένους χρήστες (Rakheja, 2011).

Ο στόχος της ταξινόμησης των δεδομένων (data classification) είναι να καθοριστεί το απαιτούμενο επίπεδο ασφάλειας για τα δεδομένα και να προστατευθούν τα δεδομένα παρέχοντας ένα επαρκές επίπεδο ασφάλειας ανάλογα με τα επίπεδα κινδύνου των δεδομένων. Η ταξινόμηση των δεδομένων συμβάλλει στον καθορισμό των βασικών στοιχείων ασφαλείας για την προστασία των δεδομένων. Το σύστημα πληροφοριών του οργανισμού πρέπει να εξεταστεί προσεκτικά και να ταξινομηθεί με βάση το επίπεδο ευαισθησίας του και την αποτελεσματικότητα του οργανισμού εάν τα δεδομένα αποκαλύπτονται, τροποποιούνται ή καταστρέφονται χωρίς άδεια. Η ταξινόμηση αναγνωρίζει και χωρίζει τα πιο ευαίσθητα δεδομένα από τα λιγότερο ευαίσθητα δεδομένα (Sood, 2012).

2.1.7 Ευαισθητοποίηση για την ασφάλεια (Security awareness)

Η ευαισθητοποίηση σχετικά με την ασφάλεια των πληροφοριών (“Information Security Awareness” - ISA) αναφέρεται ως κατάσταση συνείδησης και γνώσης σχετικά με ζητήματα ασφάλειας και συχνά επηρεάζει τη συμπεριφορά που συμμορφώνεται με την ασφάλεια (Haeussinger & Kranz, 2013).

Η συνειδητοποίηση της ασφάλειας είναι ένας παράγοντας που συχνά παραβλέπεται σε ένα πρόγραμμα ασφάλειας πληροφοριών. Ενώ οι οργανισμοί επεκτείνουν τη χρήση της προηγμένης τεχνολογίας ασφαλείας και εκπαιδεύουν συνεχώς τους επαγγελματίες ασφαλείας, ελάχιστα χρησιμοποιούνται για να αυξήσουν την ευαισθητοποίηση των χρηστών σχετικά με την ασφάλεια, καθιστώντας τους τον πιο αδύναμο σύνδεσμο σε κάθε οργανισμό. Ως αποτέλεσμα, σήμερα, οι οργανωμένοι εγκληματίες στον κυβερνοχώρο καταβάλλουν σημαντικές προσπάθειες για την έρευνα και την ανάπτυξη προηγμένων μεθόδων εισβολής (hacking) που μπορούν να χρησιμοποιηθούν για να κλέψουν χρήματα και πληροφορίες από το ευρύ κοινό. Επιπλέον, ο υψηλός ρυθμός αύξησης της διείσδυσης του διαδικτύου και η περιορισμένη ευαισθητοποίηση των χρηστών σχετικά με την ασφάλεια καθιστά ελκυστικό στόχο για τους εγκληματίες στον κυβερνοχώρο (Aloul, 2012).

Σε αυτό το κεφάλαιο έγινε μια σύντομη περιγραφή για τους διαθέσιμους μηχανισμού με τους οποίους μπορεί να ενισχυθεί η ασφάλεια της υποδομής. Το ζητούμενο είναι όλα αυτά τα αντίμετρα είναι αρκετά για την αποτελεσματικότητα της ασφάλειας. Έτσι, στο επόμενο κεφάλαιο γίνεται μια ανασκόπηση γύρω από τη γνώμη των ερευνητών σχετικά με το ζήτημα αυτό.

3. Ανάλυση και σύγκριση μεθόδων ασφαλείας

Στα προηγούμενα κεφάλαια έγινε ανάλυση σχετικά με του τύπους των επιθέσεων στον κυβερνοχώρο, αλλά και τους τρόπους με τους οποίους μπορεί να προστατευτούν οι οργανισμοί από τέτοιες επιθέσεις. Σε αυτό το κεφάλαιο γίνεται μια μελέτη γύρω από την αποτελεσματικότητα αυτών των εργαλείων και των μεθόδων για την προστασία και την ασφάλεια στον κυβερνοχώρο.

Η πρώτη μορφή ενεργής κυβερνοάμυνας που αναλύθηκε αφορά τον έλεγχο τρωτότητας. Οι έλεγχοι τρωτότητας χρησιμοποιούνται για να προσδιοριστεί εάν και πώς ένας κακόβουλος χρήστης μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε στοιχεία που επηρεάζουν τη θεμελιώδη ασφάλεια του συστήματος, αρχείων και αρχείων καταγραφής. Επίσης, για να επιβεβαιωθεί ότι ισχύουν τα κατάλληλα στοιχεία ελέγχου που απαιτούνται για το πεδίο εφαρμογής, τη διαχείριση ευπάθειας, τη μεθοδολογία και τον κατακερματισμό.

Όμως, οι έλεγχοι τρωτότητας από μόνοι τους δεν αποτρέπουν τα περιστατικά ασφάλειας και τα αποτελέσματά τους δεν παρέχουν ένδειξη για ένα τρέχον ή προηγούμενο περιστατικό ασφάλειας. Η διεξαγωγή ενός ελέγχου τρωτότητας αντικατοπτρίζει ένα στιγμιότυπο του περιβάλλοντος σε ένα συγκεκριμένο χρονικό σημείο και ο στόχος του είναι απλώς να εντοπίσει και να αναλύσει τις αδυναμίες που υπάρχουν σε ένα τεχνικό περιβάλλον. Για να υπάρξει ένα καθαρό όφελος για την ασφάλεια, πρέπει να διεξάγονται τακτικοί έλεγχοι (Bacudio et al., 2011). Οι πληροφορίες σχετικά με τυχόν ευπάθειες ασφαλείας που επιτυγχάνονται μέσω ελέγχων τρωτότητας συνήθως συσσωρεύονται και παρουσιάζονται στους διαχειριστές συστημάτων πληροφορικής και δικτύων για να βοηθήσουν τους επαγγελματίες αυτούς να καταλήξουν σε στρατηγικά συμπεράσματα και να δώσουν προτεραιότητα σε σχετικές προσπάθειες αποκατάστασης (PCI DSS, 2017).

Επίσης έγινε αναφορά στα λογισμικά για την προστασία από ιούς και κακόβουλα λογισμικά (Antivirus & Antimalware). Τα εμπορικά προγράμματα για την προστασία από κακόβουλα λογισμικά και ιούς είναι τα πιο δημοφιλή εργαλεία άμυνας που χρησιμοποιούνται από επιτραπέζιους υπολογιστές, φορητούς υπολογιστές και κινητές συσκευές. Οι τελικοί χρήστες των προγραμμάτων αυτών έχουν την προσδοκία ότι αυτά τα προγράμματα θα παρέχουν ολοκληρωμένη προστασία, συγκεκριμένα την αποτελεσματική ανίχνευση και επεξεργασία κακόβουλου λογισμικού.

Κατά συνέπεια, οι τελικοί χρήστες έχουν εμπιστοσύνη σε ένα πρόγραμμα κατά του κακόβουλου λογισμικού για την προστασία του συστήματός τους και υποθέτουν ότι το κακόβουλο λογισμικό αντιμετωπίζεται αυτόματα και αποτελεσματικά όταν ανιχνεύεται κακόβουλο λογισμικό. Ένα ενιαίο πρόγραμμα κατά του κακόβουλου λογισμικού δεν είναι πράγματι επαρκές για την υπεράσπιση του κακόβουλου λογισμικού παρόλο που είναι ευρέως αντιληπτό ότι κανένα ενιαίο πρόγραμμα κατά του κακόβουλου λογισμικού δεν μπορεί να προσφέρει εκατό τις εκατό ανίχνευση και αποτελεσματικότητα (Morales et al., 2012). Αν και πολλά σύγχρονα τείχη προστασίας είναι πιο εξελιγμένα, τα τείχη προστασίας του δικτύου δεν μπορούν να φιλτράρουν ανεπιθύμητη κίνηση, όπως το ωφέλιμο φορτίο κακόβουλου λογισμικού, το οποίο χρησιμοποιεί νόμιμες διευθύνσεις IP και θύρες (Jang-Jaccard & Nepal, 2014).

Πρακτικά, είναι αδύνατο να καταργηθεί κάθε τεχνική ευπάθειας από ένα δεδομένο περιβάλλον. Υπάρχουν πολλοί λόγοι για αυτό. Ορισμένες ευπάθειες είναι λανθάνουσες μέχρι να ανακαλυφθούν και να δημοσιοποιηθούν. Αυτές συνήθως αναφέρονται ως μηδενικές ημέρες (zerodays), δηλαδή υπάρχουν μηδέν ημέρες από τη δημοσίευση τους. Άλλα προβλήματα ευπάθειας ενδέχεται να οφείλονται σε προκλήσεις που σχετίζονται με την επιδιόρθωση συγκεκριμένων συσκευών, συμπεριλαμβανομένων εκείνων που υποστηρίζουν εφαρμογές παλαιού τύπου ή που διαχειρίζονται απευθείας εξωτερικοί προμηθευτές. Ακόμα άλλες ευπάθειες ενδέχεται να είναι δαπανηρές για την αντιμετώπιση άλλων λόγων. Αυτό με τη σειρά του σημαίνει ότι κάθε δεδομένο περιβάλλον θα έχει πολλαπλά λανθάνοντα τρωτά σημεία οποιαδήποτε στιγμή (ISACA, 2017).

Η έρευνα που πραγματοποιήθηκε στα πλαίσια της παρούσας εργασίας προσφέρει αντιφατικά αποτελέσματα όσον αφορά την επίδραση της ανάπτυξη πολιτικών ασφάλειας εταιρικών πληροφοριών (ISP). Ενώ οι D'Arcy κ.α. (2009) διαπίστωσαν ότι η ύπαρξη εταιρικών ISPs είναι αποτελεσματική για την αποτροπή της συμπεριφοράς κατάχρησης των πολιτικών ασφαλείας και αποδίδει αυτή την επίδραση στους μηχανισμούς αποτροπής, οι Lee et al. (2004) διαπίστωσαν ότι οι ISP δεν είχαν καμία επιρροή στη συμπεριφορά κατάχρησης των πληροφοριών. Ο Siponen (2000) υποστηρίζει ότι τα ασυνεπή αποτελέσματα οφείλονται στην έλλειψη συνειδητοποίησης των πολιτικών ασφάλειας των εργαζομένων. Από την άποψη αυτή, οι μελετητές υπογραμμίζουν ότι η «απλή» ISP δεν είναι αρκετή και υπογραμμίζουν τη σημασία της προώθησης των ISP και της διασφάλισης ότι είναι κατανοητά, εύκολα διαθέσιμα και κατανοητά.

Συνοψίζοντας αυτές τις πτυχές της αποτελεσματικής προώθησης των πολιτικών ασφαλείας, υπάρχουν ευρείες εμπειρικές ενδείξεις ότι η παροχή ISP συνδέεται θετικά με τη συμπεριφορά που σχετίζεται με την ασφάλεια (Chan et al., 2005).

Επίσης, οι Siponen κ.α. (2009) διαπίστωσαν ότι η προβολή των πολιτικών παίζει σημαντικό ρόλο στη συμμόρφωση των εργαζομένων με τις οργανωτικές πολιτικές ασφάλειας. Οι Herath και Rao (2009) έδειξαν επίσης ότι οι ISP θα πρέπει να είναι εύκολα προσπελάσιμοι και να είναι γραμμένοι με σαφή και κατανοητό τρόπο, καθώς αυτό έχει θετικές επιπτώσεις στην πρόθεση συμμόρφωσης.

Παρόλο που η ανταλλαγή πληροφοριών έχει γίνει ένας κοινός όρος μεταξύ των υπευθύνων χάραξης πολιτικής, οι έννοιες που σχετίζονται με την πρακτική και το σκοπό της δεν είναι πάντοτε σαφώς κατανοητές. Υπάρχει γενική συμφωνία ότι η ανταλλαγή πληροφοριών και η συνεργασία μειώνουν τον κίνδυνο ασφάλειας στον κυβερνοχώρο. Αλλά η σύγχυση και η διαμάχη παραμένουν γύρω από τα στοιχεία (Goodwin & Nicolas, 2015):

• Ποιος πρέπει να μοιράζεται πληροφορίες;

• Τι πρέπει να μοιραστούμε;

• Πότε πρέπει να μοιραστεί;

• Ποια είναι η ποιότητα και η χρησιμότητα αυτού που μοιράζεται;

• Πώς πρέπει να μοιραστεί;

• Γιατί μοιράζεται;

• Τι μπορεί να γίνει με τις πληροφορίες;

Προκειμένου να διασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων εντός της υποδομής δικτύου, είναι απαραίτητο η ομάδα ασφαλείας να είναι σε θέση να ανιχνεύει και να χειρίζεται περιστατικά ασφάλειας στον κυβερνοχώρο. Για το σκοπό αυτό, είναι ζωτικής σημασίας οι ομάδες αυτές να έχουν αρκετά δεδομένα σχετικά με τα συμβάντα και τις απειλές κατά της ασφάλειας. Αυτός είναι ο λόγος για τον οποίο οι ομάδες μοιράζονται τα δεδομένα προειδοποιήσεων και συμβάντων ασφαλείας χρησιμοποιώντας διάφορες πλατφόρμες κοινής χρήσης.

Παρόλο που το κάνουν κυρίως για την προστασία των δεδομένων και της ιδιωτικής ζωής των χρηστών, η χρήση τους οδηγεί επίσης σε πρόσθετη επεξεργασία προσωπικών δεδομένων, γεγονός που μπορεί να προκαλέσει νέους κινδύνους για την προστασία της ιδιωτικής ζωής. Ο ευρωπαϊκός νόμος για την προστασία των δεδομένων, ιδίως με την έγκριση του νέου γενικού κανονισμού για την προστασία των δεδομένων, θεσπίζει πολύ

αυστηρούς κανόνες επεξεργασίας δεδομένων προσωπικού χαρακτήρα που, αφενός, οδηγούν σε μεγαλύτερη προστασία των δικαιωμάτων των ατόμων αλλά, αφετέρου, δημιουργούν μεγάλα εμπόδια για όσους χρειάζονται να μοιραστείτε τα προσωπικά σας δεδομένα (Stupka et al., 2017).

Τα οφέλη ασφάλειας της ανταλλαγής πληροφοριών πρέπει να επιτυγχάνονται κατά τρόπο που να μην αλλοιώνει την ιδιωτική ζωή ή να έχει αρνητικές επιπτώσεις στις ελευθερίες. Η ανταλλαγή δεδομένων για τον κυβερνοχώρο μπορεί να δημιουργήσει ορισμένες ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής και τις ατομικές ελευθερίες, μεταξύ των οποίων (Goodwin & Nicolas, 2015):

• Τι είδους πληροφορίες μοιράζονται;

• Σε ποιο βαθμό μπορεί να συνδεθεί με άτομα ή οργανισμούς;

• Ποια είναι η πληροφορία που μοιράζεται (ιδιαίτερα όταν διαβιβάζεται από τον ιδιωτικό τομέα στην κυβέρνηση);

• Πώς αποθηκεύονται και χρησιμοποιούνται οι πληροφορίες;

Η ισχυρή προστασία της ιδιωτικής ζωής και των πολιτικών ελευθεριών είναι πρωταρχικής σημασίας εάν ένα πρόγραμμα ανταλλαγής πληροφοριών πρέπει να γίνει ευρέως αποδεκτό και να επιτύχει.

Στο επόμενο κεφάλαιο αναλύεται ο τρόπος με τον οποίο μπορεί να ενισχυθεί η ασφάλεια μέσω της ανταλλαγής πληροφοριών και των δεικτών σε μια πλατφόρμα ανταλλαγής πληροφοριών, όπως το MISP.

3.1 Firewall, IPS και IDS

Τόσο τα Firewall όσο και τα IPS και IDS σχετίζονται με την παροχή ασφάλειας στο δίκτυο και θεωρούνται βασικά συστατικά ενός δικτύου. Η κύρια διαφορά είναι ότι το τείχος προστασίας ορίζει από πριν τις ενέργειες όπως το κλείδωμα (blocking) και το φιλτράρισμα της κίνησης ενώ τα IPS και IDS ανιχνεύουν και ειδοποιούν έναν διαχειριστή συστήματος ή εμποδίζουν την επίθεση σύμφωνα με τη διαμόρφωση.

Ένα τείχος προστασίας επιτρέπει τη διακίνηση επισκεψιμότητας βάσει ενός συνόλου κανόνων. Βασίζεται στην πηγή, στις διευθύνσεις προορισμού και στις θύρες. Ένα τείχος προστασίας μπορεί να αρνηθεί οποιαδήποτε κίνηση που δεν πληροί τα συγκεκριμένα κριτήρια.

Αντίθετα ένα IDS είναι μια παθητική συσκευή που παρακολουθεί πακέτα δεδομένων που διασχίζουν το δίκτυο, συγκρίνοντας με τα πρότυπα υπογραφής και ενεργοποιώντας έναν συναγερμό για την ανίχνευση σε ύποπτη δραστηριότητα. Από την άλλη, ένα IPS είναι μια ενεργή συσκευή που αποτρέπει τις επιθέσεις αποκλείοντας τες.
Στους ακόλουθους πίνακες (Πίνακας 1& Πίνακας 2) προσδιορίζονται οι βασικές διαφορές μεταξύ τον συστημάτων αυτών και οι τρόποι λειτουργίας και εφαρμογής τους.

Πίνακας 1: Βασικά στοιχεία Firewalls-IPS-IDS

Παράμετροι	**Firewalls**	**IPS**	**IDS**
Φιλοσοφία	Τα τείχη προστασίας είναι μια συσκευή/λογισμικό ασφάλειας δικτύου που φιλτράρει την εισερχόμενη και εξερχόμενη κίνηση δικτύου βάσει προκαθορισμένων κανόνων	Το IPS είναι μια συσκευή/λογισμικό που ελέγχει την κυκλοφορία, εντοπίζει και ταξινομεί την κακόβουλη κίνηση από μια επίθεση.	Το IDS είναι μια συσκευή ή μια εφαρμογή λογισμικού που παρακολουθεί ένα πρότυπο κυκλοφορίας ή υπογραφές της επίθεσης και παράγει ειδοποιήσεις.
Αρχή λειτουργίας	Φιλτράρει την επισκεψιμότητα με βάση τη διεύθυνση IP και τους αριθμούς θυρών.	Ελέγχει τα πρότυπα κυκλοφορίας σε πραγματικό χρόνο ή τις υπογραφές της επίθεσης και στη συνέχεια αποτρέπει την επίθεση κατά της ανίχνευσης.	Ανιχνεύει την κυκλοφορία σε πραγματικό χρόνο και βλέπει πρότυπα ή υπογραφές επίθεσης και δημιουργεί ειδοποιήσεις.
Τοποθέτηση	Στην περίμετρο του δικτύου.	Γενικά μετά από το τείχος προστασίας.	Μη ενσωματωμένο μέσω θύρας.
Κυκλοφορία	Δεν αναλύει	Αναλύει	Αναλύει
Χρήση με άλλα συστήματα	Θα πρέπει να είναι η πρώτη γραμμή άμυνας.	Θα πρέπει να τοποθετείται μετά τη συσκευή τείχους προστασίας στο δίκτυο.	Θα πρέπει να τοποθετείται μετά το τείχος προστασίας.

Δράση κατά την ανίχνευση	Εμποδίζει (block) την κυκλοφορία.	Αποτρέπει την κυκλοφορία κατά την ανίχνευση ανωμαλίας.	Ειδοποιήσεις και συναγερμοί (alarms) σχετικά με την ανίχνευση ανωμαλιών.

Πίνακας 2: Βασικές ιδιότητες - Βασικά στοιχεία Firewalls-IPS-IDS

Παράμετροι	**Firewalls**	**IPS**	**IDS**
Βαθύ φιλτράρισμα πακέτων	+		
Επιτρέπει ή εμποδίζει την κυκλοφορία με κανόνες θυρών και πρωτοκόλλου.	+		
Ανίχνευση που βασίζεται στην ανωμαλία.		+	+
Ανίχνευση υπογραφής.		+	+
Επίθεση μηδενικής ημέρας.		+	+
Εμποδίζει την επίθεση.		+	
Παρακολούθηση.			+
Προειδοποίηση κινδύνου.			+

Ουσιαστικά, αυτοί τρεις τρόποι για την ασφάλεια της υποδομή μπορούν να χρησιμοποιηθούν συμπληρωματικά, αφού καλύπτουν διαφορετικές πτυχές σε ζητήματα ασφαλείας μιας υποδομής αλλά απαραίτητες για την αύξηση της ασφάλειας. Αξίζει να σημειωθεί ότι τα Firewalls λειτουργούν μόνο σε δικτυωμένα συστήματα σε αντίθεση με τα IPS και IDS που εκτός από το δίκτυο μπορούν να εγκατασταθούν σε κεντρικούς

υπολογιστές ή περιφερειακά. Από την άλλη ένα firewall μπορεί να εμποδίσει μια κυκλοφορία, αλλά μόνο σύμφωνα με τους κανόνες που έχουν οριστεί, ενώ ένα σύστημα IPS μπορεί να αναλύσει περισσότερα στοιχεία και να εμποδίσει μια εισβολή. Παρόμοια με τα συστήματα IPS, τα συστήματα IDS μπορούν επίσης να αναλύσουν την κυκλοφορία των δεδομένων, αλλά δεν μπορούν να αποτρέψουν μια επίθεση, αλλά να ενημερώσουν τους διαχειριστές σχετικά με τον πιθανό κίνδυνο.

3.2 Firewall και Antivirus

Τα τείχη προστασίας και τα λογισμικά προστασίας από ιούς είναι οι μηχανισμοί για την παροχή ασφάλειας στα συστήματά. Παρόλο που οι ευπάθειες είναι διαφορετικές και στις δύο περιπτώσεις. Η μεγάλη διαφορά μεταξύ τους είναι ότι το τείχος προστασίας λειτουργεί ως φραγμός για την εισερχόμενη κίνηση στο σύστημα. Ενώ, το λογισμικό προστασίας από ιούς προστατεύει από τις εσωτερικές επιθέσεις, όπως τα κακόβουλα αρχεία.

Στην ακόλουθο πίνακα δίνεται ένα συγκριτικό διάγραμμα για τα τύχει προστασίας και τα λογισμικά προστασίας από ιούς.

Πίνακας 3: Σύγκριση Firewall και Antivirus

Παράμετροι	**Firewall**	**Antivirus**
Εφαρμογή	Υλικό και λογισμικό.	Μόνο λογισμικό.
Λειτουργίες	Παρακολούθηση και φιλτράρισμα βάση συγκεκριμένων κανόνων.	Σάρωση μολυσμένων αρχείων και λογισμικού.
Πεδίο δράσης	Εξωτερικές απειλές.	Εσωτερικές και εξωτερικές απειλές.
Έλεγχος επιθέσεων	Εισερχόμενα πακέτα.	Κακόβουλο λογισμικό που βρίσκεται στο σύστημα.

Στο επόμενο κεφάλαιο αναλύεται ο τρόπος με τον οποίο μπορεί να ενισχυθεί η ασφάλεια μέσω της ανταλλαγής πληροφοριών και των δεικτών σε μια πλατφόρμα ανταλλαγής πληροφοριών, όπως το MISP.

4. Ανταλλαγή πληροφοριών και δείκτες

Σε αυτό το κεφάλαιο περιγράφεται ο τρόπος με τον οποίο μπορεί να ενισχυθεί η ασφάλεια από τις πλατφόρμες ανταλλαγής πληροφοριών μέσω της ανταλλαγής πληροφοριών και των δεικτών. Για πιο παραδειγματική περιγραφή και για να γίνει πιο κατανοητή η ανάλυση αυτή γίνεται με βάση τη λειτουργικότητα του εργαλείου MISP.
Η ανταλλαγή πληροφοριών για τις απειλές παρέχει πληροφορίες σχετικά με υπάρχουσες ή αναδυόμενες απειλές. Αυτές οι πληροφορίες έρχονται με το πλαίσιο, τους δείκτες, τις επιπτώσεις και τα δεδομένα που μπορούν να ενεργοποιηθούν.
Εισαγωγικά υπενθυμίζεται και διευκρινίζεται η έννοια των δεικτών. Για παράδειγμα, όταν υπάρχει έγκλημα, οι ντετέκτιβ έρχονται και αναζητούν ενδείξεις. Το κάνουν αυτό για να απαντήσουν σε σημαντικά ερωτήματα, όπως γιατί και πώς συνέβη. Αυτό είναι πολύ σημαντικό, όχι μόνο για την επίλυση ενός συγκεκριμένου εγκλήματος αλλά και για τη συλλογή πληροφοριών που θα μπορούσαν να βοηθήσουν στην επίλυση άλλων συσχετισμένων εγκλημάτων και ίσως ακόμη και να αποφευχθούν άλλα παρόμοια.
Αυτή είναι ακριβώς η ίδια ιδέα γύρω από τους δείκτες. Ακόμη και αν ο επιτιθέμενος προσπαθεί να ελαχιστοποιήσει τα ίχνη του, υπάρχουν πάντα μερικά. Μπορεί να είναι διευθύνσεις ηλεκτρονικού ταχυδρομείου, διευθύνσεις IP, κακόβουλα λογισμικά, διευθύνσεις URL και άλλα. Η ιδέα είναι να χρησιμοποιηθούν αυτά τα ίχνη για να ενεργοποιηθούν οι συναγερμοί σε άλλα συστήματα υπολογιστών μόλις θεωρηθεί ότι τα προστατεύουν καθώς και η συλλογή νέων πληροφοριών. Αυτός είναι ο λόγος που αυτές οι ενδείξεις καλούνται δείκτες συμβιβασμού (“Indicator Of Compromise” - IOC).
Η βάση δεδομένων του MISP περιέχει δεδομένα για τους δείκτες και επιτρέπει την αποθήκευση τεχνικών και μη τεχνικών πληροφοριών σχετικά με δείγματα, περιστατικά, επιθέσεις και πληροφορίες σχετικά με τα κακόβουλα λογισμικά. Οι αυτόματες σχέσεις συσχέτισης μεταξύ χαρακτηριστικών και δεικτών από κακόβουλο λογισμικό, επίθεση εκστρατειών ή ανάλυσης είναι επίσης μια από τις δυνατότητες του MISP. Ο μηχανισμός συσχέτισης περιλαμβάνει το συσχετισμό μεταξύ των χαρακτηριστικών και των δεικτών για τα κακόβουλα λογισμικά και τις επιθέσεις εκστρατειών ή ανάλυσης. Η αντιστοιχία μπορεί επίσης να ενεργοποιηθεί ή να απενεργοποιηθεί ένα συμβάν ανά χαρακτηριστικό.
Παράλληλα, με το ευέλικτο μοντέλο δεδομένων του MISP, τα σύνθετα αντικείμενα μπορούν να εκφραστούν και συνδεθούν μεταξύ τους για να εκφράσουν πληροφορίες απειλής, συμβάντα ή συναφή στοιχεία.

Επιπλέον, με την ενσωματωμένη λειτουργικότητα κοινής χρήσης διευκολύνεται η κοινή χρήση δεδομένων χρησιμοποιώντας διαφορετικό μοντέλο διανομών. Το MISP μπορεί να συγχρονίζει αυτόματα τα συμβάντα και τα χαρακτηριστικά μεταξύ διαφορετικών πλατφορμών ανταλλαγής πληροφοριών. Οι λειτουργίες φιλτραρίσματος μπορούν να χρησιμοποιηθούν για την κάλυψη κάθε πολιτικής κοινής χρήσης, συμπεριλαμβανομένης μιας ευέλικτης δυναμικότητας ομάδας ανταλλαγής και μηχανισμών διανομής για τα επίπεδα των χαρακτηριστικών.

Για να είναι αποτελεσματικά η ανταλλαγή πληροφοριών με άλλες πλατφόρμες θα πρέπει να βασίζονται σε ένα πρότυπο. Αυτή τη στιγμή υπάρχουν τρεις αξιόπιστες προσπάθειες δημιουργίας προτύπων για την ανταλλαγή πληροφοριών, το STIX, το TAXII και το CybOX. Ωστόσο, αυτές είναι μόνο οι προδιαγραφές και όχι τα πραγματικά εργαλεία που παρέχουν μια πλατφόρμα για την ανταλλαγή και τον εμπλουτισμό των δεδομένων απειλών (Impe, 2015). Το MISP υποστηρίζει το πρότυπο STIX και για την εξαγωγή των δεδομένων υποστηρίζει και το πρότυπο TAXII.

Η διαισθητική διεπαφή χρήστη επιτρέπει στους τελικούς χρήστες να δημιουργούν, να ενημερώνουν και να συνεργάζονται σε συμβάντα και χαρακτηριστικά ή δείκτες. Η γραφική διεπαφή διευκολύνει επίσης την εύκολη πλοήγηση μεταξύ των συμβάντων και των συσχετισμών τους. Ακόμη, περιλαμβάνει προηγμένες λειτουργίες φιλτραρίσματος και λίστα προειδοποιήσεων για να βοηθήσει τους αναλυτές να συντελέσουν τα γεγονότα και τις ιδιότητες.

Η αποθήκευση των δεδομένων γίνεται σε δομημένη μορφή γεγονός που επιτρέπει την αυτοματοποιημένη χρήση της βάσης δεδομένων για διάφορους σκοπούς, με εκτεταμένη υποστήριξη των δεικτών ασφάλειας στον κυβερνοχώρο σε δείκτες απάτης όπως στον χρηματοπιστωτικό τομέα. Η εξαγωγή των δεδομένων μπορεί να γίνει σε πολλές μορφές όπως OpenIoC, απλό κείμενο (text), CSV, MISP XML ή JSON έξοδο για την ενσωμάτωση με άλλα συστήματα (IDS δικτύου, IDS υποδοχής, προσαρμοσμένα εργαλεία). Από προεπιλογή υποστηρίζονται οι μορφές εξαγωγής δεδομένων Suricata, Snort και Bro τα οποία χρησιμοποιούνται από τα συστήματα ανίχνευση εισβολής (IDS). Περισσότερες λεπτομέρειες για τα IDS δίνονται στις ακόλουθες ενότητας της εργασίας. Από την άλλη η εισαγωγή των δεδομένων μπορεί να είναι μαζική (bulk import) ή τμηματική (batch import), και τα δεδομένα που εισάγονται μπορεί να είναι σε μορφή απλού κειμένου, από OpenIOC, GFI sandbox, σε μορφή CSV ή MISP.

Έτσι, το MISP διαθέτει ένα εργαλείο εισαγωγής κειμένου για να διευκολύνει την ενσωμάτωση των αναφορών σε MISP.

Ακόμη το MISP δίνει τη δυνατότητα για ρυθμιζόμενη ταξινόμηση και επισήμανση συμβάντων σύμφωνα με τα συστήματα ταξινόμησης του χρήστη, δηλαδή του οργανισμού ή σύμφωνα με τις υπάρχουσες ταξινομίες του MISP. Η ταξινόμηση μπορεί να είναι τοπική στο MISP, αλλά και να μοιράζεται μεταξύ των περιπτώσεων MISP. Το MISP περιλαμβάνει προεπιλεγμένο σύνολο γνωστών ταξινομήσεων και συστημάτων ταξινόμησης για την υποστήριξη της τυποποιημένης ταξινόμησης, όπως χρησιμοποιείται από πολλούς οργανισμούς.

Τέλος, το MISP διαθέτει ενσωματωμένη κρυπτογράφηση και υπογραφή των ειδοποιήσεων μέσω PGP ή S/MIME ανάλογα με τις προτιμήσεις του χρήση, καθώς επίσης διαθέτει και μονάδες επέκτασης (expansion modules) Python για την επέκταση του MISP σύμφωνα με τις υπηρεσίες του χρήστη ή την ενεργοποίηση ήδη διαθέσιμων μονάδων (MISP modules).

Η κοινή χρήση και η ανταλλαγή πληροφοριών σχετικά με τις απειλές αυξάνει τη γνώση για τους αντιπάλους, τα περιουσιακά στοιχεία και τον τρόπο με τον οποίο οι επιτιθέμενοι μπορεί να προσπαθήσουν να αποκτήσουν πρόσβαση στο περιβάλλον.

Στην ακόλουθη ενότητα γίνεται σύγκριση του εργαλείου MISP με ένα εργαλείο ανταλλαγής πληροφοριών για απειλές, την πλατφόρμα X-Force Exchange.

4.1 MISP vs X-Force Exchange

Υπάρχουν πολλά εργαλεία για την ανταλλαγή πληροφοριών απειλής, για τις ανάγκες αυτής της εργασίας συγκρίνονται το MISP και το X-Force Exchange της IBM[5]. Αν και τα δύο εργαλεία στοχεύουν στην επίτευξη των ίδιων δεδομένων ανταλλαγής αποτελεσμάτων, χρησιμοποιούν διαφορετικές προσεγγίσεις για την επίτευξη αυτού του στόχου.

Το MISP, όπως ήδη έχει αναφερθεί, είναι η πλατφόρμα ανταλλαγής πληροφοριών κακόβουλου λογισμικού, η οποία πρέπει να εγκατασταθεί σε ένα διακομιστή στην υποδομή του χρήστη. Ο χρήστης χρειάζεται έναν διακομιστή του διαδικτύου (Web Server), μια βάση δεδομένων και υποστήριξη PHP με μερικές μονάδες (modules). Όλα τα δεδομένα αποθηκεύονται στις εγκαταστάσεις του χρήστη και βρίσκονται υπό τον έλεγχό του. Η ασφάλεια του διακομιστή, η εξασφάλιση της πρόσβασης και της

[5] IBM , https://www.ibm.com/security/xforce?ce=ISM0484&ct=SWG&cr=Security&ccy=US

επικοινωνίας και η πρόβλεψη αντιγράφων ασφαλείας είναι ευθύνη του ίδιου του χρήστη. Ουσιαστικά, ο χρήστης ελέγχει πλήρως τι συμβαίνει με τα δεδομένα του.

Από την άλλη πλευρά, το X-Force Exchange της IBM είναι μια πλατφόρμα που βασίζεται σε νέφος (cloud). Ο χρήστης χρειάζεται ένα αναγνωριστικό IBM για να έχει πλήρη πρόσβαση στα διαθέσιμα δεδομένα απειλών (είναι επίσης δυνατή η ανώνυμη πρόσβαση, αλλά με περιοριστική χρήση) και μόνο ένα πρόγραμμα περιήγησης για να ξεκινήσετε. Δεν υπάρχει ανάγκη για εγκατάσταση πρόσθετου λογισμικού. Όλα τα δεδομένα αποθηκεύονται στο νέφος, οπότε δεν χρειάζεται να ανησυχεί ο χρήστης για αντίγραφα ασφαλείας ή απώλειες.

Το MISP θα ξεκινήσει με μια κενή βάση δεδομένων. Διαφορετικές περιπτώσεις MISP μπορούν να συνδεθούν μεταξύ τους. Αυτό επιτρέπει στο χρήστη να λάβει πληροφορίες απειλών από άλλες περιπτώσεις και, στη συνέχεια, να αποθηκεύσει αυτά τα δεδομένα σε τοπικό επίπεδο, πράγμα που εξασφαλίζει ότι τα ερωτήματα για πληροφορίες παραμένουν εμπιστευτικά και περιορίζονται στον διακομιστή του χρήστη. Το MISP προβλέπει τέσσερα μοντέλα κοινής χρήσης, μόνο με τον οργανισμό, μόνο με αυτήν την κοινότητα, μόνο με τις συνδεδεμένες κοινότητες και με όλες τις κοινότητες.

Από την άλλη το X-Force Exchange χρησιμοποιεί την έννοια των συλλογών, οι οποίες είναι σύνολα πληροφοριών που σχετίζονται με μια έρευνα. Οι χρήστες μπορούν να συγκεντρώσουν διαφορετικές παρατηρήσεις ή και δείκτες σε μια συλλογή και στη συνέχεια να τα μοιραστούν με όσους χρήστες θέλουν. Αυτοί οι χρήστες μπορούν να είναι μόνο θεατές ή ένας συνδυασμός θεατών και συνεισφερόντων. Οι συλλογές μπορούν επίσης να είναι ιδιωτικές ή δημόσιες.

Αυτό δεν ανταποκρίνεται πλήρως στην κοινή χρήση με το μοντέλο κοινοποίησης κοινής χρήσης του MISP, αλλά επιτρέπει το λεπτομερή φιλτραρίσματος του χρήστη που μπορεί να έχει πρόσβαση στα δεδομένα.

Και τα δύο εργαλεία έχουν υποστήριξη για το STIX. Το X-Force Exchange υποστηρίζει τα STIX και TAXII τόσο μέσω διεπαφής προγραμματισμού εφαρμογών (API) όσο και μέσω διεπαφής χρήστη του Web. Έχει τη δυνατότητα εισαγωγής και εξαγωγής εγγράφων STIX μέσα και έξω από μια συλλογή. Το MISP υποστηρίζει την εξαγωγή δεδομένων σε μορφή TAXII.

Και οι δύο πλατφόρμες διαθέτουν διασύνδεση μέσω Web, αλλά αυτό δεν αποτελεί το βέλτιστο τρόπο για την ενσωμάτωση με την υποδομή του χρήστη. Και οι δύο πλατφόρμες παρέχουν επίσης ένα API για να ξεπεραστεί αυτό το πρόβλημα.

Το API είναι απαραίτητο για την αυτόματη ενημέρωση των συσκευών ασφαλείας (όπως IDS) με τις πιο πρόσφατες διαθέσιμες πληροφορίες.

Το API X-Force Exchange παρέχει ένα ασφαλές, ξεκούραστο, βασισμένο σε JSON API που υποστηρίζει τόσο δημόσια όσο και πιστοποιημένα ερωτήματα. Ο χρήστης μπορεί να γράψει το τη δική του μονάδα (module) για να αποκτήσει πρόσβαση στο API ή να χρησιμοποίηση ένα από τα έργα που υπάρχουν ήδη στο Github.

Το MISP διαθέτει επίσης ένα ξεκούραστο, βασισμένο σε JSON API που μπορεί να χρησιμοποιηθεί για την αυτοματοποίηση και τη τροφοδότηση των συσκευών του χρήστη. Υπάρχει μια βιβλιοθήκη Python, PyMISP , που αναπτύχθηκε από το CIRCL και επιτρέπει την εύκολη πρόσβαση στο API.

Στον ακόλουθο πίνακα (Πίνακας 4) δίνεται μια συνοπτική σύγκριση των δύο αυτών εργαλείων.

Πίνακας 4: Σύγκριση εργαλείων MISP και X-Force Exchange

	MISP	X-Force Exchange
Απαιτήσεις	Τοπική εγκατάσταση - Διακομιστής Web - Βάση δεδομένων - Υποστήριξη PHP με modules	Εγκατάσταση σε νέφος - Αναγνωριστικό IBM - Πρόγραμμα περιήγησης
Αποθήκευση δεδομένων	- Στην ευθύνη του χρήστη - Πλήρης έλεγχος των δεδομένων	- Αποθήκευση στο νέφος - Δεν χρειάζονται αντίγραφα ασφαλείας
Υποστηριζόμενα πρότυπα	- STIX για εξαγωγή και εισαγωγή δεδομένων - TAXII μόνο για εξαγωγή δεδομένων	- STIX και TAXII για εισαγωγή και εξαγωγή δεδομένων.
API	- JSON API - Εύκολο στη χρήση - Δημιουργία module - Διαθέσιμα Module Python (PyMISP)	- JSON API - Εύκολο στη χρήση - Δημιουργία module - Διαθέσιμα Module

Εν κατακλείδι, το MISP είναι πολύ ισχυρό όταν πρόκειται για την οικοδόμηση κεντρικών δεικτών συμβιβαστικής βάσης δεδομένων που περιέχουν τόσο τεχνικές όσο και μη τεχνικές πληροφορίες. Εν τω μεταξύ, η έκδοση Web του X-Force Exchange παρέχει μια πολύ πιο αθόρυβη διεπαφή για την προβολή των τάσεων και της συνεχιζόμενης δραστηριότητας απειλών, δίνοντάς μια άμεση εικόνα στο χρήστη για το τι συμβαίνει.

Τα διαφορετικά εργαλεία που είναι διαθέσιμα για την ανταλλαγή πληροφοριών απειλής δεν αποκλείουν το ένα το άλλο. Μπορεί κανείς να χρησιμοποίηση λύσεις όπως το MISP σε εγκαταστάσεις και λύσεις που βασίζονται στο νέφος όπως το X-Force Exchange και, στη συνέχεια, να επιλέξει, ανάλογα με τον τύπο πληροφοριών απειλής που αντιμετωπίζει, πού να αποθηκεύσει τις πληροφορίες.

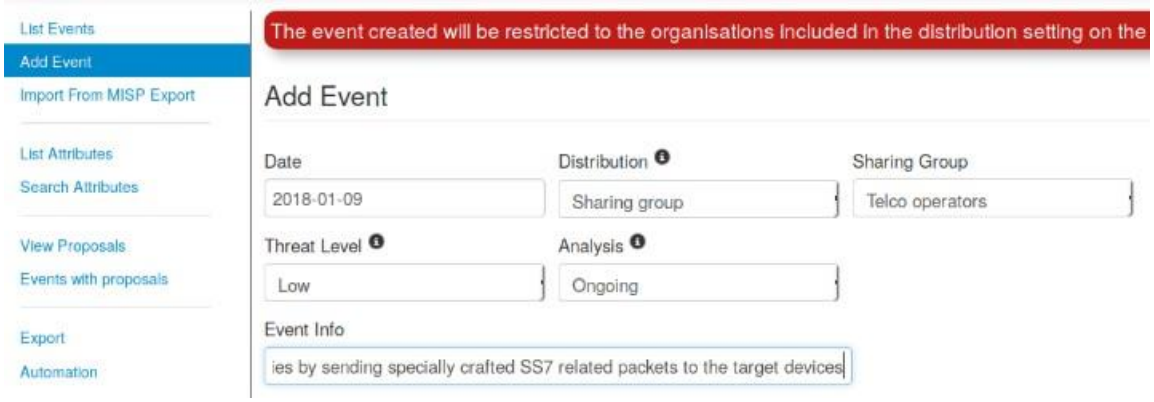
5. Καταγραφή συμβάντων μέσω του MISP

Τα τρωτά σημεία του λογισμικού και του υλικού συχνά συζητούνται, μοιράζονται, προετοιμάζονται, αναλύονται και εξετάζονται πριν από τη δημοσίευση τους. Η διαδικασία αυτή μπορεί να είναι κουραστική, καθώς συχνά περιλαμβάνει πολλαπλές ανταλλαγές μεταξύ των εμπλεκόμενων μερών, συμπεριλαμβανομένων των δημοσιογράφων, των πληρεξουσίων, των συντονιστών, των εκδοτών και ακόμη και των εμπλεκομένων μερών. Ορισμένα τρωτά σημεία ενδέχεται να μοιράζονται και να ανταλλάσσονται μεταξύ αξιόπιστων μερών για μήνες πριν δημοσιευθούν επίσημα. Αυτό μπορεί να δημιουργήσει σημαντικό φόρτο εργασίας για το προσωπικό που ασχολείται με την ασφάλειας και την αξιολόγηση της ευπάθεια.

Καθώς το MISP παρέχει την πλήρη λίστα των λειτουργιών που διευκολύνουν την ανταλλαγή πληροφοριών, η κοινή χρήση και η συνεργασία σε θέματα ευπάθειας ασφαλείας σε μια αξιόπιστη ομάδα είναι τόσο εύκολη όσο οι δείκτες κοινής χρήσης.

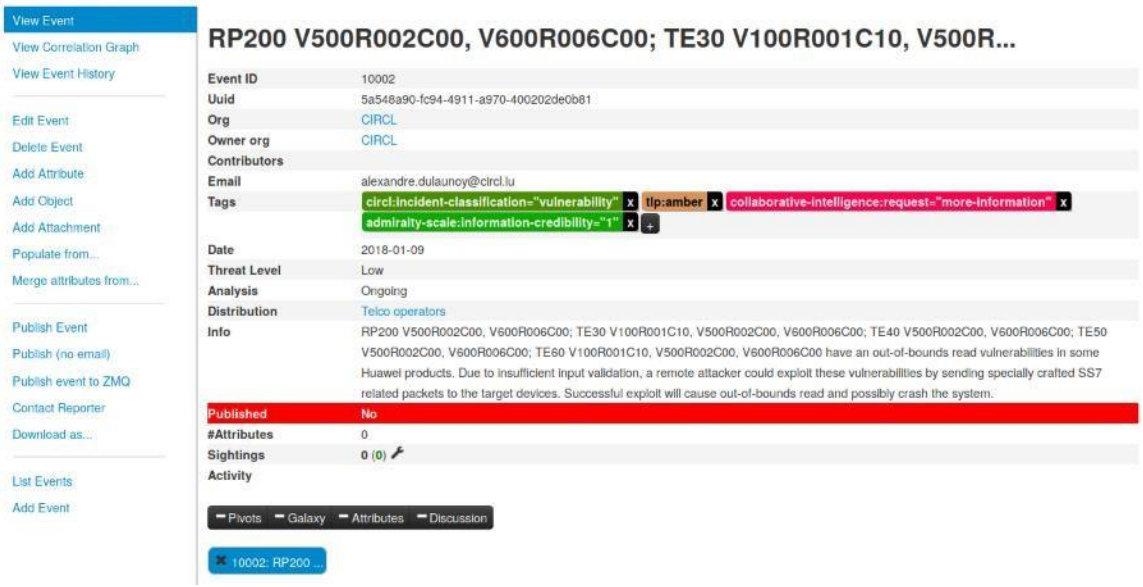
Τα αντικείμενα MISP παρέχουν έναν ευέλικτο τρόπο για να περιγράψουν τις συνδυασμένες πληροφορίες χρησιμοποιώντας ένα απλό σύστημα εργαλείων. Υπάρχει ήδη ένα αντικείμενο ευπάθειας το οποίο καλύπτει τις πιο συνηθισμένες περιπτώσεις που χρησιμοποιούνται ομάδες ασφάλειας ή ομάδες αξιολόγησης της ασφάλειας. Εάν όμως υπάρχει μια συγκεκριμένη περίπτωση χρήσης πληροφοριών ευπάθειας για κοινή χρήση, ένα αντικείμενο MISP μπορεί επίσης να κατασκευαστεί από ένα προσαρμοσμένο πρότυπο.

Η κοινή χρήση ενός συνόλου ευπαθειών σε μια αξιόπιστη ομάδα είναι απλή. Αρχικά ο χρήστης δημιουργεί ένα συμβάν (event) (Εικόνα 2) το οποίο θα περιέχει ένα ή περισσότερα τρωτά σημεία και θα αντιστοιχίσει την αντίστοιχη ομάδα κοινής χρήσης. Ένα συμβάν είναι απλώς ένα δοχείο με τα δεδομένα που σχετίζονται με αυτό, όπως μια ταξινόμηση ή μια γενική περιγραφή.



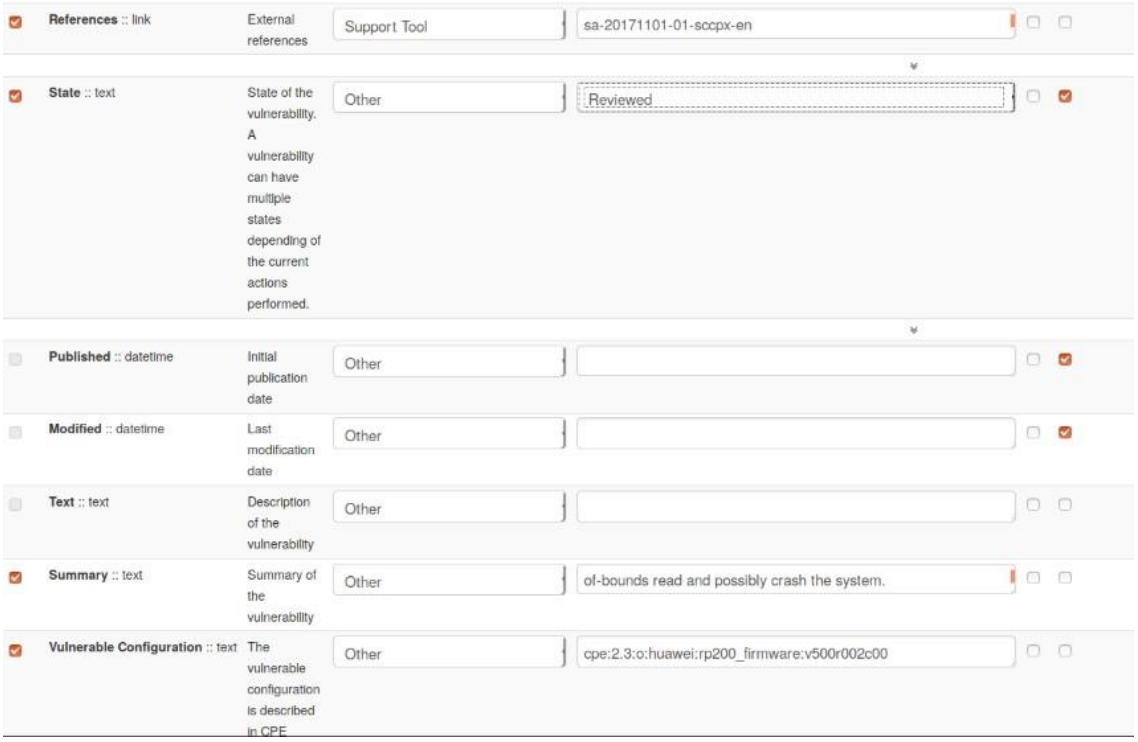
Εικόνα 2: MISP: Προσθήκη συμβάντος (Add Event) (MISP, 2018).

Στη συνέχεια, όταν δημιουργηθεί ένα νέο συμβάν, το συμβάν αυτό μπορεί να χρησιμοποιηθεί για τη σύνδεση χαρακτηριστικών ή αντικειμένων. Εάν ο χρήστης επιθυμεί μοιραστεί πληροφορίες ευπάθειας, μπορεί να προσθέσει ένα αντικείμενο ευπάθειας για να περιγράψει την ευπάθεια. Όπως φαίνεται στην ακόλουθη εικόνα (Εικόνα 3).

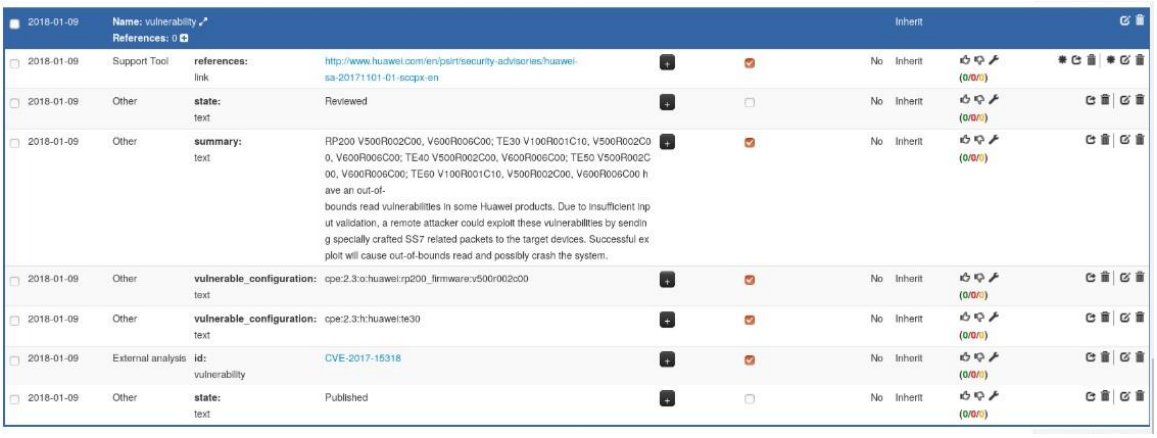


Εικόνα 3: MISP: Προσθήκη αντικειμένου (MISP, 2018).

Το αντικείμενο ευπάθειας αποτελείται από διάφορες ιδιότητες όπως η ευπάθεια διαμόρφωσης (“vulnerable configuration expressed”) που εκφράζεται ως τιμή CPE και μπορεί να προστεθεί πολλές φορές αν υπάρχουν διαφορετικές ευάλωτες διαμορφώσεις.



Εικόνα 4: MISP: Ιδιότητες αντικειμένου ευπάθειας (MISP, 2018).



Εικόνα 5: MISP: Λίστα με ευπάθειες (MISP, 2018).

5.1 Παραμετροποίηση του MISP

Το misp2.4 είναι κατασκευασμένο να λειτουργεί σε κονσόλες.

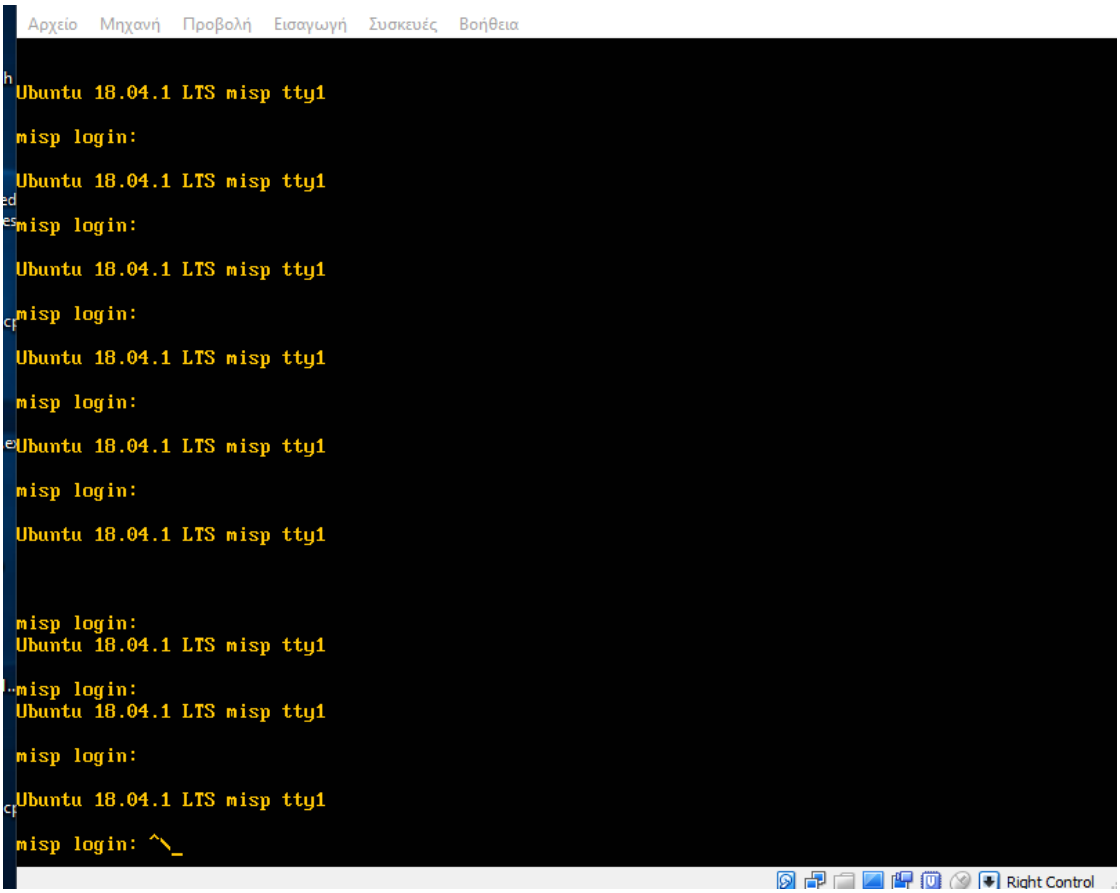
Για να λειτουργήσει σε Windows σύμφωνα με τις οδηγίες που δίνει το επίσημο site του MISP πρέπει να εγκαταστήσουμε ένα λογισμικό VIRTUAL MACHINES όπως το VMWARE ή το Virtual BOX.

Έτσι με χρήση του Virtual Box κατεβάζουμε σχετικό image και το εκτελούμε.

Στην περίπτωση μας κατεβάσαμε και λειτουργήσαμε το image

https://www.circl.lu/misp-images/latest/MISP_v2.4.94@9188d94bc4e76b81225c8e6af618d21cb837df8b.ova

Μετά την εγκατάσταση πήραμε το παρακάτω, όταν ξεκινάμε την λειτουργία του MISP



Για να κάνουμε login δίνουμε τα παρακάτω:

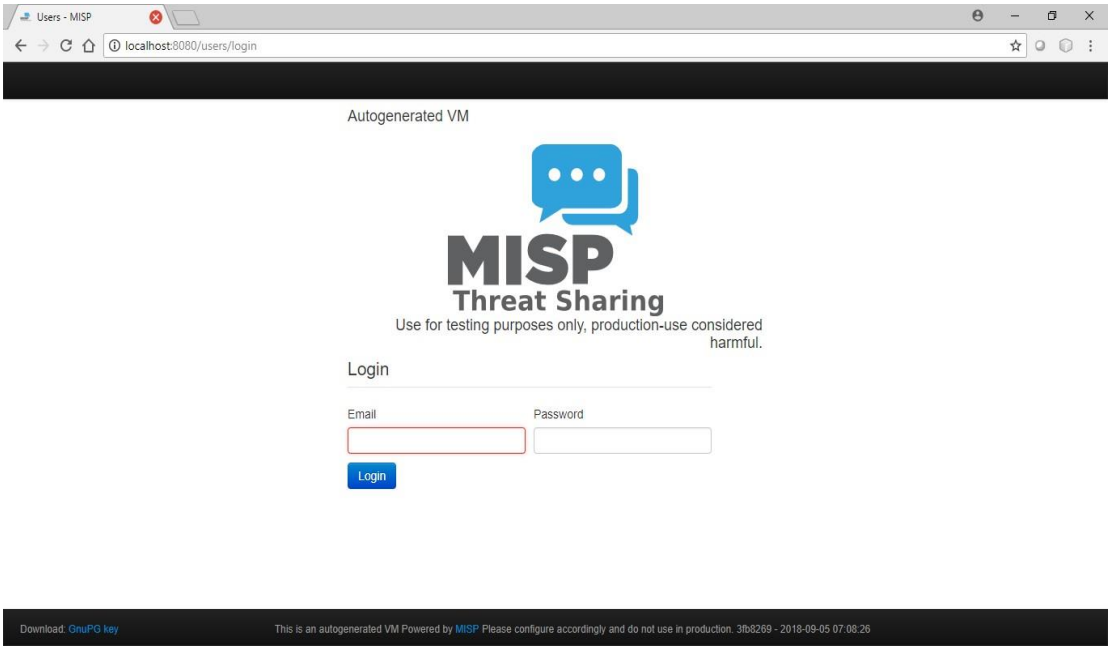
misp login: misp

password: Password1234

Αφού εκτελέσουμε το παραπάνω τότε μπορούμε να χρησιμοποιήσουμε ένα φυλλομετρητή όπως το Chrome σε οποιοδήποτε μηχάνημα Windows αρκεί να δώσουμε τη παρακάτω διεύθυνση στο φυλλομετρητή μας

Localhost:8080

Τελικά θα πάρουμε το παρακάτω:



Για να συνδεθούμε δίνουμε τα παρακάτω:

Username: admin@admin.test

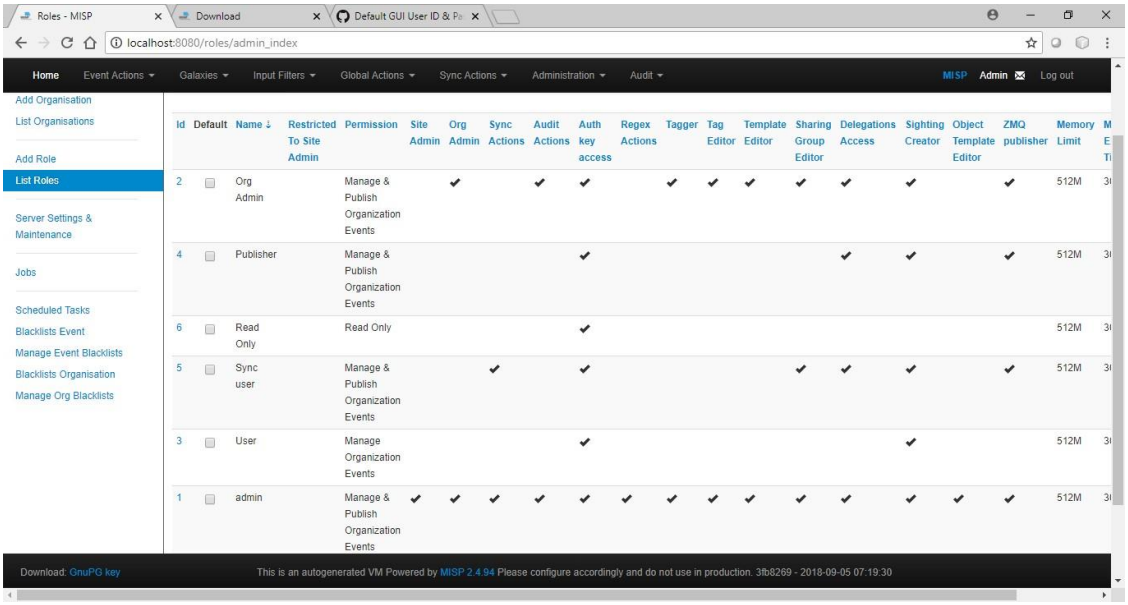
Password: admin

Με την πρώτη είσοδο είμαστε αναγκασμένοι να αλλάξουμε password

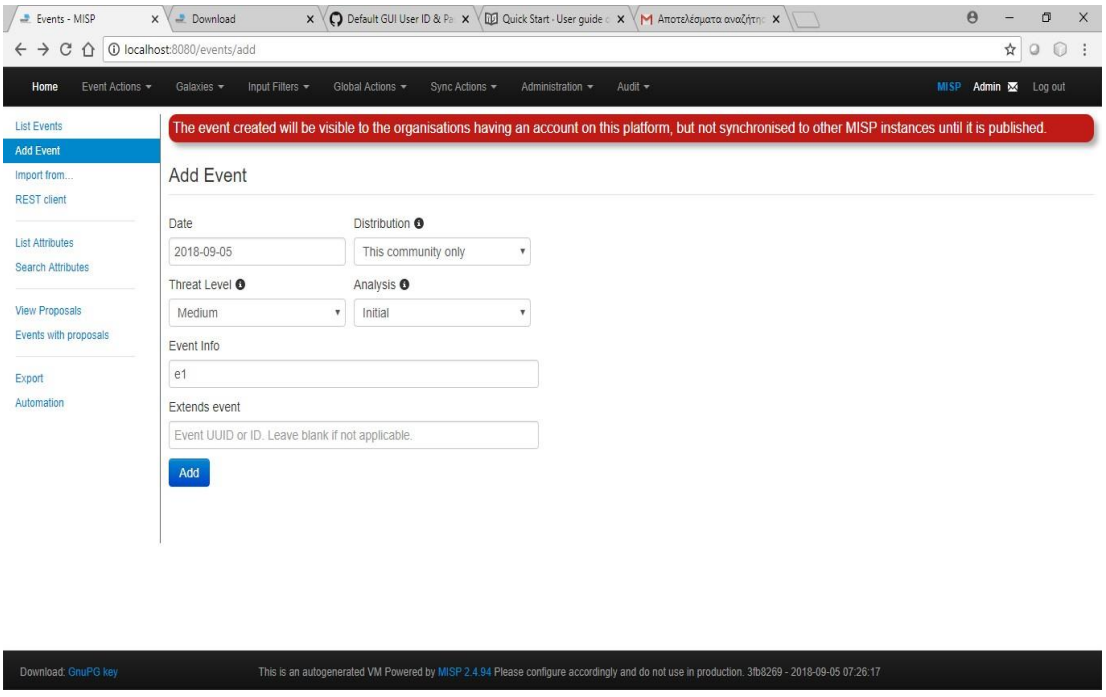
Ένα πιθανό είναι το ***Password1234***

Στην συνέχεια μπορούμε να λειτουργήσουμε αρκετά όπως να ορίσουμε ρόλους , οργανισμούς , να εισάγουμε απειλές να πάρουμε αποτελέσματα κ.α.

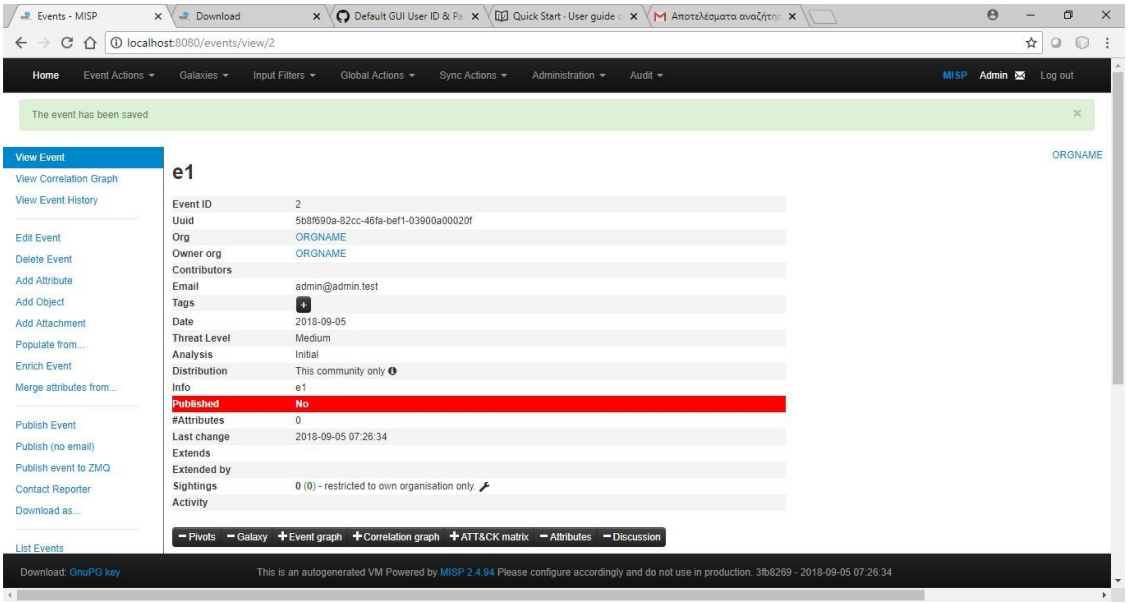
Έτσι ορίσαμε τους παρακάτω ρόλους:



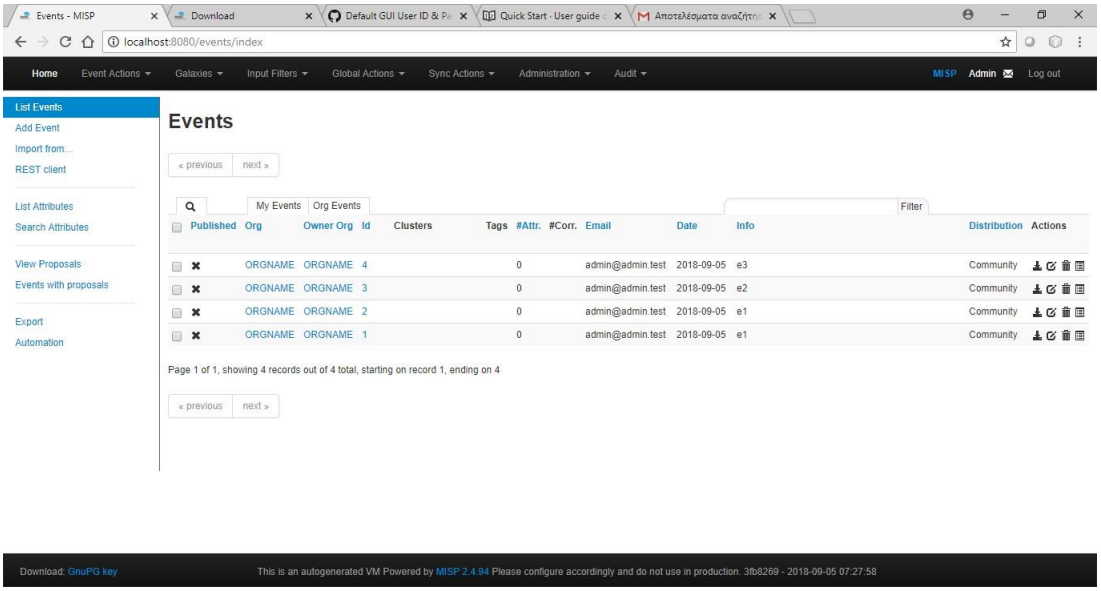
Αρχικά δημιουργούμε σειρά από events με τον παρακάτω τρόπο:



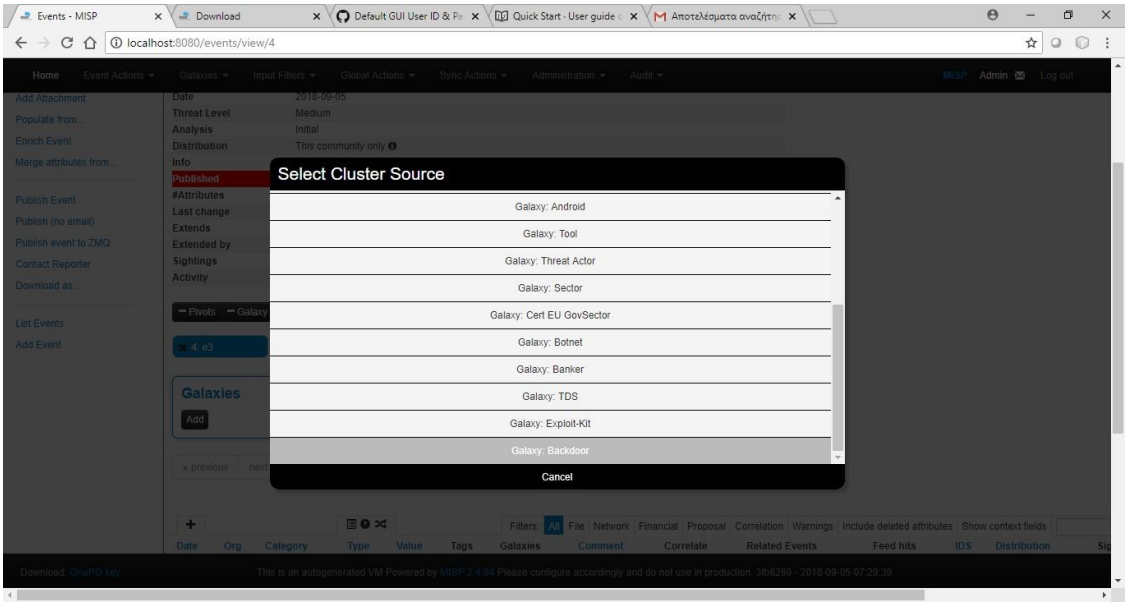
Και παίρνουμε για κάθε event το παρακάτω:



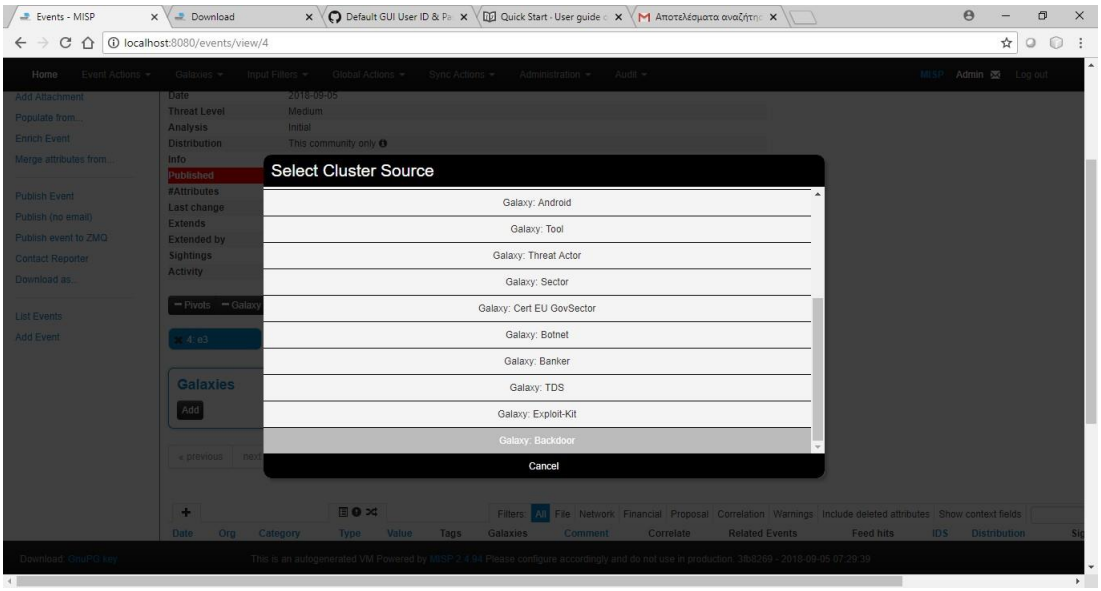
Μία λίστα από events είναι η παρακάτω:



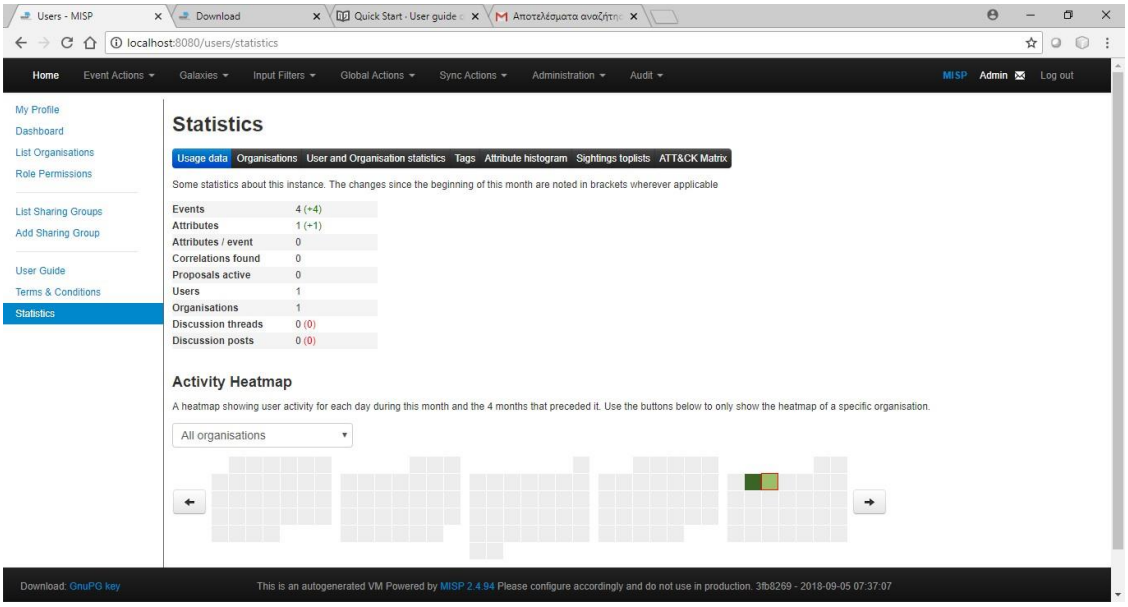
Ορίζουμε σε κάθε event σε ποιο galaxy (απειλή) θα το θέσουμε από τα παρακάτω:



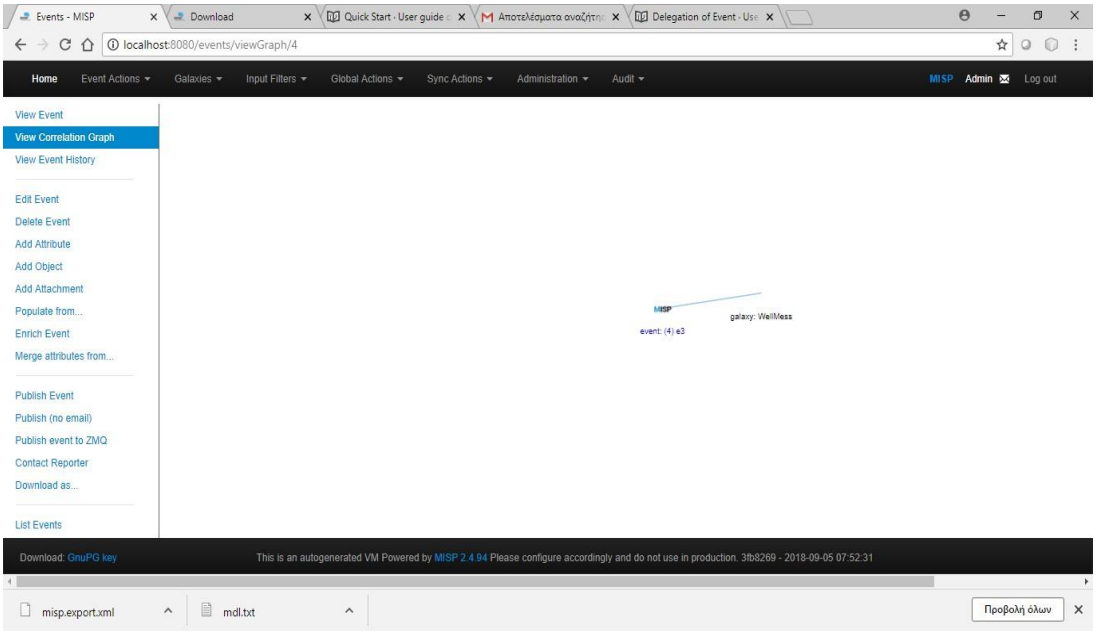
Έτσι ορίζοντας πως θα λειτουργεί έχουμε το παρακάτω αποτέλεσμα

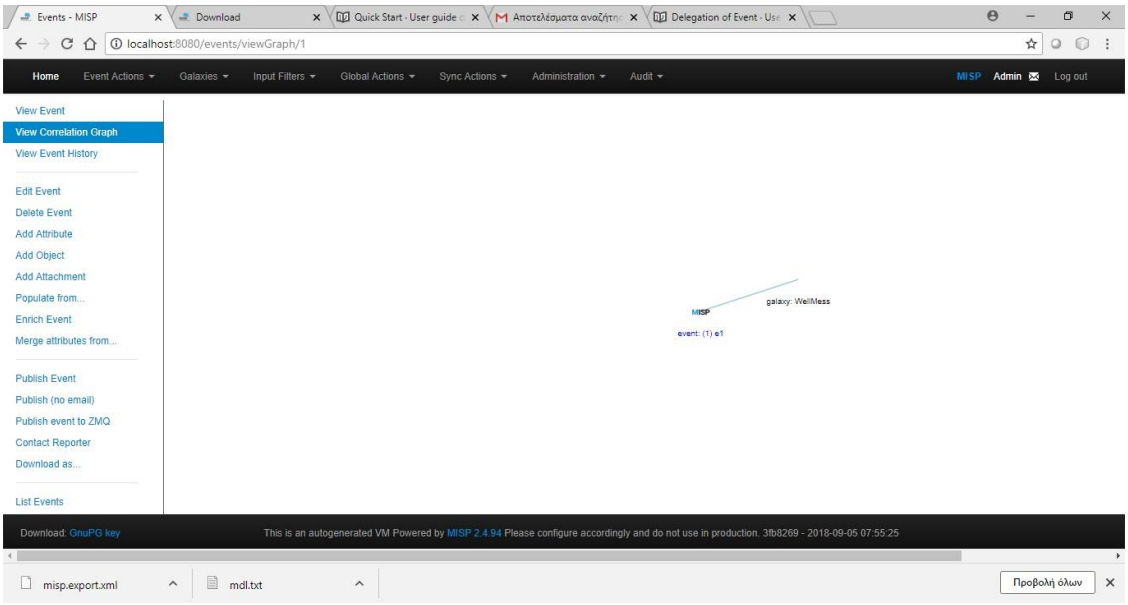


Έτσι ορίζουμε σειρά από events ώστε να πάρουμε τα στατιστικά μας και έχουμε π.χ. το παρακάτω αποτέλεσμα:

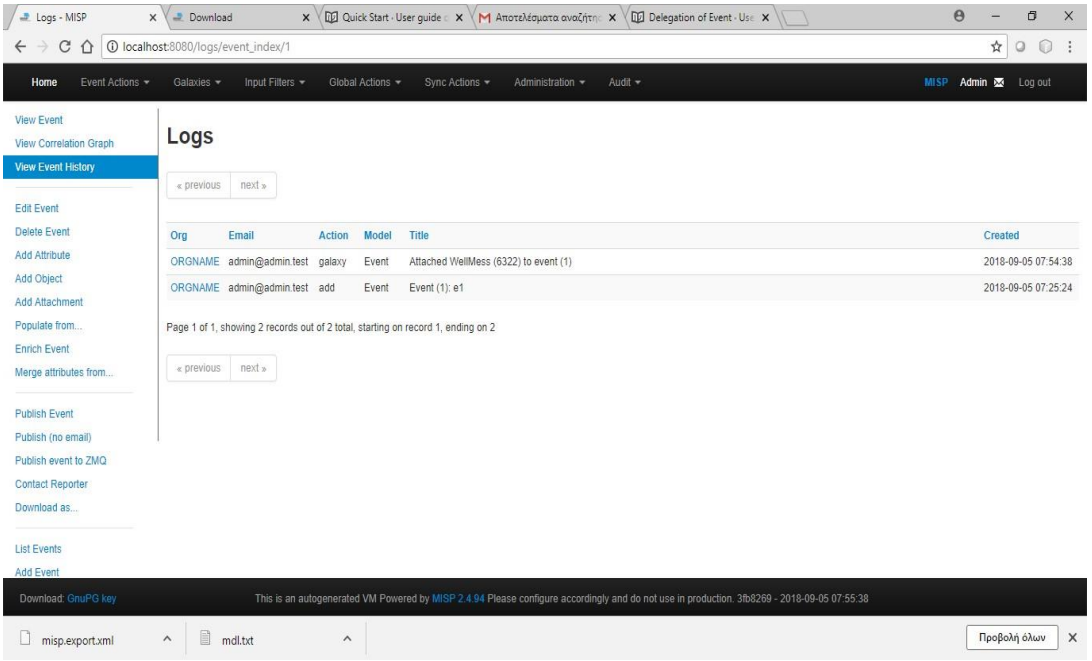


Με σειρά από νέα events μπορούμε να δημιουργήσουμε όσους ιούς θέλουμε να ορίσουμε σαν απειλές και να πάρουμε αποτελέσματα, όπως κάθε event που είναι παρακάτω:

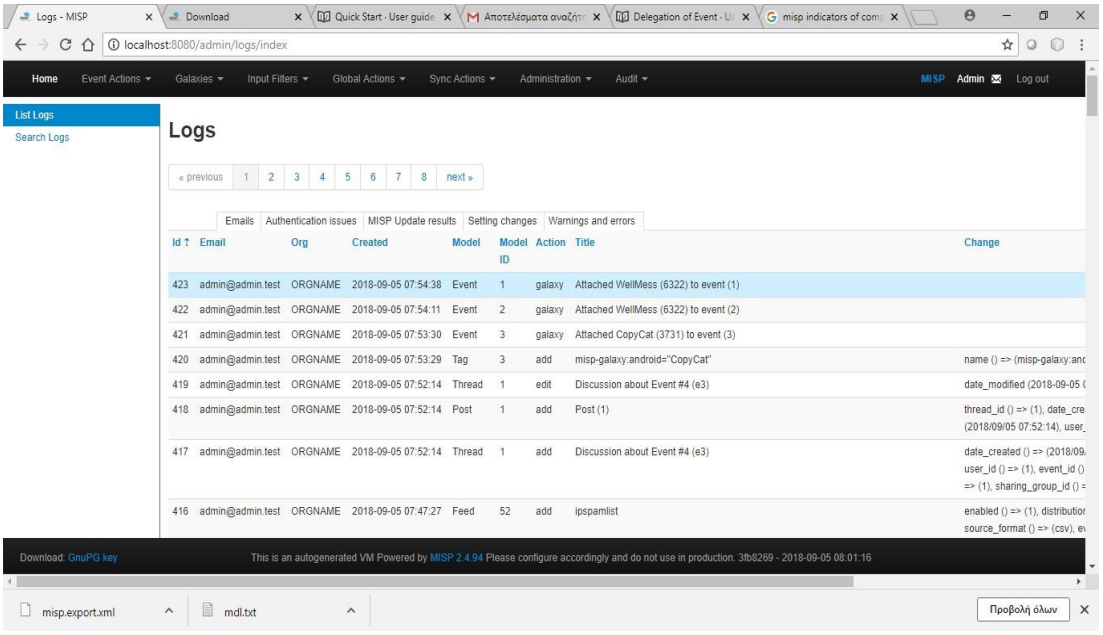




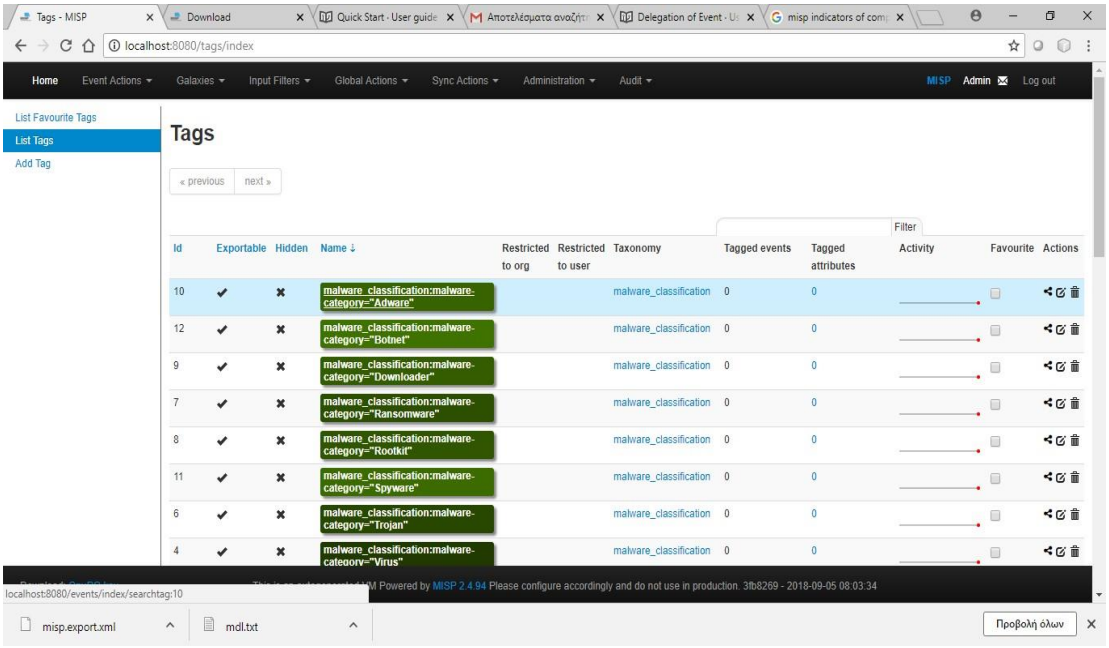
Αντίστοιχα παίρνουμε την ιστορία κάθε event



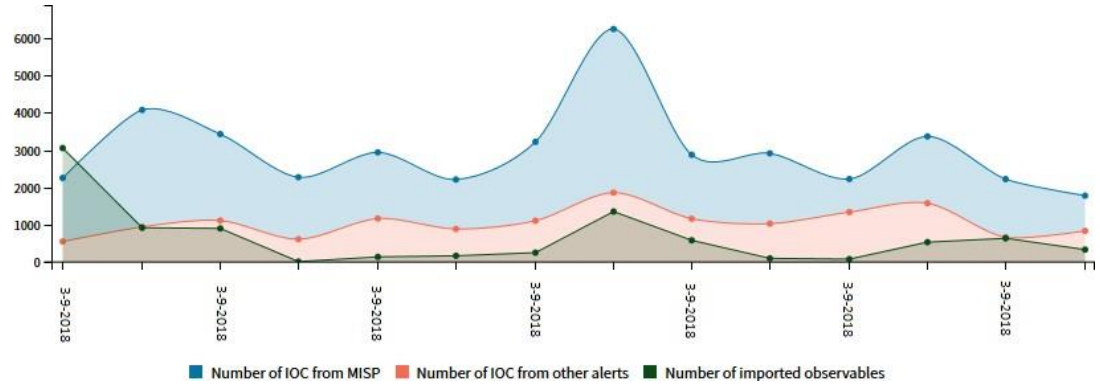
Επίσης μπορούμε να πάρουμε όλα τα logs



Ενεργοποιώντας και τις κατηγορίες έχουμε



Τελικά προσθέτοντας σειρά από δεδομένα τόσο δικά μας όσο και από πηγές στο διαδίκτυο έχουμε το παρακάτω γράφημα συνολικά με τα στοιχεία που προσθέσαμε.

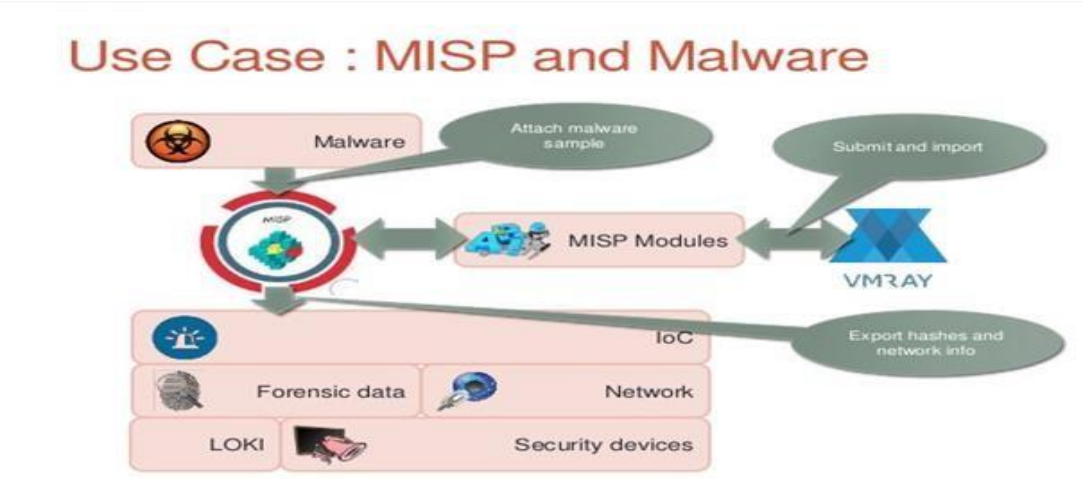


Ενοποιηση Εργαλειου MISP με την εγκατασταση του IOC Scanner Loki

Σε συνέχεια της παραπάνω ανάλυσης βάσει του εργαλείου MISP, τοπικά θα χρειαστεί να δούμε την παρουσία (η μη) των αρχείων ανίχνευσης σε πραγματικό χρόνο. Για αυτόν ακριβώς τον λόγο θα προχωρήσουμε σε τοπική εγκατάσταση του IOC Scanner ονόματι LOKI.

Το εν λόγω εργαλείο είναι ένα blackbox IOC Scanner, το οποίο σε συνέχεια της εγκατάστασης του τοπικά στον δίσκο του συστήματος μας το *ΤΡΟΦΟΔΟΤΟΥΜΕ* εμείς με την βασική πληροφορία του **που θα σκανάρει και τι θα σκανάρει.** Έτσι βάσει όλων των προαναφερθέντων παρακάτω παραθέτουμε την ολοκληρωμένη διαδικασία εγκατάστασης και παραμετροποίησης του εργαλείου LOKI.

5.2 Εγκατάσταση και Παραμετροποίηση του εργαλείου LOKI



PyMISP - Βιβλιοθήκη Python για εκτέλεσή διαδικασιών στο MISP

Το PyMISP μας επιτρέπει να μεταφέρουμε συμβάντα, να προσθέσουμε ή να ενημερώσουμε γεγονότα, χαρακτηριστικά, δείγματα ή να αναζητάμε ιδιότητες.

Install from pip

```
pip3 install pymisp
```

Install the latest version from repo

```
git clone https://github.com/MISP/PyMISP.git && cd PyMISP
git submodule update --init
pip3 install -I .[fileobjects,neo,openioc,virustotal]
```

Installing it with virtualenv

It is recommended to use virtualenv to not polute your OS python envirenment.

```
pip3 install virtualenv
git clone https://github.com/MISP/PyMISP.git && cd PyMISP
python3 -m venv ./
source venv/bin/activate
git submodule update --init
pip3 install -I .[fileobjects,neo,openioc,virustotal]
```

Running the tests

```
pip3 install -U nose pip setuptools coveralls codecov requests-mock
pip3 install git+https://github.com/kbandla/pydeep.git

git clone https://github.com/viper-framework/viper-test-files.git tests/viper-test-files
nosetests-3.4 --with-coverage --cover-package=pymisp,tests --cover-tests tests/test_*.py
```

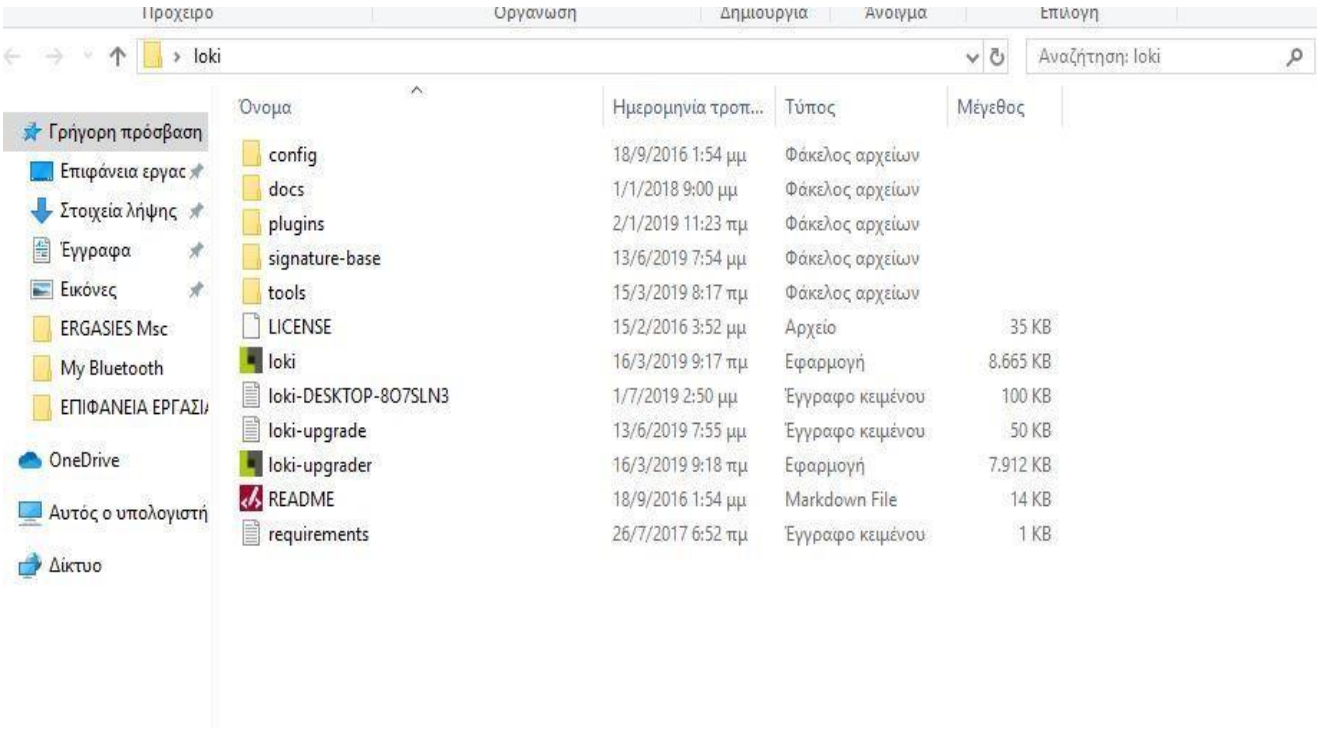
Install from pip (Python Library)

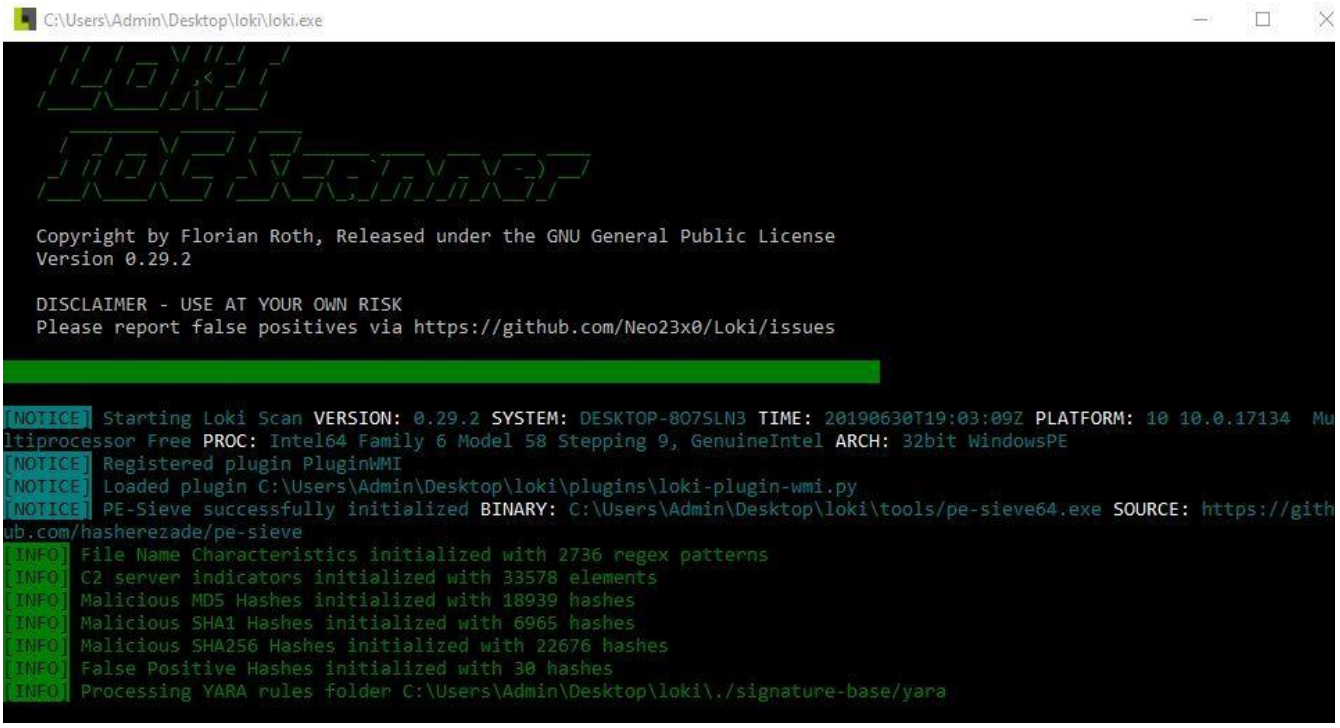
Install the latest version from repo

Loki - Simple IOC Scanner (Τι είναι και γιατί χρησιμοποιήσαμε το Loki)

Στην παρούσα εργασία χρησιμοποιήθηκε το εργαλείο Loki στη τελευταία διαθέσιμη έκδοση του. Το Loki κατά την εγκατάσταση του έτρεξε τοπικά και αρχικά του ενημερώθηκε ο στόχος για τον οποίο θα πραγματοποιηθεί το αρχικό scan. Ο εν λόγω στόχος στην περίπτωση μας είναι όλο το σύστημα των εσωτερικών δίσκων του σταθμού εργασίας. Το Loki απαιτεί την διαχείριση του και την χρήση του «ως διαχειριστής». Για τον συγκεκριμένο λόγο εκκινήσαμε το εκτελέσιμο αρχείο με δικαιώματα τοπικού διαχειριστή (local admin).

Επίσης, στην εργασία εγκαταστήσαμε το Loki στον C directory του σταθμού εργασίας και εκκινήσαμε scan σε όλο το σύστημα. Όπως φαίνεται και στις παρακάτω εικόνες η ανάλυση του εργαλείου διαχωρίζεται σε πράσινα, κίτρινα, κόκκινα στοιχεία. Στη συνέχεια ακολουθεί επιμέρους ανάλυση στο διαδίκτυο για ύποπτα αρχεία που τυχόν έχουν εντοπιστεί στο σύστημα – στόχο και η ανάλυση αυτή έχει εκκινήσει μέσω της πλατφόρμας Virustotal, μέσω της αναζήτησης του αρχείου στο διαδίκτυο χρησιμοποιώντας το όνομα του ή το μοναδικό αριθμό κατακερματισμού του (hash), είτε τέλος πραγματοποιώντας δυναμική ανάλυση μέσω των διαθέσιμων εργαλείων σε απομονωμένο περιβάλλον (sandboxes) που υπάρχουν διαθέσιμα στο διαδίκτυο.




C:\Users\Admin\Desktop\loki\loki.exe
Copyright by Florian Roth, Released under the GNU General Public License
Version 0.29.2
DISCLAIMER - USE AT YOUR OWN RISK
Please report false positives via https://github.com/Neo23x0/Loki/issues
[NOTICE] Starting Loki Scan VERSION: 0.29.2 SYSTEM: DESKTOP-8O7SLN3 TIME: 20190630T19:03:09Z PLATFORM: 10 10.0.17134 Mu
ltiprocessor Free PROC: Intel64 Family 6 Model 58 Stepping 9, GenuineIntel ARCH: 32bit WindowsPE
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin C:\Users\Admin\Desktop\loki\plugins\loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: C:\Users\Admin\Desktop\loki\tools/pe-sieve64.exe SOURCE: https://gith
ub.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2736 regex patterns
[INFO] C2 server indicators initialized with 33578 elements
[INFO] Malicious MD5 Hashes initialized with 18939 hashes
[INFO] Malicious SHA1 Hashes initialized with 6965 hashes
[INFO] Malicious SHA256 Hashes initialized with 22676 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder C:\Users\Admin\Desktop\loki\./signature-base/yara

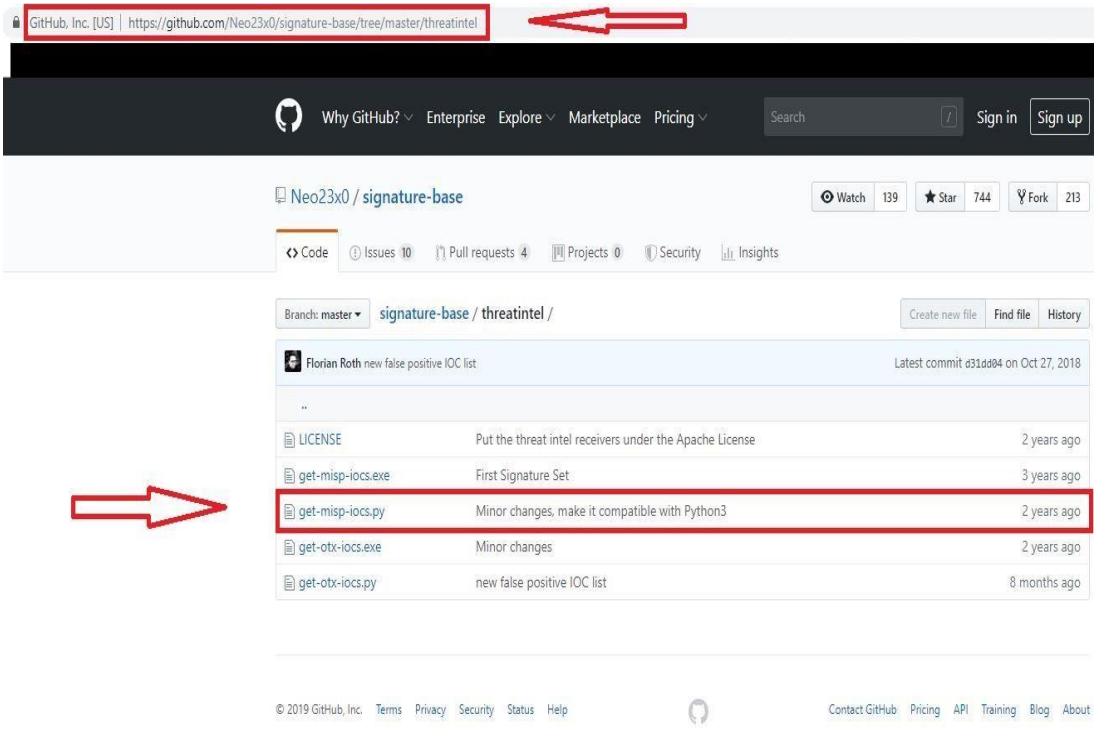

C:\Users\Admin\Desktop\loki\loki.exe
[INFO] Scanning Process PID: 4180 NAME: svchost.exe OWNER: SYSTEM CMD: c:\windows\system32\svchost.exe -k netsvcs -p -s
iphlpsvc PATH: c:\windows\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 4180 NAME: svchost.exe OWNER: SYSTEM CMD: c:\windows\system32\svchost.exe -k
netsvcs -p -s iphlpsvc PATH: c:\windows\system32\svchost.exe
[INFO] Scanning Process PID: 4316 NAME: svchost.exe OWNER: SYSTEM CMD: c:\windows\system32\svchost.exe -k netsvcs PATH:
C:\windows\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 4316 NAME: svchost.exe OWNER: SYSTEM CMD: c:\windows\system32\svchost.exe -k
netsvcs PATH: c:\windows\system32\svchost.exe
[INFO] Scanning Process PID: 5440 NAME: vmware-hostd.exe OWNER: SYSTEM CMD: "C:\Program Files (x86)\VMware\VMware Workst
ation\vmware-hostd.exe" -u "C:\ProgramData\VMware\hostd\config.xml" PATH: C:\Program Files (x86)\VMware\VMware Workstati
on\vmware-hostd.exe
[INFO] PE-Sieve reported no anomalies PID: 5440 NAME: vmware-hostd.exe OWNER: SYSTEM CMD: "C:\Program Files (x86)\VMware
\VMware Workstation\vmware-hostd.exe" -u "C:\ProgramData\VMware\hostd\config.xml" PATH: C:\Program Files (x86)\VMware\VM
ware Workstation\vmware-hostd.exe
[NOTICE] Listening process PID: 5440 NAME: vmware-hostd.exe COMMAND: "C:\Program Files (x86)\VMware\VMware Workstation\v
mware-hostd.exe" -u "C:\ProgramData\VMware\hostd\config.xml" IP: ::1 PORT: 8307
[NOTICE] Listening process PID: 5440 NAME: vmware-hostd.exe COMMAND: "C:\Program Files (x86)\VMware\VMware Workstation\v
mware-hostd.exe" -u "C:\ProgramData\VMware\hostd\config.xml" IP: :: PORT: 443
[NOTICE] Listening process PID: 5440 NAME: vmware-hostd.exe COMMAND: "C:\Program Files (x86)\VMware\VMware Workstation\v
mware-hostd.exe" -u "C:\ProgramData\VMware\hostd\config.xml" IP: 127.0.0.1 PORT: 8307
[NOTICE] Listening process PID: 5440 NAME: vmware-hostd.exe COMMAND: "C:\Program Files (x86)\VMware\VMware Workstation\v
mware-hostd.exe" -u "C:\ProgramData\VMware\hostd\config.xml" IP: 0.0.0.0 PORT: 443
[INFO] Scanning Process PID: 844 NAME: PresentationFontCache.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\Microsoft.Net\Fram
ework64\v3.0\WPF\PresentationFontCache.exe PATH: C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
[NOTICE] PE-Sieve reported hooked or detached process PID: 844 NAME: PresentationFontCache.exe OWNER: LOCAL SERVICE CMD:
C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe PATH: C:\WINDOWS\Microsoft.Net\Framework64\v3.0
\WPF\PresentationFontCache.exe HOOKED: 1 SUSPICIOUS: 0


[INFO] Scanning Process PID: 10988 NAME: svchost.exe OWNER: unknown CMD: C:\WINDOWS\system32\svchost.exe -k netsvcs -p -
s wlidsvc PATH: C:\WINDOWS\system32\svchost.exe
[WARNING] svchost.exe process owner is suspicious PID: 10988 NAME: svchost.exe OWNER: unknown CMD: C:\WINDOWS\system32\s
vchost.exe -k netsvcs -p -s wlidsvc PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Skipping LOKI Process PID: 7052 NAME: loki.exe OWNER: Admin CMD: "C:\Users\Admin\Desktop\loki\loki.exe" PATH: C:
\Users\Admin\Desktop\loki\loki.exe
[INFO] Scanning Process PID: 10616 NAME: conhost.exe OWNER: Admin CMD: \??\C:\WINDOWS\system32\conhost.exe 0x4 PATH: C:\
WINDOWS\system32\conhost.exe
[INFO] PE-Sieve reported no anomalies PID: 10616 NAME: conhost.exe OWNER: Admin CMD: \??\C:\WINDOWS\system32\conhost.exe
0x4 PATH: C:\WINDOWS\system32\conhost.exe
[INFO] Skipping LOKI Process PID: 12604 NAME: loki.exe OWNER: Admin CMD: "C:\Users\Admin\Desktop\loki\loki.exe" PATH: C
:\Users\Admin\Desktop\loki\loki.exe


[WARNING] PE-Sieve reported replaced process PID: 12600 NAME: explorer.exe OWNER: Admin CMD: C:\WINDOWS\Explorer.EXE PATH: C:\
WINDOWS\Explorer.EXE REPLACED: 1

Χρειαζόμαστε οπωσδήποτε το MISP Receiver (https://github.com/Neo23x0/Loki)

Στο πρώτο printscreen έχουμε την βιβλιοθήκη (get-misp-iocs.py) που χρειάζεται για να «μιλήσει» το MISP με το LOKI. Χρειάζεται το [-k APIKEY] από το MISP GUI.



Δέκτης εισαγωγής δεικτών από το εργαλείο MISP

Ένα απλό σενάριο που μεταφορτώνει τα συνδρομητικά σας γεγονότα / iocs από μια προσαρμοσμένη παράμετρο MISP και τα αποθηκεύει στη σωστή μορφή στον υποφάκελο './iocs'. Οι κανόνες YARA που είναι αποθηκευμένοι σε MISP θα γραφτούν στον υποφάκελο './iocs/yara' και θα αρχικοποιούνται αυτόματα κατά την εκκίνηση. Το σενάριο βρίσκεται στο φάκελο "./threatintel" και ονομάζεται "get-misp-iocs.py".

```
usage: get-misp-iocs.py [-h] [-u URL] [-k APIKEY] [-l tframe] [-o dir]
                        [-y yara-dir] [--verifycert] [--debug]

MISP IOC Receiver

optional arguments:
  -h, --help    show this help message and exit
  -u URL        MISP URL
  -k APIKEY     MISP API key
  -l tframe     Time frame (e.g. 2d, 12h - default=30d)
  -o dir        Output directory
  -y yara-dir   YARA rule output directory
  --verifycert  Verify the server certificate
  --debug       Debug output
```

Στο παρακάτω screenshot πραγματοποιούμε stop scan στο LOKI.

Από την έκδοση v0.16.2, το LOKI υποστηρίζει τον ορισμό των εξαιρέσεων που ορίζει ο χρήστης μέσω του "excludes.cfg" στο νέο "./config" φάκελο. Κάθε γραμμή αντιπροσωπεύει μια κανονική έκφραση που εφαρμόζεται στην πλήρη διαδρομή του αρχείου κατά τη διάρκεια της βάδισης του καταλόγου. Με αυτόν τον τρόπο μπορούμε να εξαιρέσουμε συγκεκριμένους καταλόγους ανεξάρτητα από το όνομα της μονάδας τους, τις επεκτάσεις αρχείων σε ορισμένους φακέλους και όλα τα αρχεία και τους καταλόγους που ανήκουν σε ένα προϊόν που είναι ευαίσθητο σε ανίχνευση ιών.

Το " 'exclude.cfg' " μοιάζει με αυτό:

```
# Excluded directories
#
# - add directories you want to exclude from the scan
# - double escape back slashes
# - values are case-insensitive
# - remember to use back slashes on Windows and slashes on Linux / Unix / OSX
# - each line contains a regex that matches somewhere in the full path (case insensitive)
#   e.g.:
#   Regex: \\System32\\
#   Matches C:\Windows\System32\cmd.exe
#
#   Regex: /var/log/[^/]+\.log
#   Matches: /var/log/test.log
#   Not Matches: /var/log/test.gz
#

# Useful examples
\\Ntfrs\\
\\Ntds\\
\\EDB[^\.]+\.log
Sysvol\\Staging\\Ntfrs_cmp
\\System Volume Information\\DFSR
```

Για να κατεβάσουμε και να έχουμε διαθέσιμο το «get-misp-iocs.py» θα πάμε στο link https://github.com/Neo23x0/signature-base/tree/master/threatintel.

Το κατεβάζουμε τοπικά στο PC και τρέχουμε στο LOKI το ίδιο αρχείο «get-misp-iocs.py» με commandline από την τοποθεσία που έχουμε το αρχείο (cd.. και path), με αποτέλεσμα το LOKI να βλέπει τα IOCs του MISP.

Στόχος του Virustotal είναι ο έλεγχος αρχείων για ιούς και malware.

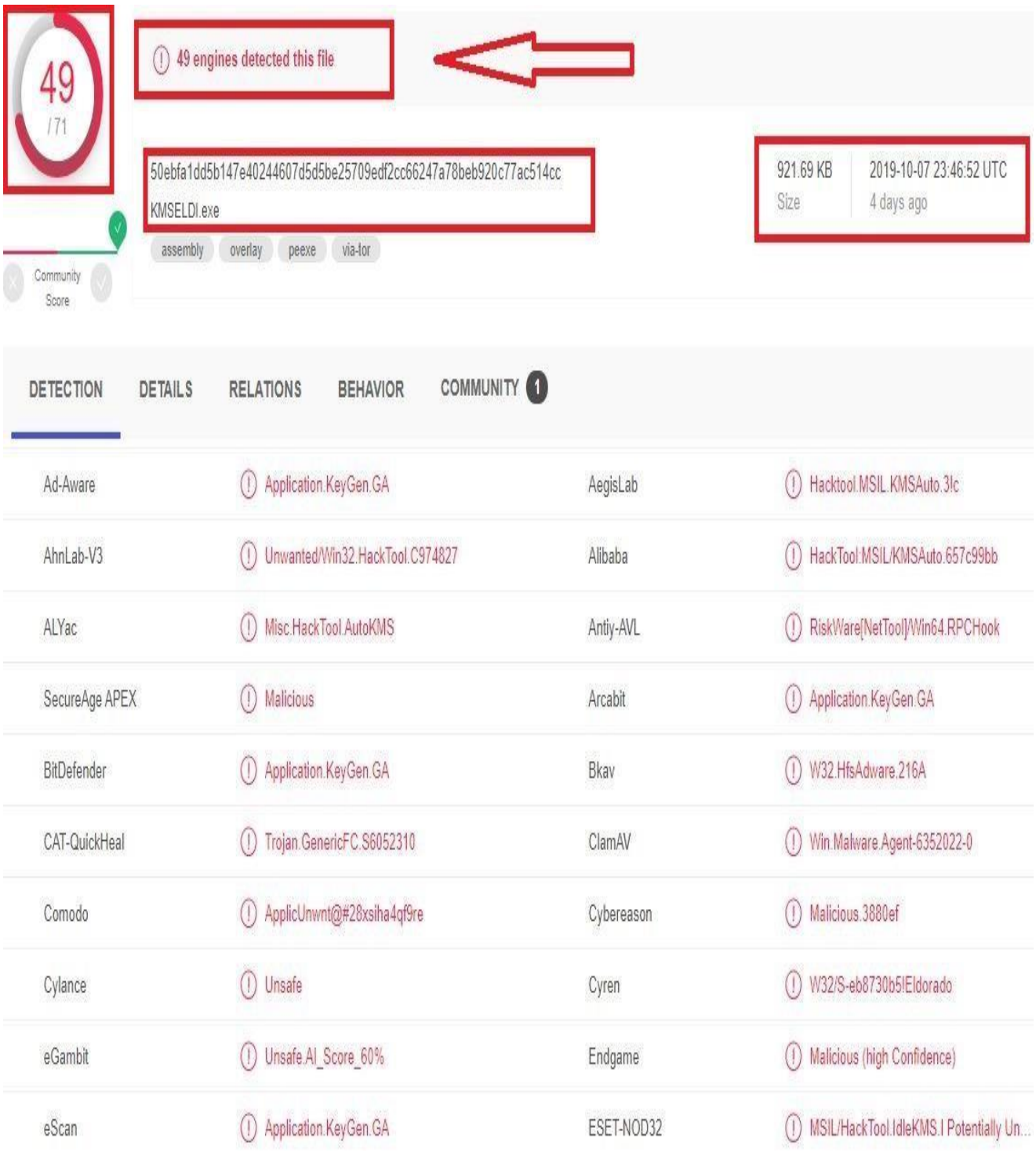
Το VirusTotal χρησιμοποιεί 53 antivirus και malware scanners, 61 μηχανές για έλεγχο malware σε ιστοσελίδες και 17 εργαλεία για το χαρακτηρισμό αρχείων.
Τα antivirus που χρησιμοποιεί το virustotal είναι πολύ γνωστά, όπως τα Avast, AVG, Avira, Bitdefender, Kaspersky, Malwarebytes, McAffee, και Symantec (Norton). Θα βρούμε όμως και αρκετές άγνωστες στο ευρύ κοινό υπηρεσίες, όπως οι AegisLab, AhnLab-V3, Bkav, Ikarus, και K7GW.

Με την χρήση των παραπάνω εργαλείων για την ανίχνευση και κατηγοριοποίηση των απειλών εντοπίστηκε στο σύστημα η σουίτα-οικογένεια λογισμικού ονόματι KMSpico, που είναι ένα εργαλείο ενεργοποίησης αντιγράφων και την μη νόμιμη χρήση των Windows 7/8 / 8.1 / 10 και Office 2010/2013/2016.
Τα περισσότερα προγράμματα αντιμετώπισης ιών (antivirus) αποδείχθηκε ότι εντοπίζουν το εκτελέσιμο μέρος της παραπάνω σουίτας, το οποίο ονομάζεται «KMSELDI.exe». Το τελευταίο ανιχνεύεται ως κακόβουλο λογισμικό από τις περισσότερες πλατφόρμες ενώ από άλλες όχι όπως για π.χ. Η Kaspersky το αναγνωρίζει ως μην ιό: NetTool.Win64.RPCHook.a και η Sophos την αναγνωρίζει ως Generic PUA GM (Potentially Unwanted/ Unknown application).

Το KMSpico εντάσσει στην σουίτα του την υπηρεσία διαχείρισης KMS (Key Management Service) - Microsoft, μια υπηρεσία που ενεργοποιεί προγράμματα μέσω του τοπικού δικτύου, χωρίς να χρειάζεται να επιτευχθεί επικοινωνία με τη ιδια την Microsoft. Το KMSpico αντικαθιστά το εγκατεστημένο κλειδί με ένα κλειδί προσωρινής άδειας, και δημιουργεί μια προσομοιωμένη παρουσία ενός διακομιστή KMS στο σύστημα του χρήστη, όπου αυτή αναγκάζει τα προγράμματα-στόχους να ενεργοποιηθούν μέσω του προσομοιωμένου διακομιστή KMS.

Στις παρακάτω εικόνες αναλύουμε το αρχείο KMSELDI.exe , κάνοντας το αναζήτηση στο Virustotal.

1. Ανίχνευση του αρχείου



2. Βασικές Πληροφορίες

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 1

Basic Properties

MD5	f0280de3880ef581bf14f9cc72ec1c16
SHA-1	43d348e164c35f9e02370f6f66186fbfb15ae2a3
SHA-256	50ebfa1dd5b147e40244607d5d5be25709edf2cc66247a78beb920c77ac514cc
Vhash	2950366555164091effff96112
Authentihash	b779f503cd1828e6fac531773ed5a7934136ae26a69f04eb5a4032926d7c6f38
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	12288:sBMSCV2RM+V8PW/+jSZOgJ38Ry3niRTiAH7UrbwIpmOs8b2i:snCEM68Lj5gNi2niRTiq7UrbnbsQ2i
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly
File size	921.69 KB (943808 bytes)
PEiD	.NET executable

History

Creation Time	2016-01-11 22:28:07
Signature Date	2019-10-01 05:44:00
First Submission	2016-01-12 05:23:55
Last Submission	2019-10-01 03:44:39
Last Analysis	2019-10-01 03:44:39

Names

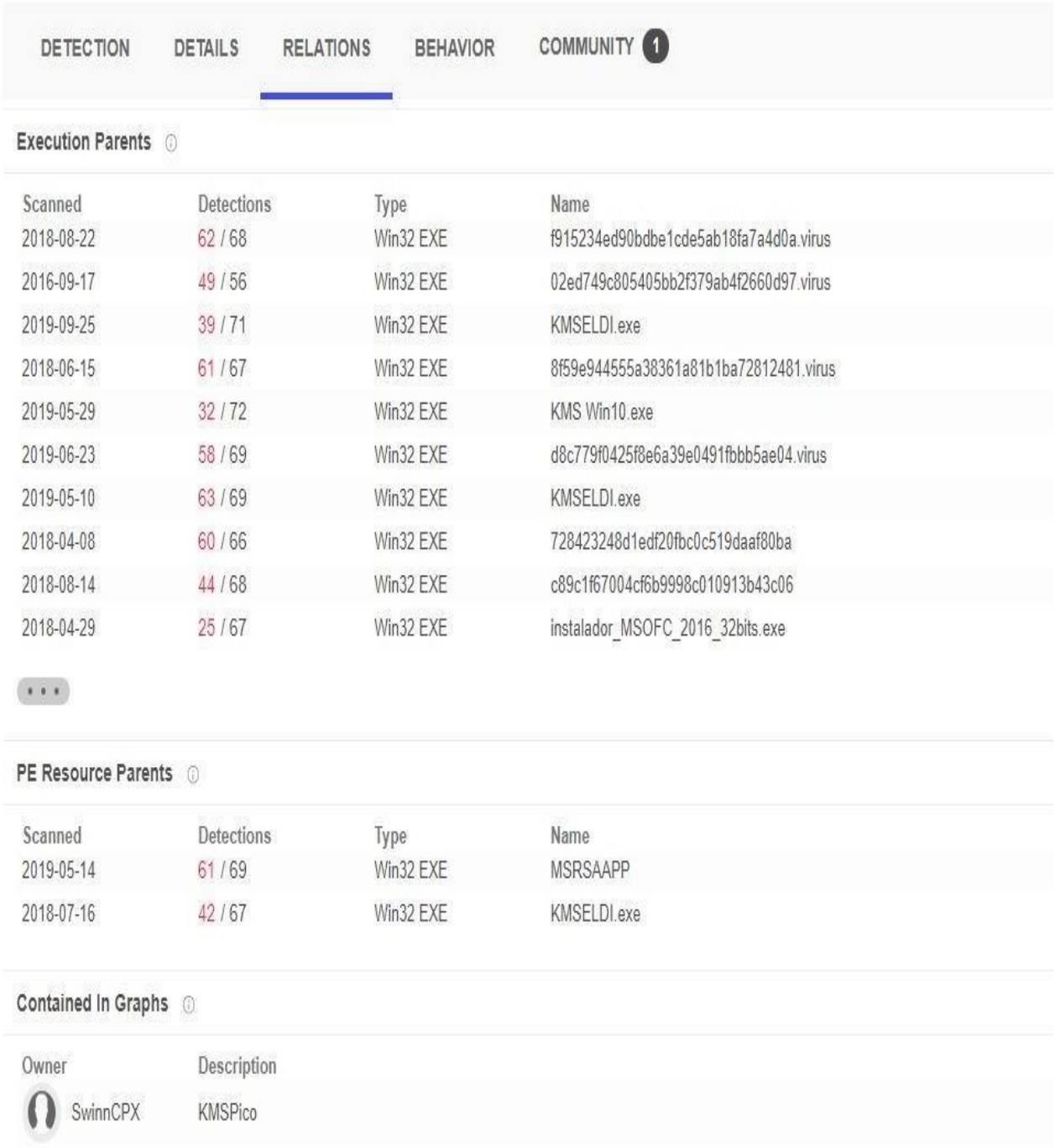
KMSELDI.exe

setup.exe

setupp.exe

important_document.exe

3. Αρχεία που έχουν εντοπιστεί και κατηγοριοποιηθεί στην οικογένεια του KMSELDI.exe



DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Execution Parents

Scanned	Detections	Type	Name
2018-08-22	62 / 68	Win32 EXE	f915234ed90bdbe1cde5ab18fa7a4d0a.virus
2016-09-17	49 / 56	Win32 EXE	02ed749c805405bb2f379ab4f2660d97.virus
2019-09-25	39 / 71	Win32 EXE	KMSELDI.exe
2018-06-15	61 / 67	Win32 EXE	8f59e944555a38361a81b1ba72812481.virus
2019-05-29	32 / 72	Win32 EXE	KMS Win10.exe
2019-06-23	58 / 69	Win32 EXE	d8c779f0425f8e6a39e0491fbbb5ae04.virus
2019-05-10	63 / 69	Win32 EXE	KMSELDI.exe
2018-04-08	60 / 66	Win32 EXE	728423248d1edf20fbc0c519daaf80ba
2018-08-14	44 / 68	Win32 EXE	c89c1f67004cf6b9998c010913b43c06
2018-04-29	25 / 67	Win32 EXE	instalador_MSOFC_2016_32bits.exe

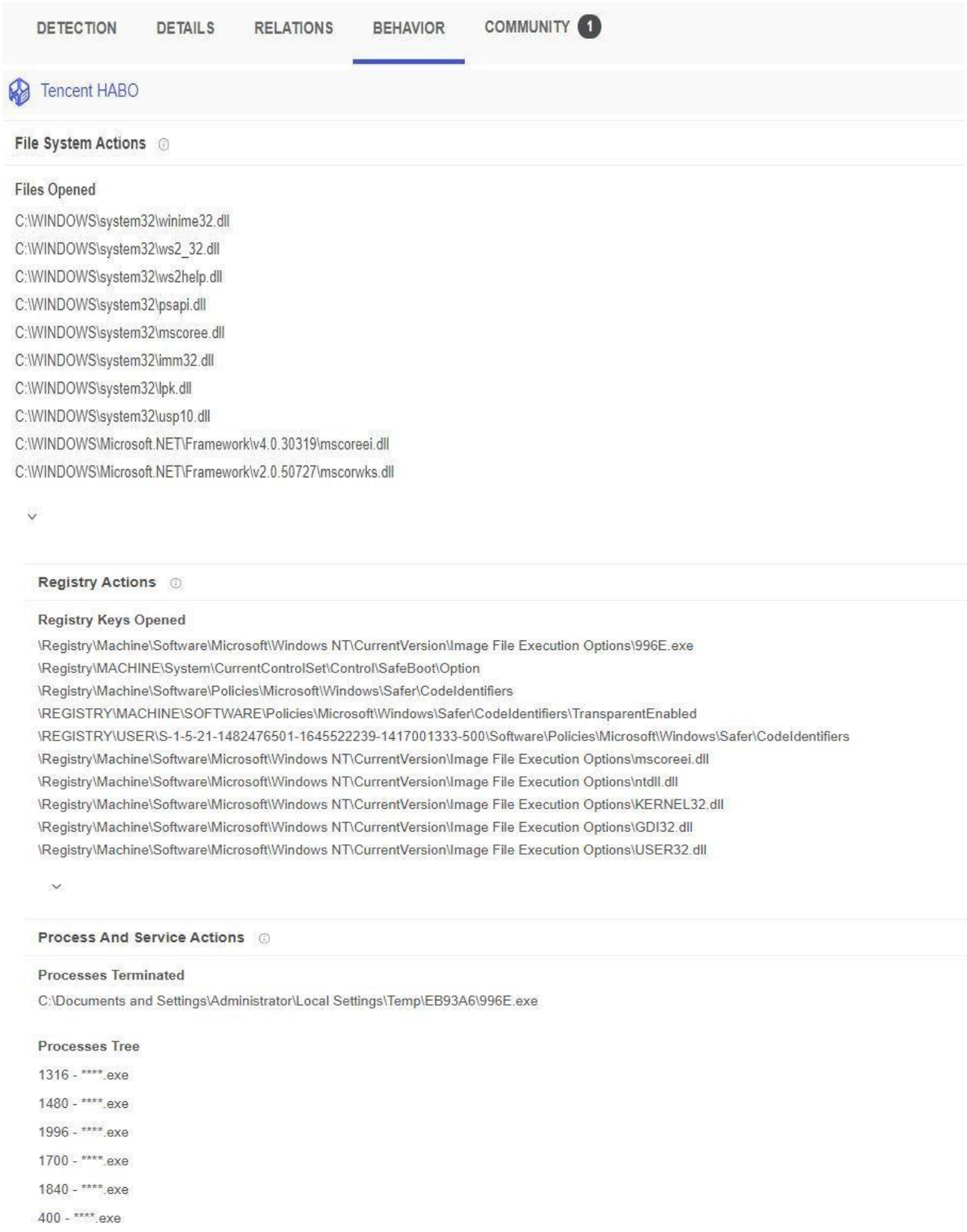
PE Resource Parents

Scanned	Detections	Type	Name
2019-05-14	61 / 69	Win32 EXE	MSRSAAPP
2018-07-16	42 / 67	Win32 EXE	KMSELDI.exe

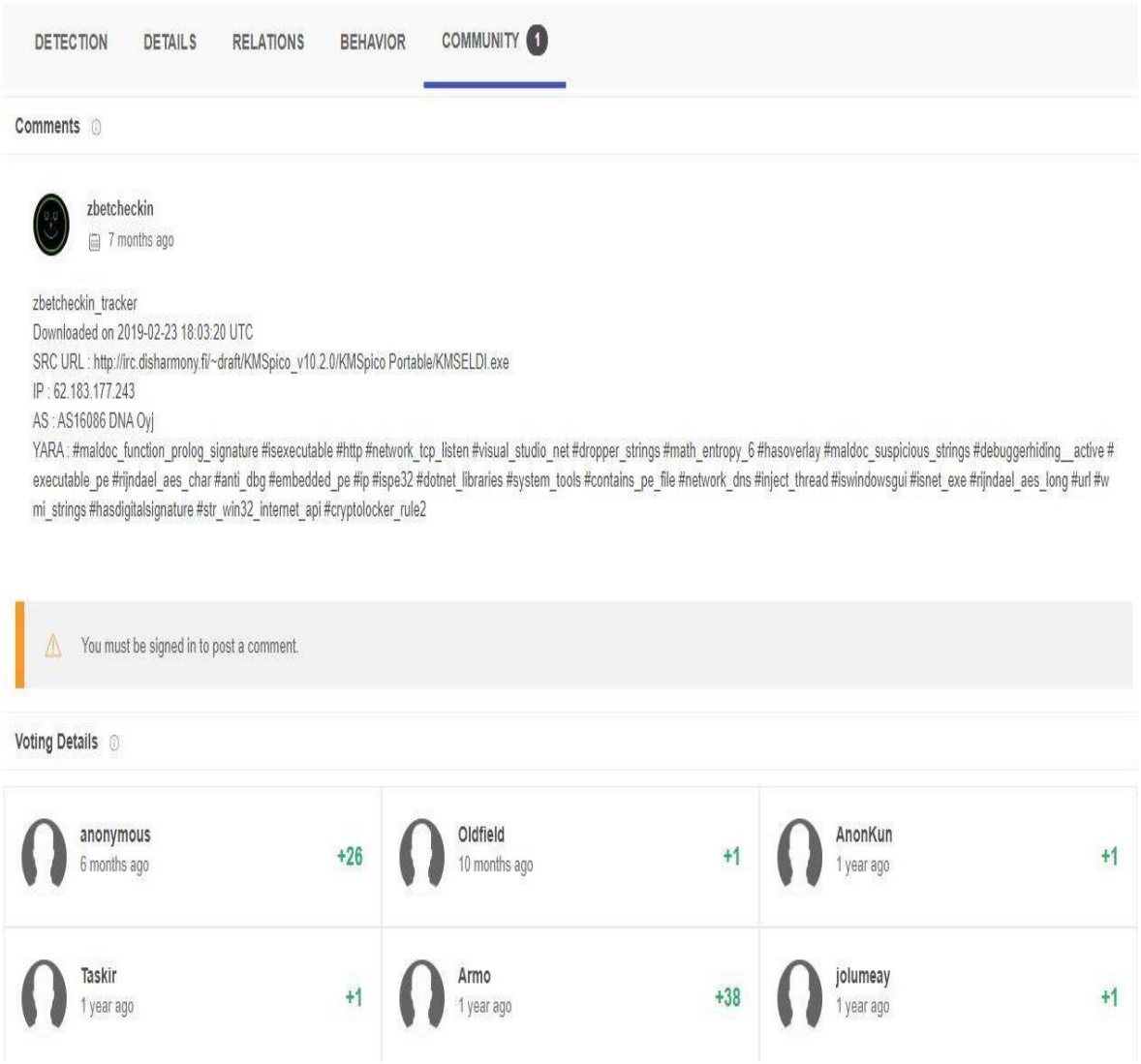
Contained In Graphs

Owner	Description
SwinnCPX	KMSPico

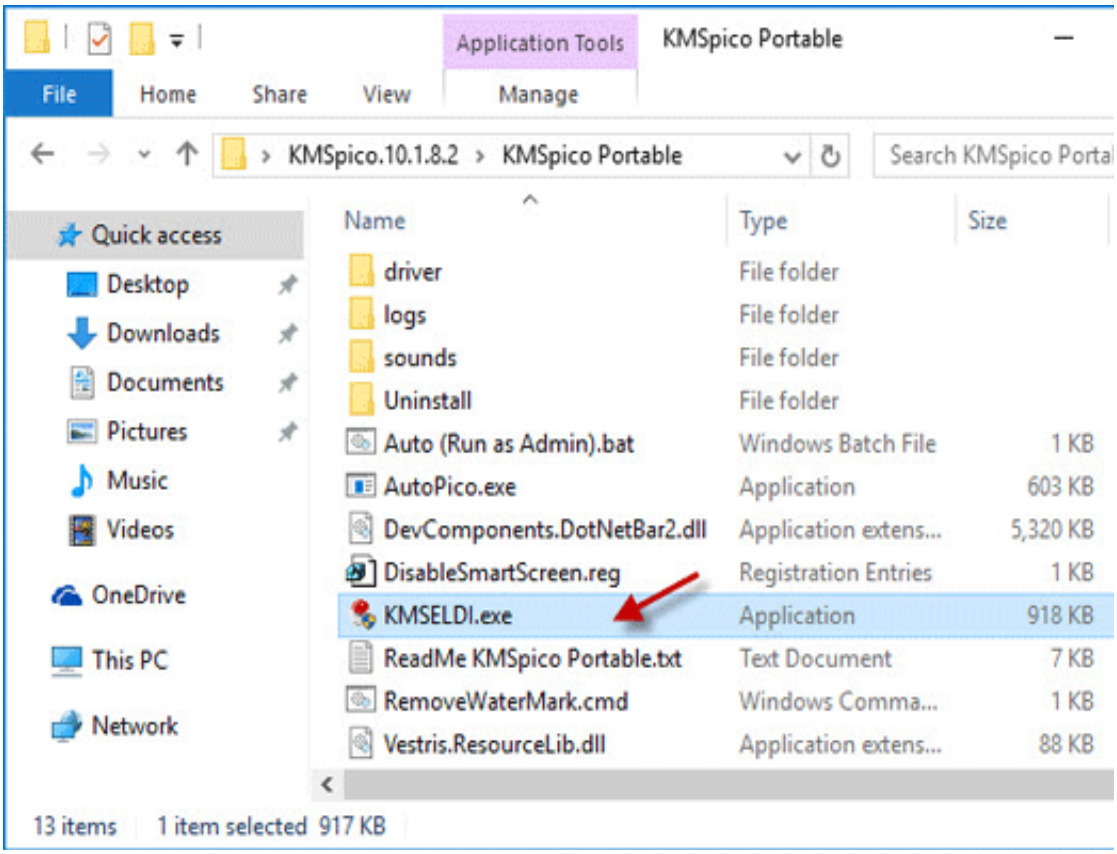
4. Παρατηρηθείσα Συμπεριφορά του αρχείου



5. Επικοινωνία των χρηστών του Virustotal (Open Source Feedback)



Σε συνέχεια ευρύτερης μελέτης, το αρχείο KMSELDI.exe ως επί το πλείστων βρίσκεται σε έναν υποφάκελο του αρχείου "C: \ Program Files" - συνήθως C: \ Program Files \ KMSpico **. Τα γνωστά μεγέθη αυτών των αρχείων στα Windows 10/8/7/XP είναι 943.808 bytes (33% όλων των εμφανίσεων), 941.760 bytes.



Το αρχείο KMSELDI.exe δεν είναι ένα βασικό αρχείο των Windows και έτσι το πρόγραμμα δεν έχει ορατό παράθυρο διαχείρισης (εκτέλεσης). Η διαδικασία εκτέλεσης χρησιμοποιεί θύρες για σύνδεση σε ή από ένα τοπικό δίκτυο προς και από το Internet. Το KMSELDI.exe είναι σε θέση να παρακολουθεί εφαρμογές και να χειρίζεται άλλα προγράμματα. Ως εκ τούτου, η τεχνική αξιολόγηση ασφαλείας είναι αρκετά επικίνδυνη. Τώρα εάν το αρχείο KMSELDI.exe βρίσκεται σε έναν υποφάκελο του φακέλου των Windows για προσωρινά αρχεία (temp location on local drive), η αξιολόγηση ασφαλείας είναι +42% επικίνδυνη. Το μέγεθος του αρχείου είναι 1.262.592 byte (33% όλων των public συμβάντων), 1.237.504 byte ή 1.260.032 byte. Όπως αναφέρθηκε και παραπάνω το εν λόγω αρχείο δεν είναι ένα αρχείο συστήματος των Windows και το πρόγραμμα δεν είναι ορατό.

Συνεπώς, πρέπει να ελεγχθεί η διεργασία KMSELDI.exe στον υπολογιστή για να τακτοποιηθεί εάν πρόκειται για απειλή. Σε αυτές τις περιπτώσεις συνίσταται το Security Task Manager για την επαλήθευση της ασφάλειας του υπολογιστή - συστήματος εκτέλεσης της διεργασίας.

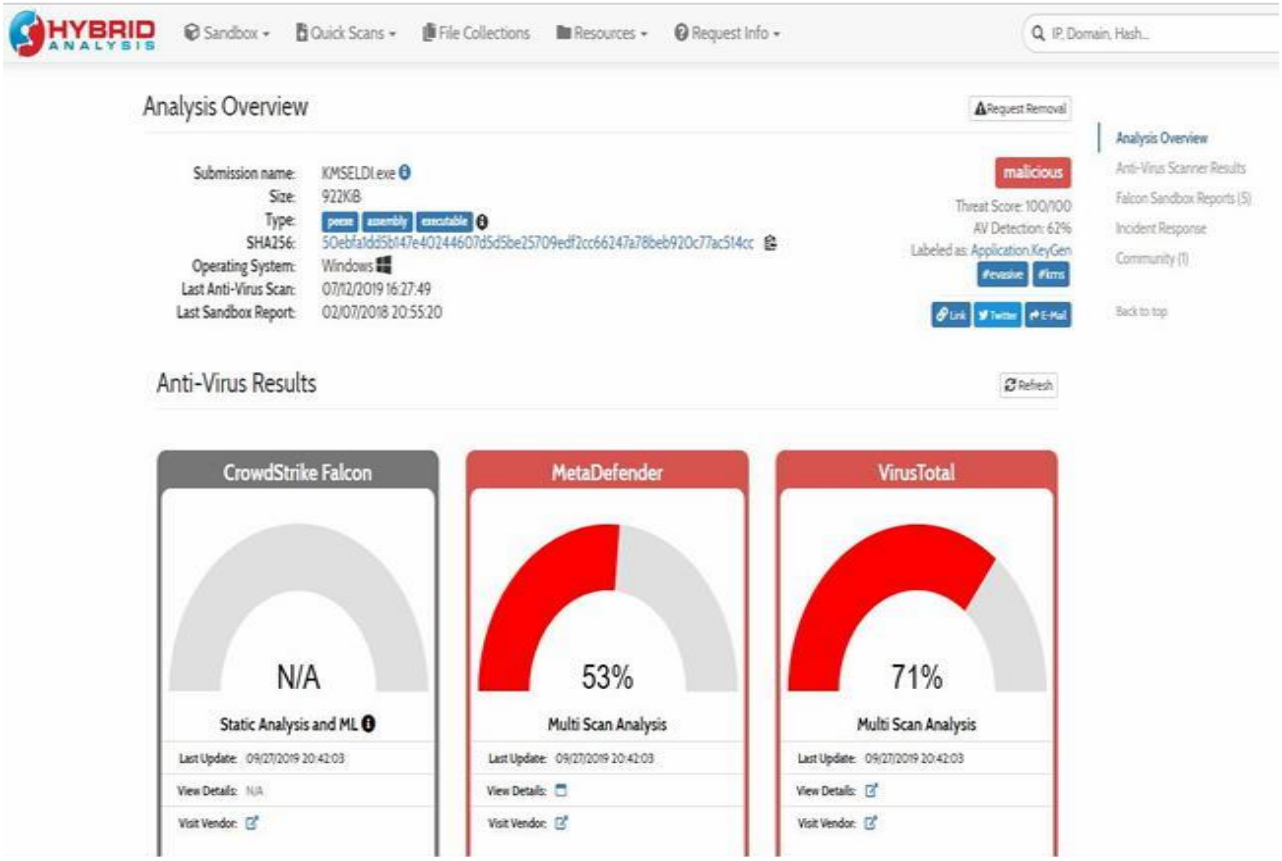
Hybrid Analysis και Open Source Falcon Sandbox

Με την τεχνολογία Hybrid Analysis και Falcon Sandbox υποβάλλουμε κακόβουλο λογισμικό για ανάλυση. Αυτή η πλατφόρμα διαθέτει εργαλεία ανάλυσης αδειών για την ανίχνευση κακόβουλων προγραμμάτων/ αρχείων & ιστότοπων URLs.

Το Hybrid Analysis είναι μια μοναδική τεχνολογία που εξοικονομεί στιγμιότυπα εκτύπωσης μνήμης με λεπτομερή έλεγχο των διεργασιών παρακολούθησης χρόνου εκτέλεσης, καθώς και πληροφορίες συμβόλων για την πραγματοποίηση μιας βαθιάς δυναμικής ανάλυσης στο στάδιο της δημιουργίας αναφορών.

Το Falcon Sandbox είναι μια αυτοματοποιημένη λύση ανάλυσης κακόβουλου λογισμικού που εξουσιοδοτεί τις ομάδες ασφαλείας. Ένα sandbox είναι ένα απομονωμένο περιβάλλον δοκιμών που επιτρέπει στους χρήστες να εκτελούν προγράμματα ή αρχεία **χωρίς να επηρεάζουν την εφαρμογή**, το σύστημα ή την πλατφόρμα στην οποία τρέχουν, για να ελέγξουν το πιθανό κακόβουλο λογισμικό.

Στην παρακάτω εικόνα παρατηρούμε την ανάλυση με την τεχνολογία Hybrid Analysis. Με βάση τα αποτελέσματα αυτής καταλήγουμε στο συμπέρασμα ότι αυτός ο ιός είναι κακεντρεχής.

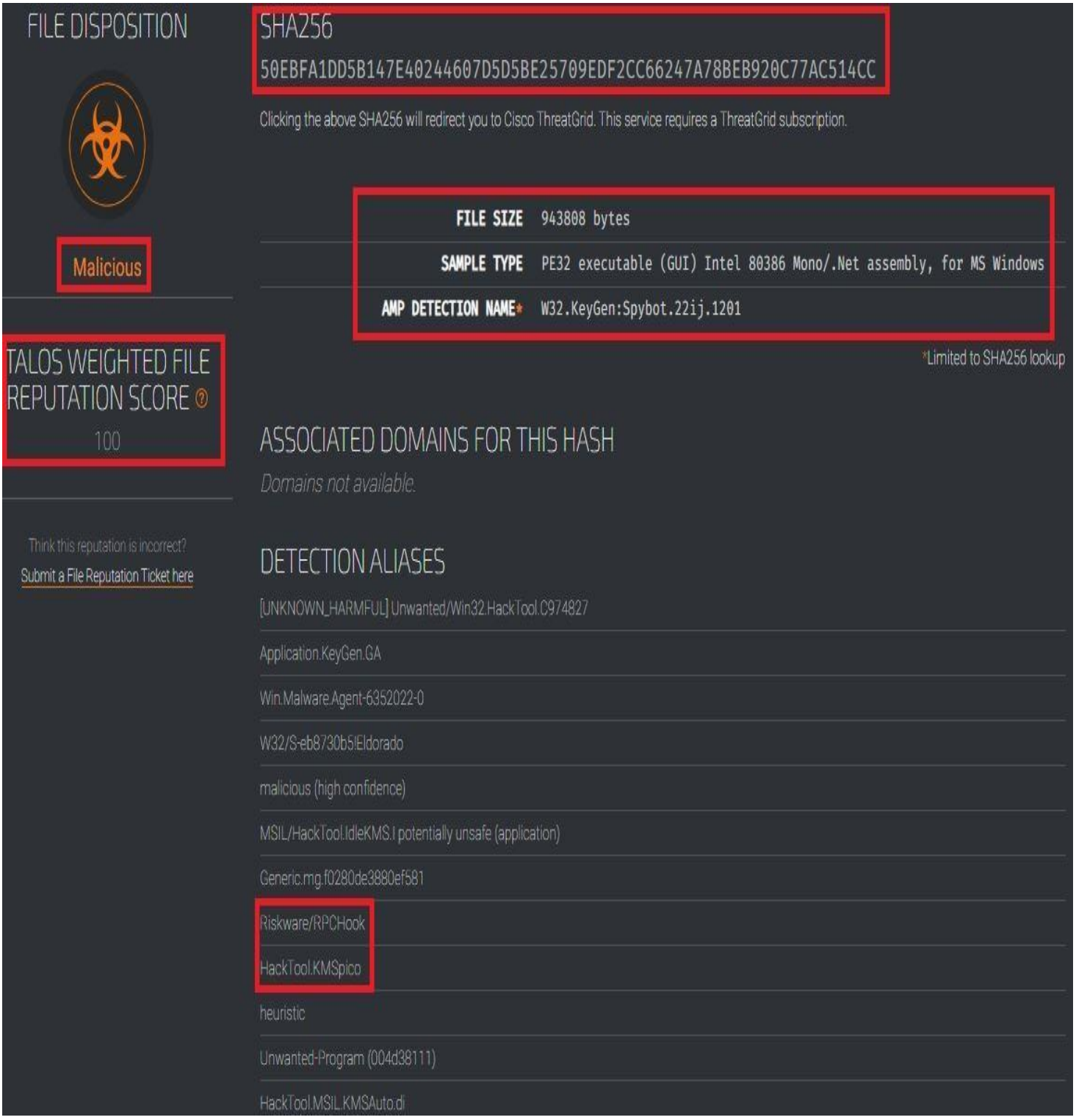


Εκθέσεις Falcon Sandbox

CISCO TALOS INTELLIGENCE FEEDBACK

Το εργαλείο Cisco Talos διαθέτει το πιο ολοκληρωμένο κέντρο αναζήτησης (reputation-based analysis) IP Addresses (διευθύνσεων IP, URLS & file hashes) και εντοπίζει απειλές σε απόλυτη σύγκριση με την βάση δεδομένων της Cisco (Cisco DBS). Με λίγα λόγια αποτελεί ένα σύνολο εμπεριστατωμένων πληροφοριών για τις απειλές στον κυβερνοχώρο.

Στην εικόνα παρατηρούμε τα αποτελέσματα της αναζήτησης του αρχείου μας στο open source εργαλείο.



Yara rules

Οι κανόνες Yara αφορούν το σύνολο των ορισμένων μεταβλητών, μέσω των οποίων ορίζεται ένα πλήθος παραμέτρων, βάσει των οποίων δύναται να λάβει χώρα μια διενέργεια ορισμένων λειτουργιών.

Μέσω των κανόνων Yara, μπορεί να γινεί μια αναλυτική προσέγγιση ενός κανονιστικού πλαισίου για την δημιουργία περιγραφών των οικογενειών κακόβουλου λογισμικού (trojan, worm κτλ). Οι κανόνες Yara αποτελούνται από σύνολα συμβολοσειρών και έχουν χαρακτηριστικά γνωρίσματα τύπου regular expression της γλώσσας προγραμματισμού Perl. Στο δικό μας παράδειγμα βλέπουμε ένα κανόνα Yara – απλού χαρακτηριστικού κανονιστικού πλαισίου - ενός εκτελέσιμου αρχείου αναγνωρισμένου ως windows crack βάσει IOCs.

```
rule Suspicious_Size_smss_exe {
    metadata:
        description = "Detects uncommon file size of smss.exe"
        author = "Alexios Petropoulos"
        score = 60
        date = "2019-08-23"
    condition:
        uint16(0) == 0x5a4d
        and filename == "smss.exe"
        and ( filesize < 40KB or filesize > 140KB )
}

rule Suspicious_Size_wininit_exe {
    metadata:
        description = "Detects uncommon file size of wininit.exe"
        author = "Alexios Petropoulos"
        score = 70
        date = "2019-07-23"
    condition:
        uint16(0) == 0x5a4d
        and filename == "wininit.exe"
        and ( filesize < 90KB or filesize > 250KB )
}

rule Suspicious_Size_KMSELDI_exe {
    metadata:
        description = "Detects uncommon file size of KMSELDI.exe"
        author = "Alexios Petropoulos"
        score = 100
        date = "2019-08-27"
    condition:
        uint16(0) == 0x5a4d
        and filename == "KMSELDI.exe"
        and ( filesize < 1000KB or filesize > 750KB )
}
```

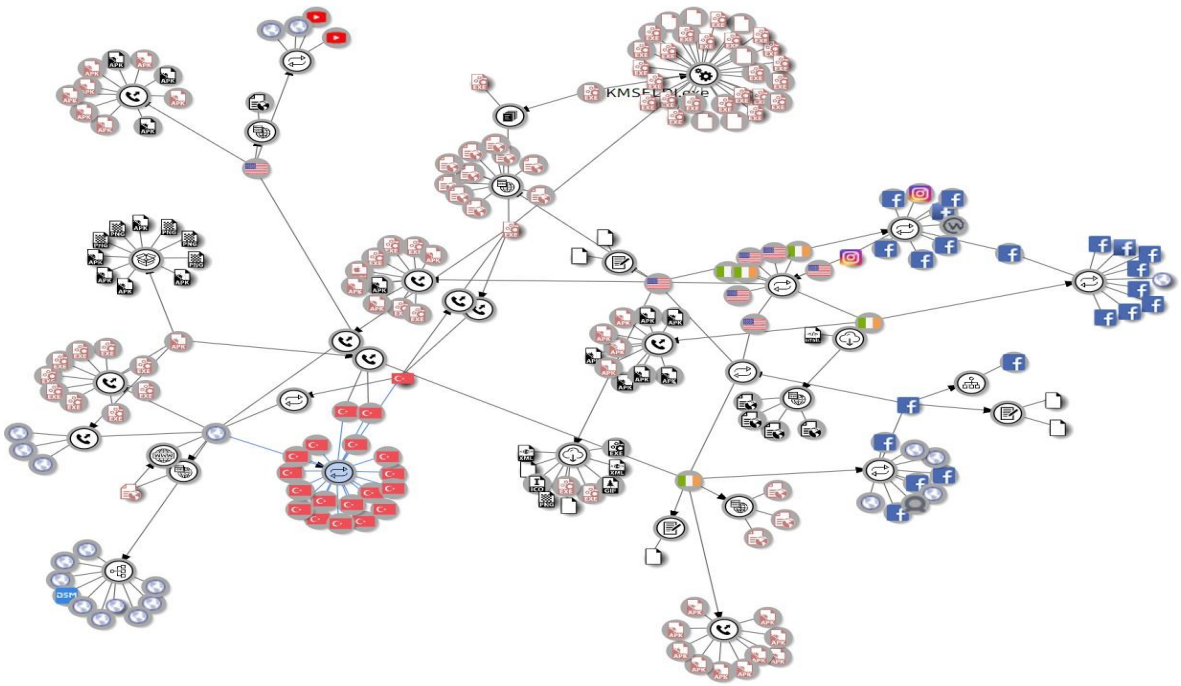
VirusTotal Graph

Το VirusTotal Graph είναι ένα εργαλείο απεικόνισης που είναι χτισμένο πάνω από το σύνολο δεδομένων του εργαλείου VirusTotal. Υποδεικνύει τη σχέση μεταξύ αρχείων, διευθύνσεων URL, τομέων, διευθύνσεων IP και άλλων αντικειμένων που συναντώνται σε μια έρευνα σε εξέλιξη. Με το Virus Total Graph, μπορεί να περιγράφει οποιοδήποτε από τα IOCs ενός malware στο γράφημα και να λάβει χώρα η σύνθεση των ευρημάτων σε έναν χάρτη απειλών.

Το Backend του VirusTotal δημιουργεί τις σχέσεις των διευθύνσεων URL από τις οποίες έχει ληφθεί ένα αρχείο, αν ένα δεδομένο αρχείο εμφανίστηκε σε κάποια άλλα αρχεία, δείχνει ποιοι είναι οι συνδετικοί κρίκοι ενός εκτελέσιμου δεδομένου (Executable), και τέλος τις αντιστοιχίσεις διευθύνσεων IP στο public δίκτυο (internet). Στο εν λόγω γράφημα είναι δυνατή η απεικόνιση 30+ συνδέσεων μεταξύ στοιχείων με κόμβους και τόξα που επιτρέπουν να ανακαλύφθει η υποδομή και τα αντικείμενα της εξάρτησης με το κύριο δεδομένο (έμμεσα ή άμεσα).

Threat Card (VT Graph+)

Μετακινώντας το δείκτη του ποντικιού πάνω από οποιονδήποτε από τους κόμβους στο VT Graph εκκινεί μια περίληψη του στοιχείου με τα πιο αντιπροσωπευτικά δεδομένα στη βάση δεδομένων VirusTotal. Κάνοντας κλικ στον κόμβο εμφανίζονται όλες οι διαθέσιμες επεκτάσεις, το γράφημα υποβολής, αλλά και οι ετυμηγορίες γνωστών AV engines (για τα αρχεία και τα urls).



6. Συμπεράσματα

Στην παρούσα εργασία χρησιμοποιήσαμε αρχικά το εργαλείο MISP για την καταγραφή και κατηγοριοποίηση των συμβάντων και των απειλών. Το συγκεκριμένο εργαλείο παρέχει την πλήρη λίστα των λειτουργιών που διευκολύνουν την ανταλλαγή πληροφοριών, η κοινή χρήση και η συνεργασία σε θέματα ευπάθειας ασφαλείας σε μια αξιόπιστη ομάδα είναι τόσο εύκολη όσο οι δείκτες κοινής χρήσης. Τα αντικείμενα στο MISP παρέχουν έναν ευέλικτο τρόπο για να περιγράψουν τις συνδυασμένες πληροφορίες χρησιμοποιώντας ένα απλό σύστημα εργαλείων.

Στην συνέχεια της εργασίας εγκαταστήσαμε το LOKI στον C directory του σταθμού εργασίας με σκοπό την ολοκληρωμένη και εμπεριστατωμένη ανίχνευση απειλών στο μηχάνημα-στόχο. Εκεί εκκινήθηκε scan για πιθανή εύρεση κατηγοριοποιημένων απειλών από ήδη εγκαταστημένο εργαλείο MISP στο σύστημα. Πραγματοποιήσαμε ανάλυση στο διαδίκτυο για ύποπτα αρχεία που τυχόν έχουν εντοπιστεί στο σύστημα – στόχο και η ανάλυση αυτή έχει εκκινήσει μέσω της πλατφόρμας VirusTotal, μέσω της αναζήτησης του αρχείου στο διαδίκτυο χρησιμοποιώντας το όνομα του ή το μοναδικό αριθμό κατακερματισμού του (hash) και τέλος πραγματοποιώντας δυναμική ανάλυση μέσω του διαθέσιμου εργαλείου ανοιχτού λογισμικού σε απομονωμένο περιβάλλον (open source sandbox) ονόματι ‘hybrid analysis sandbox’.

Το εκτελέσιμο στο οποίο εργαστήκαμε (KMSELDI.exe) ενδέχεται να φέρει συχνά κακόβουλο κώδικα λόγω της ύπαρξης του στο ανοικτό διαδίκτυο. Και το τελευταίο διότι αρκετοί κακόβουλοι προγραμματιστές ανοιχτού κώδικα τροποποιούν και παραμετροποιούν το εν λόγω εκτελέσιμο με στόχο την απομακρυσμένη εκτέλεση κώδικα στο μηχάνημα, στο οποίο έχει γίνει η εγκατάσταση του αρχείου. Η εκτέλεσή του KMSELDI.exe δεν απαιτεί κάποιον εξειδικευμένο μηχανικό λογισμικού για την ανάλυση του αρχείου (το αρχείο μπορεί να αναλυθεί και να τρέξει από έναν απλό χρήστη με την κατάλληλη προϋπόθεση του να είναι τοπικός διαχειριστής), όμως από τον χρήστη που θα εκτελεστεί η εφαρμογή πρέπει να υπάρχει η απαραίτητη γνώση για τι είναι το εν λόγω αρχείο κα σε τι αποσκοπεί.

Το KMSELDI.exe δεν είναι απαραίτητο για το λειτουργικό σύστημα των Windows και προκαλεί προβλήματα σε ενδεχομένη κακόβουλη χρήση αυτού. Το αρχείο KMSELDI.exe ως επί το πλείστων βρίσκεται σε έναν υποφάκελο του αρχείου "C: \ Program Files". Σε ενδεχομένη παρατήρηση του σε άλλον υποφάκελο του συστήματος και φυσικά σε ενδεχομένη μη γνώση του διαχειριστή το εκτελέσιμο μπορεί να

προκαλέσει κίνδυνο στο σύστημα καθώς ενδέχεται να εμπεριέχει αλλοιωμένο κώδικα. Το λογισμικό μπορεί να απεγκατασταθεί στον πίνακα ελέγχου (control panel). Το αρχείο KMSELDI.exe δεν είναι ένα βασικό αρχείο των Windows και έτσι το πρόγραμμα δεν έχει ορατό παράθυρο διαχείρισης (εκτέλεσης).
Συνεπώς, πρέπει να ελεγχθεί η διεργασία KMSELDI.exe στον υπολογιστή για να ταυτοποιηθεί εάν πρόκειται για απειλή.

Η εμπεριστατωμένη έρευνα που έλαβε χώρα στην παρούσα εργασία **καθορίζει σαφώς** τα παρακάτω:

1. Ταυτοποίηση και γνώση όλων των υλικών λογισμικού σε ένα σύστημα ή ευρύτερα σε ένα σύνολο συστημάτων
2. Κατηγοριοποίηση των ευρημάτων σε γνωστές, άγνωστες, ύποπτες και θεμιτές εφαρμογές.
3. Εκκίνηση κατηγοριοποίησης και ένταξης όλων των ευρημάτων στην εγκαταστημένη πλατφόρμα του εργαλείου MISP.
4. Ανίχνευση απειλών-κακόβουλων ευρημάτων (σε συνέχεια εκτέλεσης σκαναρίσματος του συστήματος) από το εργαλείο LOKI.
5. Εισαγωγή και έρευνα επί των στοιχείων που συλλέχθηκαν από το τελευταίο scan στα εργαλεία ανοικτού κώδικα Virus total, Cisco Talos & Hybrid Analysis με στόχο την σαφή ενημέρωση επί των αρχικών ενδείξεων και εμπεριστατωμένη ολική ανάλυση επί των δεικτών που προαναφέρθηκαν (IOCs).

Συνοψίζοντας όλων των παραπάνω, η συλλογή και κατανόηση των κυβερνοαπειλών τοπικά σε ένα δίκτυο είτε απομακρυσμένα σε ένα σύνολο καθορισμένων παραμέτρων ενός ευρύτερου δικτύου καθορίζεται από πολλούς παράγοντες για τους οποίους ο μηχανικός ασφάλειας καλείται να λάβει υπόψιν. Κύριο μέλημα είναι η **ΠΡΟΕΛΕΥΣΗ** ενός αναγνωρισμένου ως υπόπτου αρχείο-λογισμικού, η μελέτη επί του τρόπου εγκατάστασης και παραμετροποίησης στο μηχάνημα-στόχο η στο σύνολο των μηχανήματων ενός περιβάλλοντος (πρόσβαση χρηστών και δικαιώματα σε τερματικά μηχανήματα). Εν συνέχεια, και καθώς έχουν καθοριστεί όλα τα παραπάνω θα λάβει χωρά εξατομικευμένη ανάλυση δεικτών παρείσδυσης στο περιβάλλον που έχουμε θέσει προς ανάλυση.

Συμπερασματικά, καταλήγουμε στο άκρως θετικό αποτέλεσμα ότι έχουμε πολύ μεγάλη ΟΡΑΤΟΤΗΤΑ (Visibility) ενός συστήματος ή ενός συνόλου συστημάτων με την χρήση των προαναφερθέντων εργαλείων, αλλά και με τον καθορισμό διαδικασιών και ελέγχων (vulnerability assessment(s)) ανά **ΤΑΚΤΑ ΧΡΟΝΙΚΑ ΔΙΑΣΤΗΜΑΤΑ** στα επιβεβαιωμένα στοιχεία προς ανάλυση.

Βιβλιογραφία

Abdelkarim, A. & Nasereddin, H. (2011). Intrusion Prevention System. International Journal of Academic Research, Vol. 3, No. 1, pp. 432-434.

Aloul, F. (2012). The Need for Effective Information Security Awareness. Journal of Advances in Information Technology, Vol. 3, No. 3, pp. 176-183.

Bacudio, A., Yuan, X., Chu, B. & Jones, M. (2011). An Overview of Penetration Testing, *International Journal of Network Security & Its Applications (IJNSA)*, Vol.3, No.6, pp. 19-38.

Baezner, M. & Robin, P. (2017). *Hotspot Analysis: Stuxnet*. Center for Security Studies (CSS), ETH Zürich.

Bajpai, A., Dayanand, D. & Arya, A. (2018). Big Data Analytics in Cyber Security. *International Journal of Computer Sciences and Engineering*, Vol. 6, No. 7, pp. 731-734.

Bazli, B., Tuncel, M. & Llewellyn-Jones, D. (2014). Data Encryption Using Bio Molecular Information. *International Journal on Cryptography and Information Security (IJCIS)*, Vol. 4, No. 3, DOI: 10.5121/ijcis.2014.4303

Bizimana, O. & Belkhouja, T. (2017) SQL injections and mitigationsScanning and Exploitation using SQLmap. CS 539: Applied Security Concepts, University of Idaho.

Bromiley, M. (2016). *Threat Intelligence: What It Is, and How to Use It Effectively*. SANS Whitepaper, SANS & NSFOCUS.

Carstoiu, B. & Carstoiu, D. (2010). Zatara, the Plug-in-able Eventually Consistent Distributed Database. *Advanced in Information Sciences and Service Sciences*, Vol. 2, No. 3, pp. 56-67.

Carstoiu, D., Lepadatu, E. & Caspar, M. (2010). Hbase - non SQL Database, Performances Evaluation. *International Journal of Advancements in Computing Technology*, Vol. 2, No. 5, pp. 42-52.

Chan, M., Woon I. & Kankanhalli, A. (2005). Perceptions of information security at the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, Vol. 1, No. 3, pp. 18-41.

Chismon, D. & Ruks, M. (2015). *Threat Intelligence: Collecting, Analysing, Evaluating*. MWR InfoSecurity Ltd.

Christodorescu, M., Jha, S., Seshia, S., Song, S. & Bryant, R. (2005). Semantics-Aware Malware Detection. In *IEEE Symposium on Security and Privacy*, 8-11 May, Oakland, CA, USA.

CIRCL (2016). *Information Sharing and Cyber Security - The Benefits of the Malware Information Sharing Platform (MISP)*. Classification TLP:WHITE, CIRCL.

D'Arcy, J., Hovav, A. & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research,* Vol. 20, No. 1, pp. 79-98.

Department of Defense USA (2011). Department Of Defense Strategy For Operating In Cyberspace.

Dewar, R. (2017). *Active Cyber De-fense, Cyber Defense Trend Analysis,* Center for Security Studies (CSS), ETH Zürich.

ENISA (2015). *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. European Union, Heraklion, Greece.

ENISA (2014). *Standards and tools for exchange and processing of actionable information*. European Union, Heraklion, Greece.

Falliere, N. & Chien, E. (2009). *Zeus: King of the Bots*. Security Response, Symantec Corporation, Cupertino, CA, USA.

Falliere, N., Murchu, L. & Chien, E. (2011). *W32.Stuxnet Dossier*. Technical report, Symantec Corporation, Cupertino, CA, USA.

Galinec, D., Mozlik, D. & Guberina, B. (2017). Cybersecurityand cyber defence: national level strategic approach. *Automatika Journal for Control, Measurement, Electronics, Computing and Communications*, Vol. 58, No. 3, pp. 273-286.

Garcia-Alfaro, J. & Navarro-Arribas, G. (2009). A Survey on Cross-Site Scripting Attacks. arXiv:0905.4850

Ghafir, I. & Prenosil, V. (2014). Advanced Persistent Threat Attack Detection: An Overview. *International Journal of Advancements in Computer Networks and Its Security– IJCNS*, Vol. 4, No. 4, pp. 50-54.

Chaturvedi, M., Gupta, M. & Bhattacharya, J. (2009). Cyber Security Infrastructure in India: A Study.
https://www.researchgate.net/publication/228846974_Cyber_Security_Infrastructure_in_India_A_Study (30/01/2019).

Goodwin, C. & Nicholas, P. (2015). *A framework for cybersecurity information sharing and risk reduction*. Microsoft Corporation.

Condi, M., Dehghantanha, A. & Dargahi, T. (2018). Cyberthreat Intelligence: Challenges and Opportunities. In M. Codi, A. Dehghantanha & T. Dargahi (Eds), *Cyber Threat Intelligence*, Springer, pp. 1-6.

Gurusamy, V. & Hirani, B. (2018). Cyber Security for Our Digital Life. *National Conference on Innovations in Computer Technology and its Applications*, February, Guru Nanak College, Chennai.

Haeussinger, F. & Kranz, J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. *International Conference on Information Systems*, Vol. 34, Milan, Italy.

Haryanto, H., Siahaan, A., Rahim, R. & Mersan, A. (2017). Internet Protocol Security as the Network Cryptography System. *International Journal of Scientific Research in Science and Technology*, Vol. 3, No. 6, pp. 223-226.

Hasan, M., Prajapati, N. & Vohara, S. (2010). Case Study On Social Engineering Techniques for Persuasion. *International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC)*, Vol.2, No.2, pp. 17-23.

Herath, T. & Rao, G. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, Vol. 18, No. 2, pp. 106-125.

Hopping, C. (2018). What's the difference between antimalware and antivirus?, IT Pro, https://www.itpro.co.uk/malware/28153/whats-the-difference-between-antimalware-and-antivirus-1 (28/01/2018).

Impe, K. (2015). How STIX, TAXII and CybOX Can Help With Standardizing Threat Information, IBM, https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/ (30/01/2019).

Imran, M., Algamdi, A. & Ahmad, B. (2015). Role of firewall Technology in Network Security. *International Journal of Innovations & Advancement in Computer Science (IJIACS)*, Vol. 4, No. 12, pp. 3-6.

Ingham, K. & Forrest, S. (1994). Network Firewalls. DOI: 10.1201/9780849330452.ch2

Ingram Micro (2017). Four Types of Big Data Analytics and Examples of Their Use, https://imaginenext.ingrammicro.com/Trends/March-2017/Four-Types-of-Big-Data-Analytics-and-Examples-of-Their-Use (29/01/2019).

ISACA (2017). Security: Vulnerability Assessment, https://cybersecurity.isaca.org/info/cyber-aware/images/ISACA_WP_Vulnerability_Assessment_1117.pdf (27/01/2019).

Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, Vol. 80, No. 5, pp. 973-993.

Kaspersky (2018). Incident Response Guide, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07171449/Incident_Response_Guide_eng.pdf (29/01/2019).

Lee, M., Lee, G. & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information Management*, Vol. 41, No. 6, pp. 707-718.

McGraw, G. (2004). Software Security: Building Security In. *IEEE Security & Privacy*, No. 2, Vol. 2, pp. 80-83.

McMillan, R. (2013). Definition: Threat Intelligence. Gartner, https://www.gartner.com/doc/2487216/defnition-threat-intelligence (29/01/2019).

MISP (2018). Using MISP to share vulnerability information efficiently. MISP, https://www.misp-project.org/2018/01/09/Using-MISP-to-share-vulnerability-information-efficiently.html (29/01/2019).

Morales, J., Xu., S. & Sandhu, R. (2012). Analyzing Malware Detection Efficiency with Multiple Anti-Malware Programs. *ASE*, ISBN: 978-1-62561-001-0

Nachenberg, C. (1997). Computer Virus – Coevolution. Communications Of The ACM, Vol. 40, No. 1., pp. 46-51.

Narayan, S. Kolahi, S., Brookiing, K. & Vere, S. (2008). Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment. *International Conference on Advanced Computer Theory and Engineering*, 20-22 Decmber, Phuket, Thailand.

Panda, M. & Patra, M. (2013). Intrusion Detection and Prevention system. In B. Tripathy & D. Achariya (Eds), *Advances in Secure Computing, Internet Services, and Applications*. IGI Global, pp. 89-103.

PCI Security Standards Council (2017). Information Supplement: Penetration Testing Guidance, https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf (30/01/2019).

Rakheja, P. (2011). Integrating DNA Computing in International Data Encryption Algorithm (IDEA*). International Journal of Computer Applications*, Vol. 26, No.3.

Rijnetu, I. (2017). Antivirus versus Anti Malware: Which One Should I Choose?, *Heimdal Security*, https://heimdalsecurity.com/blog/antivirus-versus-anti-malware/ (28/01/2019).

Salaria, S. & Madaan, N. (2014). Firewall and Its Policies Management. *International Journal of Computer Science and Mobile Computing*, Vol. 3, No. 4, pp. 359-367.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*. Vol. 8, No. 1, pp. 31-41.

Siponen, M., Mahmood, A. & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies?. *Communications of the ACM* . Vol. 52, No. 12, pp. 145-147.

Sood, S. (2012). A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications*, Vol. 35, No. 6, pp.1831-1838.

Spitzner, L. (2002). *Honeypots: Tracking Hackers*. Addison Wesley, U.S.

Stupka, V., Horak, M. & Husak, M. (2017). Protection of personal data in security alert sharing platforms. In *Proceedings of ARES '17*, August 29-September 01, Reggio Calabria, Italy.

Su, V. (2017). *Introduction to Big Data*, Trondheim: NTNU.

Suman, S., Srivastava, N. & Pandit, R. (2014). Cyber Crimes and Phishing Attacks. *International Journal on Recent and Innovation Trends in Computing and Communication*, Vol. 2, No. 2, pp. 334-337.

Symantec (2011). Advanced Persistent Threats: A Symantec Perspective. WhitePaper: Cutting Through The Type.

Tajpour, A., Ibrahim, S. & Marsom, M. (2011). SQL Injection Detection and Prevention Techniques. *International Journal of Advancements in Computing Technology*, Vol. 3, No. 7, pp. 82-91.

Taylor-Sakyi, K. (2016). Big Data: Understanding Big Data. arXiv:1601.04602

Tiwari, M., Kumar, R., Bharti, A. & Kishan, J. (2017). Instrution Detection System. *International Journal of Technical Research and Application*, Vol. 5, No. 2, pp. 38-44.

Tutorial Point (2018). Penetration Testing, https://www.tutorialspoint.com/penetration_testing/penetration_testing_tutorial.pdf (28/01/2019).

Ularu, E., Puican, F., Apostu, A. & Velicnu, M. (2012). Perspectives on Big Data and Big Data Analytics. *Database Systems Journal*, vol. 3, No. 4.

Vaisla, K. & Saini, R. (2014). Analyzing of Zero Day Attack and its Identification Techniques. In *1st International Conference on Advances in Computing & Communication Engineering (ICACCE)*, 22-23 February, Dwarahat.

Vayansky, I. & Kumar, S. (2018). Phishing – challenges and solutions. Computer Fraud & Security, Vol. 2010, No. 1, pp. 15-20.

Villars, L., Olofson, W. & Eastwood, M. (2011). *Big data: What it is and why you should care*. IDC White Paper, IDC, Framingham.

Wall, D. (2008). *Hunting, Shooting and Phishing: New Cybercrime Challenges for Cybercanadians In the 21st Century*. The British Library.

Wanjala, M. & Jacob, N. (2017). Review of Viruses and Antivirus Patterns. *Global Journal of Computer Science and Technology*, Vol. 17., No. 3, Online ISSN: 0975-4172

Wanger, G. (2015). The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information*, Vol. 6, No. 2, pp. 183-211.

https://github.com/Neo23x0/Loki/releases

https://www.nextron-systems.com/loki/

https://securityonline.info/loki-simple-ioc-incident-response-scanner/

https://www.virustotal.com/

https://www.hybrid-analysis.com/

https://www.talosintelligence.com/sha_searches