Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Εργαστήριο Ασφάλειας Συστημάτων

Διπλωματική Εργασία

Ανάλυση Ιομορφικού Λογισμικού

Υλοποίηση Εργαστηριακής Λύσης Αυτόματης Ανάλυσης Συμπεριφοράς Ιομορφικού Λογισμικού

Φύσαρης Γεώργιος

Φεβρουάριος 2014

Επιβλέπων Καθηγητής

Σωκράτης Κάτσικας, Καθηγητής

Πανεπιστήμιο Πειραιώς

Εξεταστική Επιτροπή

Σωκράτης Κάτσικας, Καθηγητής
Πανεπιστήμιο Πειραιώς

Κωνσταντίνος Λαμπρινουδάκης, Αναπληρωτής Καθηγητής
Πανεπιστήμιο Πειραιώς

Χρήστος Ξενάκης, Επίκουρος Καθηγητής
Πανεπιστήμιο Πειραιώς

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΛΙΣΤΑ ΣΧΗΜΑΤΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΑΚΡΩΝΥΜΙΑ

Η/Υ *Ηλεκτρονικός Υπολογιστής*

ΛΣ *Λειτουργικό Σύστημα*

API *Application Programming Interface*

ASCII *American Standard Code for Information Interchange*

ASLR *Address Space Layout Randomization*

C&C *Command and Control*

DDOS *Distributed Denial of Service*

DEP *Data Execution Prevention*

HTTP *Hypertext Transfer Protocol*

HTML *HyperText Markup Language*

IP *Internet Protocol*

PCAP *Packet Capture*

URL *Uniform Resource Locator*

XML *Extensible Markup Language*

RPC *Remote Procedure Call*

SSD Solid State Drive

VDI Virtual Disk Image

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

NAT Network Address Translation

TCP Transmission Control Protocol

PE Portable Executable

DLL Dynamic Link Library

OLE Object Linking and Embedding

OCX OLE Control Extension

FTP File Transfer Protocol

SSH Secure Shell

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Περίληψη

Η ασφάλεια των σύγχρονων πληροφοριακών συστημάτων βάλλεται διαρκώς από νεοεμφανιζόμενα ιομορφικά λογισμικά, η διάδοση των οποίων γίνεται με ραγδαίους ρυθμούς. Από τη μια πλευρά, βρίσκονται οι συγγραφείς των malware οι οποίοι δημιουργούν τεχνηέντως και με τις πιο σύγχρονες τεχνικές επιθέσεων, νέα ιομορφικά λογισμικά που είναι περισσότερο αποτελεσματικά. Από την άλλη μεριά, είναι οι ερευνητές και τις εταιρίες αντι-ιομορφικού λογισμικού που καλούνται συνεχώς στην άμεση και γρήγορη ανάλυση μεγάλης ποσότητας από malware που κατακλύζουν διαρκώς το διαδίκτυο. Προκειμένου να εντοπίσουν και να περιορίσουν την εξάπλωσή τους, υλοποιούν νέα εργαλεία και εφαρμόζουν νέες τεχνικές. Η ελαχιστοποίηση του απαιτούμενου χρόνου ανάλυσης, επιτυγχάνεται με την εφαρμογή μεθόδων αυτοματοποιημένης ανάλυσης της συμπεριφοράς των malware.

Στη παρούσα διπλωματική εργασία, παρουσιάζονται οι τύποι των σύγχρονων ιομορφικών λογισμικών και προτείνεται μια μεθοδολογία ανάλυσης, η οποία αποσκοπεί στην αποκάλυψη της συμπεριφοράς και των τεχνικών που χρησιμοποιούνται από αυτά. Πραγματοποιείται επίσης, η υλοποίηση κατάλληλης εργαστηριακής λύσης αυτόματης ανάλυσης συμπεριφοράς ιομορφικού λογισμικού, με χρήση εργαλείων ανοικτού κώδικα. Γίνεται αξιολόγηση των αποτελεσμάτων της εργαστηριακής λύσης με την ανάλυση ενός άγνωστου και πρόσφατα εμφανιζόμενου malware. Υλοποιούνται καινούργιοι μηχανισμοί για την οπτικοποίηση της διαδικασίας ανάλυσης και την ανίχνευση κακόβουλης συμπεριφοράς και τέλος, εφαρμόζονται τεχνικές ανάλυσης των επιπρόσθετων αρχείων των malware.

Λέξεις κλειδιά: Ιομορφικό Λογισμικό, Κακόβουλο Λογισμικό, Ανάλυση Κακόβουλου Λογισμικού, Ανάλυση Ιομορφικού Λογισμικού, Ανάλυση Συμπεριφοράς, Επιφανειακή Ανάλυση, Δυναμική Ανάλυση, Στατική Ανάλυση.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Abstract

IT Security is constantly threatened by the rapid creation and spreading of new malicious software (malware). On the one hand the malware authors are creating new malware with additional capabilities and improved efficiency using the most modern sophisticated technical attacks. Researchers and antivirus companies, on the other hand, are challenged by instant and quick analysis of a large amount of malware spreading over the internet. In order to detect and eliminate their spreading, they implement new tools and apply new techniques. By applying methods of automated behavior analysis, they achieve minimization of the required time of malware analysis.

In this thesis, the new types of modern malware are presented and an analysis method is proposed which aims at revealing their behavior and their techniques. Furthermore a system has been implemented in order to provide automatic behavior analysis based on open source tools. In addition, an unknown and recently discovered malware sample was analyzed in order to evaluate the results of this system. Newer mechanisms are implemented for the visualization of the analysis procedure, for the detection of malicious behavior and for the analysis of the dropped files.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Keywords: Malware, Malicious Software, Malware Analysis, Malicious Software Analysis, Behavioral Based Detection, Surface Analysis, Static Analysis, Dynamic Analysis.

Κεφάλαιο 1ο

Εισαγωγή

Η ανάλυση ιομορφικού λογισμικού είναι μία σύγχρονη απαίτηση για τον εντοπισμό και τον περιορισμό των κυβερνο - επιθέσεων. Στόχος αυτής της διπλωματικής εργασίας είναι, αφενός η μελέτη και παρουσίαση των τεχνικών ανάλυσης συμπεριφοράς ιομορφικών λογισμικών και αφετέρου, η υλοποίηση κατάλληλης εργαστηριακής λύσης αυτόματης ανάλυσης συμπεριφοράς ιομορφικού λογισμικού, με χρήση εργαλείων ανοικτού κώδικα.

Προκειμένου να διαπιστώσουμε εάν η συμπεριφορά ενός λογισμικού είναι κακόβουλη ή όχι, θα πρέπει να ακολουθήσουμε συγκεκριμένη μεθοδολογία ανάλυσης. Η μεθοδολογία που προτείνουμε, χωρίζεται σε τρεις φάσεις με διαφορετικούς στόχους, διαδικασίες και τρόπο προσέγγισης. Η εργαστηριακή λύση αυτόματης ανάλυσης συμπεριφοράς ιομορφικού λογισμικού που υλοποιούμε, εφαρμόζει την προτεινόμενη μεθοδολογία ανάλυσης και βασίζεται στο λογισμικό ανοιχτού κώδικα Cuckoo. Για την παρουσίαση και την αξιολόγηση των αποτελεσμάτων ανάλυσης της εργαστηριακής λύσης, θα προβούμε σε ανάλυση ενός άγνωστου και πρόσφατα εμφανιζόμενου malware το οποίο επιλέξαμε από το διαδίκτυο. Στη συνέχεια, θα παρουσιάσουμε τα αποτελέσματα όλων των φάσεων της μεθοδολογίας που ακολουθήσαμε και τέλος, θα περιγράψουμε τη λειτουργία και τη συμπεριφορά του malware.

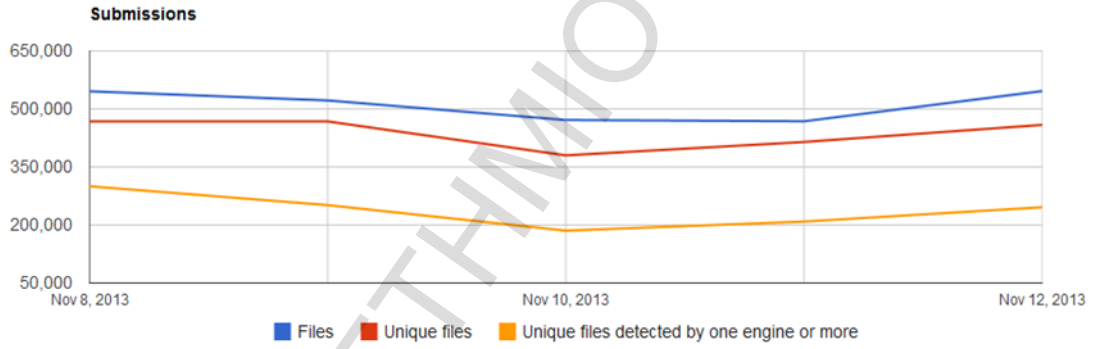
Βασιζόμενοι στην προτεινόμενη μεθοδολογία ανάλυσης και στα αποτελέσματα της εργαστηριακής λύσης, θα υλοποιήσουμε νέες κλάσεις υπογραφών ανίχνευσης και επεξεργασίας για το λογισμικό Cuckoo. Εν συνεχεία, για τη γραφική απεικόνιση της δικτυακής κίνησης, τον εντοπισμό κακόβουλων εξυπηρετητών και την κατηγοριοποίηση των malware, θα ενσωματώσουμε στο λογισμικό Cuckoo το εργαλείο ανοιχτού κώδικα Malcom. Κατόπιν, για την οπτικοποίηση της διαδικασίας ανάλυσης και των αποτελεσμάτων αυτής, θα χρησιμοποιήσουμε το λογισμικό Maltego, σε συνδυασμό με το πακέτο μετασχηματισμών cuckooforcanari. Τέλος, η επέκταση του συστήματος θα ολοκληρωθεί με την υλοποίηση μηχανισμού πολυεπίπεδης ανάλυσης, ο οποίος αποσκοπεί στην αυτοματοποιημένη ανάλυση των επιπρόσθετων αρχείων του malware.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

1.1 Περιγραφή του προβλήματος

Το ιομορφικό λογισμικό καταλαμβάνει πλέον το μεγαλύτερο ποσοστό των περιστατικών ασφάλειας που συναντούμε στα σύγχρονα πληροφοριακά συστήματα. Καθημερινά, αντιμετωπίζουμε τη διάδοση μεγάλης ποικιλίας δειγμάτων malware τα οποία έχουν σχεδιαστεί και υλοποιηθεί με τέτοιον τρόπο ώστε η αντιμετώπιση και η ανάλυσή τους να καθίσταται δύσκολη.

Στο παρακάτω διάγραμμα, απεικονίζεται ο αριθμός των αρχείων malware τα οποία έχουν υποβληθεί για έλεγχο στην υπηρεσία VirusTotal [1] σε ένα τυχαίο χρονικό διάστημα των πέντε ημερών. Η συγκεκριμένη υπηρεσία που χρησιμοποιείται κατά κόρον από ερευνητές malware, ειδικεύεται στην ανάλυση ύποπτων αρχείων και συνδέσμων URL χρησιμοποιώντας πολλαπλές μηχανές antivirus. Σύμφωνα με το ***Σχήμα 1***, το ποσοστό διαφορετικότητας του περιεχομένου των αρχείων που ελέγχονται σε σχέση με τον αριθμό των υποβληθέντων αρχείων, είναι πολύ μεγάλο.



Σχήμα 1 : Υποβληθέντα αρχεία στην υπηρεσία VirusTotal

Αυτό προκύπτει διότι τα νεοεμφανιζόμενα malware είναι παραλλαγές των υφιστάμενων malware. Τα νεοεμφανιζόμενα malware θα πρέπει να αναλυθούν ώστε να δημιουργηθούν νέες υπογραφές εντοπισμού. Σημαντικός παράγοντας είναι ο χρόνος που απαιτείται για την ολοκλήρωση της διαδικασίας ανάλυσης. Οι αναλυτές βρίσκονται πάντοτε ένα βήμα πίσω από τους δημιουργούς των malware. Ως αποτέλεσμα, θα πρέπει να αναλύουν μεγάλο αριθμό από νέα malware, πράγμα το οποίο απαιτεί την εφαρμογή συγκεκριμένων μεθόδων ανάλυσης και αυτοματοποιημένων διαδικασιών με χρήση κατάλληλων εργαλείων.

1.2 Δομή της Διπλωματικής

Η διπλωματική εργασία αποτελείται από επτά κεφάλαια. Στις επόμενες παραγράφους περιγράφεται συνοπτικά το περιεχόμενο του κάθε κεφαλαίου.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Το κεφάλαιο 1 περιέχει την περιγραφή του προβλήματος και τους στόχους, καθώς επίσης τη δομή και τη συνεισφορά της διπλωματικής.

Στο κεφάλαιο 2 αναλύονται οι κύριες κατηγορίες του ιομορφικού λογισμικού και περιγράφεται ο κύκλος ζωής του.

Στο κεφάλαιο 3 περιέχεται η προτεινόμενη μεθοδολογία ανάλυσης του ιομορφικού λογισμικού.

Εν συνεχεία, στο κεφάλαιο 4, παρουσιάζεται η υλοποίηση εργαστηριακής λύσης η οποία αποσκοπεί στην αυτοματοποιημένη ανάλυση ιομορφικού λογισμικού.

Στο κεφάλαιο 5, πραγματοποιείται ανάλυση ενός άγνωστου δείγματος ιομορφικού λογισμικού με χρήση της εργαστηριακής λύσης και παρουσιάζονται τα ευρήματα της ανάλυσης.

Το κεφάλαιο 6, περιλαμβάνει την επέκταση της εργαστηριακής λύσης με την υλοποίηση επιπρόσθετων κλάσεων για την ανίχνευση, επεξεργασία και οπτικοποίηση των αποτελεσμάτων ανάλυσης.

Η ολοκλήρωση της διπλωματικής γίνεται με το κεφάλαιο 7, όπου παρατίθενται τα γενικά συμπεράσματα από την όλη ερευνητική προσπάθεια.

1.3 Συνεισφορά της Διπλωματικής

Η ερευνητική προσπάθεια που διατελέστηκε στο πλαίσιο αυτής της διπλωματικής εργασίας συμβάλλει στην αυτοματοποίηση των διαδικασιών ανάλυσης ιομορφικού λογισμικού και έχει ως απώτερο σκοπό την ελαχιστοποίηση του απαιτούμενου χρόνου ανάλυσης:

- Προτείνει μια συγκεκριμένη μεθοδολογία ανάλυσης ιομορφικού λογισμικού, η οποία περιλαμβάνει τις πιο διαδεδομένες τεχνικές ανάλυσης.
- Παρέχει αναλυτικές οδηγίες για να την υλοποίηση και τη χρήση μιας σύγχρονης εργαστηριακής λύσης αυτόματης ανάλυσης ιομορφικού λογισμικού.
- Περιγράφει όλα τα στάδια της αυτοματοποιημένης ανάλυσης, παρουσιάζοντας αναλυτικά τα αποτελέσματά της.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

- Παρέχει οδηγίες για την υλοποίηση επιπρόσθετων μηχανισμών ανίχνευσης ιομορφικού λογισμικού.

- Εφαρμόζει τεχνικές γραφικής απεικόνισης της δικτυακής κίνησης, αποσκοπώντας στον εντοπισμό κακόβουλων εξυπηρετητών και στην ταυτοποίηση των malware.

- Οπτικοποιεί τις διαδικασίας ανάλυσης, προσφέροντας συνολική εικόνα για την λειτουργία και την αρχιτεκτονική των σύγχρονων malware.

- Προσφέρει τεχνικές αυτοματοποιημένης ανάλυσης των επιπρόσθετων αρχείων των malware με την υλοποίηση κατάλληλων μηχανισμών πολυ-επίπεδης ανάλυσης.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Κεφάλαιο 2ο

Ιομορφικό Λογισμικό

Σε αυτήν τη διπλωματική εργασία, ορίζουμε ως ιομορφικό λογισμικό ή αλλιώς κακόβουλο ή malware, *τα προγράμματα, που αποσκοπούν σε επιθέσεις κατά της Εμπιστευτικότητας, της Ακεραιότητας ή/και της Διαθεσιμότητας των υπολογιστικών συστημάτων* [2]. Για την εγκατάσταση ενός κακόβουλου λογισμικού σε έναν ηλεκτρονικό υπολογιστή (Η/Υ), συνήθως απαιτείται η ανθρώπινη συμμετοχή είτε άμεσα (π.χ. ανταλλαγή αρχείων, άνοιγμα συνημμένων ή προεπισκόπηση μηνυμάτων αλληλογραφίας αμφιβόλου προελεύσεως) ή, έμμεσα (ανεπαρκής προστασία του υπολογιστή, μη λήψη ενημερωμένων εκδόσεων του λογισμικού ασφαλείας και των προγραμμάτων) [3]. Το τμήμα του κώδικα που είναι υπεύθυνο για τις παρενέργειες του λογισμικού, ονομάζεται ωφέλιμο φορτίο (payload). Εκτός από τις παρενέργειες, το κακόβουλο λογισμικό μπορεί να περιλαμβάνει επιπλέον κώδικα με σκοπό την εξάπλωσή του στο σύστημα που προσβάλλει («μόλυνση» από πρόγραμμα σε πρόγραμμα) αλλά και, την μετάδοσή του από το σύστημα που μολύνθηκε σε άλλο/άλλα συστήματα (π.χ. από υπολογιστή σε υπολογιστή) [3].

2.1 Κατηγορίες Ιομορφικού Λογισμικού

Ανάλογα με τον τρόπο λειτουργίας του, το εκάστοτε ιομορφικό λογισμικό μπορεί να ταξινομηθεί στις παρακάτω κατηγορίες.

2.1.1 Virus

Πρόκειται για κακόβουλο λογισμικό το οποίο, αφότου μολύνει έναν Η/Υ έχει την ικανότητα να αναπαράγεται και να μολύνει και άλλα προγράμματα στον Η/Υ-ξενιστή. Η μετάδοσή του σε άλλους Η/Υ μπορεί να πραγματοποιείται αυτόματα (να έχει δηλαδή τα χαρακτηριστικά ενός Σκουληκιού–Worm) ή, να απαιτεί ανθρώπινη παρέμβαση (π.χ. αντιγραφή ενός αρχείου σε USB flash disk και άνοιγμα του αρχείου σε κάποιον Η/Υ). Ο Fred Cohen (1987) [4], περιέγραψε έναν ιό ως *«… ένα πρόγραμμα το οποίο μολύνει άλλα προγράμματα τροποποιώντας τον κώδικά τους ώστε να περιλαμβάνουν μια έκδοση του εαυτού του…* ».

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

2.1.2 Worm

Ή αλλιώς σκουλήκι, ορίζεται ως το κακόβουλο λογισμικό το οποίο αφού μολύνει έναν Η/Υ, έχει την ικανότητα να μεταδίδεται αυτόματα κάνοντας χρήση της υπάρχουσας δικτυακής υποδομής ή/και των υπηρεσιών του διαδικτύου [5]. Τα λογισμικά τύπου worm, δεν προσκολλώνται σε άλλα αρχεία προκειμένου να επιβιώσουν αλλά, λειτουργούν ως αυτόνομα προγράμματα. Το κύριο χαρακτηριστικό τους είναι ότι ενσωματώνουν κώδικα για τον πολλαπλασιασμό τους σε άλλους υπολογιστές, σε αντίθεση με τους παραδοσιακούς ιούς που απαιτούν την ανθρώπινη συμμετοχή για την εξάπλωσή τους. Για τη μετάδοσή τους χρησιμοποιούν είτε συμβατικές μεθόδους (π.χ. e-mail, αντιγραφή σε κοινόχρηστους φακέλους δικτύου κ.λπ.) ή, στην πιο επικίνδυνή τους μορφή, εκμεταλλεύονται ευπάθειες των λειτουργικών συστημάτων ή/και των δικτυακών εφαρμογών που εκτελούνται σε διασυνδεδεμένους Η/Υ.

2.1.3 Backdoor

Είναι το λογισμικό ή ο μηχανισμός ο οποίος επιτρέπει στους επιτιθέμενους να προσπεράσουν τα υφιστάμενα μέτρα ασφάλειας ενός πληροφοριακού συστήματος και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε αυτό. Η εγκατάσταση των backdoors, αποσκοπεί κυρίως στη διατήρηση απομακρυσμένης ή τοπικής πρόσβασης.

2.1.4 Trojan

Ως trojan ορίζουμε το κακόβουλο λογισμικό το οποίο αποσκοπεί στην παραπλάνηση των χρηστών [3], καθώς συνήθως μεταμφιέζεται σε μια χρήσιμη εφαρμογή η οποία όμως περιέχει κακόβουλο κώδικα. Στην πιο κλασική των περιπτώσεων, ένα trojan δημιουργεί μια κερκόπορτα (backdoor) στο σύστημα την οποία, ο επιτιθέμενος θα εκμεταλλευτεί αργότερα για να διαχειριστεί εξ αποστάσεως το σύστημα. Τις περισσότερες φορές τα trojans δεν έχουν μολυσματικό χαρακτήρα δηλαδή, δεν αναπαράγονται και για το λόγο αυτό δεν χαρακτηρίζονται επίσημα ως ιοί.

2.1.5 Rootkits

Εφόσον κάποιο υπολογιστικό σύστημα παραβιαστεί, ο επιτιθέμενος συνήθως επιθυμεί να αποκρύψει όλα τα ίχνη του και τις μελλοντικές του δραστηριότητες σε αυτό. Ως rootkit, ορίζεται ένα κακόβουλο λογισμικό το οποίο λειτουργεί σε πολύ χαμηλό

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

επίπεδο στο λειτουργικό σύστημα του Η/Υ-στόχου. Τις περισσότερες φορές ενσωματώνει λειτουργίες απόκρυψης και παρακάμπτει τους μηχανισμούς πρόληψης και ανίχνευσης [6] όπως, τοίχος προστασίας (firewall) και αντι-ιομορφικό λογισμικό (antivirus). Ένα rootkit μπορεί να ανήκει σε οποιαδήποτε από τις κατηγορίες ιομορφικού λογισμικού. Συνήθως ωστόσο, ανοίγει κερκόπορτες που θα επιτρέψουν την μετέπειτα απομακρυσμένη διαχείριση του ξενιστή από κάποιον τρίτο με μη ανιχνεύσιμο τρόπο. Ανάλογα με το στοχοποιημένο σύστημα, ένα rootkit μπορεί να προγραμματιστεί για να λειτουργήσει σε επίπεδο εφαρμογής (application-layer), σε επίπεδο βιβλιοθηκών (library-layer), σε επίπεδο πυρήνα συστήματος (kernel-layer), ακόμη και σε υλικο-λογισμικό (hardware-layer).

2.1.6 Bots

Ως bot, ορίζεται το κακόβουλο λογισμικό το οποίο εγκαθίσταται σε κάποιον Η/Υ, καθιστώντας τον μέλος ενός μεγάλου δικτύου υπολογιστών (botnet). Ο υπολογιστής–στόχος, ελέγχεται εξ αποστάσεως από τρίτους, με σκοπό την πραγματοποίηση διάφορων κακόβουλων ενεργειών. Ο όρος «bot», προέρχεται από τη λέξη «robot» και χρησιμοποιείται για να περιγράψει κάθε είδους αυτοματοποιημένης διαδικασίας. Ο Η/Υ που έχει μολυνθεί από ένα bot, συχνά αναφέρεται ως «zombie». Ένα σύγχρονο «zombie», αντιπροσωπεύει μια εκδοχή ενός εξειδικευμένου ιομορφικού λογισμικού το οποίο μπορεί να χρησιμοποιηθεί για κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDOS), για την αποστολή διαφημιστικών μηνυμάτων (SPAM), για την πραγματοποίηση επιθέσεων παραπλάνησης (Phishing Attacks) κ.ά. Τα botnets σήμερα θεωρούνται ως μια από τις μεγαλύτερες απειλές για την ασφάλεια των υπολογιστικών συστημάτων διότι, παρέχουν στον επιτιθέμενο μεγάλη υπολογιστική ισχύ αλλά και εύρος ζώνης (bandwidth).

2.1.7 Spyware και Adware

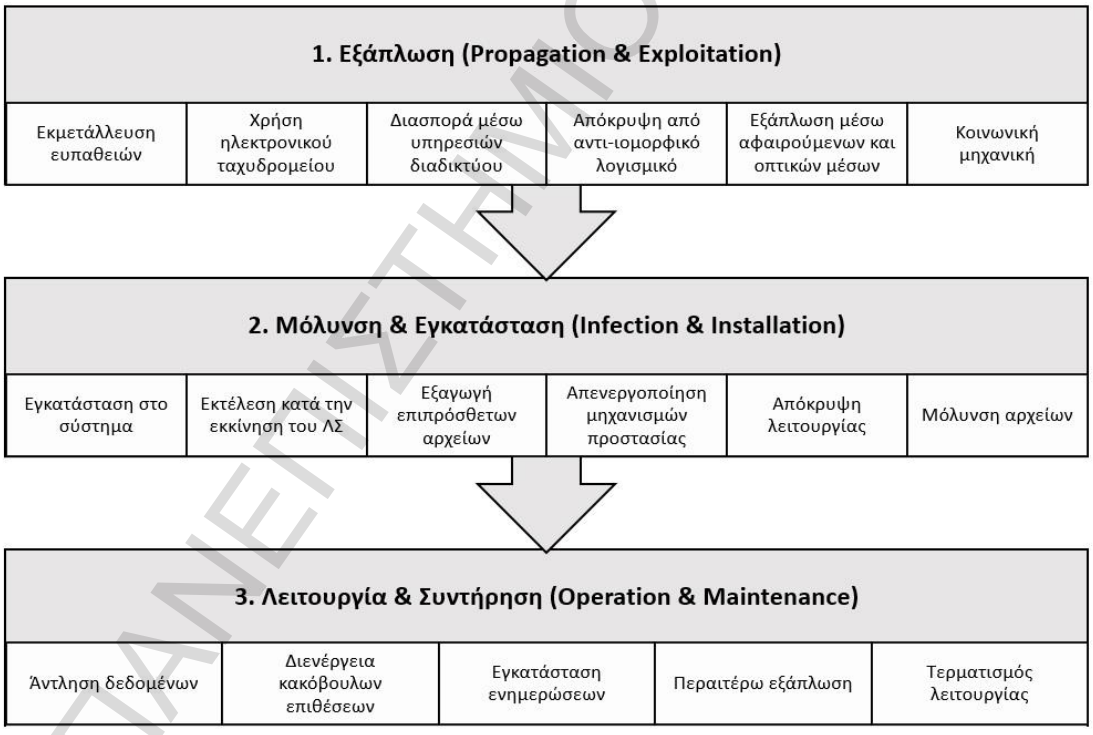
Σύμφωνα με τον John Aycock (2006) [5], ως spyware ορίζεται ένα πρόγραμμα το οποίο συλλέγει πληροφορίες από έναν υπολογιστή και τις μεταφέρει σε κάποιον τρίτο. Ως εκ τούτου, στην παρούσα εργασία ορίζουμε ως spyware, *το λογισμικό που συλλέγει και μεταδίδει πληροφορίες από έναν υπολογιστή σε έναν άλλον, χωρίς τη γνώση του χρήστη ή συγκατάθεση του ιδιοκτήτη του*. Συνήθως ο στόχος του spyware, είναι να συλλέγει προσωπικά δεδομένα όπως όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, στοιχεία

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

πιστωτικών καρτών και κωδικούς πρόσβασης. Αυτές οι πληροφορίες στη συνέχεια αξιοποιούνται από τον επιτιθέμενο για την αλίευση ευαίσθητων πληροφοριών και για τη διενέργεια κακόβουλων πράξεων. Τα adware, διαφοροποιούνται ως προς τα spyware σε σχέση με τον τύπο των πληροφοριών που υποκλέπτουν. Συνήθως στοχεύουν στην άντληση πληροφοριών οι οποίες σχετίζονται με τους χρήστες και τις συνήθειές τους [5] (π.χ. παρακολούθηση της αγοραστικής συμπεριφοράς των χρηστών κατά την περιήγηση στο διαδίκτυο και στη συνέχεια αποστολή ή εμφάνιση διαφημιστικών μηνυμάτων).

2.2 Κύκλος Ζωής Ιομορφικού Λογισμικού

Ο κύκλος ζωής των malware διαφοροποιείται ανάλογα με τον τρόπο λειτουργίας και την κατηγορία στην οποία ανήκουν. Τα βασικά στάδια εκτέλεσης ενός σύγχρονου malware είναι [7], η εξάπλωση μέσω μηχανισμών εκμετάλλευσης ευπαθειών ή μέσω κοινωνικής μηχανικής, η μόλυνση με χρήση μηχανισμών εγκατάστασης και, η κύρια λειτουργία τους σε συνδυασμό με διαδικασίες συντήρησης (***Σχήμα 2***).



Σχήμα 2 : Κύκλος ζωής του σύγχρονου ιομορφικού λογισμικού

2.2.1 Εξάπλωση

Ένα worm, μπορεί να εκτελέσει κακόβουλο κώδικα εκμεταλλευόμενο μια ή πολλές ευπάθειες λογισμικού. Με χρήση κοινωνικής μηχανικής, κάποιος χρήστης μπορεί να παραπλανηθεί και να εκτελέσει κακόβουλο λογισμικό στον υπολογιστή του. Μια

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ευπάθεια στον φυλλομετρητή ή σε άλλα προγράμματα ενός Η/Υ μπορεί να αποτελέσει κύρια αιτία εξάπλωσης ενός malware . Το payload ενός malware τις περισσότερες φορές περιέχει πολλές λειτουργίες. Εκτός από τεχνικές εκμετάλλευσης ευπαθειών, όπως buffer και heap overflows, μπορεί να περιέχει και τεχνικές παραβίασης μηχανισμών ασφάλειας όπως, ALSR και DEP. Κατά τη διαδικασία εκμετάλλευσης μιας ευπάθειας τοποθετείται στην μνήμη του στοχοποιημένου συστήματος, κώδικας. Ο κώδικας αυτός στη συνέχεια, εξάγεται από την μνήμη και εκτελείται στο σύστημα με χρήση διάφορων τεχνικών (decryption, deobfuscation).

2.2.2 Εγκατάσταση

Όπως προαναφέραμε, το payload των malware ανάλογα με τον τρόπο που έχει υλοποιηθεί μπορεί να περιέχει διάφορες λειτουργίες. Μια από αυτές τις λειτουργίες, είναι και η διαδικασία της εγκατάστασης. Κατά την αρχική εκτέλεση, χρησιμοποιείται κώδικας μεταφόρτωσης (dropper/downloader) ο οποίος αναλαμβάνει να μεταφορτώσει μέσω διαδικτύου επιπρόσθετα στοιχεία του malware. Εκτός του κώδικα μεταφόρτωσης μπορεί να χρησιμοποιείται και κώδικας απενεργοποίησης μηχανισμών ασφάλειας, κώδικας εφαρμογής ενημερώσεων ή/και κώδικας προστασίας ανίχνευσης. Με αυτόν τον τρόπο, επεκτείνονται οι δυνατότητες λειτουργίας του malware, μειώνεται το μέγεθός του και αποφεύγεται η ανίχνευση των στοιχείων που το συνθέτουν κατά την πλήρη λειτουργία του [7]. Εφόσον μεταφορτωθούν όλα τα απαραίτητα στοιχεία του malware, ολοκληρώνεται η διαδικασία της εγκατάστασης στο σύστημα και πλέον το malware είναι πλήρως λειτουργικό.

2.2.3 Λειτουργία

Εφόσον ολοκληρωθεί η εγκατάσταση του malware, αρχίζει η άντληση πολύτιμων πληροφοριών από τον στόχο. Στοιχεία πιστωτικών καρτών, στοιχεία πρόσβασης και σημαντικά έγγραφα εξάγονται και μεταφέρονται με διάφορους τρόπους στον επιτιθέμενο. Με την ολοκλήρωση της μεταφοράς, το malware επικοινωνεί με την κονσόλα διαχείρισης (C&C) [8] του επιτιθέμενου και αναμένει να δεχθεί νέες εντολές. Οι εντολές αυτές, σχετίζονται με τη διενέργεια νέων επιθέσεων, με διαδικασίες εφαρμογής ενημερώσεων (updates) ή/και με τον τερματισμό της λειτουργίας του malware.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Κεφάλαιο 3ο

Μεθοδολογία Ανάλυσης

Το πεδίο της ανάλυσης του ιομορφικού λογισμικού είναι αχανές και δεν έχει καταφέρει να τεκμηριωθεί σωστά σε μεγάλο βαθμό. Το γεγονός αυτό οφείλεται κυρίως στο ότι, οι μεγαλύτεροι αναλυτές ιομορφικού λογισμικού είναι οι εταιρίες υλοποίησης λογισμικών antivirus. Κατά συνέπεια, οι εταιρείες αυτές θέλοντας να προστατεύσουν τα συμφέροντά τους, αρνούνται να δημοσιοποιήσουν την εμπειρία και την τεχνογνωσία τους πάνω σε αυτό το θέμα. Τα περισσότερα προγράμματα antivirus βασίζουν τη λειτουργία τους στην αναγνώριση υπογραφών [9]. Κατά τη σάρωση αρχείων, χρησιμοποιούν αλγορίθμους εντοπισμού υπογραφών και βάση των αποτελεσμάτων κατηγοριοποιούν τα υπό ανάλυση αρχεία σε «καθαρά», «μολυσμένα» και «ύποπτα». Η συγκεκριμένη μέθοδος ανίχνευσης μπορεί να προσπεραστεί εύκολα από τους επιτιθέμενους, με αποτέλεσμα το ιομορφικό λογισμικό να μην εντοπίζεται από τα antivirus.

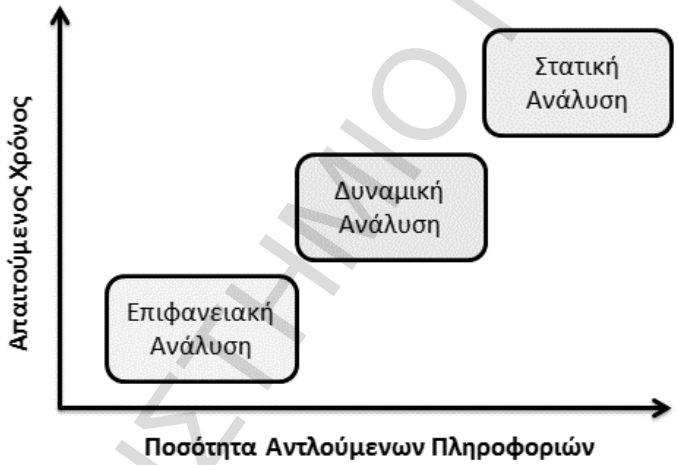
Εκτός από τις υπογραφές, χρησιμοποιούνται και μηχανισμοί ανίχνευσης με βάση τη συμπεριφορά των malware κατά την εκτέλεσή τους. Με αυτόν τον τρόπο, μπορούν να εντοπιστούν και οι παραλλαγές υφιστάμενων malware. Επιπροσθέτως, με την ανάλυση της συμπεριφοράς εκτέλεσης, τα antivirus μπορούν να εντοπίσουν και malware τα οποία εκμεταλλεύονται αδυναμίες λογισμικού (vulnerabilities). Αλλάζοντας τη ροή εκτέλεσης του κώδικα των malware, οι επιτιθέμενοι μπορούν να προσπεράσουν και αυτούς τους μηχανισμούς ανίχνευσης.

Οι εκδόσεις του λογισμικού και των λειτουργικών συστημάτων επηρεάζουν σε μεγάλο βαθμό τη διαφοροποίηση και τη λειτουργία των malware. Οι επιτιθέμενοι, ανάλογα με τις εκδόσεις που χρησιμοποιούνται περισσότερο σε παραγωγικό περιβάλλον, καλούνται να υλοποιήσουν νέους τύπους ιομορφικού λογισμικού και να υιοθετήσουν νέες τεχνικές προκειμένου να αποφύγουν τους μηχανισμούς ανίχνευσης και προστασίας. Ως παράδειγμα αναφέρουμε το πιο διάσημο λειτουργικό στον κόσμο, τα Windows XP, τα οποία θα σταματήσουν να υποστηρίζονται επίσημα τον Απρίλιο του 2014. Αυτό σημαίνει ότι, οι περισσότεροι χρήστες και οργανισμοί πλέον θα χρησιμοποιούν το

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

επόμενο πιο διαδεδομένο λειτουργικό σύστημα της Microsoft, που είναι τα Windows 7. Τα νέα λειτουργικά έχουν διαφορετικούς πυρήνες (kernels), λειτουργίες και διεπαφές προγραμματισμού εφαρμογών (API).

Η ανάλυση ιομορφικού λογισμικού δεν είναι απλά η σάρωση ενός αρχείου με χρήση ενός λογισμικού antivirus. Υπάρχουν πολλοί τρόποι για να διαπιστώσουμε εάν ένα αρχείο έχει κακόβουλη συμπεριφορά ή όχι. Σε αυτήν τη διπλωματική εργασία, ως ανάλυση ιομορφικού λογισμικού ορίζουμε *τη μεθοδολογία που πρέπει να ακολουθήσουμε προκειμένου να διαπιστώσουμε, εάν η συμπεριφορά ενός λογισμικού είναι κακόβουλη ή όχι*. Η μεθοδολογία αυτή, μπορεί να χωριστεί σε τρεις φάσεις με διαφορετικούς στόχους, διαδικασίες και τρόπο προσέγγισης. Την επιφανειακή ανάλυση (surface), τη δυναμική ανάλυση (dynamic) και τη στατική ανάλυση (static). Και οι τρεις προαναφερθείσες φάσεις ανάλυσης απαιτούν χρόνο, εργαλεία και κατάλληλη τεχνογνωσία (***Σχήμα 3***).



Σχήμα 3 : Προτεινόμενες φάσεις ανάλυσης ιομορφικού λογισμικού

3.1 Επιφανειακή Ανάλυση

Η επιφανειακή ανάλυση, είναι συνήθως η πρώτη φάση της διαδικασίας ανάλυσης ενός malware. Σε αυτήν την φάση, πραγματοποιείται σάρωση του malware με μια ή πολλές μηχανές antivirus και γρήγορη αναζήτηση στα περιεχόμενά του για στοιχεία που πιθανόν να αποκαλύπτουν την ταυτότητά του. Πληροφορίες οι οποίες προκύπτουν από τον εντοπισμό συγκεκριμένων συμβολοσειρών (strings) στα περιεχόμενα των αρχείων malware, μπορούν να αποκαλύψουν σημαντικά στοιχεία στον αναλυτή. Οι συμβολοσειρές αυτές, είναι προκαθορισμένες τιμές μεταβλητών οι οποίες εισάγονται αυτούσιες στο εκτελέσιμο αρχείο malware που παράγεται από τη διαδικασία της

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

μεταγλώττισης. Ως παράδειγμα μπορούμε να αναφέρουμε το bot BlackEnergy [10] στο οποίο εντοπίζονται τα δύο παρακάτω strings:

- Opera/9.02 (Windows NT 5.1; U; ru)
- Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.8.1.1)

Αυτά τα strings, περιέχονται ως συμβολοσειρές στο εκτελέσιμο αρχείο και μας δίνουν σημαντικές πληροφορίες για τη συμπεριφορά του bot. Το εν λόγω malware, κατά τη λειτουργία του, δημιουργεί συνδέσεις HTTP και χρησιμοποιεί στην μεταβλητή «User Agent» τις προαναφερθείσες συμβολοσειρές. Σκοπός του συγκεκριμένου malware είναι, η διενέργεια DDOS επιθέσεων με χρήση πολλαπλών αιτημάτων HTTP. Το string «ru», σχετίζεται με τη γλώσσα του φυλλομετρητή η οποία στην προκειμένη περίπτωση είναι η ρώσικη. Βασιζόμενοι στα παραπάνω χαρακτηριστικά, θα μπορούσαμε εύκολα να εντοπίσουμε την ταυτότητα του malware και να το περιορίσουμε.

Η επιφανειακή ανάλυση όπως προαναφέραμε, περιλαμβάνει και τις διαδικασίες σάρωσης του malware με χρήση προγραμμάτων antivirus. Τα antivirus, προσπαθούν να εντοπίσουν συγκεκριμένες υπογραφές στα περιεχόμενα των αρχείων του malware. Εκτός από τα antivirus τα οποία χρησιμοποιούμε στην καθημερινή μας εργασία, υπάρχουν και διαδικτυακές υπηρεσίες οι οποίες προσφέρουν δυνατότητα ελέγχου με τη χρήση πολλαπλών μηχανών antivirus.

Η φάση της επιφανειακής ανάλυσης μας δίνει μια γενική εικόνα για τη λειτουργία του malware. Βασιζόμενοι στα αποτελέσματα της σάρωσης των προγραμμάτων antivirus και στα στοιχεία που μπορούμε να αντλήσουμε από το διαδίκτυο για τα strings που εμπεριέχονται σε αυτό, εντοπίζουμε πληροφορίες που σχετίζονται με τη λειτουργία και τον τύπο του malware.

3.2 Δυναμική Ανάλυση

Η δυναμική ανάλυση περιλαμβάνει κυρίως, την εκτέλεση του malware σε κάποιον υπολογιστή και σε συνέχεια την άντληση και την επεξεργασία πληροφοριών που σχετίζονται με τη συμπεριφορά του. Αυτή η διαδικασία σε αντίθεση με την επιφανειακή ανάλυση, είναι πιο πολύπλοκη και απαιτεί περισσότερο χρόνο. Κατά την εκτέλεση του malware, μας ενδιαφέρει κυρίως να κατανοήσουμε και να καταγράψουμε τα παρακάτω στοιχεία:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

- Τις διεργασίες και τις εντολές που εκτελούνται στο σύστημα και συγκεκριμένα στην μνήμη του Η/Υ.
- Τις αλλαγές που πραγματοποιούνται στο σύστημα αρχείων και στη registry.
- Τη δικτυακή κίνηση.

Η εποπτεία της μνήμης και του αρχείου συστήματος μπορεί να μας δώσει σημαντικές πληροφορίες για τη συμπεριφορά του malware. Η δικτυακή κίνηση μας αποκαλύπτει τον τρόπο που επικοινωνεί το malware με άλλους υπολογιστές στο δίκτυο. Η καταγραφή των αλλαγών στο σύστημα αρχείων, μας παρέχει στοιχεία για νέα αρχεία που δημιουργούνται κατά την εκτέλεση του malware, για τον τρόπο εγκατάστασής του στο σύστημα, για τις τεχνικές που χρησιμοποιεί ώστε να παραμένει ενεργό κατά την εκκίνηση του συστήματος και, για τον τρόπο με τον οποίο κρύβει τα ίχνη του.

Η συλλογή και επεξεργασία της δικτυακής κίνησης μας αποκαλύπτει διευθύνσεις IP, πρωτόκολλα επικοινωνίας και στοιχεία για το περιεχόμενο που αποστέλλεται ή λαμβάνεται από το malware. Το εικονικό σύστημα στο οποίο εκτελείται το malware, θα πρέπει να δημιουργεί όσο το δυνατόν μικρότερη δικτυακή κίνηση προκειμένου να μην επηρεάζει τα αποτελέσματα της ανάλυσης. Για να αντλήσουμε περαιτέρω πληροφορίες για την επικοινωνία και τη λειτουργία των malware, θα πρέπει το περιβάλλον ανάλυσης να διαθέτει πρόσβαση στο διαδίκτυο.

Η εκτέλεση του malware σε ένα περιβάλλον το οποίο διαθέτει πρόσβαση στο διαδίκτυο, μπορεί να έχει καταστροφικές συνέπειες. Για τον λόγο αυτό, θα πρέπει να είμαστε κατάλληλα προετοιμασμένοι και να διαθέτουμε τους απαραίτητους μηχανισμούς ώστε να μπορέσουμε να εντοπίσουμε και να περιορίσουμε την εξάπλωσή του malware στο δίκτυο.

Μια επιλογή είναι να εκτελέσουμε το malware με τη χρήση κάποιου λογισμικού αποσφαλμάτωσης (debugger). Ανάλογα με τον debugger που θα χρησιμοποιήσουμε μπορούμε να εξάγουμε τον κώδικά του σε γλώσσα μηχανής (assembly). Ακολουθώντας τη ροή εκτέλεσης του κώδικα βήμα προς βήμα, είμαστε σε θέση να αντλήσουμε χρήσιμες πληροφορίες για τη λειτουργία του malware. Ακόμη, μπορούμε να επηρεάσουμε τη ροή εκτέλεσης του κώδικα και να προσπεράσουμε ελέγχους του malware ώστε να αναλύσουμε συγκεκριμένα τμήματα του κώδικά του. Η ανάλυση του κώδικα εντάσσεται στις διαδικασίες της στατικής ανάλυσης την οποία περιγράφουμε στην επόμενη ενότητα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Η εκτέλεση του malware θα πρέπει κάθε φορά να πραγματοποιείται σε ίδιο περιβάλλον ώστε να μην διαφοροποιούνται τα αποτελέσματα της ανάλυσης και για να μην χάνουμε πολύτιμο χρόνο για την επαναπαραμετροποίηση των συστημάτων εκτέλεσης. Για το σκοπό αυτό, μπορούμε να χρησιμοποιήσουμε τεχνολογίες virtualization ή sandbox. Φυσικά η διαδικασία της δυναμικής ανάλυσης είναι πολυπλοκότερη αυτής της επιφανειακής ανάλυσης και μας δίνει πολύ περισσότερες πληροφορίες για τη λειτουργία του malware.

3.3 Στατική Ανάλυση

Η τελευταία φάση της ανάλυσης είναι η στατική, η οποία περιλαμβάνει την εξέταση του κώδικα μηχανής του δυαδικού αρχείου του malware και αποσκοπεί στην αποκάλυψη πληροφοριών που σχετίζονται με τις τεχνικές που χρησιμοποιεί κατά τη λειτουργία του. Ουσιαστικά, δεν εκτελούμε το malware για να εντοπίσουμε τη συμπεριφορά του αλλά, αναλύουμε τον κώδικα μηχανής του εκτελέσιμου αρχείου. Ακόμη και αν το malware εκτελείται βήμα προς βήμα με χρήση κάποιου debugger, η ανάλυση θεωρείται πάλι στατική.

Το μειονέκτημα της στατικής ανάλυσης είναι ότι απαιτεί πολύ χρόνο και είναι ιδιαίτερα πολύπλοκη. Η εκτέλεση του malware γίνεται ελεγχόμενα από τον αναλυτή και με αυτόν τον τρόπο αποκαλύπτεται το σύνολο των λειτουργιών του. Η στατική ανάλυση τις περισσότερες φορές είναι ταυτόσημη με την αντίστροφη μηχανική (reverse engineering) η οποία, αντί να δημιουργεί ένα προϊόν προσπαθεί να κατανοήσει τον τρόπο που δημιουργήθηκε.

Η επιφανειακή ανάλυση μπορεί να γίνει αντιληπτή και ως μια μορφή στατικής ανάλυσης διότι, το malware δεν εκτελείται ποτέ. Ωστόσο, διαφοροποιούνται λόγω του ότι χρησιμοποιούνται για διαφορετικό σκοπό. Η επιφανειακή ανάλυση προσφέρει συνοπτική εικόνα για το malware σε πολύ μικρό χρονικό διάστημα ενώ αντίθετα, η στατική ανάλυση, απαιτεί πολύ χρόνο και μας δίνει λεπτομερή στοιχεία για τον κώδικα malware.

Στη στατική ανάλυση εξετάζεται ο κώδικας μηχανής σε δυαδική μορφή. Για αυτόν τον σκοπό, μπορούν να χρησιμοποιηθούν διάφορα εργαλεία. Τα πιο βασικά εργαλεία από αυτά είναι οι hex editors. Οι hex editors, διαβάζουν τα περιεχόμενα του δυαδικού αρχείου σε δεκαεξαδική μορφή απεικονίζοντας πολλές φορές τα ίδια περιεχόμενα και σε ASCII

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

μορφή. Ένας άλλος τύπος εργαλείων είναι οι debuggers. Με την χρήση των debuggers μπορούμε να εκτελέσουμε το malware βήμα προς βήμα και να αντλήσουμε πληροφορίες για τις διεργασίες που εκτελεί αλλά και για το περιεχόμενό του. Το μειονέκτημα των debuggers είναι ότι χρειάζεται να εκτελέσουν το malware προκειμένου να μας δώσουν πληροφορίες. Κάποιοι debuggers, υποστηρίζουν την απεικόνιση των δυαδικών πληροφοριών σε γλώσσα assembly χωρίς να απαιτείται η εκτέλεση του malware, λειτουργώντας ουσιαστικά ως από-συναρμολογητές (disassemblers). Οι disassemblers, είναι τα προγράμματα τα οποία απλά μεταφράζουν τον κώδικα μηχανής σε γλώσσα assembly. Οι περισσότεροι τύποι ιομορφικού λογισμικού, χρησιμοποιούν τεχνικές σύγχυσης (obfuscating techniques) στο εκτελέσιμο αρχείο για να εμποδίσουν την ανάγνωση του κώδικα assembly με χρήση disassembler. Με την χρήση διάφορων τεχνικών αλλάζουν τον κώδικα assembly καθιστώντας τον μη αναγνώσιμο και λανθασμένο.

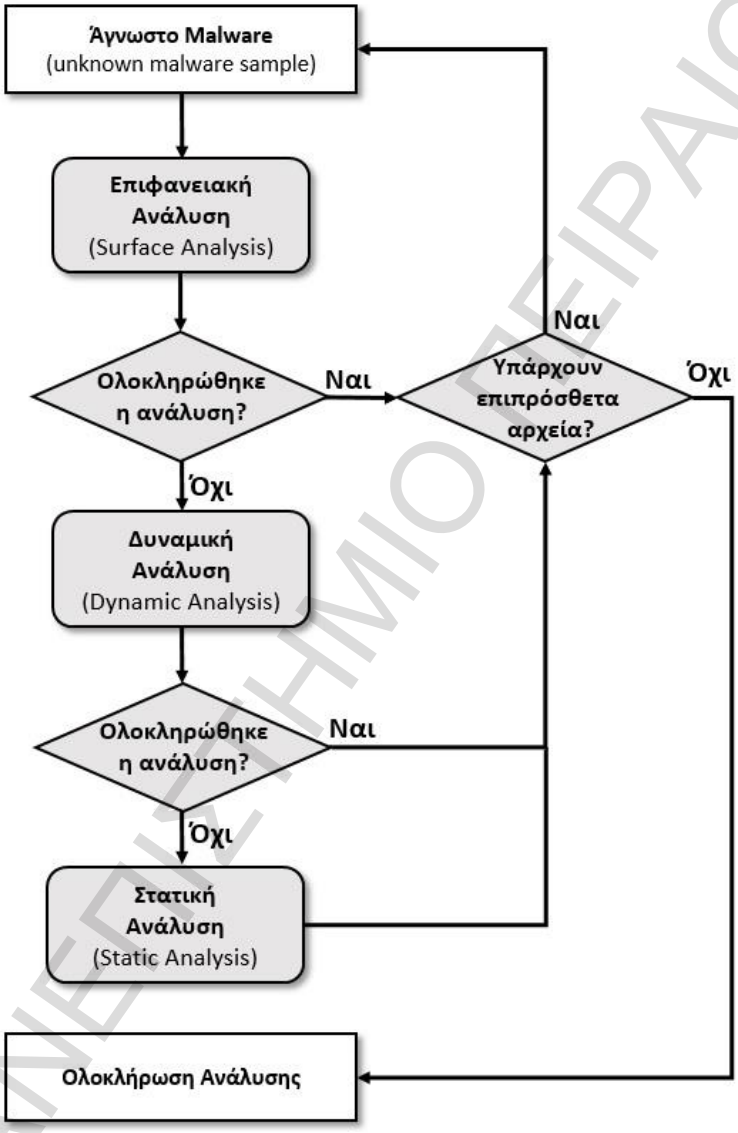
Η τελευταία κατηγορία των εργαλείων που μπορούν να χρησιμοποιηθούν στη διαδικασία της στατικής ανάλυσης είναι οι από-μεταγλωττιστές (decompilers). Τα εργαλεία αυτά προσπαθούν να μετατρέψουν τα εκτελέσιμα αρχεία σε πηγαίο κώδικα. Λόγω της πολυπλοκότητας των σημερινών μεταγλωττιστών (compilers), αυτή η διαδικασία είναι σπάνια εφικτή [10]. Ωστόσο, απο-μεταγλωττίζοντας ένα μικρό κομμάτι εκτελέσιμου αρχείου πολλές φορές μπορεί να μας βοηθήσει να κατανοήσουμε τη δομή και τη λειτουργία του κώδικά του. Ορισμένες γλώσσες προγραμματισμού και μεταγλωττιστές υποστηρίζουν τη δημιουργία εκτελέσιμων αρχείων με δυνατότητα από-μεταγλώττισης. Φυσικά, κάτι τέτοιο δεν εφαρμόζεται σχεδόν ποτέ κατά την υλοποίηση ιομορφικού λογισμικού.

Η στατική ανάλυση ενός εκτελέσιμου αρχείου πολλές φορές ίσως να μην κρίνεται απαραίτητη. Κατά την ολοκλήρωσή της, συνήθως μας δίνει τα ίδια αποτελέσματα για τη συμπεριφορά εκτέλεσης του malware με αυτά της επιφανειακής και δυναμικής ανάλυσης. Είναι σημαντικό, προτού αποφασίσουμε να προβούμε σε στατική ανάλυση, να αξιολογήσουμε αν τα αποτελέσματα της επιφανειακής και δυναμικής ανάλυσης καλύπτουν τις απαιτήσεις μας. Με αυτόν τον τρόπο, εξοικονομούμε πολύτιμο χρόνο παρακάμπτοντας την εξέταση του κώδικα μηχανής. Στην περίπτωση που επιθυμούμε να αντλήσουμε πληροφορίες που αφορούν τον κώδικα που χρησιμοποιεί το malware κατά την λειτουργία του, τότε θα πρέπει να προβούμε σε στατική ανάλυση.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

3.4 Διαδικασία Ανάλυσης

Η διαδικασία της ανάλυσης ιομορφικού λογισμικού μπορεί να περιλαμβάνει μια, δύο ή και, όλες τις προαναφερθείσες φάσεις. Στο ***Σχήμα 4***, απεικονίζεται η προτεινόμενη διαδικασία ανάλυσης ιομορφικού λογισμικού. Όσο προστίθενται φάσεις ανάλυσης, τόσο αυξάνεται ο απαιτούμενος χρόνος και οι πληροφορίες που συλλέγουμε για το malware.



Σχήμα 4 : Προτεινόμενη διαδικασία ανάλυσης ιομορφικού λογισμικού

Στην αρχή της διαδικασίας διαθέτουμε έναν τύπο ιομορφικού λογισμικού για τον οποίο δεν γνωρίζουμε απολύτως τίποτα. Όσο ακολουθούμε τα στάδια της ανάλυσης, εξάγουμε πληροφορίες για τη λειτουργία και τη συμπεριφορά του malware. Σε οποιοδήποτε στάδιο θεωρήσουμε ότι έχουμε ολοκληρώσει τον στόχο μας, μπορούμε να σταματήσουμε την ανάλυση. Τα περισσότερα malware κατά την εκτέλεσή τους

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

δημιουργούν επιπρόσθετα αρχεία (dropped files). Για κάθε αρχείο από αυτά, θα πρέπει να επαναλάβουμε τη διαδικασία από την αρχή. Με τη διεξαγωγή της ανάλυσης με αυτόν τον τρόπο, κερδίζουμε πολύτιμο χρόνο και πόρους. Παραδείγματος χάριν, εάν ένα malware έχει αναλυθεί ξανά στο παρελθόν, θα το εντοπίσουμε στο στάδιο της επιφανειακής ανάλυσης, οπότε δε θα χρειαστεί να προχωρήσουμε στα επόμενα βήματα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Κεφάλαιο 4ο

Εργαστηριακή Υλοποίηση

Για την υλοποίηση της αυτόματης ανάλυσης της συμπεριφοράς ιομορφικού λογισμικού θα βασιστούμε στο λογισμικό ανοιχτού κώδικα Cuckoo [11]. Σε αυτό το κεφάλαιο, θα εξηγήσουμε τον τρόπο λειτουργίας του συγκεκριμένου εργαλείου και στη συνέχεια θα περιγράψουμε τη διαδικασία εγκατάστασης και παραμετροποίησής του. Το εν λόγω εργαλείο, εφαρμόζει με αυτόματο τρόπο και σε πολύ μεγάλο βαθμό τις φάσεις της επιφανειακής και δυναμικής ανάλυσης, όπως τις περιγράψαμε στο κεφάλαιο 3. Η φάση της στατικής ανάλυσης δεν υλοποιείται με αυτόματο τρόπο διότι, αποτελεί χειρωνακτική διαδικασία η οποία απαιτεί την χρήση διάφορων εργαλείων σε αλληλεπίδραση με τον αναλυτή (debugging και disassembling).

4.1 Λογισμικό Αυτόματης Ανάλυσης

Το Cuckoo είναι ένα σύστημα το οποίο προσφέρει αυτοματοποιημένη ανάλυση της συμπεριφοράς ιομορφικού λογισμικού για διάφορα λειτουργικά συστήματα. Παρέχεται δωρεάν σε ανοιχτό κώδικα, έχει υλοποιηθεί σε γλώσσα προγραμματισμού Python και μπορεί να εγκατασταθεί σε οποιοδήποτε λειτουργικό σύστημα Linux. Κατά τη διαδικασία ανάλυσης, χρησιμοποιεί διάφορα πακέτα ανοιχτού κώδικα όπως τα MongoDB [12], Yara [13], SSDEEP [14] και Tcpdump [15]. Η εκτέλεση των malware, πραγματοποιείται σε εικονικό περιβάλλον με λειτουργικό σύστημα Microsoft Windows και με χρήση της εφαρμογής VirtualBox [16]. Με την ολοκλήρωση της διαδικασίας ανάλυσης, το Cuckoo μας δίνει τις παρακάτω πληροφορίες:

- Στοιχεία για τα κλήσεις API των Windows που χρησιμοποιούνται σε όλα τα στάδια εκτέλεσης του malware.
- Αρχεία που δημιουργούνται, διαγράφονται και μεταφορτώνονται μέσω δικτύου από το malware.
- Περιεχόμενα από την μνήμη του λειτουργικού συστήματος (memory dumps) τα οποία σχετίζονται με την εκτέλεση του malware.
- Πλήρη εικόνα της δικτυακής κίνησης που προκαλεί το malware σε εξαγόμενα αρχεία PCAP.

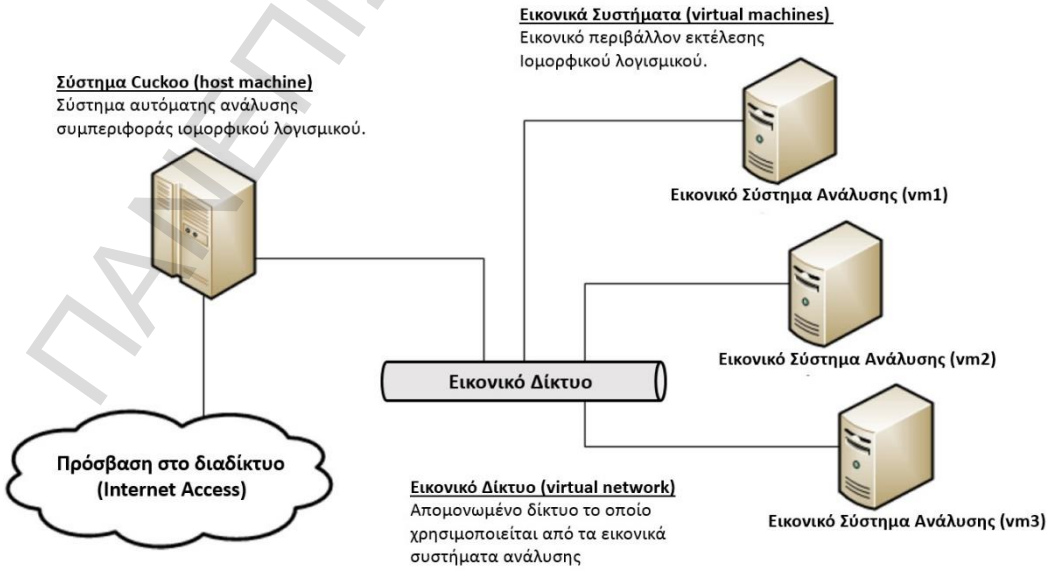
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

- Εικόνες από την επιφάνεια εργασίας (screenshots) των εικονικών συστημάτων κατά την εκτέλεση του malware.
- Δυνατότητα εξαγωγής όλου του περιεχομένου της μνήμης RAM (full memory dump) κατά την εκτέλεση του malware.

Λόγω της σχεδίασής του, είναι δυνατόν να χρησιμοποιηθεί ως απλή εφαρμογή αλλά και ως τμήμα μεγαλύτερων συστημάτων. Η υλοποίηση και η ένταξη επιπρόσθετων εφαρμογών με τη μορφή υπο-προγραμμάτων (modules) στο Cuckoo είναι εύκολα εφαρμόσιμη. Μπορεί να χρησιμοποιηθεί για την ανάλυση αρχείων και συνδέσμων, μερικά από τα οποία αναφέρονται παρακάτω:

- Generic Windows Executables
- DLL files
- PDF documents
- Microsoft Office documents
- URLs
- PHP scripts

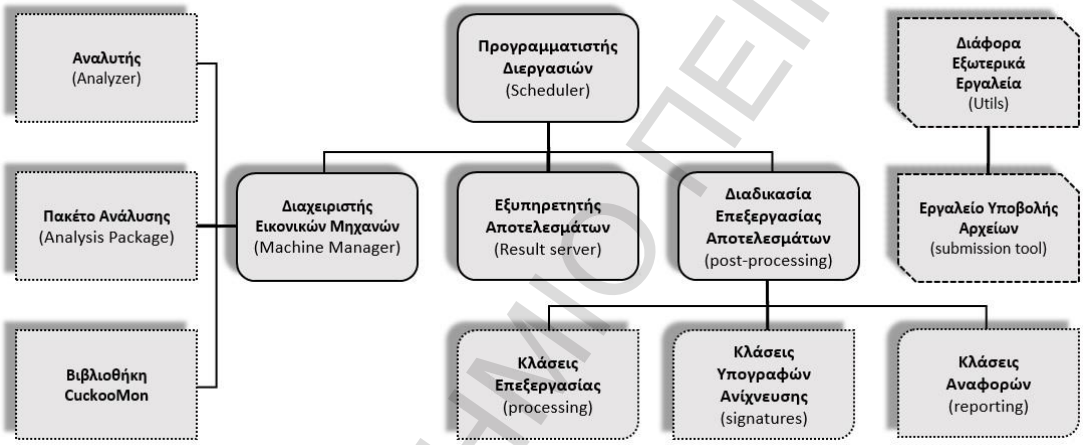
Όσον αφορά στην αρχιτεκτονική του cuckoo (***Σχήμα 5***), αποτελείται από ένα κεντρικό σύστημα διαχείρισης (host machine) το οποίο αναλαμβάνει την εκτέλεση και την ανάλυση των malware σε διάφορα απομονωμένα εικονικά συστήματα (virtual machines).



Σχήμα 5 : Αρχιτεκτονική του λογισμικού Cuckoo

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Η διαδικασία ανάλυσης ξεκινά όταν υποβληθεί αρχείο ή URL στο Cuckoo. Οι πληροφορίες που αποστέλλονται στο Cuckoo, αρχικά αποθηκεύονται σε εσωτερική βάση δεδομένων και όταν βρεθεί διαθέσιμο virtual machine αρχίζει η διαδικασία της ανάλυσης. Πριν την μεταφόρτωση του αρχείου ή του URL από τον εκάστοτε αναλυτή (analyzer), το virtual machine επανέρχεται στην αρχική του κατάσταση (clean state) μέσω της διαδικασίας επαναφοράς κατάστασης (restore snapshot). Ουσιαστικά, για την διαδικασία της ανάλυσης, το μόνο λογισμικό που εκτελείται στο virtual machine είναι ο Cuckoo Agent. Το πρόγραμμα αυτό, είναι ένας XMLRPC server ο οποίος λαμβάνει τις πληροφορίες ανάλυσης και τις μεταβιβάζει στον analyzer (***Σχήμα 6***).



Σχήμα 6 : Επιμέρους κλάσεις λειτουργίας του λογισμικού Cuckoo

Τα πακέτα ανάλυσης (analyzers) του Cuckoo, καθορίζουν τον τρόπο με τον οποίο εκτελείται το εκάστοτε αρχείο στο virtual machine. Για κάθε τύπο αρχείου χρησιμοποιείται ο αντίστοιχος analyzer. Ως παράδειγμα μπορούμε να αναφέρουμε την ανάλυση ενός αρχείου κειμένου (.doc) το οποίο ανοίγει μέσω του πακέτου Microsoft Office ή κάποιο URL το οποίο αναλύεται με χρήση του φυλλομετρητή Internet Explorer.

Εκτός από τις κύριες κλάσεις του Cuckoo υπάρχουν και κάποιες βοηθητικές (auxiliary classes). Οι κλάσεις αυτές εκτελούνται ταυτόχρονα με τη διαδικασία ανάλυσης και δεν προσφέρουν κάποια πληροφορία σχετικά με το malware. Ένα παράδειγμα μιας βοηθητικής κλάσης, είναι η χρήση του module προσομοίωσης ανθρώπινης συμπεριφοράς (***Σχήμα 1***). Σκοπός αυτού του module είναι να προσομοιώσει τη συμπεριφορά των χρηστών με τη διενέργεια πολλαπλών κλικ ή με την κίνηση του ποντικιού. Η χρήση του συγκεκριμένου module, αποτρέπει το malware από το να εντοπίσει ό,τι εκτελείται σε περιβάλλον ανάλυσης.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Πηγαίος κώδικας αρχείου human.py
(cuckoo/analyzer/windows/modules/auxiliaries/human.py)

```
...
   def __init__(self):
        Thread.__init__(self)
        self.do_run = True

    def stop(self):
        self.do_run = False

    def run(self):
        while self.do_run:
            move_mouse()
            click_mouse()
            USER32.EnumWindows(EnumWindowsProc(foreach_window), 0)
            KERNEL32.Sleep(1000)
...
```

Σχήμα 7 : Πηγαίος κώδικας του αρχείου human.py

Η κύρια λειτουργία του Cuckoo βασίζεται στη δυναμική βιβλιοθήκη cuckoomon η οποία καταγράφει όλες τις ενέργειες που πραγματοποιούνται κατά την εκκίνηση μιας διαδικασίας στο virtual machine. Αυτό επιτυγχάνεται μέσω διαδικασιών ανάλυσης κλήσεων API σε επίπεδο χρήστη. Η λειτουργία της βιβλιοθήκης αυτής, διαφοροποιείται για κάθε εκτέλεση αρχείου έτσι ώστε να μην εντοπίζεται από μηχανισμούς προστασίας εκτέλεσης σε περιορισμένο περιβάλλον (anti-sandbox). Για κάθε συνάρτηση που αναλύεται κατά την εκτέλεση αρχείων στο virtual machine, η βιβλιοθήκη cuckoomon αναλαμβάνει και την καταγραφή των στοιχείων που προκύπτουν από αυτήν.

Εφόσον ολοκληρωθεί η εκτέλεση ενός αρχείου, ενεργοποιούνται οι κλάσεις επεξεργασίας (processing modules). Οι κλάσεις επεξεργασίας, συλλέγουν όλα τα στοιχεία που προκύπτουν από την εκτέλεση του αρχείου όπως: διαδικασίες (processes), στοιχεία συμπεριφοράς, κλήσεις API κ.ά. Οι πληροφορίες αυτές στη συνέχεια προωθούνται στις ενεργοποιημένες κλάσεις ανίχνευσης με στόχο τον εντοπισμό κακόβουλης ή ύποπτης συμπεριφοράς. Ως παράδειγμα, στο *Σχήμα **8***, απεικονίζεται μια κλάση υπογραφής η οποία ελέγχει εάν το κακόβουλο λογισμικό ανήκει στην οικογένεια malware SpyEye.

Κώδικας αρχείου banker_spyeye_mutex.py
(cuckoo/ modules/signatures/banker_spyeye_mutex.py)

```
...
class SpyEyeMutexes(Signature):
    name = "banker_spyeye_mutexes"
    description = "Creates known SpyEye mutexes"
    severity = 3
    categories = ["banker"]
    families = ["spyeye"]
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
    authors = ["nex"]
    minimum = "0.5"

    def run(self):
        indicators = [
            "zXeRY3a_PtW.*",
            "SPYNET",
            "__CLEANSWEEP__",
            "__CLEANSWEEP_UNINSTALL__",
            "__CLEANSWEEP_RELOADCFG__"
        ]

        for indicator in indicators:
            if self.check_mutex(pattern=indicator, regex=True):
                return True

        return False
...
```

Σχήμα 8 : Πηγαίος κώδικας του αρχείου banker_spyeye_mutex.py

Με την ολοκλήρωση της εκτέλεσης των κλάσεων επεξεργασίας, ξεκινούν οι διαδικασίες δημιουργίας αναφορών (reporting modules). Όλα τα στοιχεία έχουν ήδη αποθηκευτεί σε εσωτερική βάση δεδομένων και πλέον ανάλογα με την κλάση αναφοράς που θα χρησιμοποιηθεί, το Cuckoo μπορεί να μας δώσει αναφορές σε οποιαδήποτε μορφή επιθυμούμε (html, pdf, raw, json κ.λπ.). Εκτός από τη δημιουργία αναφορών, μπορούμε να δημιουργήσουμε και αυτοματοποιημένες ειδοποιήσεις. Η ενεργοποίηση αυτών των ειδοποιήσεων γίνεται βάση κριτηρίων που τίθενται στα αποτελέσματα της ανάλυσης.

4.2 Περιβάλλον Εργαστηριακής Υλοποίησης

Για την εγκατάσταση και παραμετροποίηση της εφαρμογής Cuckoo (έκδοση 0.6), θα χρησιμοποιήσουμε λειτουργικό σύστημα Linux, έκδοσης Ubuntu Server TLS 12.04.3 (host machine) [17]. Η εγκατάσταση του λειτουργικού συστήματος θα βασιστεί σε VMware Workstation 9.0.1 [18] και δεν θα συμπεριληφθεί στην παρακάτω διαδικασία υλοποίησης. Για την παράλληλη εκτέλεσης πολλαπλών εικονικών συστημάτων θα χρησιμοποιήσουμε 8 GB μνήμης RAM, 8 εικονικούς επεξεργαστές Intel Core I7 στα 3.07 GHz και 100 Gb χωρητικότητας σκληρού δίσκου SSD.

4.3 Εγκατάσταση του Λογισμικού VirtualBox

Με την ολοκλήρωση της εγκατάστασης του Ubuntu Server και την ενημέρωση του λειτουργικού συστήματος με τις τελευταίες αναβαθμίσεις λογισμικού, θα προχωρήσουμε, σε πρώτη φάση, στην εγκατάσταση και παραμετροποίηση του λογισμικού VirtualBox έκδοσης v4.1.12.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
root@mae:~# apt-get install virtualbox
root@mae:~# dpkg -l | grep -i virtualbox
ii  virtualbox                          4.1.12-dfsg-2ubuntu0.3       x86
virtualization solution - base binaries
ii  virtualbox-dkms                     4.1.12-dfsg-2ubuntu0.3       x86
virtualization solution - kernel module sources for dkms
ii  virtualbox-qt                       4.1.12-dfsg-2ubuntu0.3       x86
virtualization solution - Qt based user interface
```

Στη συνέχεια, για την εύκολη διαχείριση του VirtualBox μέσω περιβάλλοντος Web, θα εγκαταστήσουμε το πακέτο λογισμικού Phpvirtualbox v4.1-11 [19] σε Web Server Apache2 με υποστήριξη php5.

```
root@mae:~# apt-get install apache2
root@mae:~# apt-get install php5
root@mae:~# cd /var/www/
root@mae:~# wget http://phpvirtualbox.googlecode.com/files/phpvirtualbox-4.1-11.zip
root@mae:~# unzip phpvirtualbox-4.1-11.zip
root@mae:~# chown -R temsec:temsec /var/www/phpvirtualbox/
root@mae:~# cp /var/www/phpvirtualbox/config.php-example
/var/www/phpvirtualbox/config.php
```

Για την εκτέλεση του VirtualBox, απαιτείται η δημιουργία τοπικού λογαριασμού χρήστη στον οποίο δηλώνουμε όνομα «temsec» και κωδικό πρόσβασης «temsec». Τα στοιχεία πρόσβασης του χρήστη, θα πρέπει να τα ορίσουμε στο αρχείο παραμετροποίησης του PhpVirtualBox το οποίο βρίσκεται στη διαδρομή «/var/www/phpvirtualbox/config.php»

```
 var $username = 'temsec';
 var $password = 'temsec';
```

Η επικοινωνία του PhpVirtualBox με το VirtualBox, πραγματοποιείται μέσω της υπηρεσίας «vboxwebsrv» την οποία ενεργοποιούμε κατά την εκκίνηση του Server. Για την απομακρυσμένη διαχείριση των εικονικών συστημάτων του VirtualBox, χρησιμοποιούμε το πακέτο επέκτασης VRDP [20].

```
root@mae:~# echo "/usr/bin/vboxwebsrv –b" >> /etc/rc.local

root@mae:~# wget
http://download.virtualbox.org/virtualbox/4.1.12/Oracle_VM_VirtualBox_Extension_Pac
k-4.1.12.vbox-extpack

root@mae:~# vboxmanage extpack install Oracle_VM_VirtualBox_Extension_Pack-
4.1.12.vbox-extpack

root@mae:~# /usr/bin/vboxwebsrv –b
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Η σύνδεση στο περιβάλλον Web (παράρτημα 1, σχήμα Π.1.1), γίνεται μέσω της διεύθυνσης «http://ipserver/phpvirtualbox» χρησιμοποιώντας τα προκαθορισμένα στοιχεία πρόσβασης admin/admin.

4.4 Εγκατάσταση του Λογισμικού Cuckoo

Για την εγκατάσταση και παραμετροποίηση του Cuckoo στο host machine, θα πρέπει να εγκατασταθούν όλες οι απαραίτητες βιβλιοθήκες Python καθώς επίσης και τα προαπαιτούμενα πακέτα λογισμικού. Επιγραμματικά, για την βασική λειτουργία του Cuckoo θα χρειαστούν:

Βιβλιοθήκες Python:

- Python-Magic [21] (απαιτείται για τον εντοπισμό τύπων αρχείων μέσω magic offsets)
- Python-dpkg [22] (απαιτείται για την εξαγωγή πληροφοριών από PCAP αρχεία)
- Python-mako [23] (απαιτείται για την εύκολη δημιουργία αναφορών HTML)
- Python-sqlalchemy [24] (απαιτείται για την λειτουργία του web server - web.py)
- Python-jinja2 [25] (απαιτείται για την λειτουργία του web server - web.py)
- Python-bottle [26] (απαιτείται για την λειτουργία του web server - web.py)

```
root@mae:~# apt-get install python
root@mae:~# apt-get install python-magic
root@mae:~# apt-get install python-dpkt
root@mae:~# apt-get install python-mako
root@mae:~# apt-get install python-sqlalchemy
root@mae:~# apt-get install python-jinja2
root@mae:~# apt-get install python-bottle
```

Πακέτα λογισμικού:

- SSDeep [14] (απαιτείται για τον παραγωγή συνόψεων (hashes))

```
root@mae:~# apt-get install ssdeep
root@mae:~# apt-get install python-pyrex
root@mae:~# apt-get install subversion
root@mae:~# apt-get install libfuzzy-dev
root@mae:~# svn checkout http://pyssdeep.googlecode.com/svn/trunk/ pyssdeep
root@mae:~# cd pyssdeep
root@mae:~# python setup.py build
root@mae:~# python setup.py install
```

- MongoDB [12] με υποστήριξη Python (απαιτείται για την αποθήκευση των στοιχείων ανάλυσης)

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
root@mae:~# apt-get install python-pymongo
root@mae:~# apt-get install mongodb
```

- Yara [13] με υποστήριξη Python (απαιτείται για τον εντοπισμό και την κατηγοριοποίηση των malwares)

```
root@mae:~# apt-get install g++
root@mae:~# apt-get install libpcre3 libpcre3-dev
root@mae:~# wget http://yara-project.googlecode.com/files/yara-1.6.tar.gz
root@mae:~# tar -xvzf yara-1.6.tar.gz
root@mae:~# cd yara-1.6
root@mae:~# ./configure
root@mae:~# make
root@mae:~# make check
root@mae:~# make install # finished yara installation
root@mae:~# wget http://yara-project.googlecode.com/files/yara-python-1.6.tar.gz
root@mae:~# tar -xvzf yara-python-1.6.tar.gz
root@mae:~# cd yara-python-1.6
root@mae:~# python setup.py build
root@mae:~# python setup.py install # finished python support installation
```

Εφόσον εγκατασταθούν όλα τα προαπαιτούμενα πακέτα λογισμικού, θα πρέπει να παραμετροποιηθεί κατάλληλα η εφαρμογή tcpdump για να μπορεί να εκτελεστεί ως απλός χρήστης συστήματος, χωρίς να απαιτεί δικαιώματα διαχειριστή.

```
root@mae:~# apt-get install python-pymongo
root@mae:~# apt-get install libcap2-bin
root@mae:~# setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
root@mae:~# getcap /usr/sbin/tcpdump
```

Πριν την εγκατάσταση της εφαρμογής Cuckoo απαιτείται η δημιουργία τοπικού λογαριασμού χρήστη με όνομα «cuckoo». Ο συγκεκριμένος χρήστης θα πρέπει να ανήκει στην ομάδα χρηστών «vboxusers» έτσι ώστε να διαθέτει δικαιώματα εκτέλεσης των virtual machines. Η μεταφόρτωση της τελευταίας έκδοσης της εφαρμογής Cuckoo πραγματοποιείται στον κατάλογο «/root/cuckoo» μέσω του εργαλείου git [27].

```
root@mae:~# sudo useradd cuckoo
root@mae:~# usermod -a -G vboxusers cuckoo
root@mae:~# apt-get install git
root@mae:~# cd
root@mae:~# git clone git://github.com/cuckoobox/cuckoo.git
```

4.5 Δημιουργία Εικονικών Συστημάτων

Όπως προαναφέραμε, η εκτέλεση των malwares πραγματοποιείται σε virtual machine με λειτουργικό σύστημα Microsoft Windows. Τις διαδικασίες ανάλυσης αναλαμβάνει για κάθε επίπεδο εκτέλεσης του malware, το λογισμικό Cuckoo. Στη δική

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

μας περίπτωση, για την προσομοίωση εκτέλεσης του malware, θα χρησιμοποιήσουμε το λειτουργικό σύστημα Microsoft Windows XP Professional SP3 αρχιτεκτονικής x86 με τα παρακάτω χαρακτηριστικά:

- 1 GB RAM Memory
- 20 GB Hard Disk space
- VDI format for the virtual disk
- Dynamically allocated storage

Με χρήση της εντολής «vboxmanage», θα δημιουργήσουμε το virtual machine και θα ολοκληρώσουμε την εγκατάσταση του λειτουργικού συστήματος Windows XP από ISO image, χρησιμοποιώντας παραθυρικό περιβάλλον.

```
root@mae:~# vboxmanage createvm --name "Win.XP.Pro.SP3.x32" --ostype WindowsXP --
register

root@mae:~# vboxmanage modifyvm " Win.XP.Pro.SP3.x32" --memory 1000 --acpi on --
boot1 dvd --nic1 nat

root@mae:~# vboxmanage createhd --filename " Win.XP.Pro.SP3.x32.vdi" --size 20000

root@mae:~# vboxmanage storagectl " Win.XP.Pro.SP3.x32" --name "IDE Controller" --
add ide --controller PIIX4

root@mae:~# vboxmanage storageattach "Win.XP.Pro.SP3.x32" --storagectl "IDE
Controller" --port 0 --device 0 --type hdd --medium " Win.XP.Pro.SP3.x32.vdi"

root@mae:~# vboxmanage storageattach "Win.XP.Pro.SP3.x32" --storagectl "IDE
Controller" --port 0 --device 1 --type dvddrive --medium /root/ISOs/winxpsetup.iso

root@mae:~# VBoxHeadless --startvm "Win.XP.Pro.SP3.x32"
```

Εφόσον ολοκληρωθεί η εγκατάσταση του virtual machine, θα πρέπει να εγκαταστήσουμε σε αυτό τα πρόσθετα πακέτα λογισμικού (guest additions) του VirtualBox [28]. Με αυτόν τον τρόπο έχουμε καλύτερη υποστήριξη μεταξύ του υλικού και του λειτουργικού συστήματος. Στη συνέχεια, θα πρέπει να συνδέσουμε το λογισμικό Cuckoo με το virtual machine έτσι ώστε, να μπορεί να επεξεργαστεί αρχεία και να αναλύσει δικτυακή κίνηση. Για τον σκοπό αυτό θα χρησιμοποιήσουμε τη δυνατότητα των κοινόχρηστων φακέλων (shared folders) του VirtualBox. Ουσιαστικά, θα δημιουργήσουμε τους δύο παρακάτω shared folders (***Πίνακας 1***) και θα τους συνδέσουμε με τους αντίστοιχους του Cuckoo στο host machine.

A/A	**Φάκελοι – Cuckoo Host Machine**	**Shared folders Virtual Machine**

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

1	/root/cuckoo/shares/Win.XP.Pro.SP3.x32	Win.XP.Pro.SP3.x32
2	/root/cuckoo/shares/Win.XP.Pro.SP3.x32.setup	Win.XP.Pro.SP3.x32.setup

Πίνακας 1 : Κοινόχρηστοι φάκελοι στο host machine

Και οι δύο shared folders, με τη χρήση της παραμέτρου «automount» θα ενεργοποιούνται κατά την εκκίνηση του virtual machine. Ο φάκελος νούμερο 2, θα χρησιμοποιηθεί για την μεταφορά αρχείων από το host machine στο virtual machine. Θα πρέπει να οριστεί ως μόνο για ανάγνωση διότι το virtual machine δε θα πρέπει να έχει δικαιώματα εγγραφής σε αυτόν. Ο φάκελος νούμερο 1, θα χρησιμοποιηθεί για την αποθήκευση του αρχείου «dump.pcap», στο οποίο θα εξάγεται όλη η δικτυακή κίνηση του virtual machine μέσω της παραμέτρου «nictrace1».

```
root@mae:~# vboxmanage controlvm "Win.XP.Pro.SP3.x32" poweroff

root@mae:~# mkdir -p /root/cuckoo/shares/ Win.XP.Pro.SP3.x32
root@mae:~# mkdir -p /root/cuckoo/shares/ Win.XP.Pro.SP3.x32.setup

root@mae:~# vboxmanage sharedfolder add "Win.XP.Pro.SP3.x32" --name
"Win.XP.Pro.SP3.x32" --hostpath /root/cuckoo/shares/Win.XP.Pro.SP3.x32 --automount

root@mae:~# vboxmanage sharedfolder add "Win.XP.Pro.SP3.x32" --name
"Win.XP.Pro.SP3.x32.setup" --hostpath /root/cuckoo/shares/Win.XP.Pro.SP3.x32.setup
--automount --readonly

root@mae:~# vboxmanage modifyvm "Win.XP.Pro.SP3.x32" --nictrace1 on --nictracefile1
/root/cuckoo/shares/Win.XP.Pro.SP3.x32/dump.pcap

root@mae:~# vboxheadless --startvm "Win.XP.Pro.SP3.x32"
```

Για να ενεργοποιήσουμε την πρόσβαση του virtual machine στο διαδίκτυο, θα πρέπει παραμετροποιήσουμε κατάλληλα το host και το virtual machine. Αρχικά, δημιουργούμε ένα νέο «hostonly» [30] δίκτυο με όνομα «vboxnet0» με διεύθυνση IP 192.168.56.0/24 και πύλη (gateway) 192.168.56.1. Σε αυτό το δίκτυο συνδέουμε την κάρτα δικτύου του virtual machine. Λόγω του ότι έχουμε απενεργοποιημένη την υπηρεσία DHCP θα πρέπει στην κάρτα δικτύου των Windows XP να δηλώσουμε τις απαραίτητες ρυθμίσεις. Στην περίπτωσή μας χρησιμοποιούμε για το virtual machine διεύθυνση IP 192.168.56.101, gateway 192.168.56.1 και DNS 8.8.8.8 & 8.8.4.4.

```
root@mae:~# vboxmanage hostonlyif create

root@mae:~# vboxmanage list hostonlyifs
Name:            vboxnet0
GUID:            786f6276-656e-4074-8000-0a0027000000
Dhcp:            Disabled
IPAddress:       192.168.56.1
NetworkMask:     255.255.255.0
IPV6Address:
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
IPV6NetworkMaskPrefixLength: 0
HardwareAddress: 0a:00:27:00:00:00
MediumType:      Ethernet
Status:          Down
VBoxNetworkName: HostInterfaceNetworking-vboxnet0

root@mae:~# vboxmanage modifyvm "Win.XP.Pro.SP3.x32" --nic1 hostonly
root@mae:~# vboxmanage modifyvm "Win.XP.Pro.SP3.x32" --hostonlyadapter1 vboxnet0
```

Κατόπιν, στο host machine, με χρήση του πακέτου IPTables [29] το οποίο παρέχεται από το λειτουργικό σύστημα, ενεργοποιούμε NAT στο δίκτυο «vboxnet0». Για να ενεργοποιούνται οι παρακάτω κανόνες κατά την εκκίνηση του host machine, θα τους πρέπει να τους δηλώσουμε στο αρχείο συστήματος «/etc/rc.local».

```
root@mae:~# iptables -A FORWARD -o eth0 -i vboxnet0 -s 192.168.56.0/24 -m conntrack
--ctstate NEW -j ACCEPT

root@mae:~# iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j
ACCEPT

root@mae:~# iptables -A POSTROUTING -t nat -j MASQUERADE

root@mae:~# sysctl -w net.ipv4.ip_forward=1
```

Στην επόμενη φάση, θα πρέπει να αντιγράψουμε τον agent (agent.py) της εφαρμογής Cuckoo στο virtual machine. Η επικοινωνία του agent με την εφαρμογή Cuckoo στο host machine γίνεται μέσω της πόρτας tcp 8080. Για τη σωστή λειτουργία του agent, θα χρειαστεί να προβούμε στις παρακάτω ενέργειες:

- Εγκατάσταση του Compiler της Python [30] για λειτουργικό σύστημα Windows.
- Εγκατάσταση του Module PIL Python [31] για τη δημιουργία desktop screenshots κατά την εκτέλεση των malware.
- Απενεργοποίηση του Windows Firewall.
- Απενεργοποίηση των Windows Updates.
- Εγκατάσταση επιπρόσθετου λογισμικού (Office/Acrobat Reader/Flash Player κ.λπ.).
- Παραμετροποίηση συστήματος για την εκτέλεση του Agent κατά την εκκίνηση των Windows μέσω της registry.

Η αντιγραφή του agent.py μπορεί να γίνει στον κατάλογο «C:\Python27\» του virtual machine. Για να μην εμφανίζεται παράθυρο εντολών κατά την εκτέλεσή του, θα πρέπει να τον μετονομάσουμε από «agent.py» σε «agent.pyw». Για την αυτόματη

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

εκτέλεση του agent κατά την εκκίνηση των Windows, δημιουργούμε το παρακάτω κλειδί (***Πίνακας 2***) στη Registry των Windows.

Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Name	Agent
Type	REG_SZ
Data	C:\Python27\agent.pyw

Πίνακας 2 : Κλειδί registry για την αυτόματη εκκίνηση του Cuckoo agent

Εφόσον ολοκληρώσουμε την παραμετροποίηση του virtual machine και έχουμε εγκαταστήσει όλες τις απαραίτητες εφαρμογές, πριν προχωρήσουμε στην παραμετροποίηση της εφαρμογής Cuckoo θα πρέπει να δημιουργήσουμε ένα snapshot του virtual machine ενώ βρίσκεται σε λειτουργία. Ως όνομα snapshot μπορούμε να δηλώσουμε ότι επιθυμούμε.

4.6 Παραμετροποίηση του Λογισμικού Cuckoo

Για την επικοινωνία της εφαρμογής Cuckoo με το virtual machine, θα πρέπει να παραμετροποιήσουμε τα αρχεία ρυθμίσεων «cuckoo/conf/virtualbox.conf» και «cuckoo/conf/cuckoo.conf» τα οποία παρουσιάζονται παρακάτω.

Παράμετροι αρχείου «cuckoo.conf»:

```
root@mae:~# cat cuckoo.conf | grep -v "#"  | egrep -v "^[[:space:]]*$"
[cuckoo]
version_check = on
delete_original = off
machine_manager = virtualbox
memory_dump = off

[resultserver]
ip = 192.168.56.1
port = 2042
store_csvs = off
upload_max_size = 10485760

[processing]
analysis_size_limit = 104857600
resolve_dns = on

[database]
connection =
timeout =

[timeouts]
default = 120
critical = 600
vm_state = 300
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
[sniffer]
enabled = yes
tcpdump = /usr/sbin/tcpdump
interface = vboxnet0

[graylog]
enabled = no
host = localhost
port = 12201
level = error
```

Παράμετροι αρχείου «virtualbox.conf»:

```
root@mae:~# cat virtualbox.conf | grep -v "#"  | egrep -v "^[[:space:]]*$"
[virtualbox]
mode = headless
path = /usr/bin/VBoxManage
machines = Win.XP.Pro.SP3.x32
[Win.XP.Pro.SP3.x32]
label = Win.XP.Pro.SP3.x32
platform = windows
ip = 192.168.56.101
```

Για την εκκίνηση της εφαρμογής Cuckoo, θα πρέπει να εκτελέσουμε στο host machine το αρχείο «cuckoo.py»:

```
root@mae:~/cuckoo/cuckoo# cd /root/cuckoo/cuckoo/ ; python cuckoo.py


                 _
 ____ _   _  ____| |  _ ___   ___
/ ___) | | |/ ___) |_/ ) _ \ / _ \
( (___| |_| ( (___|  _ ( |_| | |_| |
 \____)____/ \____)_| \_)___/ \___/

Cuckoo Sandbox 0.6
www.cuckoosandbox.org
Copyright (c) 2010-2013

Checking for updates...
Good! You have the latest version available.

2013-11-03 04:51:08,088 [lib.cuckoo.core.scheduler] INFO: Using "virtualbox"
machine manager
2013-11-03 04:51:08,140 [lib.cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2013-11-03 04:51:08,141 [lib.cuckoo.core.scheduler] INFO: Waiting for analysis
tasks...
```

4.7 Διαδικασία Ανάλυσης Ιομορφικού Λογισμικού

Η υποβολή των αρχείων malware προς ανάλυση, μπορεί να πραγματοποιηθεί μέσω γραμμής εντολών ή μέσω εφαρμογής Web. Για την ανάλυση αρχείων με χρήση της γραμμής εντολών, χρησιμοποιούμε την εντολή «submit.py».

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
root@mae:~/cuckoo/cuckoo/utils# ./submit.py  -h
usage: submit.py [-h] [--url] [--package PACKAGE] [--custom CUSTOM]
                 [--timeout TIMEOUT] [--options OPTIONS] [--priority PRIORITY]
                 [--machine MACHINE] [--platform PLATFORM] [--memory]
                 [--enforce-timeout]
                 target

...
root@mae:~/cuckoo/cuckoo/utils# ./submit.py
/root/Malware.Samples/0ad45273ca5c78da3fb35c824b49e624.exe

Success: File "/root/Malware.Samples/0ad45273ca5c78da3fb35c824b49e624.exe" added as
task with ID 42
```

Εφόσον ολοκληρωθεί η διαδικασία ανάλυσης, τα αποτελέσματα της διαδικασίας αποθηκεύονται στον φάκελο «/cuckoo/storage/analyses/<ID>/reports». Στην περίπτωση που επιθυμούμε να χρησιμοποιήσουμε περιβάλλον Web, θα πρέπει πρώτα να εκτελέσουμε την εφαρμογή «web.py». Η εφαρμογή αυτή, βρίσκεται στον κατάλογο «utils» της εγκατάστασης του Cuckoo. Η διαδικασία υποβολής αρχείων μέσω Web καθώς επίσης και η παρουσίαση των αποτελεσμάτων της ανάλυσης, πραγματοποιείται από την διεύθυνση «http://ip-address-of-host-machine:8080» (σχήματα παραρτήματος Π.1.1 και Π.1.2).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Κεφάλαιο 5ο

Μελέτη Περίπτωσης

Στο κεφάλαιο αυτό, θα παρουσιάσουμε τη διαδικασία ανάλυσης ενός άγνωστου malware (***Πίνακας 3***) το οποίο αντλήσαμε από την ιστοσελίδα malwared.ru [32]. Η εν λόγω ιστοσελίδα, αποτελεί μια ελεύθερη βάση δεδομένων με πληροφορίες από malware τα οποία πρωτοεμφανίζονται στο διαδίκτυο. Ο σκοπός της ανάλυσης, είναι η κατανόηση της λειτουργίας, της συμπεριφοράς και των τεχνικών που χρησιμοποιούνται από το συγκεκριμένο malware. Η μεθοδολογία που θα ακολουθήσουμε κατά τη διαδικασία της ανάλυσης, θα είναι αυτή που περιγράψαμε στην ενότητα 3.4. Ως κύριο εργαλείο ανάλυσης, θα χρησιμοποιήσουμε το λογισμικό Cuckoo το οποίο εγκαταστήσαμε και παραμετροποιήσαμε στο κεφάλαιο 4. Αρχικά θα παρουσιάσουμε τα αποτελέσματα της επιφανειακής ανάλυσης, στη συνέχεια τα αποτελέσματα της δυναμικής ανάλυσης και τέλος, θα περιγράψουμε τη λειτουργία και την συμπεριφορά του malware καθώς και των στοιχείων που το συνθέτουν.

Filename	unknown.exe
File Size	111.5 KB (114128 bytes)
Source	http://malwared.ru

Πίνακας 3 :Ιομορφικό λογισμικό μελέτης περίπτωσης

5.1 Επιφανειακή Ανάλυση

5.1.1 Στοιχεία Εκτελέσιμου Αρχείου

Η πρώτη φάση της επιφανειακής ανάλυσης περιλαμβάνει τη δημιουργία υπογραφών οι οποίες χαρακτηρίζουν μοναδικά το malware το οποίο θα αναλύσουμε. Για τη δημιουργία αυτών των υπογραφών, χρησιμοποιούνται πέντε διαφορετικές συναρτήσεις σύνοψης οι οποίες είναι: CRC32, MD5, SHA1, SHA256 και SHA512 (***Πίνακας 4***). Οι υπογραφές αυτές, συνθέτουν την ταυτότητα του malware και μπορούν να χρησιμοποιηθούν ως σημείο αναφοράς για τον εντοπισμό περαιτέρω στοιχείων από το διαδίκτυο.

File name	malware.exe
File size	114128 bytes
File type	PE32 executable (console) Intel 80386, for MS Windows

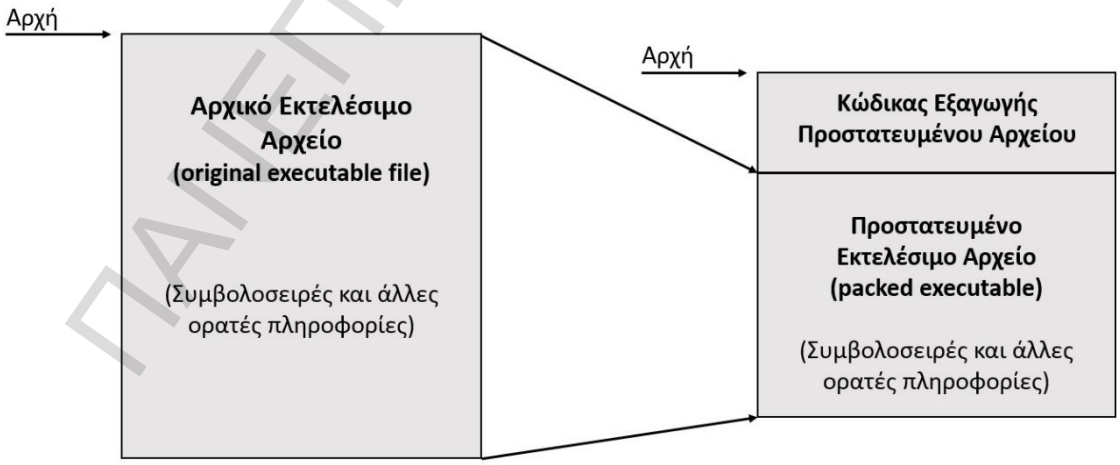
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

CRC32	B2CAD38A
MD5	12e44195d5bf5003730ad80343771ebd
SHA1	cb7a1bf177d3047284a124961e13e00fd6662a5b
SHA256	fdf0fcaae47db4c468a08968cf345df5c35f797561d00aed58c23adf428af1e0
SHA512	0e3deb070ae2f40c8ed2a467c755c6ec470fc16284159d091dbcbb99ae6bd6676fb4399f6d61f9c52e9a3953c45b02a2e2c4d08d7eafddce72a30852024a8f8f
Ssdeep	1536:xzzFH4cPhxBJMFI6Zvu5Tg+uvJaZp2/VB9vV09Fj9MpDUcV:dzFYcPNGc5kTMZym9FeDvV
PEiD	Armadillo v1.71
Yara	None matched

Πίνακας 4 : Στοιχεία εκτελέσιμου αρχείου malware

Το συγκεκριμένο αρχείο, είναι εκτελέσιμο τύπου PE32 για λειτουργικό σύστημα Microsoft Windows με αρχιτεκτονική 32 bit και εκτελείται μόνο σε περιβάλλον γραμμής εντολών (console). Ο τύπος αρχείων PE, είναι ουσιαστικά μια δομή δεδομένων η οποία περιλαμβάνει όλες τις πληροφορίες που απαιτούνται για την εκτέλεση κώδικα από το λειτουργικό σύστημα Microsoft Windows. Στην κεφαλίδα των αρχείων PE (header), περιέχονται σημαντικές πληροφορίες σχετικά με τον κώδικα, τον τύπο της εφαρμογής και τις βιβλιοθήκες που χρησιμοποιούνται από το εκτελέσιμο αρχείο.

Τα αποτελέσματα του προγράμματος PEiD [35] αποκαλύπτουν ότι, το εκτελέσιμο αρχείο έχει συμπιεστεί και προστατευτεί (packed) με χρήση του εμπορικού προγράμματος Armadillo [33] έκδοσης v1.71. Με αυτόν τον τρόπο, οι δημιουργοί των malware προστατεύουν τον εκτελέσιμο κώδικα του malware από τα antivirus και δυσχεραίνουν σε μεγάλο βαθμό τη διαδικασία της στατικής ανάλυσης. Τα packed αρχεία περιλαμβάνουν κώδικα αποκρυπτογράφησης ή/και αποσυμπίεσης (unpacking code/wrapper program).



Σχήμα 9: Δομή packed εκτελέσιμων αρχείων

Κατά την εκτέλεση του προστατευμένου αρχείου, αρχικά εκτελείται ο κώδικας unpacking (***Σχήμα 9***). Ο κώδικας αυτός, αναλαμβάνει να εξάγει στην μνήμη RAM τον

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

αρχικό κώδικα του προστατευμένου αρχείου και στην συνέχεια τον εκτελεί. Ως αποτέλεσμα της παραπάνω τεχνικής προστασίας, η σάρωση του εκτελέσιμου αρχείου με χρήση των προγραμμάτων Ssdeep και Yara δε μας δίνει κάποιο αποτέλεσμα.

5.1.2 Σάρωση με Αντι-Ιομορφικό Λογισμικό

Η χρήση πολλαπλών μηχανών antivirus για την σάρωση του malware, μπορεί να μας δώσει πολύ σημαντικές πληροφορίες για τον τύπο και τη λειτουργία του ιομορφικού λογισμικού. Στην περίπτωσή μας, πραγματοποιήθηκε ανάλυση του εκτελέσιμου αρχείου στις 18/11/2013 και ώρα 18:38:04 UTC, με χρήση της online υπηρεσίας VirusTotal. Η εν λόγω υπηρεσία, παρέχεται δωρεάν και υποστηρίζει 47 διαφορετικές μηχανές ελέγχου. Σύμφωνα με τα αποτελέσματα του VirusTotal (***Πίνακας 5***), το αρχείο unknown.exe εντοπίζεται ως ιομορφικό λογισμικό από 35 διαφορετικές μηχανές antivirus και είχε ελεγχθεί ξανά στο παρελθόν στις 13/08/2013 και ώρα 14:40:40 UTC.

Antivirus	**Result**
Bkav	None
MicroWorld-eScan	Trojan.GenericKD.1178846
nProtect	None
CAT-QuickHeal	None
McAfee	BackDoor-FJW
Malwarebytes	Trojan.FakeMS
K7AntiVirus	Trojan (0001140e1)
K7GW	Trojan (0001140e1)
TheHacker	None
NANO-Antivirus	Trojan.Win32.Tepfer.cboklm
F-Prot	W32/Trojan3.FUG
Symantec	Trojan.Gen.3
Norman	Sinowal.PDB
TotalDefense	None
TrendMicro-HouseCall	TSPY_FAREIT.AGT
Avast	Win32:Fareit-IV [Trj]
ClamAV	None
Kaspersky	Trojan-PSW.Win32.Tepfer.pjnz
BitDefender	Trojan.GenericKD.1178846
Agnitum	None
SUPERAntiSpyware	None
Sophos	Troj/Agent-ADEX
Comodo	UnclassifiedMalware
F-Secure	Trojan.GenericKD.1178846
DrWeb	Trojan.PWS.Stealer.946
VIPRE	Trojan.Win32.Generic!BT
AntiVir	TR/PSW.Agent.SQO
TrendMicro	TSPY_FAREIT.AGT
McAfee-GW-Edition	BackDoor-FJW
Emsisoft	Trojan.GenericKD.1178846 (B)
Jiangmin	None

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Antiy-AVL	Trojan/Win32.Tepfer
Kingsoft	Win32.PSWTroj.Undef.(kcloud)
Microsoft	PWS:Win32/Fareit
ViRobot	None
AhnLab-V3	Trojan/Win32.Tepfer
GData	Trojan.GenericKD.1178846
Commtouch	W32/Trojan.FNNT-6851
ByteHero	None
VBA32	TrojanPSW.Tepfer
Baidu-International	Trojan.Win32.InfoStealer.aA
ESET-NOD32	Win32/PSW.Fareit.A
Rising	None
Ikarus	Trojan-PWS.Tepfer
Fortinet	W32/Tepfer.PJNZ!tr.pws
AVG	PSW.Generic11.BUNZ
Panda	Trj/dtcontx.G

Πίνακας 5 : Αποτελέσματα σάρωσης από την υπηρεσία VirusTotal

Με βάση τις περιγραφές εντοπισμού του εκάστοτε antivirus, μπορούμε να συμπεράνουμε ότι το malware ανήκει στην κατηγορία Trojan χωρίς όμως να υπάρχει αναφορά για κάποιο συγκεκριμένο όνομα λογισμικού.

5.1.3 Εξαγωγή Συμβολοσειρών ASCII

Αναλύοντας τις συμβολοσειρές του εκτελέσιμου αρχείου, μπορούμε να εντοπίσουμε σημαντικά στοιχεία για την λειτουργία του malware. Πληροφορίες που αφορούν συνδέσμους διαδικτύου, ονόματα καταλόγων και μηνύματα οθόνης συνήθως αποθηκεύονται αυτούσια στο εκτελέσιμο αρχείο κατά την μεταγλώττιση. Στον ***Πίνακας 6***, περιέχονται μερικές από τις πιο σημαντικές συμβολοσειρές που υπάρχουν στο εκτελέσιμο αρχείο unknown.exe.

Πίνακας Συμβολοσειρών ASCII – Αρχείο : unknown.exe		
File Position	**Memory Position**	**ASCII String**
...	...	...
00000000F312	00000040F312	LoadCursorA
00000000F320	00000040F320	LoadCursorW
00000000F32C	00000040F32C	USER32.dll
00000000F33A	00000040F33A	InterlockedCompareExchange
00000000F358	00000040F358	FreeConsole
00000000F366	00000040F366	GetModuleHandleA
00000000F37A	00000040F37A	GetLastError
00000000F38A	00000040F38A	GetCurrentDirectoryW
00000000F3A2	00000040F3A2	GetEnvironmentVariableA
00000000F3BC	00000040F3BC	LoadLibraryW
00000000F3CC	00000040F3CC	LoadLibraryA
00000000F3DC	00000040F3DC	GetSystemInfo
00000000F3EC	00000040F3EC	SetLastError
00000000F3FC	00000040F3FC	GetLocalTime
00000000F40C	00000040F40C	GetFileType

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

00000000F41A	00000040F41A	WaitForSingleObject
00000000F430	00000040F430	GetCurrentThread
00000000F444	00000040F444	EnterCriticalSection
00000000F45A	00000040F45A	KERNEL32.dll
00000000F46A	00000040F46A	islower
00000000F474	00000040F474	printf
00000000F47C	00000040F47C	MSVCRT.dll
...	...	...
00000001BA36	00000041BA36	VS_VERSION_INFO
00000001BA92	00000041BA92	StringFileInfo
00000001BAB6	00000041BAB6	041904B0
00000001BACE	00000041BACE	CompanyName
00000001BB1A	00000041BB1A	FileDescription
00000001BB6D	00000041BB6D	TCP/IP
00000001BB82	00000041BB82	FileVersion
00000001BB9C	00000041BB9C	5.1.2600.0 (xpclient.010817-1148)
00000001BBE6	00000041BBE6	InternalName
00000001BC00	00000041BC00	nbtinfo.exe
00000001BC1E	00000041BC1E	LegalCopyright
00000001BC9E	00000041BC9E	OriginalFilename
00000001BCC0	00000041BCC0	nbtinfo.exe
00000001BCDE	00000041BCDE	ProductName
00000001BD52	00000041BD52	ProductVersion
00000001BD70	00000041BD70	5.1.2600.0
00000001BD8E	00000041BD8E	VarFileInfo
00000001BDAE	00000041BDAE	Translation
...	...	...

Πίνακας 6 : Συμβολοσειρές ASCII του εκτελέσιμου αρχείου

Όπως προαναφέραμε στην ενότητα 5.1.1, το αρχείο malware έχει προστατευτεί με χρήση του εργαλείου Armadillo. Ως αποτέλεσμα αυτής της διαδικασίας, οι παραπάνω συμβολοσειρές ASCII δεν προκύπτουν από το περιεχόμενο του κώδικα malware αλλά από το περιεχόμενο του κώδικα unpacking. Οι συναρτήσεις LoadLibrary (00000000F3BC, 00000000F3CC) και GetCurrentThread (00000000F430) εντοπίζονται πολύ συχνά σε packed και obfuscated malware διότι χρησιμοποιούνται για να φορτώσουν και να αποκτήσουν πρόσβαση σε άλλες βασικές συναρτήσεις [34]. Οι συμβολοσειρές που εντοπίζονται μεταξύ των διευθύνσεων 00000001BACE και 00000041BDAE μας αποκαλύπτουν στοιχεία για την έκδοση του αρχείου.

5.1.4 Στοιχεία Έκδοσης Αρχείου

Τα στοιχεία έκδοσης αρχείων αποθηκεύονται στο resource VERSIONINFO [35] των εκτελέσιμων αρχείων και χρησιμοποιούνται κυρίως από τις εφαρμογές και το λειτουργικό σύστημα για τη διευκόλυνση των διαδικασιών εγκατάστασης και αναβάθμισης. Τα στοιχεία αυτά, εκτός από την έκδοση του εκάστοτε αρχείου, περιέχουν και επιπρόσθετα πεδία όπως όνομα εταιρείας, όνομα προϊόντος, εσωτερικό όνομα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

αρχείου κ.ά. Στον ***Πίνακας 7***, περιλαμβάνονται τα πεδία που υπάρχουν στο resource VERSIONINFO του αρχείου unknown.exe.

Legal Copyright:	\xa9 \x41a\x43e\x440\x43f\x43e\x440\x430\x446\x438\x44f \x41c\x430\x439\x43a\x440\x43e\x441\x43e\x444\x442. \x412\x441\x435 \x43f\x440\x430\x432\x430 \x437\x430\x449\x438\x449\x435\x43d\x44b.
Internal Name:	nbtinfo.exe
File Version:	5.1.2600.0 (xpclient.010817-1148)
Company Name:	\x41a\x43e\x440\x43f\x43e\x440\x430\x446\x438\x44f \x41c\x430\x439\x43a\x440\x43e\x441\x43e\x444\x442
Product Name:	\x41e\x43f\x435\x440\x430\x446\x438\x43e\x43d\x43d\x430\x44f \x441\x438\x441\x442\x435\x43c\x430 Microsoft\xae Windows\xae
Product Version:	5.1.2600.0
File Description:	\x421\x432\x435\x434\x435\x43d\x438\x44f \x43e NetBios \x447\x435\x440\x435\x437 TCP/IP
Original Filename:	nbtinfo.exe
Translation:	0x0419 0x04b0

Πίνακας 7 : Πληροφορίες από το resource VERSIONINFO

Αναλύοντας τις παραπάνω πληροφορίες, παρατηρούμε ότι το εκτελέσιμο αρχείο του malware χρησιμοποιεί τα ίδια στοιχεία έκδοσης με το αρχείο nbtscan.exe του λειτουργικού συστήματος Windows XP. Το αρχείο αυτό, υπάρχει εγκατεστημένο στον φάκελο «C:\Windows\System32» και το FileVersion «5.1.2600.0 (xpclient.010817-1148)» παραπέμπει σε έκδοση αναβάθμισης Service Pack 3. Στο πεδίο Translation, η τιμή «0x0419» μας αποκαλύπτει ότι χρησιμοποιείται η ρώσικη γλώσσα για τους χαρακτήρες του resource VERSIONINFO σε Unicode character-set «0x04b0». Η τεχνική της κλωνοποίησης των στοιχείων έκδοσης των αρχείων, χρησιμοποιείται συχνά από τους δημιουργούς ιομορφικού λογισμικού και αποσκοπεί στην παραπλάνηση των χρηστών και στην αποφυγή εντοπισμού του malware από μηχανές antivirus.

5.1.5 Τομείς Εκτελέσιμου Αρχείου

Τα εκτελέσιμα αρχεία PE32 περιλαμβάνουν κατ' ελάχιστο δύο τμήματα (sections), ένα για τον εκτελέσιμο κώδικα και ένα για τα δεδομένα. Στα λειτουργικά συστήματα που βασίζονται σε πυρήνα Windows NT, τα εκτελέσιμα αρχεία μπορεί να διαθέτουν μέχρι εννέα διαφορετικά sections τα οποία είναι: .text, .bss, .rdata, .data, rsrc, .edata, idata, .pdata και .debug [36]. Στις περισσότερες εφαρμογές δε χρειάζονται όλα τα προαναφερθέντα τμήματα για τη λειτουργία των εκτελέσιμων αρχείων. Συνήθως, οι προγραμματιστές χρησιμοποιούν τα παρακάτω:

- **.text:** περιλαμβάνει τον εκτελέσιμο κώδικα του αρχείου.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

- **.rdata:** περιλαμβάνει δεδομένα που χρησιμοποιούνται μόνο για ανάγνωση κατά την εκτέλεση.
- **.data:** περιλαμβάνει όλες τις μεταβλητές που χρησιμοποιούνται από τον εκτελέσιμο κώδικα.
- **.rsrc:** περιλαμβάνει τους πόρους (resources) του αρχείου, όπως φωτογραφίες, εικονίδια, στοιχεία έκδοση αρχείου κ.ά.
- **.edata:** περιλαμβάνει τα ονόματα και τις διευθύνσεις των εξαγόμενων συναρτήσεων (στην περίπτωση που δεν υπάρχει αυτό το τμήμα στο εκτελέσιμο αρχείο οι πληροφορίες αυτές αποθηκεύονται στο section .rdata).
- **.idata:** περιλαμβάνει τα ονόματα και τις διευθύνσεις των εισαγόμενων συναρτήσεων (στην περίπτωση που δεν υπάρχει αυτό το τμήμα στο εκτελέσιμο αρχείο οι πληροφορίες αυτές αποθηκεύονται στο section .rdata).

Το λειτουργικό σύστημα εντοπίζει τα τμήματα των εκτελέσιμων αρχείων χρησιμοποιώντας τον πίνακα τμημάτων (section table). Ο πίνακας αυτός, βρίσκεται αμέσως μετά την επικεφαλίδα PE και περιλαμβάνει τα ονόματα των τμημάτων που περιέχονται στο εκτελέσιμο αρχείο καθώς και τις διευθύνσεις τους. Για κάθε τμήμα του αρχείου, αποθηκεύονται οι παρακάτω πληροφορίες στο section table:

- **Name1:** περιέχει το όνομα του τμήματος.
- **VirtualSize:** περιέχει το μέγεθος που καταλαμβάνει όταν μεταφορτωθεί στην μνήμη RAM.
- **VirtualAddress:** περιλαμβάνει την διεύθυνση που θα αποθηκευτεί το τμήμα στην μνήμη RAM.
- **SizeOfRawData:** περιέχει το μέγεθος του τμήματος στο εκτελέσιμο αρχείο.
- **PointerToRawData:** περιέχει τιμή (offset) η οποία ορίζει την απόσταση του τμήματος από την αρχή του αρχείου.
- **Characteristics:** περιέχει στοιχεία για τον τύπο των περιεχομένων του τμήματος.

Σύμφωνα με τα στοιχεία του ***Πίνακας 8***, το εκτελέσιμο αρχείο που αναλύουμε διαθέτει τέσσερα sections. Το section .text με μέγεθος 36864 bytes και βαθμό εντροπίας 6,94 το .rdata με μέγεθος 20480 bytes και βαθμό εντροπίας 7,23, το .data με μέγεθος 36864 bytes και βαθμό εντροπίας 4,7 και το .rsrc με μέγεθος 11728 bytes και βαθμό εντροπίας 4,02.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
.text	0x1000	0x94c2	0xa000	6.94081451196
.rdata	0xb000	0x45c8	0x5000	7.23677005432
.data	0x10000	0x85ec	0x9000	4.70854289745
.rsrc	0x19000	0x3000	0x2dd0	4.02896551233

Πίνακας 8 : Τομείς του εκτελέσιμου αρχείου

Κατά την ανάλυση πληροφοριών, χρησιμοποιούμε ως τιμή μονάδας το byte και τα αποτελέσματα τα εκφράζουμε ως bits per bytes. Αυτό έχει ως αποτέλεσμα, ο βαθμός εντροπίας ενός αρχείου να μπορεί να δεχτεί τιμές μεταξύ 0 και 8 [36]. Όσο μεγαλώνει η τιμή της εντροπίας ενός αρχείου, τόσο διαφοροποιούνται τα περιεχόμενα του αρχείου. Στην περίπτωσή μας, παρατηρούμε ότι ο βαθμός εντροπίας του section .text του κώδικα εκτέλεσης, είναι πολύ μεγάλος. Αυτό μας οδηγεί στο συμπέρασμα ότι χρησιμοποιείται κάποιος μηχανισμός προστασίας του εκτελέσιμου κώδικα, γεγονός το οποίο εξηγεί και τα αποτελέσματα του λογισμικού PEiD της ενότητας 5.1.1.

5.1.6 Εισαγόμενες Συναρτήσεις

Οι βιβλιοθήκες DLL (Dynamic Link Library) περιέχουν συναρτήσεις οι οποίες μπορούν να κληθούν δυναμικά από οποιοδήποτε εκτελέσιμο πρόγραμμα χωρίς να είναι ενσωματωμένες εξαρχής σε αυτό. Οι συναρτήσεις που διαθέτουν, χωρίζονται σε εσωτερικές και εξωτερικές. Οι εσωτερικές συναρτήσεις χρησιμοποιούνται μόνο για την εσωτερική λειτουργία των βιβλιοθηκών ενώ, οι εξωτερικές συναρτήσεις μπορούν να χρησιμοποιηθούν από οποιαδήποτε εφαρμογή. Τα ονόματα των βιβλιοθηκών DLL, ορίζονται στις δομές δεδομένων «Import Directory» και «Import Address Table» [37] οι οποίες περιέχονται στο section .rdata που αναφέραμε στην προηγούμενη ενότητα. Παρατηρώντας τα αποτελέσματα του ***Πίνακας 9***, το εκτελέσιμο αρχείο κατά τη λειτουργία του χρησιμοποιεί τις βιβλιοθήκες User32.dll, Kernel32.dll και Msvcrt.dll.

Library USER32.dll:	Library KERNEL32.dll:	Library MSVCRT.dll:
0x40b088 LoadCursorW	0x40b000 GetCurrentThread	0x40b040 __dllonexit
0x40b08c LoadCursorA	0x40b004 WaitForSingleObject	0x40b044 _controlfp
-	0x40b008 InterlockedCompareExchange	0x40b048 _onexit
-	0x40b00c FreeConsole	0x40b04c islower
-	0x40b010 GetModuleHandleA	0x40b050 printf
-	0x40b014 GetLastError	0x40b054 _exit
-	0x40b018 GetCurrentDirectoryW	0x40b058 _XcptFilter
-	0x40b01c GetEnvironmentVariableA	0x40b05c exit
-	0x40b020 LoadLibraryW	0x40b060 __p___initenv
-	0x40b024 LoadLibraryA	0x40b064 __getmainargs
-	0x40b028 GetSystemInfo	0x40b068 _initterm
-	0x40b02c SetLastError	0x40b06c __setusermatherr

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

-	0x40b030 GetLocalTime	0x40b070 _adjust_fdiv
-	0x40b034 GetFileType	0x40b074 __p__commode
-	0x40b038 EnterCriticalSection	0x40b078 __p__fmode
-	-	0x40b07c _set_app_type
-	-	0x40b080 _except_handler3

Πίνακας 9 : Εισαγόμενες συναρτήσεις εκτελέσιμου αρχείου

Από την κάθε βιβλιοθήκη DLL, καλούνται συγκεκριμένες συναρτήσεις. Αναλύοντας τις βιβλιοθήκες και τις συναρτήσεις που χρησιμοποιεί το εκτελέσιμο αρχείο, μπορούμε να αντλήσουμε σημαντικές πληροφορίες για τη συμπεριφορά του. Η βιβλιοθήκη Kernel32.dll είναι μια από τις βασικότερες βιβλιοθήκες των Windows και περιέχει σημαντικές συναρτήσεις που σχετίζονται με την πρόσβαση και τον χειρισμό μνήμης, αρχείων και πόρων υλικού. Η βιβλιοθήκη User32.dll περιέχει όλα τα στοιχεία που σχετίζονται με την διεπαφή του χρήστη, όπως κουμπιά και στοιχεία που χρησιμοποιούνται για τον έλεγχο και την ενεργοποίηση ενεργειών. Η βιβλιοθήκη Msvcrt.dll χρησιμοποιείται για την εκτέλεση εφαρμογών που έχουν δημιουργηθεί με χρήση του μεταγλωττιστή Microsoft Visual C και περιέχει βασικές συναρτήσεις για τη διαχείριση της μνήμης, τον χειρισμό αλφαριθμητικών κ.ά.

Σχετικά με τις καλούμενες συναρτήσεις και σύμφωνα με τις πληροφορίες που αντλήσαμε από τη διαδικτυακή βιβλιοθήκη της Microsoft MSDN [38]:

- Η συνάρτηση «GetCurrentDirectoryW» επιστρέφει τη διαδρομή του καταλόγου από τον οποίο εκτελείται το malware.
- Η συνάρτηση «GetSystemInfo» επιστρέφει στοιχεία για το λειτουργικό σύστημα και το υλικό του υπολογιστή.
- Η συνάρτηση «GetEnvironmentVariableA» αντλεί τιμές από μεταβλητές του περιβάλλοντος εργασίας του χρήστη.
- Η συνάρτηση «GetLocalTime» επιστρέφει την τοπική ημερομηνία και ώρα του συστήματος.
- Οι συναρτήσεις «GetModuleHandleA» και «LoadLibrary» χρησιμοποιούνται για την φόρτωση αρχείων DLL στην μνήμη.

5.1.7 Εξαγόμενες Συναρτήσεις

Όπως και στις εισαγόμενες συναρτήσεις, τα εκτελέσιμα αρχεία και οι βιβλιοθήκες DLL μπορούν να διαθέτουν και εξαγόμενες συναρτήσεις για να αλληλοεπιδρούν με άλλα προγράμματα. Τα ονόματα των εξαγόμενων συναρτήσεων, ορίζονται στη δομή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

δεδομένων «Export Directory» [37] η οποία βρίσκεται στο τμήμα .rdata του εκτελέσιμου αρχείου. Η εξαγωγή των συναρτήσεων μπορεί να γίνει με δύο διαφορετικούς τρόπους, με χρήση του ονόματος της συνάρτησης ή με χρήση ordinal. Ordinal είναι ένας αριθμός των 16 bit ο οποίος προσδιορίζει μοναδικά μια συνάρτηση σε κάποιο DLL ή εκτελέσιμο αρχείο.

Οι εισαγόμενες συναρτήσεις, λόγω του ότι καλούνται από βιβλιοθήκες του λειτουργικού συστήματος έχουν συγκεκριμένα ονόματα και μπορούμε εύκολα να αντλήσουμε πληροφορίες για αυτές από το διαδίκτυο. Σε αντίθεση με τα ονόματα των εισαγόμενων συναρτήσεων, τα ονόματα των εξαγόμενων συναρτήσεων καθορίζονται από τους ίδιους τους προγραμματιστές. Στην περίπτωση των malware, οι προγραμματιστές ορίζουν τυχαία ονόματα στις εξαγόμενες συναρτήσεις των εκτελέσιμων αρχείων με σκοπό να τα διαφοροποιήσουν και να τα προστατεύσουν από μηχανισμούς ανίχνευσης και αντιμετώπισης. Στην περίπτωσή μας, η τεχνική αυτή χρησιμοποιείται στο εκτελέσιμο αρχείο που αναλύουμε. Σύμφωνα με τα στοιχεία του ***Πίνακας 10***, το malware διαθέτει δύο εξαγόμενες συναρτήσεις με τα τυχαία ονόματα «dGNBuaXqBlMC» και «dqXdMimoyiwyxSfD».

Ordinal	Address	Name
2	0x4185b4	dGNBuaXqBlMC
3	0x4185b8	dqXdMimoyiwyxSfD

Πίνακας 10 : Εξαγόμενες συναρτήσεις εκτελέσιμου αρχείου

5.2 Δυναμική Ανάλυση

5.2.1 Αντικείμενα Συγχρονισμού Mutex

Σύμφωνα με το δίκτυο MSDN [38], το λειτουργικό σύστημα Microsoft Windows αποτρέπει την ταυτόχρονη προσπέλαση δύο ή περισσότερων διεργασιών σε κοινόχρηστους πόρους χρησιμοποιώντας mutexes. Τα mutexes είναι αντικείμενα συγχρονισμού τα οποία επιτρέπουν την αποκλειστική πρόσβαση μιας διεργασίας σε έναν κοινόχρηστο πόρο. Αν κάποια διεργασία αποκτήσει μια τιμή mutex και την ίδια χρονική στιγμή μια δεύτερη διεργασία αιτηθεί την ίδια τιμή, τότε η δεύτερη διεργασία αναστέλλεται έως ότου η πρώτη ελευθερώσει την τιμή mutex που κατέχει.

Υπάρχουν δύο τύποι mutexes, τα τοπικά mutexes (local) τα οποία δε διαθέτουν κάποιο συγκεκριμένο όνομα και αποδίδονται αυτόματα από το λειτουργικό σύστημα και τα ονομαστικά mutexes, τα οποία ορίζονται από τους προγραμματιστές και αφορούν

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

αποκλειστικά στις εφαρμογές τους. Τα local χρησιμοποιούνται κατά την εσωτερική λειτουργία των διεργασιών του λειτουργικού συστήματος ενώ τα ονομαστικά, δημιουργούνται από τους προγραμματιστές για τον συγχρονισμό των διεργασιών που εκτελούνται από τις εφαρμογές τους. Τα mutexes χρησιμοποιούνται συχνά από τα malware για να διασφαλίσουν ότι δεν εκτελούνται παραπάνω από μια φορά στο ίδιο λειτουργικό σύστημα. Η χρήση τους, διευκολύνει σε μεγάλο βαθμό τους αναλυτές στον εντοπισμό και την κατηγοριοποίηση των malware.

Στην περίπτωσή μας, η εκτέλεση του malware στο περιβάλλον ανάλυσης δημιουργεί μόνο τοπικά mutexes (***Πίνακας 11***). Τα mutexes αυτά, δημιουργούνται αυτόματα από το λειτουργικό σύστημα κατά την εκκίνηση εσωτερικών διεργασιών οι οποίες προκαλούνται κατά την εκτέλεση του κώδικα του malware.

	Mutexes
1	Local_!MSFTHISTORY!_
2	Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
3	Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
4	Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
5	Local\!IETld!Mutex
6	Local\c:!users!user!appdata!roaming!microsoft!windows!ietldcache!
7	Local\WininetStartupMutex
8	Local\WininetConnectionMutex
9	Local\WininetProxyRegistryMutex
10	Local\ZonesCounterMutex
11	Local\ZoneAttributeCacheCounterMutex
12	Local\ZonesCacheCounterMutex
13	Local\ZonesLockedCacheCounterMutex

Πίνακας 11 : Λίστα αντικειμένων mutex

Παρατηρώντας τα ονόματα των mutexes του πίνακα 5.2.1.1, συμπεραίνουμε ότι το malware έχει προσπελάσει δεδομένα τα οποία αφορούν στον φυλλομετρητή Internet Explorer. Συγκεκριμένα, προσπέλασε στοιχεία που αφορούν στα αρχεία cookies (3), στο ιστορικό πλοήγησης (1,4), στην προσωρινή μνήμη αποθήκευσης (2,6), στον τρόπο σύνδεσης (7-9) και στις ρυθμίσεις ασφάλειας και πρόσβασης στο διαδίκτυο (10-13).

5.2.2 Κλειδιά Registry

Η registry των Windows χρησιμοποιείται από το λειτουργικό σύστημα και τις εφαρμογές για την αποθήκευση διάφορων ρυθμίσεων παραμετροποίησης (configuration information). Όπως και το σύστημα αρχείων, έτσι και η ανάλυση του registry μπορεί να μας δώσει πολύ σημαντικές πληροφορίες για τη λειτουργία και την συμπεριφορά των

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

malware. Στις προηγούμενες εκδόσεις των Windows, οι παράμετροι ρυθμίσεων αποθηκεύονταν σε αρχεία ini. Πλέον, στις σύγχρονες εκδόσεις, χρησιμοποιείται η ιεραρχική βάση δεδομένων registry, η οποία προσφέρει κεντρικοποιημένη αποθήκευση ρυθμίσεων, αυξημένη ταχύτητα προσπέλασης και ομοιομορφία.

Τα malware συνήθως χρησιμοποιούν την registry για να αποθηκεύσουν παραμέτρους ρυθμίσεων που σχετίζονται με τη λειτουργία τους, για να εξασφαλίσουν την εκτέλεσή τους κατά την εκκίνηση του υπολογιστή και για να αντλήσουν στοιχεία που αφορούν στο λειτουργικό σύστημα και στις εγκατεστημένες εφαρμογές [34].

Τα κύρια κλειδιά του registry είναι:

- **HKEY_LOCAL_MACHINE (HKLM):** Αποθηκεύονται πληροφορίες που αφορούν στο λειτουργικό σύστημα.
- **HKEY_CURRENT_USER (HKCU):** Αποθηκεύονται πληροφορίες που αφορούν στο λογαριασμό του χρήστη.
- **HKEY_CLASSES_ROOT:** Αποθηκεύονται παράμετροι ορισμού τύπων (types definition).
- **HKEY_CURRENT_CONFIG:** Αποθηκεύονται οι ρυθμίσεις του υλικού.
- **HKEY_USERS:** Αποθηκεύονται βασικοί παράμετροι λειτουργίας των προφίλ των προκαθορισμένων χρηστών, των νέων χρηστών και των υφιστάμενων χρηστών του συστήματος.

Για την προσπέλαση και τη δημιουργία νέων κλειδιών στο registry, τα malware χρησιμοποιούν συνήθως τα κύρια κλειδιά HKLM και HKCU. Η πρόσβαση στην registry πραγματοποιείται με την χρήση των παρακάτω κλήσεων συστήματος (system calls):

- **RegOpenKeyEx:** Επιτρέπει την προσπέλαση και την εγγραφή πληροφοριών από και προς συγκεκριμένα κλειδιά.
- **RegSetValueEx:** Δημιουργεί καινούργια κλειδιά και θέτει παραμέτρους σε αυτά.
- **RegQueryValueEx:** Επιστρέφει τις τιμές ενός συγκεκριμένου κλειδιού από το registry.

Στην περίπτωσή μας, το malware χρησιμοποιεί την κλήση «RegSetValueEx» για να δημιουργήσει δύο καινούργια κλειδιά (***Πίνακας 12***). Το πρώτο κλειδί έχει όνομα HWID και αποθηκεύεται στη διαδρομή «HKCU\Software\WinRAR». Η τιμή που

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ορίζεται στο κλειδί HWID είναι τυχαία, και δημιουργείται κατά την πρώτη εκτέλεση του malware. Το δεύτερο κλειδί έχει όνομα «gacvxm» και δημιουργείται στο υπο-κλειδί «HKCU\Software\Microsoft\Windows\CurrentVersion\Run». Η τιμή που ορίζεται σε αυτό το κλειδί παραπέμπει στην εκτέλεση της εντολής συστήματος «regsvr32.exe /s "C:\ProgramData\gacvxm.dat"».

Εγγραφές Registry		
Call	**Key**	**Value**
RegSetValueEx	HKCU\Software\WinRAR\HWID	vcvkdhfsd
RegSetValueEx	HKCU\Software\Microsoft\ Windows\CurrentVersion\Run\gacvxm	regsvr32.exe /s "C:\ProgramData\gacvxm.dat"

Πίνακας 12 : Κλειδιά registry για την αυτόματη εκκίνηση του malware

Τα κλειδιά που τοποθετούνται στο υπο-κλειδί «HKCU\Software\Microsoft\ Windows\CurrentVersion\Run» περιέχουν τιμές οι οποίες παραπέμπουν σε αρχεία τα οποία εκτελούνται κατά την εκκίνηση του συστήματος. Η εντολή «regsvr32.exe» ανήκει στο λειτουργικό σύστημα και χρησιμοποιείται για την καταχώρηση στοιχείων ελέγχου OLE όπως, αρχεία DLL ή OCX (ActiveX Controls). Η χρήση αυτής της εντολής, προκαλεί την εκτέλεση του malware κατά την εκκίνηση του λειτουργικού συστήματος. Η παράμετρος «/s» ενεργοποιεί την αθόρυβη καταχώρηση του αρχείου DLL αποκρύπτοντας οτιδήποτε μηνύματα εμφανίζονται στην οθόνη.

Εκτός από τη δημιουργία νέων κλειδιών, το malware κατά την εκτέλεσή του προσπαθεί να προσπελάσει δεδομένα από διάφορα κλειδιά του registry χρησιμοποιώντας την κλήση συστήματος «RegGueryValueEx». Παρατηρώντας τα αποτελέσματα της ανάλυσης (παράρτημα 2) διαπιστώνουμε ότι αντλεί πληροφορίες που σχετίζονται με εφαρμογές οι οποίες αποθηκεύουν στοιχεία πρόσβασης για δικτυακές υπηρεσίες FTP, HTTP και SSH.

5.2.3 Προσπέλαση Συστήματος Αρχείων

Τα περισσότερα malware κατά την εκτέλεσή τους, χρησιμοποιούν το σύστημα αρχείων για την ανάγνωση και την αποθήκευση δεδομένων. Σε ορισμένες περιπτώσεις, έχουν εντοπιστεί malware τα οποία λειτουργούν αποκλειστικά σε επίπεδο μνήμης χωρίς να αλληλοεπιδρούν με το σύστημα αρχείων. Η πρώτη επαφή των malware με το σύστημα αρχείων πραγματοποιείται κατά την αρχική τους εκτέλεση όπου, το λειτουργικό σύστημα αναλαμβάνει τη μεταφορά των δεδομένων τους από το σκληρό δίσκο στη μνήμη. Στη

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

συνέχεια, για τη δημιουργία νέων αρχείων ή την προσπέλαση υφιστάμενων αρχείων χρησιμοποιούνται συγκεκριμένες κλήσεις συστήματος. Οι βασικότερες από αυτές είναι:

- **NtOpenFile:** Ανοίγει ένα αρχείο, κατάλογο, ή συσκευή του συστήματος για ανάγνωση ή εγγραφή.
- **NtCreateFile:** Δημιουργεί ένα καινούργιο αρχείο ή κατάλογο.
- **NtReadFile:** Διαβάζει τα περιεχόμενα από ένα ανοιχτό αρχείο.

Σύμφωνα με τα αποτελέσματα της ανάλυσης (παράρτημα 3), το malware που αναλύουμε προσπαθεί να προσπελάσει διάφορα αρχεία και καταλόγους σε επίπεδο προφίλ χρήστη αλλά και σε επίπεδο συστήματος. Τα ονόματα των καταλόγων και των αρχείων που στοχοποιεί, μας οδηγούν στο συμπέρασμα ότι αποσκοπεί στην υποκλοπή στοιχείων πρόσβασης από γνωστές εμπορικές και δωρεάν εφαρμογές. Επιπροσθέτως, η αναζήτηση αρχείων σε επίπεδο προφίλ χρήστη υποδεικνύει ότι το εν λόγω malware μπορεί να λειτουργήσει και σε λογαριασμό χρήστη με περιορισμένα δικαιώματα (limited user). Τα αποτελέσματα της ανάλυσης αρχείων, μας αποκαλύπτουν περισσότερα στοιχεία για τις εφαρμογές που στοχοποιεί το malware από ότι τα αποτελέσματα της ανάλυσης του registry της ενότητας 5.2.2.

5.2.4 Δικτυακή Κίνηση

Οι διευθύνσεις IP και τα domain names που χρησιμοποιεί κάποιο malware, μπορούν να μας οδηγήσουν στην ταυτότητα του επιτιθέμενου αλλά και στο σημείο έναρξης της επίθεσης. Τα πρωτόκολλα επικοινωνίας αποκαλύπτουν τον τρόπο επικοινωνίας του malware με τον επιτιθέμενο και τις τεχνικές που χρησιμοποιούνται για την εξάπλωσή του μέσω του δικτύου. Η ανάλυση του περιεχομένου της δικτυακής κίνησης, προσφέρει στοιχεία για τις πληροφορίες που μεταφέρονται από το malware προς τον επιτιθέμενο και μας βοηθά στην περαιτέρω κατανόηση της λειτουργίας του malware [39].

Τα περισσότερα malware προκειμένου να αυξήσουν τη βιωσιμότητα και την ανθεκτικότητά τους, χρησιμοποιούν domain names για τη λειτουργία τους. Με αυτόν τον τρόπο είναι πολύ εύκολο να προστατέψουν και να αλλάξουν τις IP διευθύνσεις που χρησιμοποιούν, ενημερώνοντας απλά εγγραφές DNS. Στην περίπτωσή μας, το malware που αναλύουμε δεν χρησιμοποιεί κάποιο domain name. Κατά την εκτέλεσή του, επικοινωνεί με δύο διαφορετικούς εξυπηρετητές Web (***Πίνακας 13***).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

URL	Data
http://195.137.188.59/padmin/gate.php	POST /padmin/gate.php HTTP/1.0 Host: 195.137.188.59 Accept: */* Accept-Encoding: identity, *;q=0 Content-Length: 4901 Connection: close Content-Type: application/octet-stream Content-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
http://195.137.188.52/crypted_inst_6.exe	GET /crypted_inst_6.exe HTTP/1.0 Host: 195.137.188.52 Accept: */* Accept-Encoding: identity, *;q=0 Connection: close User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)

Πίνακας 13: HTTP συνδέσεις του malware

Η σύνδεση και στους δύο εξυπηρετητές γίνεται με τη χρήση του πρωτοκόλλου HTTP. Σε πρώτη φάση καλείται το script «gate.php» το οποίο βρίσκεται στη διαδρομή «http://195.137.188.59/padmin/gate.php». Με χρήση της εντολής HTTP «POST», το malware αποστέλλει στον εξυπηρετητή του επιτιθέμενου όλα τα δεδομένα που έχει αντλήσει από το σύστημα σε κρυπτογραφημένη μορφή. Εφόσον ολοκληρωθεί η μεταφορά των δεδομένων, συνδέεται στον δεύτερο εξυπηρετητή «195.137.188.52» και μεταφορτώνει το εκτελέσιμο αρχείο «crypted_inst_6.exe» το οποίο στη συνέχεια εκτελεί στο σύστημα. Για να αναλύσουμε τη λειτουργία του αρχείου «crypted_inst_6.exe», θα πρέπει να εφαρμόσουμε ξανά τη διαδικασία που περιγράψαμε στην ενότητα 3.4. Ωστόσο, η ανάλυση του εν λόγω αρχείου δεν περιλαμβάνεται στην παρούσα εργασία.

Με χρήση του εργαλείου whois, εντοπίσαμε ότι οι IP διευθύνσεις που χρησιμοποιεί το malware ανήκουν σε εξυπηρετητές του Πανεπιστημίου Al-Quds το οποίο βρίσκεται στην Παλαιστίνη (παράρτημα 4). Οι εξυπηρετητές αυτοί, πιθανών να παραβιάστηκαν από τους επιτιθέμενους για να αξιοποιηθούν προς όφελός τους. Στο ***Σχήμα 10***, απεικονίζονται τα δημοσιευμένα αρχεία του εξυπηρετητή Web «195.137.188.59».

Αρχεία Εξυπηρετητή Web

```
Index of /padmin
[ICO]  Name   Last modified  Size   Description
[DIR]  Parent Directory             -
[TXT]  404.html       17-May-2011 19:51     348
[ ]    admin.php      09-Jun-2012 08:39     49K
[ ]    config.php     09-Aug-2013 10:05     1.2K
[ ]    gate.php       09-Jun-2012 09:05     4.7K
[DIR]  includes/      18-Jun-2013 09:24     -
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
[ ]    redirect.php   18-Apr-2012 12:47     3.6K
[TXT]  robots.txt     24-May-2011 05:03     28
[ ]    setup.php      09-Jun-2012 09:07     5.0K
[DIR]  temp/   07-Dec-2013 08:22     -
Apache/2.2.16 (Debian) Server at 195.137.188.59 Port 81
```

Σχήμα 10 : Περιεχόμενα εξυπηρετητή C&C

Εκτός από το script «gate.php» το οποίο χρησιμοποιείται για την αποστολή δεδομένων και γενικά για την επικοινωνία του malware με την κονσόλα διαχείρισης του επιτιθέμενου (C&C), στον εξυπηρετητή υπάρχουν και επιπλέον αρχεία τύπου php τα οποία χρησιμοποιούνται για περαιτέρω λειτουργίες. Ως παράδειγμα μπορούμε να αναφέρουμε τα αρχεία «admin.php» και «setup.php». Σύμφωνα με τις εικόνες του παραρτήματος Π.1.4 και Π.1.5, το αρχείο «admin.php» χρησιμοποιείται για την πρόσβαση στην κονσόλα διαχείρισης του malware και το αρχείο «setup.php» χρησιμοποιείται για την εγκατάστασή της στον Web server.

Η αναζήτηση πληροφοριών στα εκτεθειμένα αρχεία του εξυπηρετητή Web θα μπορούσε να μας αποκαλύψει σημαντικά στοιχεία για την ταυτότητα του malware. Εκτός από τα scripts php τα οποία εκτελούνται στον εξυπηρετητή, τα υπόλοιπα αρχεία τύπου text και εικόνων μπορούμε να τα μεταφορτώσουμε και να τα αναλύσουμε τοπικά. Από τα περιεχόμενα του αρχείου «style_full.css» (***Σχήμα 11***) και από το «favicon.ico» (παράρτημα Π.1.4) συμπεραίνουμε ότι το malware που αναλύουμε ονομάζεται Pony [40]. Το εν λόγω malware, χρησιμοποιείται κυρίως για την υποκλοπή κωδικών πρόσβασης από διάφορες εμπορικές και open source εφαρμογές για λειτουργικά συστήματα Microsoft Windows (παράρτημα 5).

Περιεχόμενα Αρχείου style_full.css

```
...
.pony_hdr_text{
        float:right;
        padding:5px 0px 30px 40px;
        font:bold 11px/16px Arial, Helvetica, sans-serif;
        color:#C89601;
        background-color:inherit;
        background:url(images/pony_icon.png) 0px 0px no-repeat;
}
...
```

Σχήμα 11 : Πηγαίος κώδικας αρχείου style_full.css

Σύμφωνα με τα στοιχεία που συλλέξαμε από πηγές του διαδικτύου [40] [41] [42], το malware αυτό πρωτοεμφανίστηκε τον Ιούνιο του 2013 και εικάζεται ότι έχει χρησιμοποιηθεί για την υποκλοπή κωδικών πρόσβασης για περίπου 2 εκατομμύρια ιστοσελίδες και υπηρεσίες διαδικτύου.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

5.3 Στατική Ανάλυση

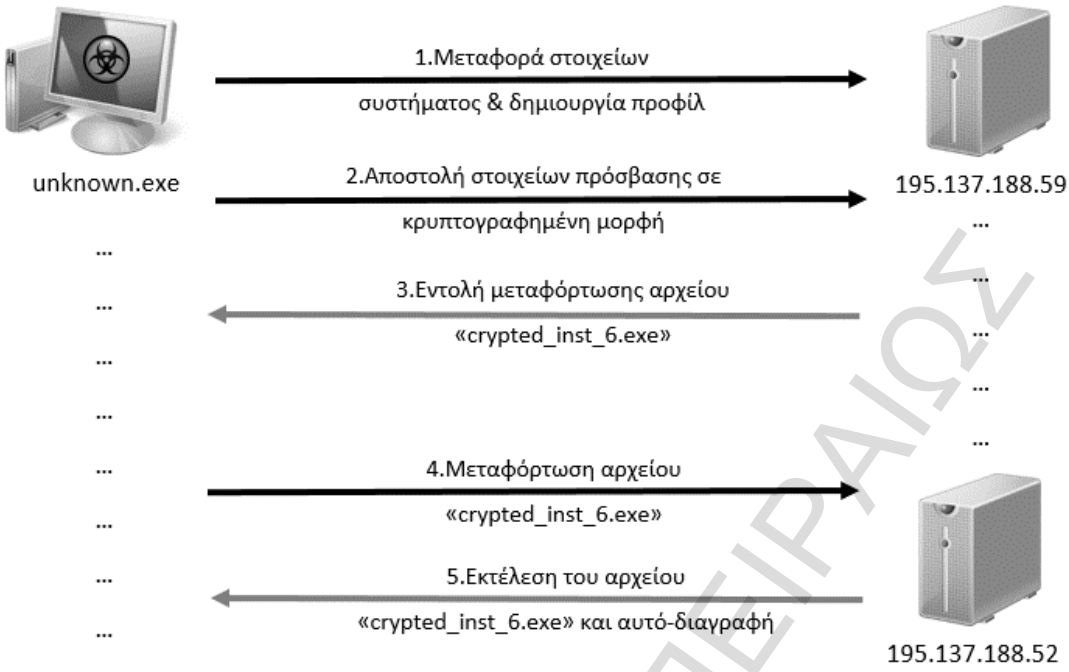
Η στατική ανάλυση περιλαμβάνει την ελεγχόμενη εξέταση του κώδικα μηχανής των εκτελέσιμων αρχείων. Αποτελεί μια χρονοβόρα και πολύπλοκη διαδικασία η οποία δεν μπορεί να αυτοματοποιηθεί με την χρήση ενός ή πολλών εργαλείων. Στη δική μας μελέτη περίπτωσης, δεν κρίνεται απαραίτητη η εφαρμογή στατικής ανάλυσης. Τα αποτελέσματα της αυτοματοποιημένης επιφανειακής και δυναμικής ανάλυσης που παρουσιάζονται στην επόμενη ενότητα, συνθέτουν μια ολοκληρωμένη εικόνα για τη λειτουργία και τη συμπεριφορά του malware που αναλύουμε. Η εφαρμογή στατικής ανάλυσης στο εκτελέσιμο αρχείο και στα dropped files του malware με την χρήση κατάλληλων εργαλείων debugging και disassembling δεν αποτελεί μέρος αυτής της εργαστηριακής υλοποίησης.

5.4 Αποτελέσματα Μελέτης Περίπτωσης

Τα αποτελέσματα της εργαστηριακής λύσης με χρήση του λογισμικού Cuckoo, μας έχουν αποκαλύψει πολύ σημαντικές πληροφορίες για το malware σε πολύ μικρό χρονικό διάστημα. Παρατηρούμε ότι, κατά την αρχική του εκτέλεση, προσπαθεί να αντλήσει αποθηκευμένα στοιχεία πρόσβασης και πιστοποιητικά ασφάλειας από το σύστημα και το προφίλ του συνδεδεμένου χρήστη. Εφόσον ολοκληρωθεί η διαδικασία συλλογής, κρυπτογραφεί τα στοιχεία αυτά και τα αποστέλλει στον εξυπηρετητή του επιτιθέμενου, με χρήση του πρωτοκόλλου HTTP.

Εκτός από τα υποκλαπέντα στοιχεία, στον ίδιο εξυπηρετητή αποστέλλονται πληροφορίες που αφορούν στο σύστημα καθώς επίσης και στο μοναδικό αναγνωριστικό (ID) του malware. Βάση αυτού του αναγνωριστικού, ο επιτιθέμενος μπορεί να διαχειριστεί ξεχωριστά τις πληροφορίες που συλλέγει από το κάθε μολυσμένο σύστημα. Κατόπιν, το malware χρησιμοποιεί έναν δεύτερο εξυπηρετητή από τον οποίο μεταφορτώνει και εκτελεί ένα άλλο malware με όνομα αρχείου «crypted_inst_6.exe». Με την εκτέλεση αυτού του αρχείου, το αρχικό malware «unknown.exe» αυτοδιαγράφεται από το σύστημα και τερματίζεται η λειτουργία του (***Σχήμα 12***).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ



Σχήμα 12 : Επικοινωνία του malware με τον εξυπηρετητή C&C

Η εκτέλεση του «crypted_inst_6.exe» δημιουργεί στον κατάλογο του συστήματος «C:\ProgramData» ένα αρχείο DLL με τυχαίο όνομα και επέκταση «.dat». Το αρχείο αυτό περιέχεται κρυπτογραφημένο στο payload του malware. Στη συνέχεια, εκτελείται ο κώδικας του DLL, αυτοδιαγράφεται το αρχείο «crypted_inst_6.exe» και τερματίζεται η λειτουργία του.

Το αρχείο DLL εκτελείται συνεχώς στο σύστημα χωρίς να γίνεται αντιληπτό από τον χρήστη. Ελέγχει για νέα στοιχεία πρόσβασης και μόλις τα εντοπίσει τα αποστέλλει με κρυπτογραφημένο τρόπο στον εξυπηρετητή C&C του επιτιθέμενου. Για να διασφαλίσει την εκτέλεσή του κατά την εκκίνηση του συστήματος δημιουργεί ένα κλειδί στη registry. Σε κάθε κύκλο εκτέλεσης ελέγχει την ύπαρξη του κλειδιού εκκίνησης και του αρχείου «.dat» και σε περίπτωση που δεν τα εντοπίσει, τα επαναδημιουργεί.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Κεφάλαιο 6ο

Επέκταση Συστήματος

Στο κεφάλαιο αυτό, βασιζόμενοι στη μεθοδολογία ανάλυσης και στα αποτελέσματα της μελέτης περίπτωσης, υλοποιήσαμε νέες κλάσεις υπογραφών ανίχνευσης και επεξεργασίας. Για τη γραφική απεικόνιση της δικτυακής κίνησης, τον εντοπισμό κακόβουλων εξυπηρετητών και την κατηγοριοποίηση των malware, ενσωματώσαμε στο λογισμικό Cuckoo το λογισμικό Malcom. Στη συνέχεια, για την οπτικοποίηση της διαδικασίας ανάλυσης και των αποτελεσμάτων αυτής, χρησιμοποιήσαμε το λογισμικό Maltego [43] σε συνδυασμό με το πακέτο μετασχηματισμών (transformations) cuckooforcanari [44]. Τέλος, η επέκταση του συστήματος ολοκληρώθηκε με την υλοποίηση μηχανισμού πολυεπίπεδης ανάλυσης ο οποίος, αποσκοπεί στην αυτοματοποιημένη ανάλυση των dropped files των malware.

6.1 Κλάσεις Υπογραφών Ανίχνευσης

Όπως αναφέραμε στην ενότητα 4.1, το λογισμικό Cuckoo μας επιτρέπει να υλοποιήσουμε κλάσεις υπογραφών ανίχνευσης σε γλώσσα προγραμματισμού Python και να τις εφαρμόσουμε στα αποτελέσματα της διαδικασίας ανάλυσης. Με αυτόν τον τρόπο, χρησιμοποιώντας κατάλληλα πρότυπα μπορούμε να κατηγοριοποιήσουμε τα αρχεία που αναλύουμε και να εντοπίσουμε εύκολα και γρήγορα κακόβουλες ενέργειες. Κατά τη δημιουργία κλάσεων υπογραφών ανίχνευσης θα πρέπει να ορίσουμε τις παρακάτω βασικές παραμέτρους:

- **Name:** Ορίζεται το όνομα της κλάσης ανίχνευσης.
- **Description:** Ορίζεται το κείμενο που θα επιστρέψει η κλάση ως αποτέλεσμα.
- **Severity:** Υποδηλώνει τον βαθμό επικινδυνότητας της ενέργειας που ανιχνεύεται και μπορεί να πάρει τιμές από ένα έως τρία: 1 - χαμηλός, 2 - μεσαίος και 3 – υψηλός.
- **Categories:** Ορίζεται η κατηγορία στην οποία ανήκει η συγκεκριμένη υπογραφή (banker, injection, anti-vm, infostealer κτλ.).
- **Authors:** Ορίζεται το όνομα των δημιουργών της υπογραφής.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

- **Minimum:** Ορίζεται η μικρότερη δυνατή έκδοση του Cuckoo στην οποία μπορεί να λειτουργήσει η υπογραφή.

Τα αρχεία του πηγαίου κώδικα των υπογραφών ανίχνευσης, θα πρέπει να τοποθετηθούν στον φάκελο «cuckoo/modules/signatures» ούτως ώστε να ενεργοποιηθούν αυτόματα από το Cuckoo.

Κατά τη μελέτη περίπτωσης, παρατηρήσαμε ότι το malware που αναλύουμε προσπαθεί να υποκλέψει πιστοποιητικά ασφάλειας από το λειτουργικό σύστημα προσπελαύνοντας προκαθορισμένο φάκελο στο προφίλ του χρήστη. Για τον εντοπισμό αυτής της κακόβουλης ενέργειας από το Cuckoo, υλοποιήσαμε την κλάση υπογραφής CERTSStealer (***Σχήμα 13***).

Πηγαίος κώδικας αρχείου infostealer_certs.py
(cuckoo/modules/signatures/infostealer_certs.py)

```
1  from lib.cuckoo.common.abstracts import Signature
2
3  class CERTSStealer(Signature):
4      name = “infostealer_certs”
5      description = “Harvests certificates from local client softwares”
6      severity = 3
7      categories = [“infostealer”]
8      authors = [“temsec”]
9      minimum = “0.1”
10
11     def run(self):
12         indicators = [
13             “.*\\\\Microsoft\\\\SystemCertificates\\\\My\\\\.*”
14         ]
15
16         for indicator in indicators:
17             if self.check_file(pattern=indicator, regex=True):
18                 return True
19
20         return False
21
```

Σχήμα 13 : Πηγαίος κώδικας αρχείου infostealer_certs.py

Η κλάση υπογραφής ανίχνευσης SSHStealer (***Σχήμα 14***) με βαθμό επικινδυνότητας 3, αποσκοπεί στον εντοπισμό ενεργειών υποκλοπής κωδικών πρόσβασης από γνωστούς SSH clients. Συγκεκριμένα, οι clients που υποστηρίζει είναι οι SecureCRT, NetDrive, ExpanDrive και NetSarang.

Πηγαίος κώδικας αρχείου infostealer_ssh.py
(cuckoo/modules/signatures/infostealer_ssh.py)

```
1  from lib.cuckoo.common.abstracts import Signature
2
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
3  class SSHStealer(Signature):
4      name = "infostealer_ssh"
5      description = "Harvests credentials from local SSH clients"
6      severity = 3
7      categories = ["infostealer"]
8      authors = ["temsec"]
9      minimum = "0.1"
10
11     def run(self):
12         indicators = [
13             ".*\\\\VanDyke\\\\Config\\\\Sessions.*",
14             ".*\\\\NetDrive\\\\.*",
15             ".*\\\\ExpanDrive\\\\.*",
16             ".*\\\\NetSarang\\\\.*"
17         ]
18
19         for indicator in indicators:
20             if self.check_file(pattern=indicator, regex=True):
21                 return True
22
23         return False
24
```

Σχήμα 14: Πηγαίος κώδικας αρχείου infostealer_ssh.py

Η κλάση υπογραφής ανίχνευσης MAILStrealer (***Σχήμα 15***) έχει βαθμό επικινδυνότητας 3 και ελέγχει εάν το malware προσπέλασε φάκελους του συστήματος αρχείων οι οποίοι σχετίζονται με τα προγράμματα διαχείρισης ηλεκτρονικής αλληλογραφίας BatMail και Pocomail.

Πηγαίος κώδικας αρχείου infostealer_email.py
(cuckoo/modules/signatures/infostealer_email.py)

```
1  from lib.cuckoo.common.abstracts import Signature
2
3  class MAILStealer(Signature):
4      name = "infostealer_email"
5      description = "Harvests credentials from local Email clients"
6      severity = 3
7      categories = ["infostealer"]
8      authors = ["temsec"]
9      minimum = "0.1"
10
11     def run(self):
12         indicators = [
13             ".*\\\\BatMail\\\\.*",
14             ".*\\\\Pocomail\\\\.*"
15         ]
16
17         for indicator in indicators:
18             if self.check_file(pattern=indicator, regex=True):
19                 return True
20
21         return False
22
```

Σχήμα 15 : Πηγαίος κώδικας αρχείου infostealer_email.py

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Εκτός από την υλοποίηση των παραπάνω κλάσεων, βελτιώσαμε τις υφιστάμενες κλάσεις εντοπισμού υπογραφών infostealer_browser και infostealer_ftp (παράρτημα Π.6.1 & Π.6.2). Η κλάση infostealer_browser εντοπίζει ενέργειες υποκλοπής κωδικών πρόσβασης από γνωστούς φυλλομετρητές και αντίστοιχα, η κλάση infostealer_ftp από γνωστούς ftp clients. Η απεικόνιση των αποτελεσμάτων στο Web περιβάλλον του Cuckoo (παράρτημα Π.1.6) πραγματοποιείται με αυτόματο τρόπο διότι οι επιστρεφόμενες τιμές της κλάσης που χρησιμοποιούμε είναι τύπου signature.

6.2 Κλάσεις Επεξεργασίας

Οι κλάσεις επεξεργασίας του Cuckoo συλλέγουν όλα τα στοιχεία, τα οποία προκύπτουν από την εκτέλεση του malware όπως, διαδικασίες (processes), πρόσβαση σε σύστημα αρχείων, πρόσβαση στη registry, κλήσεις API. Οι πληροφορίες αυτές στη συνέχεια προωθούνται στις ενεργοποιημένες κλάσεις ανίχνευσης, οι οποίες με τη σειρά τους τις αναλύουν, με στόχο να εντοπίσουν κακόβουλη ή ύποπτη συμπεριφορά.

Στα πλαίσια της επέκτασης του συστήματος και προκειμένου να επεξεργαστούμε τα αποτελέσματα ανάλυσης που αφορούν στη δικτυακή κίνηση που προκαλείται από το malware, υλοποιήσαμε την κλάση επεξεργασίας infogather (παράρτημα Π.6.3). Η κλάση αυτή, επεξεργάζεται το αρχείο PCAP της τρέχουσας ανάλυσης για να εντοπίσει τις IP διευθύνσεις και τις συνδέσεις HTTP που χρησιμοποιούνται κατά την εκτέλεση του malware.

Για κάθε IP διεύθυνση, συλλέγει διάφορες πληροφορίες με χρήση της διαδικτυακής υπηρεσίας whois μέσω της βιβλιοθήκης bulkwhois [45] και στη συνέχεια, τις καταχωρεί στη δομή δεδομένων της τρέχουσας ανάλυσης. Επιπροσθέτως, για τον προσδιορισμό της ταυτότητας του malware, εντοπίζει URL τα οποία σχετίζονται με την κονσόλα διαχείρισης C&C. Συγκεκριμένα, αναζητούνται προκαθορισμένα πρότυπα αρχείων ή καταλόγων σε όλους τους εξυπηρετητές Web με τους οποίους επικοινώνησε το malware ενεργοποιώντας συνδέσεις HTTP. Για τον αυτόματο εντοπισμό του Pony malware kit, ορίσαμε ως πρότυπο αναγνώρισης το URL «http://<ip-address>/includes/password_modules.php». Το εν λόγω URL, αποτελεί μέρος της κονσόλας διαχείρισης του συγκεκριμένου malware (παράρτημα Π.5.2).

Πηγαίος κώδικας αρχείου infogather.py
(cuckoo/modules/processing/infogather.py)

```
1  ...
```


ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
2         # Whois Module
3         whoisdata = []
4
5         try:
6             if self.unique_hosts:
7                     for ipz in self.unique_hosts:
8                         whoisdata.append(ipz)
9                         bulk_whois = BulkWhoisShadowserver()
10                        records = bulk_whois.lookup_ips([ipz])
11
12                        for record in records:
13                            whoisdata.append([records[record]["ip"],
14 records[record]["asn"], records[record]["bgp_prefix"]
15 ,records[record]["as_name"], records[record]["cc"],
16 records[record]["register"], records[record]["org_name"]])
17
18        except  ValueError as e:
19            raise CuckooProcessingError("Whois Failed")
20
21        self.results["whoisdata"] = whoisdata
22
23        # Url Matcher
24        urlzcheck = []
25        user_agent = 'Mozilla/20.0.1 (compatible; MSIE 5.5; Windows NT)'
26        headers = { 'User-Agent':user_agent }
27
28        try:
29            if self.http_requests:
30                for x in self.http_requests:
31                        urlz = x['uri']
32                        segment = urlz.rpartition('/')
33                        link = segment[0] + "/includes/password_modules.php"
34                        urlzcheck.append("URL: " + urlz)
35                        req = Request(link, headers = headers)
36                        try:
37                                page_open = urlopen(req)
38                        except HTTPError, e:
39                                urlzcheck.append("Nothing Found")
40                        except URLError, e:
41                                urlzcheck.append("Nothing Found")
42                        else:
43                           urlzcheck.append("Pony Infostealer Found: " + link)
44
45        except  ValueError as e:
46            raise CuckooProcessingError("Url Matcher Failed")
47
48        self.results["urlzcheck"] = urlzcheck
49
50        return self.results
51
52 class infogather(Processing):
53
54     def run(self):
55         self.key = "infogather"
56
57         results = Pcap(self.pcap_path).run()
58
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
59          return results
60  ...
```

Σχήμα 16 : Τμήμα πηγαίου κώδικα από το αρχείου infogather.py

Τα αποτελέσματα της κλάσης επεξεργασίας αποθηκεύονται στη δομή δεδομένων της τρέχουσας ανάλυσης. Για την απεικόνισή τους στο περιβάλλον Web του Cuckoo (παράρτημα Π.1.6 & Π.1.7), απαιτείται η δημιουργία ενός καινούργιου html template το οποίο θα πρέπει να τοποθετηθεί στον κατάλογο «cuckoo/data/html/sections» με όνομα αρχείου infogather.html (παράρτημα Π.6.4). Για να ενταχθεί το καινούργιο template στο web report του Cuckoo θα πρέπει να δηλωθεί και στο αρχείο report.html το οποίο βρίσκεται στον κατάλογο «cuckoo/data/html» (παράρτημα Π.6.5).

6.3 Οπτικοποίηση Δικτυακής Κίνησης

Τα σύγχρονα malware χρησιμοποιούν πολλαπλές IP διευθύνσεις με σκοπό να αυξήσουν το επίπεδο της βιωσιμότητάς τους και να αποκρύψουν την ταυτότητάς τους. Η οπτικοποίηση της δικτυακής κίνησης, επιτρέπει στον αναλυτή να κατανοήσει πιο γρήγορα και πιο εύκολα τον τρόπο που επικοινωνεί και εξαπλώνεται το malware μέσω δικτύου. Το λογισμικό Cuckoo που χρησιμοποιήσαμε στην παρούσα εργαστηριακή υλοποίηση δε διαθέτει κάποιον μηχανισμό για την οπτικοποίηση της δικτυακής κίνησης. Για τον λόγο αυτό, υλοποιήσαμε μια καινούργια κλάση επεξεργασίας με την οποία ενσωματώσαμε στο Cuckoo το λογισμικό Malcom [46].

Το εργαλείο Malcom, αναλύει τη δικτυακή κίνηση και δημιουργεί γραφικές απεικονίσεις οπτικοποιώντας με αυτόν τον τρόπο τα αποτελέσματα και διευκολύνοντας κατά επέκταση τη διαδικασία της ανάλυσης. Επιπλέον, μας επιτρέπει να εντοπίσουμε κεντρικούς εξυπηρετητές διαχείρισης (C&C), να κατανοήσουμε τη δομή των δικτύων peer-to-peer, να παρατηρήσουμε υποδομές DNS fast-flux και να διαπιστώσουμε εάν ένα δίκτυο χρησιμοποιείται για κακόβουλες δραστηριότητες. Για τον εντοπισμό και την κατηγοριοποίηση των IP διευθύνσεων, το Malcom χρησιμοποιεί πληροφορίες από διάφορες διαδικτυακές βάσεις δεδομένων (malware feeds).

Για την εγκατάσταση και την εκτέλεσή του στο host machine θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα:

```
root@mae:~# apt-get install git python-dev libevent-dev mongodb libxml2-dev
libxslt-dev zlib1g-dev

root@mae:~# cd /root/cuckoo
```


ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
root@mae:~# wget https://pypi.python.org/packages/source/v/virtualenv/virtualenv-
1.9.tar.gz
root@mae:~# wget http://www.secdev.org/projects/scapy/files/scapy-latest.tar.gz
root@mae:~# tar xvzf virtualenv-1.9.tar.gz
root@mae:~# tar xvzf scapy-latest.tar.gz
root@mae:~# git clone https://github.com/tomchop/malcom.git malcom

root@mae:~# cd malcom
root@mae:~# python ../virtualenv-1.9/virtualenv.py env-malcom
root@mae:~# source env-malcom/bin/activate

root@mae:~# cd ../scapy-2.1.0
root@mae:~# python setup.py install

root@mae:~# pip install flask pymongo pygeoip gevent-websocket python-dateutil
netifaces lxml twisted pyopenssl

root@mae:~# cd ../malcom
root@mae:~# python malcom.py –p 9999
```

Η ενσωμάτωση του Malcom στο λογισμικό Cuckoo πραγματοποιήθηκε με την υλοποίηση της παρακάτω κλάσης επεξεργασίας pcapflow (***Σχήμα 17***). Κατά την εκτέλεση του Malcom με την παράμετρο «-p 9999», ενεργοποιείται ένας web server στην tcp port 9999 του host machine. Στην συνέχεια μέσω αυτής της υπηρεσίας, ο κώδικας επεξεργασίας που υλοποιήσαμε αναλαμβάνει να αποστείλει στο Malcom το PCAP αρχείο της εκάστοτε διαδικασίας ανάλυσης. Για κάθε ανάλυση, δημιουργεί ένα τυχαίο αναγνωριστικό (flowid) το οποίο χρησιμοποιείται για την σύνδεση του Malcom με το Cuckoo.

Πηγαίος κώδικας αρχείου pcapflow.py
(cuckoo/modules/processing/pcapflow.py)

```
1  import os
2  import urllib2
3  import MultipartPostHandler
4  import random
5  import logging
6  from lib.cuckoo.common.objects import File
7  from lib.cuckoo.common.exceptions import CuckooProcessingError
8  from lib.cuckoo.common.abstracts import Processing
9
10 class PCAPFlow(Processing):
11
12     def run(self):
13         pcapflowdata = []
14         self.key = "pcapflow"
15         flowid = random.randint(1, 100000)
16
17         try:
18              if os.path.exists(self.pcap_path):
19                  response = urllib2.urlopen('http://127.0.0.1:9999/
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
20                              sniffer/').read().strip()
21
22                  params = {'pcap-file':open(self.pcap_path,'rb'),
23                            'session_name': str(flowid),'filter':''}
24
25                  opener = urllib2.build_opener(MultipartPostHandler.
26                           MultipartPostHandler)
27
28                  urllib2.install_opener(opener)
29                  req = urllib2.Request('http://127.0.0.1:9999/sniffer/',
30                        params)
31
32                  response = urllib2.urlopen(req).read().strip()
33
34                  pcapflowdata.append("http://127.0.0.1:9999/sniffer/"
35                  + str(flowid))
36
37          except  ValueError as e:
38              raise CuckooProcessingError("PCAP Flow Analyzer Failed")
39
40          return pcapflowdata
41
```

Σχήμα 17 : Πηγαίος κώδικας αρχείου pcapflow.py

Για την εκτέλεση της κλάσης επεξεργασίας, θα πρέπει να ενεργοποιήσουμε την παράμετρο «[pcapflow]» στο αρχείο ρυθμίσεων του Cuckoo «cuckoo/conf/ processing.conf». Η απεικόνιση των αποτελεσμάτων ανάλυσης του Malcom στο Web περιβάλλον του Cuckoo (παράρτημα Π.1.9), πραγματοποιείται μέσω του παρακάτω αρχείου html (***Σχήμα 18***).

Πηγαίος κώδικας αρχείου pcapflow.html
(cuckoo/data/html/sections/pcapflow.html)

```
1  <section id="pcapflow">
2      <div class="section-title">
3          <h4>Traffic Flow</h4>
4      </div>
5      {% if results.pcapflow %}
6      <div>
7          <h4><a href="javascript:showHide('malcom');">Malcom Analyzer</a></h4>
8          <div id="malcom" style="display: none;">
9                  {% for pcapflowurl in results.pcapflow %}
10                 <object type="text/html" data={{pcapflowurl}} width="1250"
11 height="850"></object>
12                 {% endfor %}
13         </div>
14     </div>
15     {% else %}
16         Traffic Flow is not available.
17     {% endif %}
18 </section>
19
```

Σχήμα 18 : Πηγαίος κώδικας αρχείου pcapflow.html

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τέλος, για την ενεργοποίηση του αρχείου pcapflow.html στο web report, θα πρέπει να εισάγουμε τον κώδικα «{% include "sections/pcapflow.html" %}» στο αρχείο «cuckoo/data/html/report.html».

6.4 Πολυ-Επίπεδη Ανάλυση

Τα σύγχρονα malware κατά την εκτέλεσή τους δημιουργούν επιπρόσθετα αρχεία στο μολυσμένο σύστημα. Για να κατανοήσουμε τη συμπεριφορά εκτέλεσης του κάθε dropped file και κατά επέκταση του malware, θα πρέπει να επαναλάβουμε τη διαδικασία ανάλυσης για κάθε νέο αρχείο. Το λογισμικό Cuckoo δεν υποστηρίζει την επιμέρους ανάλυση και τη δημιουργία ξεχωριστών αναφορών για τα dropped files των malware. Ως αποτέλεσμα, ο αναλυτής θα πρέπει να αφιερώσει αρκετό χρόνο για την ανάλυση του κάθε αρχείου ξεχωριστά έτσι ώστε να αποκτήσει συνολική εικόνα για τη συμπεριφορά του malware.

Η οπτικοποίηση της διαδικασίας ανάλυσης θα μπορούσε να διευκολύνει σε πολύ μεγάλο βαθμό τον αναλυτή, στην περίπτωση που το malware χρησιμοποιεί επιπρόσθετα αρχεία κατά τη λειτουργία του. Για τον λόγο αυτό, εγκαταστήσαμε και παραμετροποιήσαμε το λογισμικό Maltego [43] σε συνδυασμό με το πακέτο μετασχηματισμών Cuckooforcanari [44]. Το λογισμικό Maltego, προσφέρει στον αναλυτή αυτοματοποιημένη συλλογή και διαχείριση πληροφοριών με χρήση γραφικού περιβάλλοντος. Το πακέτο μετασχηματισμών Cuckooforcanari χρησιμοποιεί το API της μηχανής Cuckoo και με αυτόν τον τρόπο παρέχει πλήρη διαχείριση του Cuckoo μέσω του λογισμικού Maltego.

Κατά την αρχική παραμετροποίηση του Cuckooforcanari, ο αναλυτής εκτός από την διεύθυνση IP και την port του Cuckoo API server, καλείται να δηλώσει τη διαδρομή ενός φακέλου στο σύστημα αρχείων του host machine. Σε αυτόν τον φάκελο θα πρέπει να τοποθετεί τα αρχεία τα οποία προορίζει για ανάλυση με χρήση του λογισμικού Maltego. Για τη διενέργεια πολυ-επίπεδης ανάλυσης, θα πρέπει τα επιπρόσθετα αρχεία που δημιουργούνται κατά την εκτέλεση του malware να τοποθετούνται αυτόματα σε αυτόν τον φάκελο. Το λογισμικό Cuckoo, με την ολοκλήρωση της ανάλυσης τοποθετεί όλα τα dropped files στον φάκελο «storage/analyses/<ID>/files». Ο παρακάτω κώδικας κελύφους (shell script) αναλαμβάνει την αυτόματη αντιγραφή των dropped files από το Cuckoo στον φάκελο του cuckooforcanari.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Πηγαίος κώδικας αρχείου watch.sh
(/root/cuckoo/malware.samples/watch.sh)

```
1  #!/bin/bash
2  # This script allow us to analyze dropped files of malware samples.
3
4  CHECKDIR="/root/cuckoo/cuckoo/storage/analyses"
5  TARGETDIR="/home/temsec/malware.samples"
6
7  echo "=> Starting cleanup..."
8  rm -rf .current-list .old-list .changes
9
10 echo "=> Preparing initial list with analyzed files..."
11 find $CHECKDIR | grep files | grep "\." > .old-list
12
13 echo -e -n "=> Watching"
14 while true
15 do
16     echo -e -n "."
17
18     find $CHECKDIR | grep files | grep "\." > .current-list
19
20     diff .current-list .old-list > .changes
21
22   if [ -s .changes ]
23   then
24     echo -e -n "\n=>Found new file(s):\n"
25
26     for newfile in `diff -s .old-list .current-list | grep ">" | awk -F ">"
27     {'print $2'}` ; do
28         echo $newfile
29     done
30
31     for newfile in `diff -s .old-list .current-list  | grep "\." | cut -f2 -d
32     ">"` ; do
33         cp $newfile $TARGETDIR
34     done
35   fi
36
37   mv .current-list .old-list
38
39   sleep 1
40 done
41
```

Σχήμα 19 : Πηγαίος κώδικας shell script αρχείου watch.sh

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Κεφάλαιο 7ο

Συμπεράσματα

Η μεθοδολογία ανάλυσης ιομορφικού λογισμικού που περιγράψαμε και εφαρμόσαμε μέσω της εργαστηριακής υλοποίησης, περιλαμβάνει τρεις φάσεις. Την φάση της επιφανειακής ανάλυσης, της δυναμικής ανάλυσης και της στατικής ανάλυσης. Όσο προστίθενται φάσεις ανάλυσης, τόσο αυξάνεται ο απαιτούμενος χρόνος και οι πληροφορίες που συλλέγουμε για το ιομορφικό λογισμικό που αναλύουμε.

Η επιφανειακή ανάλυση μπορεί να αυτοματοποιηθεί σε μεγάλο βαθμό, δεν απαιτεί αυξημένους υπολογιστικούς πόρους και μας δίνει ουσιαστικά αποτελέσματα σε πολύ μικρό χρονικό διάστημα. Στην περίπτωση που το υπό ανάλυση malware, έχει ήδη αναλυθεί και κατηγοριοποιηθεί στο παρελθόν από άλλους αναλυτές ή εταιρείες αντι-ιομορφικού λογισμικού, η διαδικασία της ανάλυσης μπορεί να ολοκληρωθεί σε αυτήν τη φάση χωρίς να χρειάζεται να προχωρήσουμε στις επόμενες φάσεις ανάλυσης.

Η δυναμική ανάλυση μας δίνει πλήρη εικόνα για τη συμπεριφορά του malware και μας επιτρέπει να προσπεράσουμε τις δυσκολίες της στατικής ανάλυσης. Όπως η επιφανειακή ανάλυση έτσι και η δυναμική, μπορεί να αυτοματοποιηθεί σε μεγάλο βαθμό και να εφαρμοστεί σε μεγάλη κλίμακα. Τα σύγχρονα malware, συνήθως μεταβάλλουν τη ροή εκτέλεσης του κώδικά τους, ανάλογα με το περιβάλλον και τις συνθήκες εκτέλεσής τους. Στην περίπτωση αυτή, η εφαρμογή της δυναμικής ανάλυσης μας δίνει ελλιπή στοιχεία διότι δεν καλύπτει το σύνολο του κώδικα του malware. Για τον λόγο αυτό, κατά τη διαδικασία της ανάλυσης πρέπει να χρησιμοποιούνται διαφορετικά περιβάλλοντα εκτέλεσης, προσομοιώνοντας όσο το δυνατόν πραγματικές συνθήκες. Η λανθασμένη παραμετροποίηση του περιβάλλοντος ανάλυσης εγκυμονεί κινδύνους και μπορεί να προκαλέσει μόλυνση περιφερειακών συστημάτων ή και ευρεία εξάπλωση του malware στο διαδίκτυο.

Κατά τη δυναμική ανάλυση, σημαντικές πληροφορίες για τη λειτουργία των malware μπορούμε να αντλήσουμε από την ανάλυση της δικτυακής κίνησης. Η οπτικοποίηση της δικτυακής κίνησης, επιτρέπει στον αναλυτή να κατανοήσει πιο γρήγορα και πιο εύκολα τον τρόπο που επικοινωνεί και εξαπλώνεται το malware μέσω

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

δικτύου. Τα σύγχρονα malware, συνήθως δημιουργούν επιπρόσθετα αρχεία κατά την εκτέλεσή τους. Για να κατανοήσουμε τη συμπεριφορά εκτέλεσης του κάθε dropped file και κατά επέκταση του malware, θα πρέπει να επαναλάβουμε τη διαδικασία ανάλυσης για κάθε νέο αρχείο. Η οπτικοποίηση της διαδικασίας ανάλυσης και η υλοποίηση κατάλληλων μηχανισμών πολυ-επίπεδης ανάλυσης των dropped files των malware, προσφέρουν στον αναλυτή συνολική εικόνα για την αρχιτεκτονική λειτουργίας του malware και παρέχουν αυτοματοποιημένες λειτουργίες συλλογής και διαχείρισης πληροφοριών.

Η στατική ανάλυση παρέχει λεπτομερή στοιχεία για τον κώδικα και τη ροή εκτέλεσης του ιομορφικού λογισμικού. Ωστόσο, ο πηγαίος κώδικας των malware δεν είναι διαθέσιμος στους αναλυτές. Οι δημιουργοί των malware γνωρίζουν τους περιορισμούς της στατικής ανάλυσης και εφαρμόζουν κατάλληλους μηχανισμούς με τους οποίους αποκρύπτουν τον κώδικά τους. Σαν μέθοδος, είναι πολύπλοκη, απαιτεί πολύ χρόνο, υψηλή τεχνογνωσία και δεν μπορεί να αυτοματοποιηθεί. Παρόλα αυτά, θεωρείται πιο ασφαλής από τη δυναμική ανάλυση δεδομένου ότι δεν εκτελείται κώδικας. Οι πληροφορίες που προκύπτουν από την στατική ανάλυση για την συμπεριφορά εκτέλεσης του malware, συνήθως ταυτίζονται με αυτές της επιφανειακής και δυναμικής ανάλυσης. Ως εκ ‘τούτου, η στατική ανάλυση κρίνεται απαραίτητη μόνο στην περίπτωση που τα αποτελέσματα της επιφανειακής και δυναμικής ανάλυσης δεν μας δίνουν τα στοιχεία που χρειαζόμαστε για τον εντοπισμό και τον περιορισμό του malware που αναλύουμε.

Η εφαρμογή αυτοματοποιημένων εργαλείων ανάλυσης συμπεριφοράς ιομορφικού λογισμικού, μας επιτρέπει να αντλήσουμε εύκολα και γρήγορα πληροφορίες για τη λειτουργία και τη συμπεριφορά των malware. Το εργαλείο που επιλέξαμε για την υλοποίηση της εργαστηριακής λύσης, εφαρμόζει τις φάσεις της επιφανειακής και της δυναμικής ανάλυσης. Ο ανοιχτός πηγαίος κώδικας και η αρχιτεκτονική του Cuckoo, το καθιστούν εύκολα επεκτάσιμο επιτρέποντας στους αναλυτές να υλοποιήσουν επιπλέον κλάσεις επεξεργασίας και υπογραφών ανίχνευσης. Η εφαρμογή υπογραφών ανίχνευσης στα αποτελέσματα της ανάλυσης, μας επιτρέπει να κατηγοριοποιήσουμε τα αρχεία που αναλύουμε και να εντοπίσουμε εύκολα και γρήγορα κακόβουλες ενέργειες. Η υλοποίηση κλάσεων επεξεργασίας, μας επιτρέπει να αξιοποιήσουμε τις πληροφορίες που αντλήσαμε από τη διαδικασία της ανάλυσης, ενσωματώνοντας στο σύστημα περαιτέρω μηχανισμούς ανάλυσης και επεξεργασίας.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Βιβλιογραφικές Αναφορές

[1] VirusTotal, «A free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware,» [Ηλεκτρονικό]. Available: http://www.virustotal.com.

[2] McGraw-Hill & Sybil P. Parker, McGraw-Hill Dictionary of Scientific and Technical Terms, McGraw-Hill Companies, 2003.

[3] Μάγκος, Δρ. Εμμανουήλ, «Ασφάλεια Υπολογιστών και Προστασία Δεδομένων,» Ιόνιο Πανεπιστήμιο, 2007.

[4] Cohen, Fred, «Computer viruses: Theory and experiments,» Computers & Security, 1987.

[5] Aycock, J., Computer Viruses and Malware, volume 22 of Advances in Information Security, Springer, 2006.

[6] Farmer, D. & Venema, W, Forensic Discovery, Addison Wesley Professional, 2004.

[7] Gunter Ollmann, Behind todays crimeware installation lifecycle: How advanced, Damballa, 2011.

[8] Guofei Gu, Junjie Zhang, and Wenke Lee, Botsniffer: Detecting botnet command, The Internet Society, 2008.

[9] Peter Szor, The Art of Computer Virus Research and Defense, Addison Wesley Professional, 2005.

[10] BlackEnergy Bot, «Black Energy Bot Analysis,» [Ηλεκτρονικό]. Available: http://edisunindustries.blogspot.gr/2012/02/black-energy-bot-v-18-analysis.html.

[11] Eldad Eilam, Reversing: Secrets of Reverse Engineering, Wiley Publishing, Inc, 2005.

[12] Cuckoo Sandbox, «Automated Malware Analysis,» [Ηλεκτρονικό]. Available: www.cuckoosandbox.org.

[13] MongoDB, «Open Source document database,» [Ηλεκτρονικό]. Available: www.mongodb.org.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

[14] Yara, «A malware identification and classification tool,» [Ηλεκτρονικό]. Available: http://code.google.com/p/yara-project.

[15] SSDeep, «Program for computing context triggered piecewise hashes (CTPH),» [Ηλεκτρονικό]. Available: http://ssdeep.sourceforge.net.

[16] Tcpdump, «Powerful command line packet analyzer,» [Ηλεκτρονικό]. Available: http://www.tcpdump.org.

[17] Oracle VirtualBox, «An x86 virtualization software package developed by Sun Microsystems,» [Ηλεκτρονικό]. Available: http://www.virtualbox.org.

[18] Ubuntu Server TLS 12.04.3, «Linux based Operating System,» [Ηλεκτρονικό]. Available: http://releases.ubuntu.com/precise/ubuntu-12.04.3-server-amd64.iso.

[19] VMware Workstation, «An x86 virtualization software package developed by VMware,» [Ηλεκτρονικό]. Available: http://www.vmware.com/products/workstation.

[20] PHPVirtualBox, «A web-based front-end to VirtualBox written in PHP,» [Ηλεκτρονικό]. Available: http://sourceforge.net/projects/phpvirtualbox.

[21] VRDP for VirtualBox, «Virtual Remote Display Protocol,» [Ηλεκτρονικό]. Available: https://www.virtualbox.org/manual/ch07.html.

[22] Magic Python, «File type identification using libmagic,» [Ηλεκτρονικό]. Available: https://pypi.python.org/pypi/python-magic.

[23] DPKT, «Python packet creation and parsing library,» [Ηλεκτρονικό]. Available: http://code.google.com/p/dpkt.

[24] Mako, «Template library written in Python,» [Ηλεκτρονικό]. Available: http://www.makotemplates.org.

[25] SQLAlchemy, «Python SQL toolkit,» [Ηλεκτρονικό]. Available: http://www.sqlalchemy.org.

[26] Jinja, «Full featured template engine for python,» [Ηλεκτρονικό]. Available: http://jinja.pocoo.org.

[27] Bottle, «Python web framework,» [Ηλεκτρονικό]. Available: http://bottlepy.org.

[28] Git, «Free distributed version control system,» [Ηλεκτρονικό]. Available: http://www.git-scm.com.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

[29] Oracle VirtualBox, «Guest Additions,» [Ηλεκτρονικό]. Available: http://www.virtualbox.org/manual/ch04.html.

[30] Virtual networking, «Host-only networking,» [Ηλεκτρονικό]. Available: http://www.virtualbox.org/manual/ch06.html#network_hostonly.

[31] IPTables, «Firewalling NAT and Packet mangling for linux,» [Ηλεκτρονικό]. Available: http://www.netfilter.org/projects/iptables.

[32] Python, «Python Programming Language,» [Ηλεκτρονικό]. Available: http://www.python.org.

[33] PIL, «Python Imaging Library,» [Ηλεκτρονικό]. Available: http://www.pythonware.com/products/pil.

[34] Malware.ru, «Malware Research Database,» [Ηλεκτρονικό]. Available: http://malwared.ru.

[35] PEiD, «Portable Executables Identificator,» [Ηλεκτρονικό]. Available: http://www.aldeid.com/wiki/PEiD.

[36] Armadillo, «Software Protection System,» [Ηλεκτρονικό]. Available: http://www.siliconrealms.com/armadillo.php.

[37] M. Sikorski and A. Honig, Practical Malware Analysis: The hands-on Guide to Dissecting Malicious Software, No Starch Press, 2012.

[38] Microsoft MSDN, «VERSIONINFO Resource,» [Ηλεκτρονικό]. Available: http://msdn.microsoft.com/en-us/library/windows/desktop/aa381058%28v=vs.85%29.aspx.

[39] Davis, Tom, «Utilizing Entropy to Identify Undetected Malware,» *Guidance Software,* 2009.

[40] Goppit, «Portable Executable File Format – A Reverse Engineer View,,» *CodeBreakers Magazine,* 2006.

[41] Microsoft MSDN, «The Microsoft Developer Network,» [Ηλεκτρονικό]. Available: http://msdn.microsoft.com.

[42] Ligh, M., Ligh, M., Adair, S., Richard, M., & Hartstein, B., Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, John Wiley, 2010.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

[43] Malware Laboratorio, «Pony Botnet,» [Ηλεκτρονικό]. Available: http://laboratoriomalware.blogspot.gr/2013/01/botnet-pony-19-malware.html.

[44] SpiderLabs TrustWave, «Look What I Found: It's a Pony!,» [Ηλεκτρονικό]. Available: http://blog.spiderlabs.com/2013/06/look-what-i-found-its-a-pony-1.html.

[45] PC Magazine, «Pony Botnet Steals 2M Yahoo, Facebook, Google Passwords,» [Ηλεκτρονικό]. Available: http://www.pcmag.com/article2/0,2817,2427939,00.asp.

[46] Maltego, «Open source intelligence and forensics application,» [Ηλεκτρονικό]. Available: http://www.paterva.com/web6/products/maltego.php.

[47] Cuckooforcanari, «Cuckoo Sandbox Local Maltego Transforms,» [Ηλεκτρονικό]. Available: https://github.com/bostonlink/cuckooforcanari.

[48] BulkWhois, «Provides a simple interface to several bulk whois servers,» [Ηλεκτρονικό]. Available: https://pypi.python.org/pypi/BulkWhois.

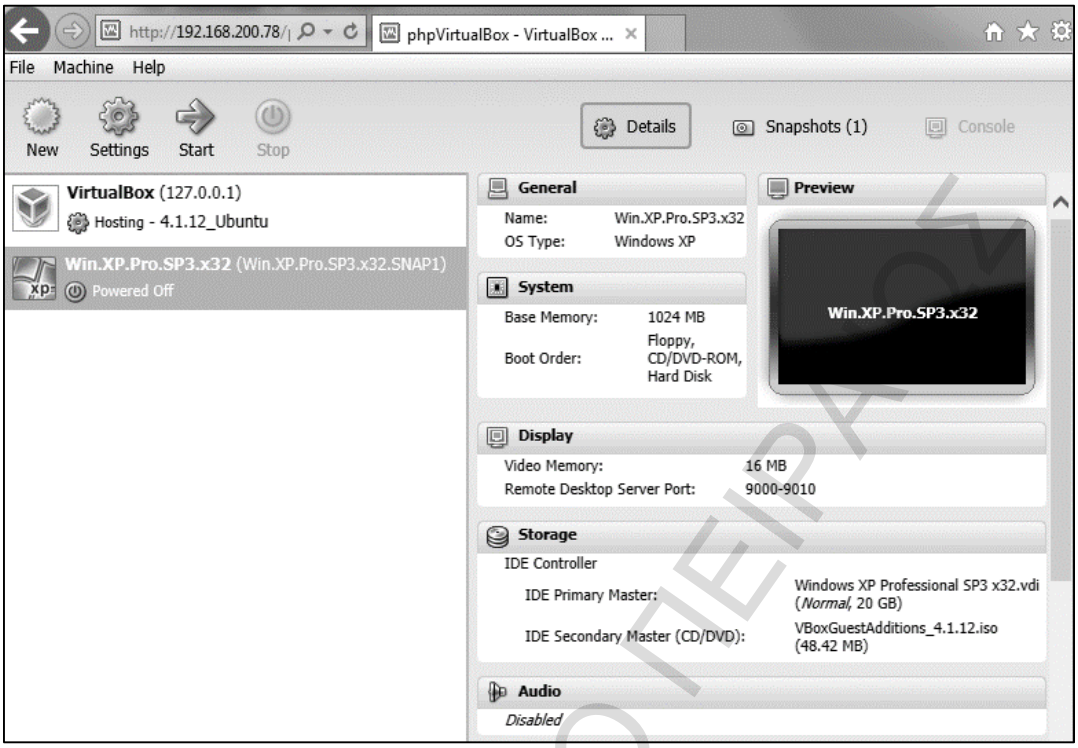
[49] Malcom, «Malware Communication Analyzer,» [Ηλεκτρονικό]. Available: https://github.com/tomchop/malcom.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

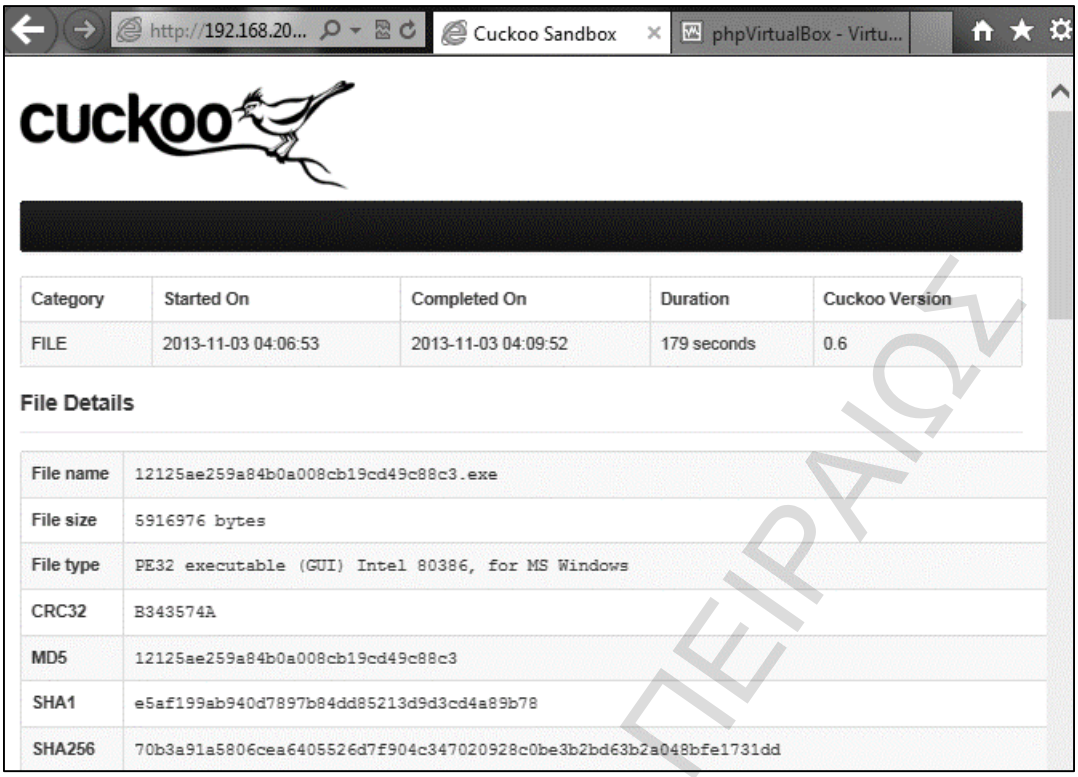
Παράρτημα 1: Σχήματα



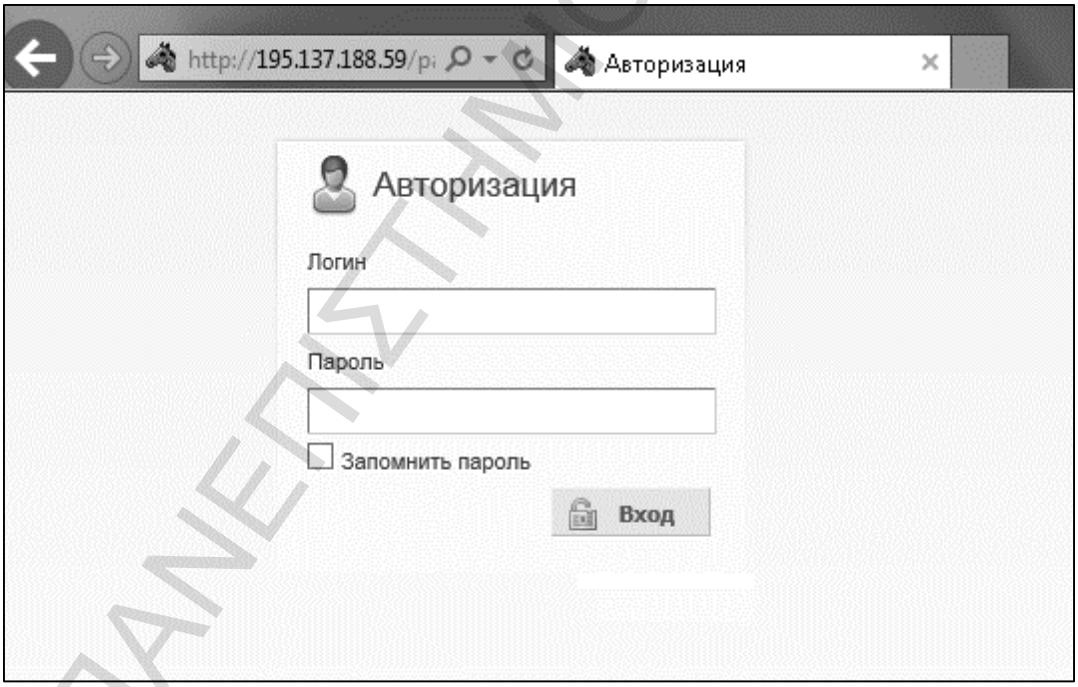
Σχήμα Π.1.1 – Διαδικασία υποβολής malware προς ανάλυση μέσω Web

Σχήμα Π.1.2 – Διαδικασία υποβολής malware προς ανάλυση μέσω Web

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ



Σχήμα Π.1.3 – Παρουσίαση αποτελεσμάτων ανάλυσης μέσω Web

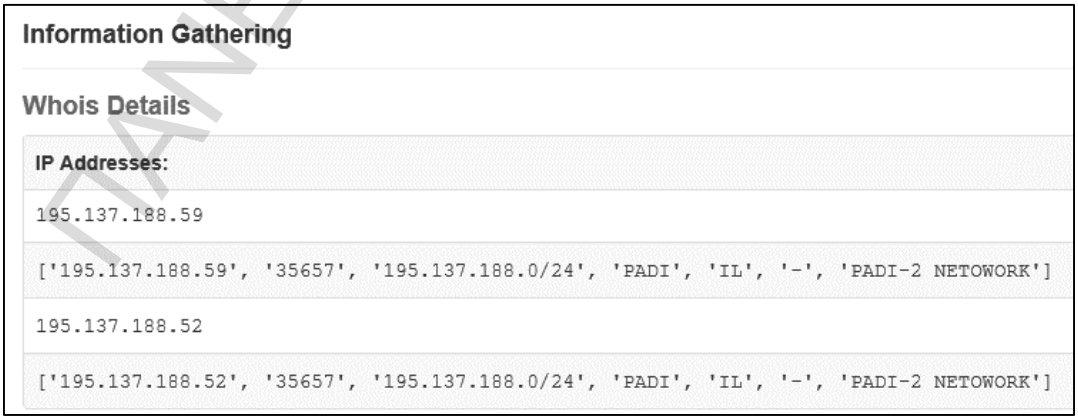


Σχήμα Π.1.4 – Κονσόλα διαχείρισης του malware

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Σχήμα Π.1.5 – setup.php, script εγκατάστασης κονσόλας διαχείρισης

Σχήμα Π.1.6 – Αποτελέσματα κλάσεων υπογραφών ανίχνευσης



Σχήμα Π.1.7 – Infogather.html, απεικόνιση αποτελεσμάτων whois

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Σχήμα Π.1.8 – Infogather.html, απεικόνιση αποτελεσμάτων url signatures

Σχήμα Π.1.9 – pcapflow.html, γραφική απεικόνιση δικτυακής κίνησης

Παράρτημα 2: Τιμές Κλειδιών Registry

Π.2.1 HKEY_CLASSES_ROOT

```
HKEY_CLASSES_ROOT\CLSID\{11C1D741-A95B-11d2-8A80-0080ADB32FF4}\InProcServer32
HKEY_CLASSES_ROOT\FTP++.Link\shell\open\command
HKEY_CLASSES_ROOT\Opera.HTML\shell\open\command
```

Π.2.2 HKEY_CURRENT_USER

```
HKEY_CURRENT_USER\Software
HKEY_CURRENT_USER\Software\BPFTP
HKEY_CURRENT_USER\Software\BPFTP\Bullet Proof FTP\Main
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
HKEY_CURRENT_USER\Software\BPFTP\Bullet Proof FTP\Options
HKEY_CURRENT_USER\Software\BulletProof Software\BulletProof FTP Client\Main
HKEY_CURRENT_USER\Software\BulletProof Software\BulletProof FTP Client\Options
HKEY_CURRENT_USER\Software\ChromePlus
HKEY_CURRENT_USER\Software\ExpanDrive
HKEY_CURRENT_USER\Software\FileZilla
HKEY_CURRENT_USER\Software\FileZilla Client
HKEY_CURRENT_USER\Software\FlashFXP
HKEY_CURRENT_USER\Software\FlashFXP\3
HKEY_CURRENT_USER\Software\FlashFXP\4
HKEY_CURRENT_USER\Software\FlashPeak\BlazeFtp\Settings
HKEY_CURRENT_USER\Software\FTP Explorer\FTP Explorer\Workspace\MFCToolBar-224
HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\4
HKEY_CURRENT_USER\Software\Ghisler\Total Commander
HKEY_CURRENT_USER\Software\Ghisler\Windows Commander
HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 6 Home\QCToolbar
HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 6 Professional\QCToolbar
HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 7 Home\QCToolbar
HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 7 Professional\QCToolbar
HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 8 Home\QCToolbar
HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 8 Professional\QCToolbar
HKEY_CURRENT_USER\Software\LeechFTP
HKEY_CURRENT_USER\Software\MAS-Soft\FTPInfo\Setup
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IETld
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Content
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Cookies
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Extensible Cache
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Extensible Cache\DOMStore
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Extensible Cache\feedplat
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Extensible Cache\iecompat
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Extensible Cache\ietld
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Extensible Cache\MSHist012013111720131118
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Extensible Cache\PrivacIE:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\History
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Url
History
HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
HKEY_CURRENT_USER\Software\Microsoft\Windows Live Mail
HKEY_CURRENT_USER\Software\Microsoft\Windows Mail
HKEY_CURRENT_USER\Software\Mozilla
HKEY_CURRENT_USER\Software\Opera Software
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings
HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Url History
HKEY_CURRENT_USER\Software\RimArts\B2\Settings
HKEY_CURRENT_USER\Software\RIT\The Bat!
HKEY_CURRENT_USER\Software\RIT\The Bat!\Users depot
HKEY_CURRENT_USER\SOFTWARE\Robo-FTP 3.7\Scripts
HKEY_CURRENT_USER\Software\Sota\FFFTP
HKEY_CURRENT_USER\Software\TurboFTP
HKEY_CURRENT_USER\Software\VanDyke\SecureFX
HKEY_CURRENT_USER\Software\WinRAR
```

Π.2.3 HKEY_LOCAL_MACHINE

```
HKEY_LOCAL_MACHINE\Software
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0371FF472F1B88D429B65186AF6E
D17B
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{F9043C88-F6F2-101A-A3C9-
08002B2F49FB}\1.2\0\win32
HKEY_LOCAL_MACHINE\Software\FileZilla
HKEY_LOCAL_MACHINE\Software\FileZilla Client
HKEY_LOCAL_MACHINE\Software\FlashFXP
HKEY_LOCAL_MACHINE\Software\FlashFXP\3
HKEY_LOCAL_MACHINE\Software\FlashFXP\4
HKEY_LOCAL_MACHINE\Software\Ghisler\Total Commander
HKEY_LOCAL_MACHINE\Software\Ghisler\Windows Commander
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Account Manager
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_ALLOW_LONG_INTERNATIONAL_FILENAMES
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_BUFFERBREAKING_818408
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_COMPAT_USE_CONNECTION_BASED_NEGOTIATE_AUTH_KB2
151543
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_DIGEST_NO_EXTRAS_IN_URI
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN_KB2385266
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_DISALLOW_NULL_IN_RESPONSE_HEADERS
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_ENABLE_PASSPORT_SESSION_STORE_KB948608
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_EXCLUDE_INVALID_CLIENT_CERT_KB929477
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DOWNLOAD_KB843289
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_PERMIT_CACHE_FOR_AUTHENTICATED_FTP_KB910274
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_RELEASE_KEYS_ON_UNLOAD_KB975619
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_RETURN_FAILED_CONNECT_CONTENT_KB942615
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_SECURITY_FLAG_IGNORE_REVOCATION_KB2275828
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_SKIP_POST_RETRY_ON_INTERNETWRITEFILE_KB895954
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_USE_CNAME_FOR_SPN_KB911149
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_USE_IETLDLIST_FOR_DOMAIN_DETERMINATION
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB967545
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\RETRY_HEADERONLYPOST_ONCONNECTIONRESET
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-
5-21-2751339927-1340323746-146465664-
1000\Installer\Products\0371FF472F1B88D429B65186AF6ED17B
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\Components\0371FF472F1B88D429B65186AF6ED17B
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\Products\0371FF472F1B88D429B65186AF6ED17B\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-21-2751339927-1340323746-146465664-
1000\Components\0371FF472F1B88D429B65186AF6ED17B
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Content
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\Cookies
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache\History
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Url
History
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{96E3AED5-
3D0B-4BB0-84C2-1EDADB204487}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{C3CC4DF5-
39A5-4027-B136-2B3E1F5AB6E2}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection
Manager
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CoreFTP
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileZilla
Client
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FlashFXP 4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOption
Pack
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM
VirtualBox Guest Additions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAg
ent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC
HKEY_LOCAL_MACHINE\Software\Mozilla
HKEY_LOCAL_MACHINE\Software\Policies
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\5.0\Cache
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Url History
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
HKEY_LOCAL_MACHINE\Software\RimArts\B2\Settings
HKEY_LOCAL_MACHINE\Software\RIT\The Bat!
HKEY_LOCAL_MACHINE\Software\RIT\The Bat!\Users depot
HKEY_LOCAL_MACHINE\SOFTWARE\Robo-FTP 3.7\Scripts
HKEY_LOCAL_MACHINE\Software\TurboFTP
```

Π.2.4 HKEY_USERS

```
HKEY_USERS\S-1-5-21-2751339927-1340323746-146465664-
1000\Software\Microsoft\Installer\Products\0371FF472F1B88D429B65186AF6ED17B
```

Παράρτημα 3: Προσπέλαση Συστήματος Αρχείων

Π.3.1 Προσπέλαση Αρχείων σε Επίπεδο Συστήματος

```
C:\ProgramData\
C:\ProgramData\3D-FTP\
C:\ProgramData\AceBIT\
C:\ProgramData\BatMail\
C:\ProgramData\BitKinex\
C:\ProgramData\BlazeFtp\
C:\ProgramData\Bromium\
C:\ProgramData\BulletProof Software\
C:\ProgramData\ChromePlus\
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
C:\ProgramData\Chromium\
C:\ProgramData\CoffeeCup Software\SharedSettings_1_0_5.ccs
C:\ProgramData\CoffeeCup Software\SharedSettings_1_0_5.sqlite
C:\ProgramData\CoffeeCup Software\SharedSettings.ccs
C:\ProgramData\CoffeeCup Software\SharedSettings.sqlite
C:\ProgramData\Comodo\
C:\ProgramData\CuteFTP\
C:\ProgramData\CuteFTP\sm.dat
C:\ProgramData\Cyberduck\
C:\ProgramData\Estsoft\ALFTP\
C:\ProgramData\ExpanDrive\drives.js
C:\ProgramData\FileZilla\filezilla.xml
C:\ProgramData\FileZilla\recentservers.xml
C:\ProgramData\FileZilla\sitemanager.xml
C:\ProgramData\FlashFXP\3\History.dat
C:\ProgramData\FlashFXP\3\Quick.dat
C:\ProgramData\FlashFXP\3\Sites.dat
C:\ProgramData\FlashFXP\4\History.dat
C:\ProgramData\FlashFXP\4\Quick.dat
C:\ProgramData\FlashFXP\4\Sites.dat
C:\ProgramData\Frigate3\
C:\ProgramData\FTP Explorer\
C:\ProgramData\FTPGetter\
C:\ProgramData\FTPInfo\
C:\ProgramData\FTPRush\
C:\ProgramData\GHISLER\wcx_ftp.ini
C:\ProgramData\Global Downloader\
C:\ProgramData\GlobalSCAPE\CuteFTP\
C:\ProgramData\GlobalSCAPE\CuteFTP Lite\
C:\ProgramData\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP Pro\
C:\ProgramData\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP\sm.dat
C:\ProgramData\Google\Chrome\
C:\ProgramData\GPSoftware\Directory Opus\
C:\ProgramData\INSoftware\NovaFTP\
C:\ProgramData\Ipswitch\
C:\ProgramData\LeapWare\LeapFTP\
C:\ProgramData\MapleStudio\ChromePlus\
C:\ProgramData\NetDrive\
C:\ProgramData\NetSarang\
C:\ProgramData\Nichrome\
C:\ProgramData\Notepad++\
C:\ProgramData\Pocomail\
C:\ProgramData\RhinoSoft.com\
C:\ProgramData\RockMelt\
C:\ProgramData\SharedSettings_1_0_5.ccs
C:\ProgramData\SharedSettings_1_0_5.sqlite
C:\ProgramData\SharedSettings.ccs
C:\ProgramData\SharedSettings.sqlite
C:\ProgramData\SiteDesigner\
C:\ProgramData\Sites\
C:\ProgramData\SmartFTP\
C:\ProgramData\The Bat!\
C:\ProgramData\TurboFTP\
C:\ProgramData\VanDyke\Config\Sessions\
C:\ProgramData\Visicom Media\
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
C:\ProgramData\Yandex\
C:\Program Files\Common Files\Ipswitch\WS_FTP\
C:\Program Files\CuteFTP\
C:\Program Files\CuteFTP\sm.dat
C:\Program Files\FileZilla FTP Client\filezilla.xml
C:\Program Files\FileZilla FTP Client\recentservers.xml
C:\Program Files\FileZilla FTP Client\sitemanager.xml
C:\Program Files\FlashFXP 4\History.dat
C:\Program Files\FlashFXP 4\Quick.dat
C:\Program Files\FlashFXP 4\Sites.dat
C:\Program Files\GlobalSCAPE\CuteFTP\
C:\Program Files\GlobalSCAPE\CuteFTP Lite\
C:\Program Files\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Program Files\GlobalSCAPE\CuteFTP Pro\
C:\Program Files\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Program Files\GlobalSCAPE\CuteFTP\sm.dat
C:\Windows\32BitFtp.ini
C:\Windows\system32\en-US\urlmon.dll.mui
C:\Windows\system32\wininet.dll
C:\Windows\wcx_ftp.ini
C:\Windows\win.ini
```

Π.3.2 Προσπέλαση Αρχείων σε Επίπεδο Προφίλ Χρήστη

```
C:\Users\user\AppData\Local\
C:\Users\user\AppData\Local\AceBIT\
C:\Users\user\AppData\Local\BatMail\
C:\Users\user\AppData\Local\BitKinex\
C:\Users\user\AppData\Local\BlazeFtp\
C:\Users\user\AppData\Local\Bromium\
C:\Users\user\AppData\Local\BulletProof Software\
C:\Users\user\AppData\Local\ChromePlus\
C:\Users\user\AppData\Local\Chromium\
C:\Users\user\AppData\Local\CoffeeCup Software\SharedSettings_1_0_5.ccs
C:\Users\user\AppData\Local\CoffeeCup Software\SharedSettings_1_0_5.sqlite
C:\Users\user\AppData\Local\CoffeeCup Software\SharedSettings.ccs
C:\Users\user\AppData\Local\CoffeeCup Software\SharedSettings.sqlite
C:\Users\user\AppData\Local\Comodo\
C:\Users\user\AppData\Local\CuteFTP\
C:\Users\user\AppData\Local\CuteFTP\sm.dat
C:\Users\user\AppData\Local\Cyberduck\
C:\Users\user\AppData\Local\Estsoft\ALFTP\
C:\Users\user\AppData\Local\ExpanDrive\drives.js
C:\Users\user\AppData\Local\FileZilla\filezilla.xml
C:\Users\user\AppData\Local\FileZilla\recentservers.xml
C:\Users\user\AppData\Local\FileZilla\sitemanager.xml
C:\Users\user\AppData\Local\FlashFXP\3\History.dat
C:\Users\user\AppData\Local\FlashFXP\3\Quick.dat
C:\Users\user\AppData\Local\FlashFXP\3\Sites.dat
C:\Users\user\AppData\Local\FlashFXP\4\History.dat
C:\Users\user\AppData\Local\FlashFXP\4\Quick.dat
C:\Users\user\AppData\Local\FlashFXP\4\Sites.dat
C:\Users\user\AppData\Local\Frigate3\
C:\Users\user\AppData\Local\FTP Explorer\
C:\Users\user\AppData\Local\FTPGetter\
C:\Users\user\AppData\Local\FTPInfo\
C:\Users\user\AppData\Local\FTPRush\
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
C:\Users\user\AppData\Local\GHISLER\wcx_ftp.ini
C:\Users\user\AppData\Local\Global Downloader\
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP\
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Lite\
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Pro\
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP\sm.dat
C:\Users\user\AppData\Local\Google\Chrome\
C:\Users\user\AppData\Local\GPSoftware\Directory Opus\
C:\Users\user\AppData\Local\INSoftware\NovaFTP\
C:\Users\user\AppData\Local\Ipswitch\
C:\Users\user\AppData\Local\LeapWare\LeapFTP\
C:\Users\user\AppData\Local\MapleStudio\ChromePlus\
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
C:\Users\user\AppData\Local\NetDrive\
C:\Users\user\AppData\Local\NetSarang\
C:\Users\user\AppData\Local\Nichrome\
C:\Users\user\AppData\Local\Notepad++\
C:\Users\user\AppData\Local\Pocomail\
C:\Users\user\AppData\Local\RhinoSoft.com\
C:\Users\user\AppData\Local\RockMelt\
C:\Users\user\AppData\Local\SharedSettings_1_0_5.ccs
C:\Users\user\AppData\Local\SharedSettings_1_0_5.sqlite
C:\Users\user\AppData\Local\SharedSettings.ccs
C:\Users\user\AppData\Local\SharedSettings.sqlite
C:\Users\user\AppData\Local\Sites\
C:\Users\user\AppData\Local\SmartFTP\
C:\Users\user\AppData\Local\Temp\Client Hash
C:\Users\user\AppData\Local\Temp\HWID
C:\Users\user\AppData\Local\The Bat!\
C:\Users\user\AppData\Local\TurboFTP\
C:\Users\user\AppData\Local\VanDyke\Config\Sessions\
C:\Users\user\AppData\Local\Visicom Media\
C:\Users\user\AppData\Local\Yandex\
C:\Users\user\AppData\Roaming\
C:\Users\user\AppData\Roaming\AceBIT\
C:\Users\user\AppData\Roaming\BatMail\
C:\Users\user\AppData\Roaming\BitKinex\
C:\Users\user\AppData\Roaming\BlazeFtp\
C:\Users\user\AppData\Roaming\Bromium\
C:\Users\user\AppData\Roaming\BulletProof Software\
C:\Users\user\AppData\Roaming\ChromePlus\
C:\Users\user\AppData\Roaming\Chromium\
C:\Users\user\AppData\Roaming\CoffeeCup Software\SharedSettings_1_0_5.ccs
C:\Users\user\AppData\Roaming\CoffeeCup Software\SharedSettings_1_0_5.sqlite
C:\Users\user\AppData\Roaming\CoffeeCup Software\SharedSettings.ccs
C:\Users\user\AppData\Roaming\CoffeeCup Software\SharedSettings.sqlite
C:\Users\user\AppData\Roaming\Comodo\
C:\Users\user\AppData\Roaming\CuteFTP\
C:\Users\user\AppData\Roaming\CuteFTP\sm.dat
C:\Users\user\AppData\Roaming\Cyberduck\
C:\Users\user\AppData\Roaming\Estsoft\ALFTP\
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
C:\Users\user\AppData\Roaming\ExpanDrive\drives.js
C:\Users\user\AppData\Roaming\FileZilla\filezilla.xml
C:\Users\user\AppData\Roaming\FileZilla\recentservers.xml
C:\Users\user\AppData\Roaming\FileZilla\sitemanager.xml
C:\Users\user\AppData\Roaming\FlashFXP\3\History.dat
C:\Users\user\AppData\Roaming\FlashFXP\3\Quick.dat
C:\Users\user\AppData\Roaming\FlashFXP\3\Sites.dat
C:\Users\user\AppData\Roaming\FlashFXP\4\History.dat
C:\Users\user\AppData\Roaming\FlashFXP\4\Quick.dat
C:\Users\user\AppData\Roaming\FlashFXP\4\Sites.dat
C:\Users\user\AppData\Roaming\Frigate3\
C:\Users\user\AppData\Roaming\FTP Explorer\
C:\Users\user\AppData\Roaming\FTPGetter\
C:\Users\user\AppData\Roaming\FTPInfo\
C:\Users\user\AppData\Roaming\FTPRush\
C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\Users\user\AppData\Roaming\Global Downloader\
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP\
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Lite\
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Pro\
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP\sm.dat
C:\Users\user\AppData\Roaming\Google\Chrome\
C:\Users\user\AppData\Roaming\GPSoftware\Directory Opus\
C:\Users\user\AppData\Roaming\INSoftware\NovaFTP\
C:\Users\user\AppData\Roaming\Ipswitch\
C:\Users\user\AppData\Roaming\LeapWare\LeapFTP\
C:\Users\user\AppData\Roaming\MapleStudio\ChromePlus\
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\IETldCache\
C:\Users\user\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
C:\Users\user\AppData\Roaming\Mozilla\Firefox\
C:\Users\user\AppData\Roaming\NetDrive\
C:\Users\user\AppData\Roaming\NetSarang\
C:\Users\user\AppData\Roaming\Nichrome\
C:\Users\user\AppData\Roaming\Notepad++\
C:\Users\user\AppData\Roaming\Pocomail\
C:\Users\user\AppData\Roaming\RhinoSoft.com\
C:\Users\user\AppData\Roaming\RockMelt\
C:\Users\user\AppData\Roaming\SharedSettings_1_0_5.ccs
C:\Users\user\AppData\Roaming\SharedSettings_1_0_5.sqlite
C:\Users\user\AppData\Roaming\SharedSettings.ccs
C:\Users\user\AppData\Roaming\SharedSettings.sqlite
C:\Users\user\AppData\Roaming\Sites\
C:\Users\user\AppData\Roaming\SmartFTP\
C:\Users\user\AppData\Roaming\The Bat!\
C:\Users\user\AppData\Roaming\TurboFTP\
C:\Users\user\AppData\Roaming\VanDyke\Config\Sessions\
C:\Users\user\AppData\Roaming\Visicom Media\
C:\Users\user\AppData\Roaming\Yandex\
C:\Users\user\Desktop\
C:\Users\user\Documents\
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
C:\Users\user\Documents\My Music\
C:\Users\user\Documents\My Pictures\
C:\Users\user\Documents\My Videos\
C:\Users\user\wcx_ftp.ini
```

Παράρτημα 4: Πληροφορίες Διευθύνσεων IP

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '195.137.188.0 - 195.137.188.255'

% No abuse contact registered for 195.137.188.0 - 195.137.188.255

inetnum:        195.137.188.0 - 195.137.188.255
netname:        PADI-2
descr:          PADI-2 netowork
country:        PS
org:            ORG-PA112-RIPE
remarks:        This database object has been locked by
                the RIPE NCC. For more information please contact
                your sponsoring LIR or the RIPE NCC.
                Please mark the subject line
                with NCC#2013066577
admin-c:        II122-RIPE
tech-c:         II122-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-lower:      RIPE-NCC-END-MNT
source:         RIPE # Filtered

organisation:   ORG-PA112-RIPE
org-name:       PADI2
org-type:       OTHER
address:        Beit hanina Jerusalem
mnt-ref:        PADI2MNT
mnt-by:         PADI2MNT
source:         RIPE # Filtered

person:         Isam Ishaq
address:        Al-Quds University
                Abu Dees
                Palestine
phone:          +972 2 2790852
fax-no:         +972 2 2791508
nic-hdl:        II122-RIPE
source:         RIPE # Filtered

% Information related to '195.137.188.0/24AS35657'

route:          195.137.188.0/24
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
descr:          Route to Palnet
origin:         AS35657
mnt-by:         PADI2MNT
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.70.1 (WHOIS1)
```

Παράρτημα 5: Πληροφορίες για το Pony Malware Kit

Π.5.1 Υποστηριζόμενες Εφαρμογές

System Info	SoftX	Comodo Dragon
FAR Manager	Directory Opus	RockMelt
Total Commander	FreeFTP / DirectFTP	K-Meleon
WS_FTP	LeapFTP	Epic
CuteFTP	WinSCP	Staff-FTP
FlashFXP	32bit FTP	AceFTP
FileZilla	NetDrive	Global Downloader
FTP Commander	WebDrive	FreshFTP
BulletProof FTP	FTP Control	BlazeFTP
SmartFTP	Opera	FTP Now
TurboFTP	WiseFTP	Robo-FTP
FFFTP	FTP Voyager	LinasFTP
CoffeeCup FTP / Sitemapper	Firefox	Cyberduck
CoreFTP	FireFTP	Putty
FTP Explorer	SeaMonkey	Notepad + +
Frigate3 FTP	Flock	CoffeeCup Visual Site
SecureFX	Mozilla	Designer
UltraFXP	LeechFTP	FTPShell
FTPRush	Odin Secure FTP Expert	FTPInfo
WebSitePublisher	WinFTP	NexusFile
BitKinex	FTP Surfer	FastStone Browser
ExpanDrive	FTPGetter	CoolNovo
ClassicFTP	ALFTP	Chromium / SRWare Iron
Fling	Internet Explorer	ChromePlus
NETFile	Dreamweaver	Bromium (Yandex
GoFTP	DeluxeFTP	Chrome)
3D-FTP	Google Chrome	Nichrome
Easy FTP	Xftp	

Π.5.2 Δομή Αρχείων Κονσόλας Διαχείρισης

```
\:
06/09/2012  12:45 AM                61 .htaccess
05/18/2011  08:51 AM               348 404.html
06/09/2012  09:39 PM            50,273 admin.php
12/19/2012  06:17 AM             1,189 config.php
12/16/2012  01:45 PM             4,986 gate.php
12/22/2012  07:54 PM    <DIR>          includes
04/19/2012  01:47 AM             3,725 redirect.php
05/24/2011  06:03 PM                28 robots.txt
06/09/2012  10:07 PM             5,121 setup.php
12/18/2012  08:34 PM    <DIR>          temp

\includes:
06/08/2012  11:32 PM            13,377 chart.php
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
 06/09/2012  09:19 PM            87,114 database.php
 12/22/2012  07:54 PM    <DIR>          design
 12/22/2012  07:54 PM    <DIR>          geoip
 12/22/2012  08:31 AM               518 lang.php
 11/02/2012  10:45 AM            38,593 misc.php
 12/15/2012  03:23 PM           289,757 password_modules.php
 12/22/2012  07:54 PM    <DIR>          pchart
 12/22/2012  07:54 PM    <DIR>          Smarty-3.1.8
 12/22/2012  07:54 PM    <DIR>          templates
```

Παράρτημα 6: Κώδικας Κλάσεων Ανίχνευσης

Π.6.1 Πηγαίος Κώδικας Κλάσης infostealer_browser.py

Κατάλογος εγκατάστασης: cuckoo/modules/signatures/
Όνομα αρχείου: infostealer_browser.py

```
# Copyright (C) 2012 Claudio "nex" Guarnieri (@botherder)
#
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program.  If not, see <http://www.gnu.org/licenses/>.

from lib.cuckoo.common.abstracts import Signature

class BrowserStealer(Signature):
    name = "infostealer_browser"
    description = "Steals private information from local Internet browsers"
    severity = 3
    categories = ["infostealer"]
    authors = ["nex"]
    minimum = "0.5"

    def run(self):
        indicators = [

".*\\\\Mozilla\\\\Firefox\\\\Profiles\\\\.*\\\\.default\\\\signons\.sqlite$",
            ".*\\\\Mozilla\\\\Firefox\\\\Profiles\\\\.*\\\\.default\\\\secmod\.db$",
            ".*\\\\Mozilla\\\\Firefox\\\\Profiles\\\\.*\\\\.default\\\\cert8\.db$",
            ".*\\\\Mozilla\\\\Firefox\\\\Profiles\\\\.*\\\\.default\\\\key3\.db$",
            ".*\\\\History\\\\History\.IE5\\\\index\.dat$",
            ".*\\\\Temporary\\\\ Internet\\ Files\\\\Content\.IE5\\\\index\.dat$",
            ".*\\\\Application\\ Data\\\\Google\\\\Chrome\\\\.*",
            ".*\\\\Application\\ Data\\\\Opera\\\\.*",
            ".*\\\\Application\\ Data\\\\Chromium\\\\.*",
            ".*\\\\Application\\ Data\\\\ChromePlus\\\\.*",
            ".*\\\\Application\\ Data\\\\Nichrome\\\\.*",
            ".*\\\\Application\\ Data\\\\Bromium\\\\.*",
            ".*\\\\Application\\ Data\\\\RockMelt\\\\.*",

            # Custom Filters - temsec
            ".*\\\\Cookies\\\\\index\.dat$",
            ".*\\\\Yandex\\\\.*",
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
        ]

        for indicator in indicators:
            if self.check_file(pattern=indicator, regex=True):
                return True

        return False
```

Π.6.2 Πηγαίος Κώδικας Κλάσης infostealer.py

Κατάλογος εγκατάστασης: cuckoo/modules/signatures/
Όνομα αρχείου: infostealer_ftp.py

```
# Copyright (C) 2012 Claudio "nex" Guarnieri (@botherder)
#
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program.  If not, see <http://www.gnu.org/licenses/>.

from lib.cuckoo.common.abstracts import Signature

class FTPStealer(Signature):
    name = "infostealer_ftp"
    description = "Harvests credentials from local FTP client softwares"
    severity = 3
    categories = ["infostealer"]
    authors = ["nex"]
    minimum = "0.5"

    def run(self):
        indicators = [
            ".*\\\\CuteFTP\\\\sm\.dat$",
            ".*\\\\FlashFXP\\\\.*\\\\Sites\.dat$",
            ".*\\\\FlashFXP\\\\.*\\\\Sites\.dat$",
            ".*\\\\FileZilla\\\\sitemanager\.xml$",
            ".*\\\\FileZilla\\\\recentservers\.xml$",
            ".*\\\\VanDyke\\\\Config\\\\Sessions.*",
            ".*\\\\FTP Explorer\\\\.*"
            ".*\\\\SmartFTP\\\\.*",
            ".*\\\\TurboFTP\\\\.*",
            ".*\\\\FTPRush\\\\.*",
            ".*\\\\LeapFTP\\\\.*",
            ".*\\\\FTPGetter\\\\.*",
            ".*\\\\ALFTP\\\\.*",

            # Custom Filters - temsec
            ".*\\\\3D-FTP\\\\.*",
            ".*\\\\BlazeFtp\\\\.*",
            ".*\\\\SiteDesigner\\\\.*",
            ".*\\\\BulletProof Software\\\\.*",
            ".*\\\\Global Downloader\\\\.*",
            ".*\\\\Directory Opus\\\\.*",
            ".*\\\\RhinoSoft.com\\\\.*",
            ".*\\\\Frigate3\\\\.*",
            ".*\\\\FTPInfo\\\\.*",
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
            ".*\\\\Cyberduck\\\\.*",
            ".*\\\\IPswitch\\\\WS_FTP\.*",
            ".*\\\\FileZilla FTP Client\\\\.*",
            ".*\\\\FlashFXP 4\\\\.*",
            ".*\\\\FlashFXP 3\\\\.*",
            ".*\\\\BitKinex\\\\.*",
            ".*\\\\Visicom Media\\\\.*",
            ".*\\\\NovaFTP\\\\.*"

        ]

        for indicator in indicators:
            if self.check_file(pattern=indicator, regex=True):
                return True

        return False
```

Π.6.3 Πηγαίος Κώδικας Κλάσης infogather.py

Κατάλογος εγκατάστασης: cuckoo/modules/processing/
Όνομα αρχείου: infogather.py

```
import os
import re
import sys
import socket
import logging
import subprocess

from bulkwhois.shadowserver import BulkWhoisShadowserver
from urllib2 import Request, urlopen, HTTPError, URLError
from urlparse import urlunparse, urlparse

from lib.cuckoo.common.utils import convert_to_printable
from lib.cuckoo.common.abstracts import Processing
from lib.cuckoo.common.config import Config
from lib.cuckoo.common.dns import resolve
from lib.cuckoo.common.objects import File
from lib.cuckoo.common.exceptions import CuckooProcessingError

try:
    import dpkt
    IS_DPKT = True
except ImportError:
    IS_DPKT = False

class Pcap:

    def __init__(self, filepath):
        self.filepath = filepath

        # List containing all IP addresses involved in the analysis.
        self.unique_hosts = []
        # List containing all TCP packets.
        self.tcp_connections = []
        # List containing all UDP packets.
        self.udp_connections = []
        # List containing all HTTP requests.
        self.http_requests = []
        # Dictionary containing all the results of this processing.
        self.results = {}

    def _add_hosts(self, connection):
        try:
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
            if connection["src"] not in self.unique_hosts:
                self.unique_hosts.append(convert_to_printable(connection["src"]))
            if connection["dst"] not in self.unique_hosts:
                self.unique_hosts.append(convert_to_printable(connection["dst"]))
        except Exception:
            return False

        return True

    def _check_http(self, tcpdata):
        try:
            r = dpkt.http.Request()
            r.method, r.version, r.uri = None, None, None
            r.unpack(tcpdata)
        except dpkt.dpkt.UnpackError:
            if r.method != None or r.version != None or r.uri != None:
                return True
            return False

        return True

    def _add_http(self, tcpdata, dport):
        try:
            http = dpkt.http.Request()
            http.unpack(tcpdata)
        except dpkt.dpkt.UnpackError:
            pass

        try:
            entry = {}

            if "host" in http.headers:
                entry["host"] = convert_to_printable(http.headers["host"])
            else:
                entry["host"] = ""

            entry["port"] = dport
            entry["data"] = convert_to_printable(tcpdata)
            entry["uri"] = convert_to_printable(urlunparse(("http", entry["host"],
http.uri, None, None, None)))
            entry["body"] = convert_to_printable(http.body)
            entry["path"] = convert_to_printable(http.uri)

            if "user-agent" in http.headers:
                entry["user-agent"] = convert_to_printable(http.headers["user-
agent"])

            entry["version"] = convert_to_printable(http.version)
            entry["method"] = convert_to_printable(http.method)

            self.http_requests.append(entry)
        except Exception:
            return False

        return True

    def _tcp_dissect(self, conn, data):
        if self._check_http(data):
            self._add_http(data, conn["dport"])

    def run(self):
        log = logging.getLogger("Processing.Pcap")

        if not IS_DPKT:
            log.error("Python DPKT is not installed, aborting PCAP analysis.")
            return None
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
        if not os.path.exists(self.filepath):
            log.warning("The PCAP file does not exist at path \"%s\"." %
self.filepath)
            return None

        if os.path.getsize(self.filepath) == 0:
            log.error("The PCAP file at path \"%s\" is empty." % self.filepath)
            return None

        try:
            file = open(self.filepath, "rb")
        except (IOError, OSError):
            log.error("Unable to open %s" % self.filepath)
            return None

        try:
            pcap = dpkt.pcap.Reader(file)
        except dpkt.dpkt.NeedData:
            log.error("Unable to read PCAP file at path \"%s\"." % self.filepath)
            return None
        except ValueError:
            log.error("Unable to read PCAP file at path \"%s\". File is corrupted or
wrong format." % self.filepath)
            return None

        for ts, buf in pcap:
            try:
                eth = dpkt.ethernet.Ethernet(buf)
                ip = eth.data

                connection = {}
                if isinstance(ip, dpkt.ip.IP):
                    connection["src"] = socket.inet_ntoa(ip.src)
                    connection["dst"] = socket.inet_ntoa(ip.dst)
                elif isinstance(ip, dpkt.ip6.IP6):
                    connection["src"] = socket.inet_ntop(socket.AF_INET6, ip.src)
                    connection["dst"] = socket.inet_ntop(socket.AF_INET6, ip.dst)

                self._add_hosts(connection)

                if ip.p == dpkt.ip.IP_PROTO_TCP:

                    tcp = ip.data

                    if len(tcp.data) > 0:
                        connection["sport"] = tcp.sport
                        connection["dport"] = tcp.dport
                        self._tcp_dissect(connection, tcp.data)
                        self.tcp_connections.append(connection)
                    else:
                        continue
                elif ip.p == dpkt.ip.IP_PROTO_UDP:
                    udp = ip.data

                    if len(udp.data) > 0:
                        connection["sport"] = udp.sport
                        connection["dport"] = udp.dport
                        self.udp_connections.append(connection)

            except AttributeError:
                continue
            except dpkt.dpkt.NeedData:
                continue

        file.close()
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
        # Build results dict.
        self.results["hosts"] = self.unique_hosts
        self.results["tcp"] = self.tcp_connections
        self.results["udp"] = self.udp_connections
        self.results["http"] = self.http_requests

        # Whois Module
        whoisdata = []

        try:
            if self.unique_hosts:
                    for ipz in self.unique_hosts:
                        whoisdata.append(ipz)
                        bulk_whois = BulkWhoisShadowserver()
                        records = bulk_whois.lookup_ips([ipz])

                        for record in records:
                            whoisdata.append([records[record]["ip"],
records[record]["asn"], records[record]["bgp_prefix"] ,records[record]["as_name"],
records[record]["cc"], records[record]["register"], records[record]["org_name"]])

        except  ValueError as e:
            raise CuckooProcessingError("Whois Failed")

        self.results["whoisdata"] = whoisdata

        # Url Matcher
        urlzcheck = []
        user_agent = 'Mozilla/20.0.1 (compatible; MSIE 5.5; Windows NT)'
        headers = { 'User-Agent':user_agent }

        try:
            if self.http_requests:
                for x in self.http_requests:
                        urlz = x['uri']
                        segment = urlz.rpartition('/')
                        link = segment[0] + "/includes/password_modules.php"
                        urlzcheck.append("URL: " + urlz)
                        req = Request(link, headers = headers)
                        try:
                                page_open = urlopen(req)
                        except HTTPError, e:
                                urlzcheck.append("Nothing Found")
                        except URLError, e:
                                urlzcheck.append("Nothing Found")
                        else:
                                urlzcheck.append("Pony Infostealer Found: " + link)

        except  ValueError as e:
            raise CuckooProcessingError("Url Matcher Failed")

        self.results["urlzcheck"] = urlzcheck

        return self.results

class infogather(Processing):

    def run(self):
        self.key = "infogather"

        results = Pcap(self.pcap_path).run()

        return results
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Π.6.4 Πηγαίος Κώδικας Αρχείου infogather.html

Κατάλογος εγκατάστασης: cuckoo/data/html/sections/
Όνομα αρχείου: infogather.html

```
<section id="infogather">
    <div class="section-title">
        <h4>Information Gathering</h4>
    </div>

    {% if results.infogather %}
        {% if results.infogather.whoisdata %}
            <div>
                <h4><a href="javascript:showHide('whoisdata');">Whois
Details</a></h4>
                <div id="whoisdata" style="display: none;">
                    <table class="table table-striped table-bordered">
                        <tr>
                            <th>IP Addresses:</th>
                        </tr>
                        {% for whois in results.infogather.whoisdata %}
                        <tr>
                            <td><span class="mono">{{whois}}</span></td>
                        </tr>
                        {% endfor %}
                    </table>
                </div>
            </div>
        {% endif %}

        {% if results.infogather.urlzcheck %}
            <div>
                <h4><a href="javascript:showHide('urlzcheck');">URL
Signatures</a></h4>
                <div id="urlzcheck" style="display: none;">
                    <table class="table table-striped table-bordered">
                        <tr>
                            <th>Results:</th>
                        </tr>
                        {% for urlz in results.infogather.urlzcheck %}
                        <tr>
                            <td><span class="mono">{{urlz}}</span></td>
                        </tr>
                        {% endfor %}
                    </table>
                </div>
            </div>
        {% endif %}

    {% else %}
        Nothing to display.
    {% endif %}
</section>
```

Π.6.5 Πηγαίος Κώδικας Αρχείου report.html

Κατάλογος εγκατάστασης: cuckoo/data/html/
Όνομα αρχείου: report.html

```
{% extends "base-report.html" %}
{% block content %}
    {% include "sections/info.html" %}
    {% include "sections/errors.html" %}
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

```
    {% if results.info.category == "file" %}
        {% include "sections/file.html" %}
    {% elif results.info.category == "url" %}
        {% include "sections/url.html" %}
    {% endif %}
    {% include "sections/signatures.html" %}
    {% include "sections/screenshots.html" %}
    {% if results.info.category == "file" %}
        {% include "sections/static.html" %}
    {% endif %}
    {% include "sections/dropped.html" %}
    {% include "sections/network.html" %}
    {% include "sections/infogather.html" %}
    {% include "sections/pcapflow.html" %}
    {% include "sections/behavior.html" %}
{% endblock %}
```

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ