ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΟΛΙΤΙΣΜΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΣ

Π Τ Υ Χ Ι Α Κ Η Ε Ρ Γ Α Σ Ι Α

ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ: Μορφές, Δυνατότητες, Περιορισμοί

Θυμιάνης Νικόλαος Α.Μ. 131/2011047

Επιβλέπων Καθηγητής : Δρ. Καλλονιάτης Χρήστος
(Επίκουρος Καθηγητής)

ΣΕΠΤΕΜΒΡΙΟΣ 2015
ΜΥΤΙΛΗΝΗ

Στους Γονείς μου,

Ευχαριστίες

Η ενότητα αυτή γράφτηκε τελευταία. Πρέπει όμως να διαβαστεί πρώτα από όλα τα κεφάλαια γιατί ανταποκρίνεται σε όλες τις προσπάθειες που χρειάστηκαν για την ολοκλήρωση της πτυχιακής αυτής.

Νιώθω μεγάλη ευγνωμοσύνη στον επιβλέποντα καθηγητή μου κ. Καλλονιάτη Χρήστο για την αμέριστη βοήθεια και εμπιστοσύνη που μου επέδειξε παράλληλα με την επιστημονική επίβλεψη και καθοδήγηση που μου παρείχε. Το συνεχές ενδιαφέρον του και η εύστοχη καθοδήγησή του υπήρξαν ουσιαστικά στοιχεία για την ολοκλήρωση της παρούσας πτυχιακής.Μέσα από την καρδιά μου ένα μεγάλο ευχαριστώ.

Τον θαυμασμό μου και την ευγνωμοσύνη για την άριστη στάση απέναντι μου εκφράζω στον καθηγητή μου κύριο Αναγνωστόπουλο Χρήστο-Νικόλαο με τον οποίο εργάστηκα στο εργαστήριο Ευφυών Πολυμέσων και Εικονικής Πραγματικότητας και έδωσε κίνητρο για περισσότερο ζήλο σ' αυτή την πτυχιακή.

Επιπλέον τον τρόπο έρευνας τον οφείλω στους ερευνητές Παπαμαρτζίβανο, Τσιάτσικα και Φάκη από τους οποίους διδάχτηκα πολλά για την εικονική πληροφορική(VirtualComputing) στο σεμινάριο IPICS 2015.

Τέλος μεγάλη θα χαρακτήριζα την βοήθεια του καθηγητή Στέφανου Γκρίτζαλη ο οποίος, με την τεράστια εμπειρία του μου δώσε στόχους και προβλέψεις για το μέλλον μου.

Νικόλαος Θυμιάνης

Περιεχόμενα

Περίληψη

Μια από τις σημαντικότερες προκλήσεις στο χώρο της πληροφορικής είναι η αντιμετώπιση και η πρόληψη των κακόβουλων απειλών που βλάπτουν τα πληροφοριακά συστήματα . Αυτές οι απειλές παίρνουν την μορφή κακόβουλου λογισμικού(malicioussoftware), το οποίο επηρεάζει την εμπιστευτικότητα(confidentiality), ακεραιότητα(integrity) ή διαθεσιμότητα(availability) του συστήματος και μερικές φορές μπορεί και όλα μαζί.

Οι ερευνητικές περιοχές που ασχολούνται με την ανάλυση, αντιμετώπιση και πρόληψη αυτών των κακόβουλων απειλών ανήκουν στον κλάδο της Ασφάλειας Δικτύου(NetworkSecurity). Από την δημιουργία ενός ενιαίου δικτύουόπως το ξέρουμε σήμερα αυτές οι απειλές έχουν λάβει παγκόσμιες διαστάσεις.

Στο πλαίσιο της παρούσας πτυχιακής:

- Διερευνήθηκαν οι τύποι κακόβουλου λογισμικού και έγινε μια εκτενής ανάλυση του κάθε τύπου.
- Παρουσιάστηκε μια ιστορική αναδρομή σχετικά με το κακόβουλο λογισμικό.
- Αναλύθηκαν οι τύποι ιομορφικού λογισμικού μαζί με έρευνα που έγινε στα πλαίσια ενόςεικονικού συστήματος(Sandboxes).
- Παρουσιάστηκε το δημιουργημένο υλικό της έρευνας το οποίο και χρησιμοποιήθηκε στην ανάλυση.
- Αναλύθηκε ένα χειροκίνητος τρόπος αντιμετώπισης του κακόβουλου λογισμικού.
- Προτάθηκε ένας νέος τρόπος πρόληψης του κακόβουλου λογισμικού.

- Αναφέρθηκαν οι αδυναμίες του κακόβουλου λογισμικού που αναλύθηκε.

Executive Summary

A major challenge in the area of Computer Science is the confrontation and prevention of malicious threats that harm the computer systems. Those threats take the form of malicious software (malware), whichinfluences confidentiality, integrity and availability and sometimes altogether.

The Scientific Areas concerned withthe analysis confrontation and prevention of these threats belong to Network Security. Since the beginning of the Internet as we know it malware have been the talk of the world.

In the context of this thesis:

- Research has been conducted regarding the types of malicious software and there has been a extensive analysis of each type.
- A historical recursion was made.
- The types of viral software were analyzedwith research that worked in the context of a virtual system (Sandboxes).
- A manual way of malicious software confrontation was analyzed.
- A new way of malicious software prevention was proposed.
- The weaknesses of the malicious software were reported.

ΛίσταΕικόνων

Λίστα Πινάκων

1 Εισαγωγή

Η ακόλουθη πτυχιακή εργασία, αφορά το Κακόβουλο Λογισμικό, το οποίο απασχολεί ιδιαίτερα τόσο την επιστημονική κοινότητα, όσο και τους υπεύθυνους διαχείρισης Πληροφοριακών Συστημάτων, λόγω της μεγάλης εξάπλωσής του.[1]

Συγκεκριμένα, γίνεται εκτενής αναφορά στο Ιομορφικό λογισμικό και την αντιμετώπιση του.

Η πτυχιακή εργασία αποτελείται από 4 κεφάλαια.

Το κεφάλαιο 1 ξεκινά με τον ορισμό του Κακόβουλο Λογισμικού. Παρουσιάζεται μία κατηγοριοποίηση του κακόβουλου λογισμικού, με περισσότερη ανάλυση στην κατηγορία του Μη Ιομορφικού Λογισμικού. Αναλύονται τα οκτώ είδη του Μη Ιομορφικού λογισμικού, με ορισμό και παραδείγματα.

Στο κεφάλαιο 2, ορίζεται το ιομορφικό λογισμικό, οι τύποι του, και παρουσιάζονται αντίστοιχα παραδείγματα.

Στο Κεφάλαιο 3, γίνεται αναφορά στους τρόπους αντιμετώπισης των παραδειγμάτων του κεφαλαίου 2.

Τέλος, στο κεφάλαιο 4, αναφέρονται συμπεράσματα και προτείνονται κατευθύνσεις μελλοντικής ερευνητικής δραστηριότητας.

[1] Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

1.1. Τι είναι το Κακόβουλο Λογισμικό;

Σύμφωνα με τον Ηλιάδη:«κακόβουλο λογισμικό ορίζεται το λογισμικό που περιέχει τις απαιτούμενες εντολές για μια επίθεση σ' ένα υπολογιστικό σύστημα.»

Βασικόείναι, προσθέτει, ότι ο όρος «Κακόβουλο λογισμικό»(malicious software) δεν είναι απολύτως δόκιμος. Κακώς βουλόν λογισμικό σημαίνει ότι το λογισμικό έχει δικιά του βούληση πράγμα που πιθανώς δεν γίνεται διότι αναφερόμαστε σε άψυχη οντότητα και ούτε μπορούμε να αναφερθούμε στις κακές προθέσεις του προγραμματιστή που το δημιούργησε για να αιτιολογήσουμε ένα τύπο λογισμικού. Τέλος, αυτός ο ορισμός μας προβάλει το εξής ερώτημα: Τι είναι μια επίθεση σ' ένα υπολογιστικό σύστημα;

Ο Ηλιάδης προσθέτει ότι «επίθεση σ' ένα υπολογιστικό σύστημα είναι η παραβίαση της εμπιστευτικότητας , ακεραιότητας , ή διαθεσιμότητας ενός συστήματος».[2]

Σύμφωνα με το University of California: «Κακόβουλο Λογισμικό είναι το λογισμικό που παρέχει πλήρη ή εν μέρει έλεγχο ενός υπολογιστικού συστήματος με σκοπό να επιτελέσει τους δόλιους σκοπούς του δημιουργού του. Τέλος προσθέτει ότι το κακόβουλο λογισμικό δεν περιορίζεται σ' ένα υπολογιστικό σύστημα μόνο αλλά μπορεί να εισβάλει και σε όλόκληρο δίκτυο.»[3]

Τέλος σύμφωνα με τη Technopedia: « Κακόβουλο Λογισμικό γνωστό και ως «malware» είναι κάθε λογισμικό που βλάπτει το υπολογιστή ή τον χρήστη. Μερικές μορφές κακόβουλου λογισμικού κατασκοπεύουν την

[2]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[3]http://www.seas.ucla.edu/security/malware.html Ορισμός Κακόβουλου Λογισμικού, UCLA Engineering, 03/03/2015

κίνηση των χρηστών στο Internet. Άλλες μορφές μπορούν να πολλαπλασιάζονται και να υπομονεύουν ένα ολόκληρο υπολογιστικό σύστημα Αυτές οι μορφές μπορούν επίσης να κάνουν λειτουργίες χωρίς την αντίληψη του χρήστη. Έτσι τα προγράμματα αντιμετώπισης κακόβουλου λογισμικού πρέπει να στοχεύουν στην πρόληψη και όχι στην διόρθωση των συστημάτων που προσβλήθηκαν από κακόβουλο λογισμικό.»[4]

[4]http://www.techopedia.com/definition/4015/malicious-software-malware , Ορισμός Κακόβουλου Λογισμικού, Technopedia, 03/03/2015).

1.2. Τύποι κακόβουλου λογισμικού

Το κακόβουλο λογισμικό χωρίζεται αρχικά σε λογισμικό που χρειάζεται ξενιστή και σε λογισμικό που δεν χρειάζεται ξενιστή. Έπειτα μπορεί να χωριστεί ανάλογα με το αν αναπαράγει τον εαυτό του ή όχι. Σύμφωνα με τον Ηλιάδη το κακόβουλο λογισμικό χωρίζεται στις παρακάτω κατηγορίες: κερκόπορτες(backdoors), λογικές βόμβες (logicalbombs), ιούς(viruses) Δούρειοι Ίπποι(Trojanhorses), Βακτήρια (Bacteria) και Αναπαραγωγοί(worms).[5] Από την άλλη όμως η VeraCodeπροσθέτει σ' αυτές τις κατηγορίες και τους διαφημιστές(adware), το Σφάλμα (bug), τους Κατασκόπους (spyware) , τα «Rootkit»και τους Λυτροαποδόχους(ransomware).[6]

Λόγω του γεγονότος ότι οι ιοί έχουν πολλές και διάφορες κατηγορίες, ο Ηλιάδης κάνει άλλη μια κατηγοριοποίηση χωρίζοντάς το λογισμικό σε ιομορφικό και το μη ιομορφικό.[7]Παραθέτεται επίσης και ένα διάγραμματης Kapresky με τις κατηγορίες κακόβουλου λογισμικού ξεκινώντας από τον τύποεπίθεσης που σχεδιάζει ο επιτιθέμενος να πράξει και τις κατηγορίες κακόβουλου λογισμικού που θα χρησιμοποιήσει για να αρχίσει την επίθεση του. Το διάγραμμα δεν είναι τυπική διαδικασία.[8]

Στην συνέχεια θα γίνει ανάλυση καθενός από τους τύπους μη ιομορφικού λογισμικού μαζί με ένα παράδειγμα για το καθένα.

---

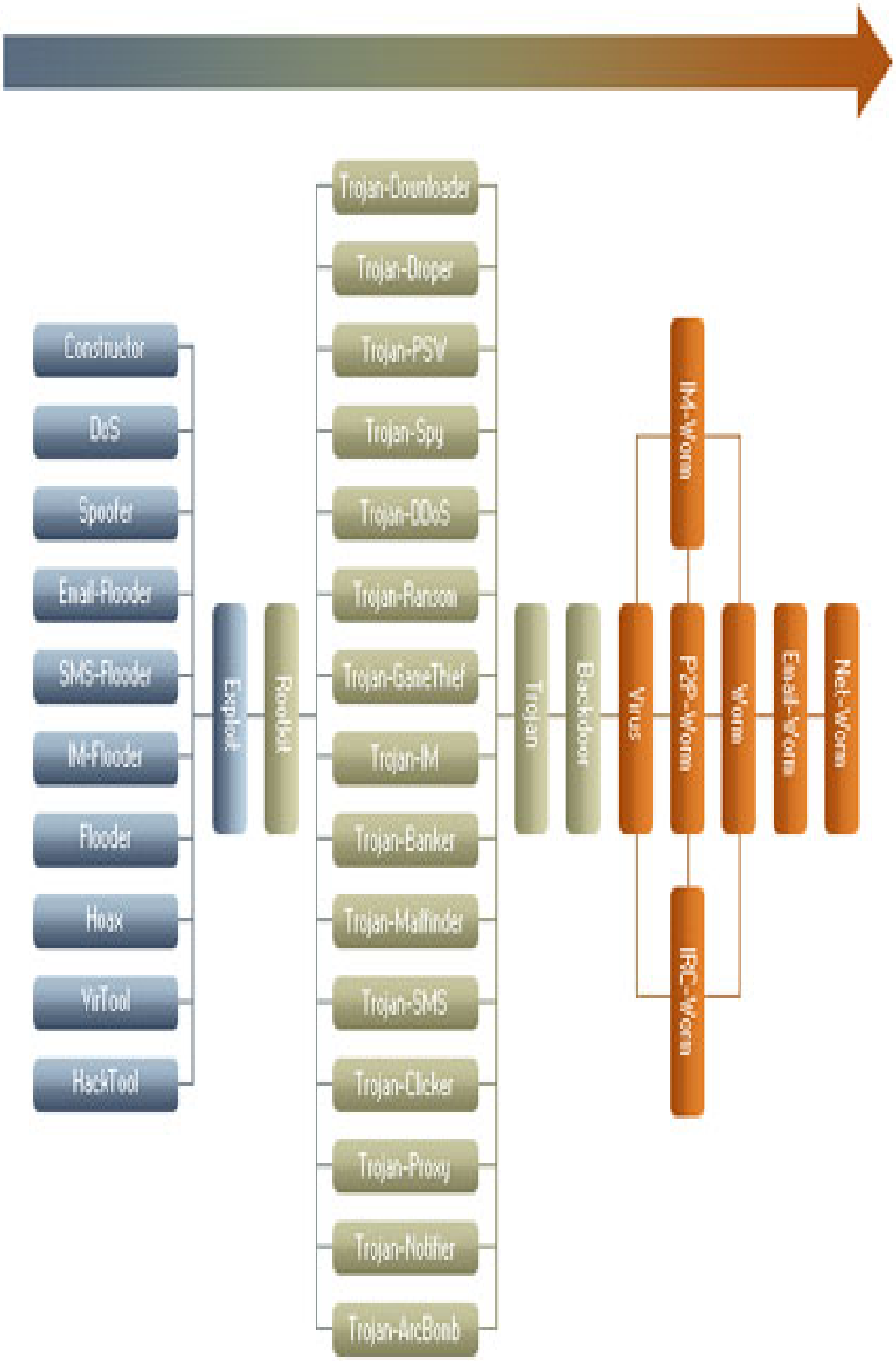
[5] Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[6]https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101 , 10/05/2015

[7] Παρόμοια και στο 57

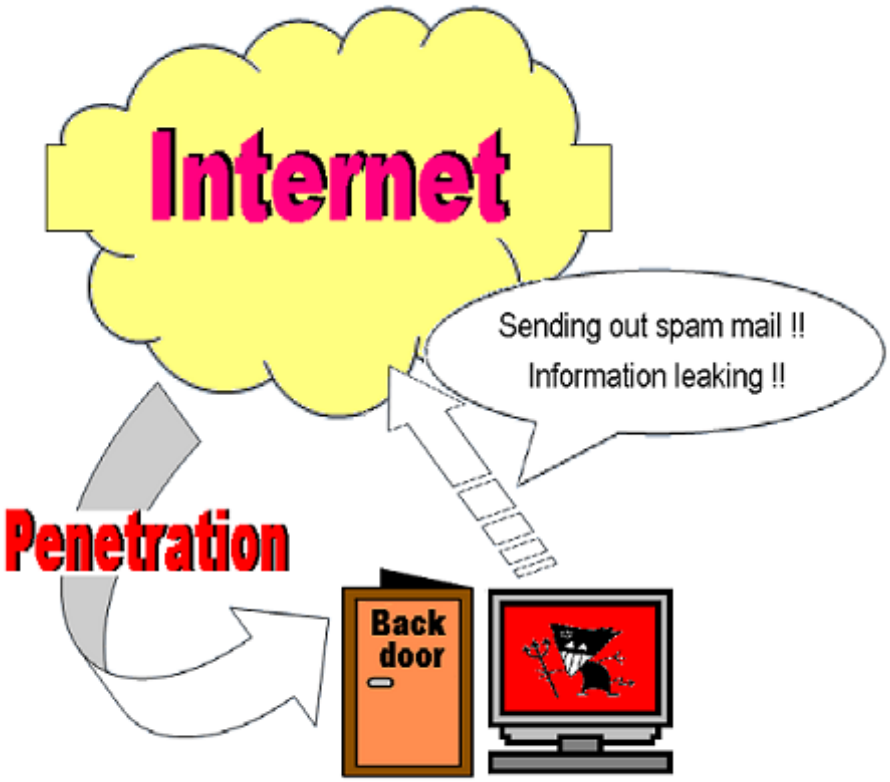
[8]http://www.kaspersky.com/internet-security-center/threats/malware-classifications, 10/05/2015

Σχήμα 1. Σχεδιάγραμμα Κακόβουλου Λογισμικού(Kapresky)



1.2.1 Κερκόπορτες (Backdoors/Trapdoors)

Οι Κερκόπορτες είναι μη ιομορφικό λογισμικό καιδεν απαιτούν ξενιστή. Σύμφωνα με τον Ηλιάδη, «είναι σημεία εισόδου που παρακάμπτουν τη συνηθισμένη διαδικασία πρόσβασης ασφάλειας επιτρέποντας την πρόσβαση σ' ένα σύστημα.» [9]



Εικόνα 1 Κερκόπορτα λειτουργία

Σύμφωνα με το ComputerHope ο όρος κερκόπορτα αναφέρεται σε μια κρυφή μέθοδο η οποία επιτρέπει σ' έναν κακόβουλο χρήστη να ελέγξει τον υπολογιστή στον οποίο αυτή τοποθετήθηκε. Τεχνικά, ένας προγραμματιστής μπορεί να τοποθετήσει ένα κομμάτι κώδικα ο οποίος

[9] Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

να του επιτρέψει την πρόσβαση σ' έναν υπολογιστή ή μια ασφαλή τοποθεσία μ' έναν κωδικό που μόνο ο ίδιος γνωρίζει. [10] Μας δημιουργείται η απορία: Ποιος μπορεί να είναι ο κακόβουλος χρήστης και προγραμματιστής;

Ο Edwards απαντά χρησιμοποιώντας ένα αρχαίο ρητό «Quis custodiet ipsos custodes?» δηλαδή ποιος επιθεωρεί τους ίδιους τους επιθεωρητές; Με αυτό τον τρόπο θέλει να δείξει ότι για όλα φταίνε οι τεχνικοί ασφάλειας, οι οποίοι μπορεί και να έχουν παραβιάσει το σύστημα τοποθετώντας για δική τους πρόληψη απόλυσης, μία κερκόπορτα.[11] Ο Ηλιάδης όμως αντιτίθεται σ' αυτή την άποψη, αναφέροντας πως οι προγραμματιστές χρησιμοποιούν κερκόπορτες για νομότυπους σκοπούς, κατά τις διαδικασίες ελέγχου και αποσφαλμάτωσης των εφαρμογών που κατασκευάζουν.

Όμως, από την άλλη πλευρά οι κακόβουλοι επιτιθέμενοι, θα χρησιμοποιήσουν την αδυναμία αυτή του συστήματος για να επιτεθούν. Επίσης, οι hackers έχοντας δοκιμάσει να εισέλθουν στο σύστημα, ως συνήθως προτιμούν να αφήσουν μια κερκόπορτα, η οποία θα τους επιτρέψει την είσοδο σε μελλοντικό χρόνο.[12]

Στο σημείο αυτό αναφερόμαστε σε ένα γνωστό παράδειγμα κερκόπορτας που αφορά την Sendmailτου λειτουργικού συστήματος BerkeleyUnix, όπως αναλύθηκε στην SANS.

HSendmailείναιμιαεφαρμογήτηςUnixηοποίαχρησιμοποιούσετηνSMTP(SimpleMailTransferProtocol) ή αλλιώς Port 25 και ήταν πάντα το θύμα για πολλούς hackers. Η Sendmailλοιπόν έστελνε τα μηνύματα από τις ιστοσελίδες σε εφαρμογές αντί σε αρχεία εισερχομένων. Χρησιμοποιώντας την εντολή Debugτης εφαρμογής επέτρεπε την

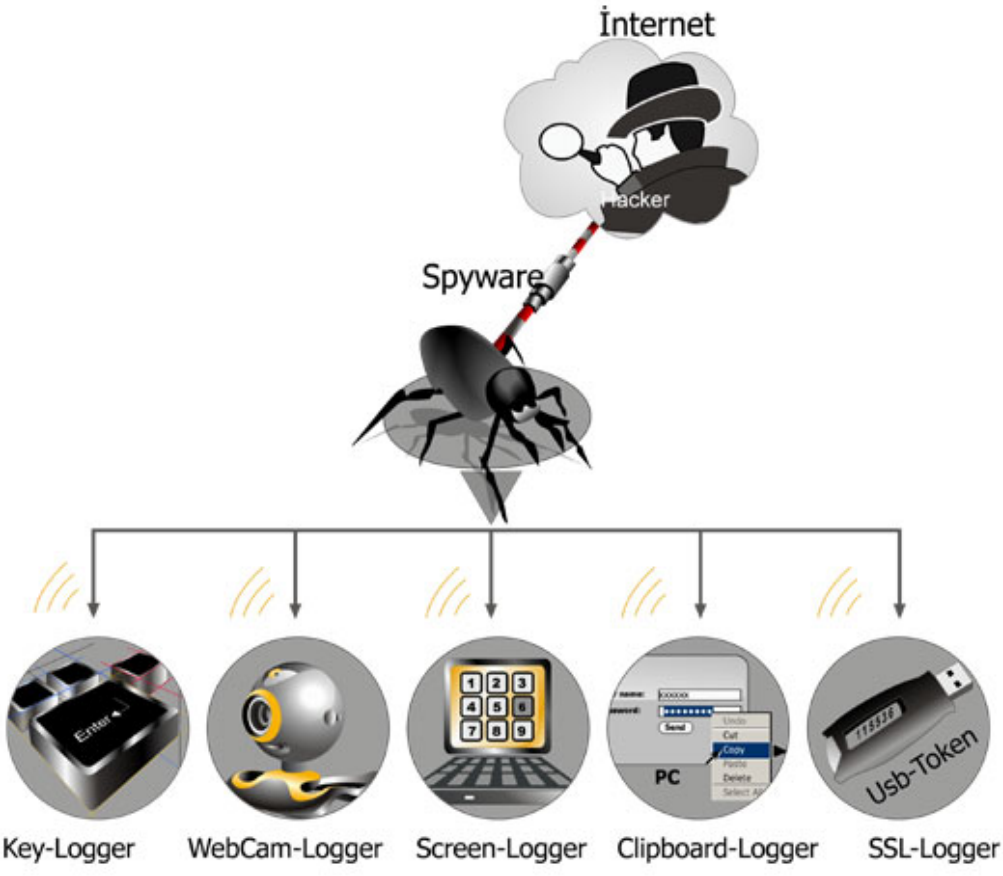
[10] http://www.computerhope.com/jargon/b/backdoor.htm, 28/07/2015
[11] http://www.itsecurity.com/features/trapdoors-backdoors-103007/ 18/05/2015
[12] Παρόμοια και στο 80

πρόσβαση στο σύστημα Sendmailμε την χρήση γραμμής εντολών αντί την χρήση χρήστη και κωδικού. Έτσι ο επιτιθέμενος μπορούσε να στείλει γραμμές εντολών για να εκτελεστούν στον υπολογιστή ο οποίος θα λάμβανε το email. Η έρευνα όμως συνεχίζει αποτυπώνοντας το γεγονός ότι τελικά δεν φταίνε οι προγραμματιστές της συγκεκριμένης αλλά ο Μεταγλωττιστής (compiler)που τοποθέτησε αυτόματα την παραπάνω λειτουργία. [13]

[13]http://www.sans.edu/research/security-laboratory/article/log-bmb-trp-door#__utma=21257146.1574720757.1433083109.1433083109.1433083109.1&__utmb=21257146.6.9.1433083269726&__utmc=21257146&__utmx=-&__utmz=21257146.1433083109.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)&__utmv=-&__utmk=15162085821/5/2015

1.2.2 Πράκτορες(Spyware)

Οι πράκτορες(Spyware) είναι μη ιομορφικό λογισμικό και δεν αναπαράγονται. Πράκτορες,ονομάζονται τα λογισμικά εκείνα, που συλλέγουν πληροφορίες και τις μεταβιβάζουν σ' ένα δεύτερο χρήστη, τον επιτιθέμενο. Οι πληροφορίες μπορεί να περιλαμβάνουν ένα ημερολόγιο ενεργειών (audit trail) ακόμα και ποιες ιστοσελίδες επισκέφθηκε ο χρήστης, τι κωδικούς και ονόματα χρήστη έδωσε, κ.λπ. Συνήθως τέτοιου είδους προγράμματα χρησιμοποιούνται για διαφημιστικούς σκοπούς. Όμως κατά το ήμισυ αυτά τα προγράμματα χρησιμοποιούνται για την διάδοση κακόβουλου λογισμικού ή γενικώς την διάδοση πληροφοριών οι οποίες πωλούνται από τον κακόβουλο χρήστη.



Εικόνα 2 Spyware Λειτουργία

Υπάρχουν πολλά παραδείγματα αλλά θαγίνει αναφορά στο πως λειτουργεί ένας τέτοιος τύπος λογισμικού. Το λογισμικό αυτό λοιπόν προσπαθεί να παραμένει εγκατεστημένο στοπαρασκήνιο, δηλαδή να μην γίνεται αντιληπτό από τον χρήστη. Υπάρχουν περιπτώσεις που αυτό το λογισμικό κάνει στοχευόμενες διαφημίσεις στις οποίες αν ο χρήστης τις δεχτεί υπάρχει περίπτωση να προσβληθεί. Στην συνέχεια αλλάζει τις επιλογές στο πρόγραμμα περιήγησης(browser) του χρήστη. Τέλος επικοινωνεί μόνο του με το Internet.

Σύμφωνα με τον Cadrette, το ότι οι χρήστες εγκαθιστούν προγράμματα τέτοιου τύπου οικειοθελώς οφείλεται στο γεγονός ότι ποτέ δεν διαβάζουν τη άδεια που υπάρχει μαζί μ' ένα εγκατεστημένο πρόγραμμα. Πολλές φορές όταν γίνεται για διαφημιστικούς σκοπούς το spyware αναγράφεται στην άδεια, πολλές φορές πάλι όχι, τότε είναι που πρέπει να παρέχεται μεγαλύτερη προσοχήαπό τους χρήστες.[14]

Όπως αναφέρει ο Skoudis, οι ενέργειες που κάνει ένα τέτοιο κακόβουλο λογισμικό είναι οι ακόλουθες:

- Αλλαγή στις επιλογές δικτύου
- Απενεργοποιεί τα αντιβιοτικά λογισμικά και τα λογισμικά antispyware.
- Απενεργοποιούν τις αυτόματες ενημερώσεις λογισμικού και το κέντρο ασφάλειας της Microsoft.
- Εγκαθιστά ψεύτικα πιστοποιητικά
- Υπερχείλισηαρχείων(Cascading File Dropper)
- Καταμέτρηση πληκτρολόγησης
- Παρακολούθηση κίνησης στο Internet, αντιγραφή φόρμας και αποστολή print-screen
- Ενεργοποιεί την κάμερα ή/και το μικρόφωνο

[14]https://www.sans.org/search/results01/06/2015

- Παριστάνει το αντιβιοτικό πρόγραμμα
- Αλλάζει τα αποτελέσματα αναζήτησης
- Μεταδίδει αυτόκλητα μηνύματα
- Τοποθετεί rootkit για να αποτρέψει την διαγραφή του
- Δημιουργεί ένα bot το οποίο μπορεί ο επιτιθέμενος να χειριστεί
- Λαμβάνει προσωπικά έγγραφα τα οποία επιθυμεί ο επιτιθέμενος
- Τοποθετεί έναν ανιχνευτή(sniffer)[15]

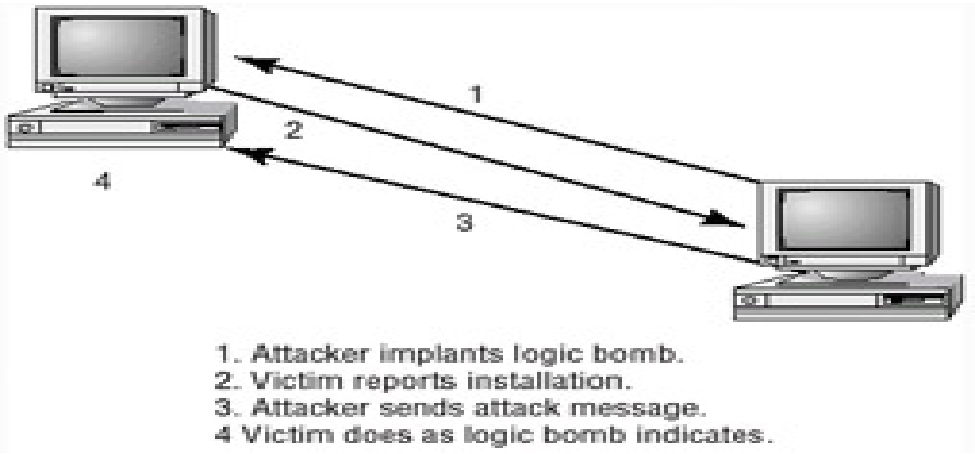
Παραδείγματα τέτοιου τύπου λογισμικού είναι το Gator[16], CoolWebSearch[17], InternetOptimizer[18], κτλ.

[15] http://www.sans.org/security-resources/top15_mal_spyware.php, 01/06/2015
[16] http://download.cnet.com/Gator/3000-18501_4-10785.html, 26/07/2015
[17] http://download.cnet.com/CWShredder/3000-8022_4-10301587.html, 26/07/2015
[18] http://www.downloadcrew.com/article/23452-auslogics_internet_optimizer,26/07/2015

1.2.3 Λογικές Βόμβες (Logical Bombs)

Οι λογικές Βόμβες είναι μη ιομορφικό λογισμικό και δεν αναπαράγονται. Θεωρούνται προγράμματα τα οποία εκτελούν μια εντολή παραβιάζοντας την πολιτική ασφάλειας ενός συστήματος, όταν βέβαια πληρείται συγκεκριμένη λογική συνθήκη, όπως για παράδειγμα, συγκεκριμένη χρονική στιγμή.[19]

Συμφωνα με τον Robillard, οι λογικές βόμβες έχουν 2 φάσεις λειτουργίας, πρώτον η πυροδότηση και η σειρά λειτουργιών του κακόβουλου λογισμικού τα οποία θα αναφερθούν παρακάτω.



Εικόνα 3 Λειτουργία Λογικής Βόμβας

Όσον αφορά στην πυροδότηση, μία ομοιότητα που έχουν οι λογικές βόμβες με τις κανονικές βόμβες, μπορεί να λάβει τις παρακάτω μορφές. Πρώτον ως συνθήκη μπορεί να λάβει κάποια ημερομηνία & ωρά. Δεύτερον κάποια αντίστροφη μέτρηση. Επίσης μπορεί να την ενεργοποιήσει ένα τρίτο πρόγραμμα όπως το WindowsSchedulerκαι άλλα. Αυτού του είδους οι λογικές βόμβες φτιάχνονται εύκολα αφού ο κώδικας πυροδότησης υπάρχει ήδη. Επίσης υπάρχει και η επαναφορά(Reset), όπου

[19] Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

ο επιτιθέμενος διατηρεί την βόμβα σε κατάσταση επώασηςπληρώντας κάποιες προϋποθέσεις. Τέλος η αλλαγή κατάστασης δεδομένων, για παράδειγμα η διαγραφή ενός ατόμου από την λίστα προσωπικού μιας εταιρίας και στην συνέχεια επιτελείται η σειρά ενεργειών της λογικής βόμβας.

Ο Robillard επίσηςαναφέρει ότι «μπορούμε να φανταστούμε και άλλους μηχανισμούς πυροδότησης όπως ένα σύστημα εισαγωγής πλήκτρων στο οποίο αν πατηθεί μια συγκεκριμένη αλληλουχία πλήκτρων ενεργοποιείται η σειρά ενεργειών του κακόβουλου λογισμικού. Η φαντασία του δυσαρεστημένου εργαζόμενου είναι το όριο στο τι μπορεί να αποτελέσει τύπο πυροδότησης γι' αυτό να είσαι έτοιμος για οτιδήποτε.»

Η σειρά ενεργειών αναφέρει ο Robillard, μπορεί να κυμαίνεται από την πιο απλή εντολή, όπως «format c:/autotest» (αυτή η εντολή έχει πάψει να υφίσταται από τα Windows 2000 και έπειτα)ή κάτι πιο διακριτικό όπως η αλλαγή μιας συγκεκριμένης εισαγωγής στην βάση δεδομένων της επιχείρησης που θα είναι αρκετά δύσκολο να εντοπιστεί μετέπειτα. Επιπλέον αναφέρει και θέματα πρόσβασης των υπαλλήλων σε συγκεκριμένα αρχεία τα οποία μπορούν να τροποποιούν σε αόριστο χρόνο. Επίσης αναφέρεται στο ότι όταν κάποιος ψάχνει να βρει μια λογική βόμβα θα ήταν βέλτιστο να ψάχνει σε αρχεία που μπορούν να έχουν πρόσβαση οι υπάλληλοί του.

Τέλος αναφέρει ότι «όταν μιλάμε για πρόσβαση ενός χρήστη μιλάμε και για πρόσβαση που μπορεί να λάβει και μέσω άλλων μέσων. Οι υπάλληλοι δεν θα έχουν ως στόχο μόνο κρίσιμα συστήματα, όπως τη βάση δεδομένων προσωπικού αλλά συστήματα με λιγότερη σημασία που μπορεί να ωφελήσουν το μέλλον της επιχείρησης, για παράδειγμα

μπορούν να αλλάξουν τις ρυθμίσεις του δικτύου της επιχείρησης, μπλοκάροντας έτσι την επικοινωνία μεταξύ των χρηστών του δικτύου».[20]

Ένα καλό παράδειγμα λογικής βόμβας είναι ο ιός της Ιερουσαλήμ(Jerusalem Virus) στους υπολογιστές της DOS. Ο ιός αυτός έσβηνε αρχεία κάθε Τρίτη και 13. Μόλις μόλυνε έναν υπολογιστή γινόταν κάτοικος της μνήμης(memory resident) καταλαμβάνοντας 2Kb της μνήμης. Έπειτα μόλυνε κάθε εκτελέσιμο αρχείο εκτός από το COMMAND.COM. Η μόλυνση έκανε τα εκτελέσιμα αρχεία .EXE να μεγαλώνουν έως ότου να μην μπορούν πλέον να εκτελεσθούν. Επιπλέον το πρόγραμμα σταματούσε την επεξεργασία και άλλες χαμηλού επιπέδου λειτουργίες στην DOS. Ένα από τα στοιχεία ότι ένας υπολογιστής έχει μολυνθεί είναι η λάθασμένα γραμμένη εμφάνιση του μηνύματος "Bad command or filename" που γράφεται "Bad Command or filename". Η καταστροφική σειρά ενεργειών του κάθε Τρίτη και 13 διέργαφε κάθε εκτελέσιμο αρχείο που εκτελούταν.[21]

[20] https://www.sans.org/search/results 01/06/2015

[21] https://en.wikipedia.org/wiki/Jerusalem_%28computer_virus%29#Mendoza_.28Jerusalem_Mendoza.29 10/06/2015

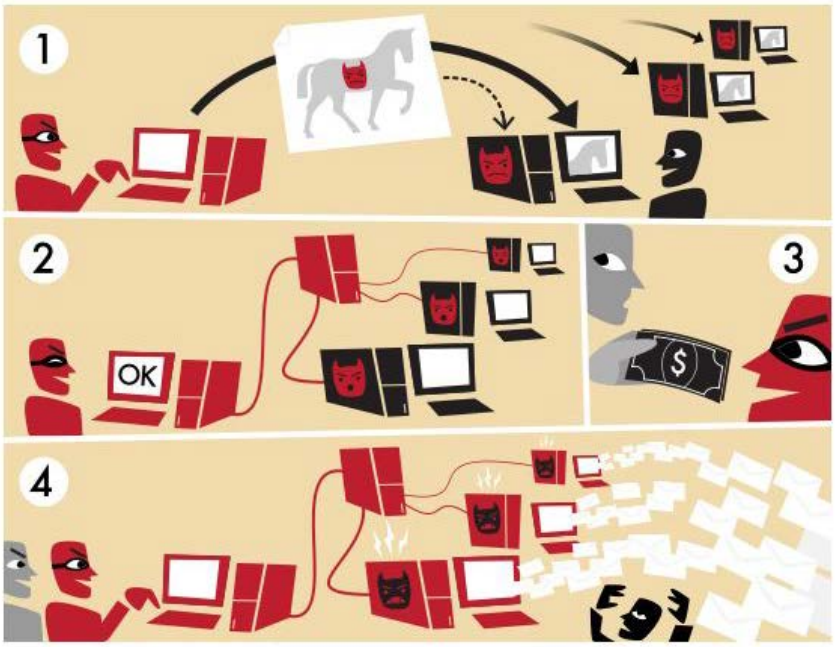
1.2.4 Τρωικοί/Δούρειοι Ίπποι(Trojan Horses)

Οι Τρωικοί/Δούρειοι Ίπποι είναι μη ιομορφικό λογισμικό και δεν αναπαράγονται. Σύμφωνα με τονSummers: «οιδούρειοι ίπποι είναι «φαινομενικά» χρήσιμα προγράμματαπου περιλαμβάνουν κρυφές λειτουργίες, οι οποίες μπορούν να εκμεταλλευτούν τα δικαιώματα του χρήστη που εκτελεί το πρόγραμμα με συνέπεια μια απειλή στην ασφάλεια. Ένας Δούρειός Ίππος εκτελεί λειτουργίες που ο χρήστης του δεν σκόπευε.»[22]

Επιπλέον, η Jamie Crapanzano αναφέρει πως οι τρωικοί ίπποι είναι από τα παλαιότερα όπλα των hacker, συγκεκριμένα των script-kiddies, που χρησιμοποιούν για να προκαλέσουν χάος στον Κυβερνοχώρο. Όπως και ο Ηλιάδης, κάνει μνεία ότι η Τρωικοί ίπποι είναι προγράμματα που παριστάνουν τα χρήσιμα ή διασκεδαστικά αλλά από πίσω μπορεί να βρίσκονται είτε ιοί (;) είτε RATs.

Η Carpanzano στην συνέχεια αναφέρειότι όχι μόνο ο επιτιθέμενος που έστειλε το μήνυμα με τον τρωικό ίππο, αλλά και άλλοι επιτιθέμενοι με την χρήση θυρών (ports) μπορούν να εκμεταλλευτούν τον μολυσμένο χρήστη.Ένας τρωικός ίππος με λειτουργία απομακρυσμένου ελέγχου(RAT) είναι ένα σταθερό πρόγραμμα που δεν αναπαράγεται αλλά εκτελεί αόρατα εντολές από τον επιτιθέμενο. Ένας τρωικός ίππος που υφίσταται στο Internet και τον κατεβάζεις εύκολα, αναφέρει η Carpanzano, είναι το SubSeven, λογισμικό που κατασκευάστηκε από τον hacker Mobman.

[22]Summers, Rita, Secure Computing Threats and Safeguards, McGraw-Hill, 1997.



Εικόνα 4 Λειτουργία Τρωικού Ίππου

Το SubSeven είναι ένα λογισμικό που αποτελείται από τρία προγράμματα, το SubSeven εξυπηρετητή, τον πελάτη, και τέλος την επεξεργασία του εξυπηρετητή. Το πρώτο πρόγραμμα πρέπει να ενεργοποιηθεί από το στοχευόμενο υπολογιστή έτσι ώστε να ενεργοποιήσει το σύστημα του Τρωικού Ίππου και να επιτραπεί στον πελάτη (επιτιθέμενο) να εκτελέσει εντολές. Η επεξεργασία εξυπηρετητή επιτρέπει στον επιτιθέμενο να εκτελέσει διάφορες εντολές, για παράδειγμα, το σύστημα του στοχευόμενου υπολογιστή στέλνει ένα email στον επιτιθέμενο κάθε φορά που ο υπολογιστής βρίσκεται στο Internet, και άλλες τέτοιες εντολές.

Η μετάδοση του SubSeven γίνεται μέσω email. Ο επιτιθέμενος στέλνει το email παρακινώντας τον χρήστη να το ανοίξει. Επίσης μόλυνση μπορεί να γίνει εάν υπάρχουν ανασφάλιστοι τομείς του σκληρού δίσκου

τις οποίες μπορεί να εκμεταλλευτεί ο επιτιθέμενος. Και καθώς ο χρήστης ενεργοποιεί τον τρωικό ίππο και βλέπει το μήνυμα που στόχο έχει να τον παραπλανήσει, ο επιτιθέμενος λοιπόν τοποθετεί τα αρχεία του ιού στους σωστούς καταλόγους (directories) και αλλάζει το μητρώο του μολυσμένου υπολογιστή έτσι ώστε να ενεργοποιείται ο τρωικός ίππος κάθε φορά που ο χρήστης ανοίγει τον υπολογιστή. Στο παραπάνω σενάριο ο χρήστης είναι ανυποψίαστος για την μόλυνση που γίνεται στον υπολογιστή του.[23]

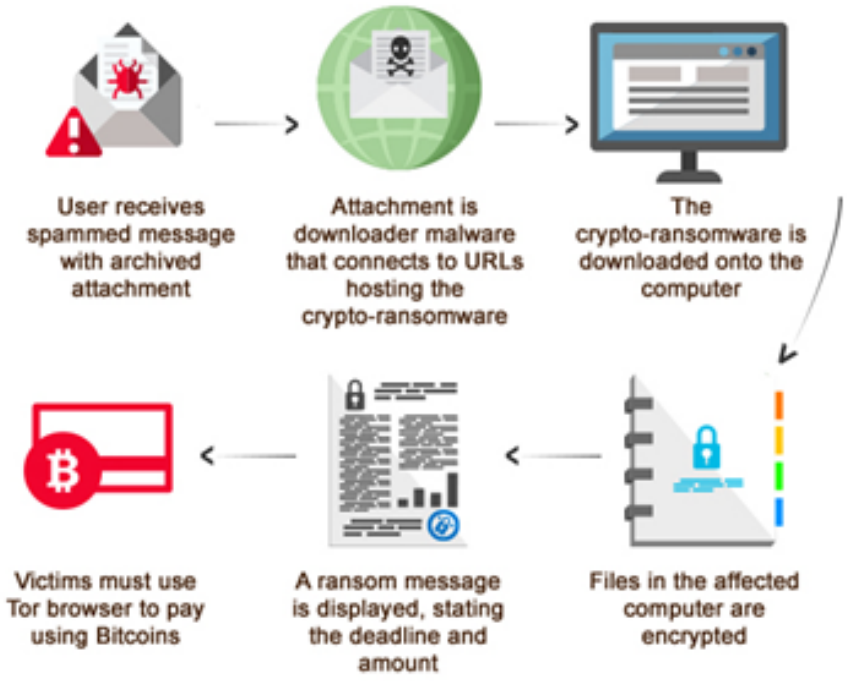
[23]https://www.sans.org/search/results 19/06/2015

1.2.5 Απαγωγείς (Ransomware)

Το Ransomwareείναι μη ιομορφικό λογισμικό και δεν αναπαράγεται. ToRansomware,ήαλλιώς απαγωγέας, είναι ένα κακόβουλο λογισμικό, που περιορίζει ή αποτρέπει την πρόσβαση του χρήστη στο υπολογιστικό σύστημα και ζητάει λύτρα για την επαναχρησιμοποίηση του ή την επιστροφή των αρχείων του χρήστη στην αρχική τους κατάσταση.

Η τιμή των λύτρων κυμαίνεται από21 ευρώ έως 540 ευρώ ανάλογα με το λογισμικό. Βέβαια η αποπληρωμή των λύτρων δεν εγγυάται τίποτα.

Αυτού του είδους το κακόβουλο λογισμικό λέγεται ότι έχει τις ρίζες του στην Ρωσία.[24]



Εικόνα 5ΛειτουργίαCryptorlocker

Και ενώ λέγεται ότι η κρυπτογραφία για πολύ καιρό αποτελούσε ένα σύστημα άμυνας των χρηστών από τους κακόβουλους χρήστες, τώρα αυτοί οι χρήστες, το χρησιμοποιούν για να αποσπάσουν χρήματα από

[24]http://www.trendmicro.com/vinfo/us/security/definition/ransomware 19/06/2015

τους μη-κακόβουλους χρήστες.[25] Βασικό παράδειγμα τέτοιου είδους αποτελεί το Cryptorlocker.

Το Cryptorlocker, αποτελεί ένα πρόγραμμα, το οποίο λαμβάνει όλα τα αρχεία ενός χρήστη είτε αυτά βρίσκονται σε εξωτερικούς ή onlineκαταλόγους (directories) και τα κρυπτογραφεί,ζητώντας από τον χρήστη να πληρώσει ένα ποσό σε λύτρα για να λάβει το κλειδί αποκρυπτογράφησης. Βέβαια η πληρωμή των λύτρων με κανέναν τρόπο δεν εγγυάται το ότι θα δοθεί ένα κλειδί που να λειτουργεί ή ότι θα δοθεί ένα κλειδί.

Θα πρέπει επίσης να γίνει σαφές ότι το υπολογιστικό σύστημα που έχει μολυνθεί, δεν θα κατεβάσει αμέσως το Cryptorlocker. Μπορεί να περάσει ακόμα και μία μέρα από τότε που ο υπολογιστής θα εμφανίσει τα μηνύματα τουCryptorlockerγια λύτρα. Έτσι αυτό που πρέπει να γίνει είναι να διαγνωστεί ο υπολογιστής ότι είναι μολυσμένος όσο το δυνατόν γρηγορότερα και να αντιμετωπιστεί προτού προξενήσει τα παραπάνω συμπτώματα.[26]

[25] http://vxheaven.org/lib/pdf/Future%20Trends%20in%20Malicious%20Code%20-%202006%20Report.pdf 19/06/2015

[26] https://blog.cisecurity.org/cis-cyber-alert/ 20/06/2015

1.2.6 Αναπαραγωγοί (Worms)

Το μη ιομορφικό λογισμικό των αναπαραγωγών (Worms) αποτελεί προγράμματα που μεταφέρονται από υπολογιστή σε υπολογιστή δημιουργώντας αντίγραφα του εαυτού τους χωρίς να απαιτούν ξενιστή.

Ο Ηλιάδης αναφέρει, ότι οι αναπαραγωγοί μεταφέρονται μέσω των ηλεκτρονικών μηνυμάτων και του βιβλίου διευθύνσεων του μολυσμένου χρήστη. Στην συνέχεια δημιουργεί μια σύνδεση με το απομακρυσμένο σύστημα που βρήκε στο βιβλίο διευθύνσεων. Τέλος δημιουργεί ένα αντίγραφο στο σύστημα το όποιο βρήκε εκεί και αυτό εκτελεί την σειρά εντολών που προοριζόταν να εκτελέσει, για παράδειγμα αλλοίωση αρχείων κλπ και επαναλαμβάνει τον παραπάνω κύκλο.[27]

Αν και πολλοί συγκρίνουν αυτού του τύπου λογισμικού με τους ιούς υπολογιστών, οι διαφορές τους είναι πολύ μεγάλες. Αρχικώς ο ιός θεωρείται ένα τμήμα λογισμικού ενώ ο αναπαραγωγός ένα εξ ολοκλήρου λογισμικό. Επίσης ο αναπαραγωγός δεν χρειάζεται την καθοδήγηση ενός ψηφιακού εγκληματία , ακολουθεί τον κώδικα του και αναπαράγεται κατά «βούληση».[28]

Θα γίνει αναφορά σ' έναν αναπαραγωγό του 2003 τον Sobig ο οποίος μόλυνε εκατομμύρια υπολογιστές. Ο Sobigλοιπόν μεταφερόταν μέσω emailκαι παρίστανε ένα καλό emailόπως: Re: WickedScreensaverκλπ άρα έμοιαζε και μ' έναν τρωικό ίππο. Στην συνέχεια αυτό που έκανε ήταν να χρησιμοποιεί τον μολυσμένο υπολογιστή για την αποστολή εκατομμυρίων spamμηνυμάτων τα οποία είχε συνημμένο το αρχείο του αναπαραγωγού. Χρησιμοποιούσε αρχεία που περιείχαν διευθύνσεις ηλεκτρονικού ταχυδρομείου. Έτσι δημιουργώντας πανικό στις εταιρίες, η Microsoftτον Νοέμβριο του 2003 ζητούσε πληροφορίες για τον δημιουργό

[27] Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[28] http://www.pctools.com/security-news/what-is-a-computer-worm/ 29/06/2015

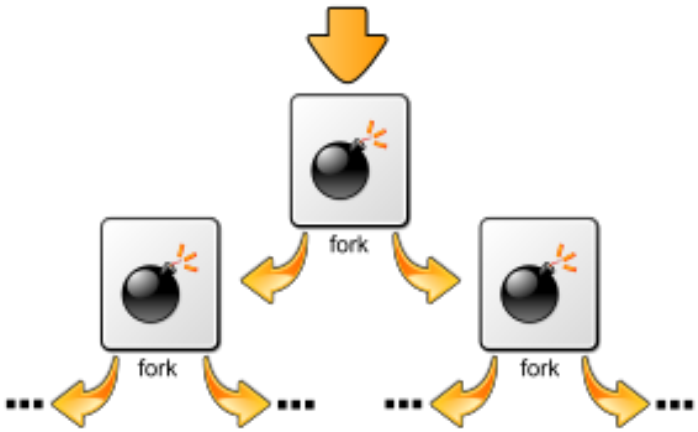
του Sobigπληρώνοντας ένα ποσό 250.000$. Μέχρι σήμερα όμως ο επιτιθέμενος δεν έχει αποκαλυφθεί [29]

[29] https://en.wikipedia.org/wiki/Sobig, 26/07/2015

1.2.7 Βακτήρια (Bacteria)

Όπως και οι αναπαραγωγοί έτσι και τα βακτήρια είναι μη ιομορφικά λογισμικά που αναπαράγονται χωρίς την ύπαρξη ξενιστή. Ο Ηλιάδης αναφέρει ότι το λογισμικό αυτό δεν αλλοιώνει τα δεδομένα του μολυσμένου υπολογιστή αλλά μόνος στόχος του είναι η αναπαραγωγή του σε επιμέρους αντίγραφα. Καταναλώνοντας πολλούς πόρους του συστήματος σε μεγάλο βαθμό, τα βακτήρια μειώνουν τη διαθεσιμότητα του συστήματος. Σε αντίθεση με τους υπόλοιπους τύπους κακόβουλου λογισμικού τα βακτήρια προσβάλουν τη διαθεσιμότητα και όχι την ακεραιότητα του συστήματος.[30]

Ένα καλό παράδειγμα αυτού του τύπου κακόβουλου λογισμικού, είναι το Rabbit/Wabbit (1978) το οποίο ήταν ένα λογισμικό που πολλαπλασιαζόταν δύο φορές κάθε φορά που εκτελούταν μέχρι που μπλόκαρε τον υπολογιστή και λειτουργούσε σε πολύ αργούς ρυθμούς ή ακόμα και καθόλου. Επίσης παράδειγμα αποτελεί και το Forkbombπου κάνει ακριβώς ότι και το Rabbit/Wabbit.[31]



Εικόνα 6 Λειτουργία Fork Bomb

[30] Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[31] http://jazz.he.fi/jargon/html/W/wabbit.html 29/06/2015

1.2.8 Adware (Διαφημιστές)

Τα adware ή διαφημιστές είναι μη ιομορφικάλογισμικά και δεν αναπαράγονται. Αυτόματα στέλνουν διαφημίσεις για προϊόντα. Συχνά παραδείγματα adwareαποτελούν τα επικαλυπτόμενα παράθυρα διαφημίσεων τα οποία αν ο χρήστης πατήσει τις υπερσυνδέσεις τους τότε μολύνεται από ένα τέτοιου είδους λογισμικό ειδικά όταν πρόκειται για δωρεάν προγράμματα. Ένα adwareόμως μόνο του εκτός από την ενόχληση που μπορεί να προκαλέσει στον χρήστη, μπορεί να συμπεριλαμβάνει και ένα spyware, για το οποίο αναφερθήκαμε παραπάνω. [32]

Παράδειγμα ενός adware αποτελεί τοZangoτο οποίο έχει επίσης τα ονόματα Hotbarκαι 180solutions, και είναι ένα από τα επικρατέστερα adware. Βέβαια η εταιρία που το δημιούργησε αρνήθηκε οποιαδήποτε κακόβουλη επισύναψη του λογισμικού της και έκανε μήνυση στην FTC. Η FederalTableCommission όμως αναφέρει πως το λογισμικό εγκαθιστούσε άλλα adwarekαι απέτρεπε την διαγραφή του από τους χρήστες παραβιάζοντας τον νόμο.

Το Zango είχε όμως μερικά ανεπιθύμητα χαρακτηριστικά:

[32]https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101 , 29/06/2015

- Το Zango Easy Messenger, λέγεται ότι λειτουργούσε ως spyware.
- ToZango Cash Toolbar, είχε μερικά links σε βίντεο από το youtube τα οποία φιλοξενούνταν σε ιστοσελίδες οι οποίες ήταν γεμάτες spyware.
- Τα προγράμματα της Zango χαρακτηρίστηκαν PUPs(PotentiallyUnwantedPrograms) από διάφορα ProgramVendors.[33]

Στην συνέχεια θα γίνει εκτενής αναφορά σε σημαντικά ιστορικά παραδείγματα κακόβουλου λογισμικού.

[33]http://www.spamlaws.com/zango-adware.html, 29/06/2015

1.3. Ιστορία Κακόβουλου Λογισμικού

Η αρχή του κακόβουλου Λογισμικού μπορεί να τοποθετηθεί το 1949 όταν ο επιστήμονας John Von Neumann(1903-1957) ανέπτυξε την θεωρία των ρομπότ που μπορούσαν να πολλαπλασιάζονται. Φυσικά οι λεπτομέρειες της τεχνικής αυτής της εφαρμογής δεν μπορούσαν να νοηθούν αυτήν την περίοδο.

Στην συνέχειααπό το 1970 και έπειτα αναπτύχθηκε στην πληροφορική ένα παιχνίδι το Core Wars όπου προγράμματα γραμμένα στην γλώσσα Redcode πολεμούν μεταξύ τους.Σκοπός αυτών των προγραμμάτων είναι η επιβίωση στην μονάδα της μνήμης(memory area). Όμως τα αποκαλούμενα «ερεθίσματα» σβήνουν κομμάτια της μνήμης στην τύχη. Επίσης υπάρχουν μερικές παραλλάγες των Core Wars όπου τα προγράμματα πολλαπλασιάζονται. Εδώ λοιπόν βρίσκονται οι ρίζες για το λογισμικό των ιών υπολογιστών.[34]

Την δεκαετία του ’70, εμφανίστηκε ο ιός Creeper,ο οποίος όταν μόλυνε ένα υπολογιστικό σύστημα εμφάνιζε ένα μήνυμα το οποίο προκαλούσε το χρήστη να «πιάσει τον Creeper». Δημιουργημένο ως πείραμα ο Creeper δεν δημιουργούσε καμία βλάβη στο σύστημα αλλά ήταν μια πρόβλεψη για το τι επρόκειτο να ακολουθήσει. Το πρόγραμμα Reaper, το πρώτο θα λέγαμε antivirus ήταν ο μόνος τρόπος αντιμετώπισης του Creeper.

Επίσης την ίδια περίοδο ο πρώτος τρωικός ίππος απελευθερώνεται. Ένα πρόγραμμα το “ANIMAL”, το οποίο μόλις ενεργοποιούνταν μπορούσε να μεταφέρεται σ’ όλους τους υπολογιστές ενός δικτύου πολλαπλασιάζοντας τον εαυτότου ενώ ο χρήστης που το ενεργοποιούσε έπαιζε ένα παιχνίδι εικασιών.

[34]https://www.gdata-software.com/security-labs/information/history-of-malware, 04/04/2015

Το 1975 ο όρος «worm» πρωτοεμφανίζεται στο βιβλίο επιστημονικής φαντασίας του John Brunner, Shockwave Rider με την ερμηνεία ως ένα πρόγραμμα που πολλαπλασιάζεται μέσω ενός υπολογιστικού δικτύου.

Την δεκαετία του 1980 αναπτύσσεται το πρώτο πρόγραμμα RAT(Remote Administration Tool) με όνομα SubSeven το οποίο είναι ένα κακόβουλο λογισμικό τύπου κερκόπορτας αλλά και τρωικός ίππος το οποίο εγκαθίσταται από hacker για να μπορούν να ελέγχουν τους υπολογιστές. Αναπτύχθηκε από τον hacker Mobman ο οποίος ήθελε να κάνει εύκολη την εμπειρία του hacking και έτσι διέδωσε αυτό το πρόγραμμα μέχρι που το 1995 απαγορεύτηκε από τα Ηνωμένα Έθνη. [35]

Το 1981 ο ιός Elk Cloner για τους υπολογιστές Apple 2 δημιουργείται. Ο Elk Cloner μεταφερόταν μέσω δισκέτας και εμφάνιζε ένα χλευαστικό ποίημα που το είχε γράψει ο δημιουργός του

Αξίζει να αναφερθούμε και στην δημιουργία του πρωτόκολλου Internet το 1982.Έτσι το κακόβουλο λογισμικό απέκτησε τάσεις εισόδου στο δίκτυο και δημιουργούνταν πλέον λογισμικό που μεταφερόταν από υπολογιστή σε υπολογιστή.

Το 1983, σε μια νουβέλα του Frederick Cohen, ο όρος ιός υπολογιστών χρησιμοποιείται για να περιγράψει ένα πρόγραμμα υπολογιστή. Έτσι λοιπόν ξεκίνησε να χρησιμοποιείται ο όρος και στην επιστημονική βιβλιογραφία. Στο ίδιο έτοςυπήρξε και ένας τρωικός ίππος για τους υπολογιστές της IBM ο ARF-ARF, ο οποίος ισχυριζόταν ότι θα τακτοποιούσε τον τομέα της δισκέτας στην DOS, πράγμα επιθυμητό διότι η DOS δεν έβαζε τα αρχεία σε αλφαβητική σειρά το 1983. Αντίθετα όμως μόλις ενεργοποιούνταν έσβηνε όλα τα αρχεία στην δισκέτα καθάριζε την οθόνη και έγραφε ARFπροερχόμενο από τις λέξεις Abort, Retry Fail λέξεις

[35]http://www.elite-hackers.com/hacking-tools/sub7, 12/04/2015

που εμφανίζονταν όταν δεν μπορούσε ο υπολογιστής να κάνει επανεκκίνηση από τη δισκέτα.

Τον Ιανουάριο του 1986 ο Basit Farooq Alvi ένας προγραμματιστής μόλις 19 χρονών και ο αδερφός του ο Amijad δημιούργησαν τον πρώτο ιό για υπολογιστές της IBM, τον Brain, ο οποίος επηρέαζε τις δισκέτες, τις έκανε να αργούν υπερβολικά και επηρέαζε tobootsectorτης μνήμης RAM. Ήταν ο πρώτος κρυφός ιός που όταν τον έβρισκε ο χρήστης ο ιός έδινε την διεύθυνση του δημιουργού του. Τον Δεκέμβριο του ίδιου έτους, ο Ralf Burger παρουσίασε το μοντέλο προγραμμάτων Virdem στο Chaos Computer Club της Γερμανίας. Τα Virdem ήταν τα πρώτα προγράμματα που μπορούσαν να προσθέσουν τον κώδικα τους σε εκτελέσιμα αρχεία COM της DOS και να πολλαπλασιάζονται δηλαδή οι πρώτοι ιοί όπως τους γνωρίζουμε σήμερα.

Το 1987 έχουμε την εμφάνιση του ιού Vienna ο οποίος ακολούθως εξουδετερώθηκε, γεγονός που συνέβει για πρώτη φορά στα συστήματα της IBM. Έχουμε την εμφάνιση του ιού Lehigh, ο οποίος εμφανίστηκε στο ομώνυμο πανεπιστήμιο, και άλλους ιούς που επηρέαζαν τον τομέα εκκίνησης όπως ο Yale στις Ηνωμένες πολιτείες, ο Stoned στην Νέα Ζηλανδία, ο ιός PingPong στην Ιταλία και τέλος ο πρώτος αναπαραγωγικός ιός αρχείων Cascade. Ο Lehigh όπως και ο Yale αντιμετωπίστηκαν στα Πανεπιστήμια και δεν εξαπλώθηκαν περαιτέρω. Την ίδια περίοδο ένας προγραμματιστής στο Tel Aviv έκανε πειράματα για την δημιουργία ιών. Ο πρώτος του ιός ήταν ο suriv-01 ο οποίος λειτουργούσε στον τομέα της μνήμης και προσέβαλε όποιοδήποτε αρχείο με κατάληξη COM. Ο δεύτερος ο suriv-02 ήταν ο πρώτος ιός που μόλυνε και τα αρχεία EXE. Ο επόμενος suriv-03 μόλυνε και τα COM και τα EXE αρχεία. Στην τέταρτη αυτή προσπάθεια έχουμε τη δημιουργία της λογικής βόμβας με όνομα Jerusalem ή αλλιώς Omega. Σχεδιάστηκε για να

προσβάλει τον τομέα εκκίνησης χωρίς να δημιουργεί περαιτέρω βλάβες στον υπολογιστή. Μόνο κάθε Παρασκευή και 13 δεν επέτρεπε την εκκίνηση του υπολογιστή και έσβηνε ότι αρχείο εκτελούνταν. Συνεχίζει να υπάρχει ακόμα και σήμερα σε διαφορετικές μορφές και με χειρότερες επιπτώσεις όπως την διαγραφή αρχείων. Ο συγκεκριμένος ιός όμως δεν μόλυνε το αρχείο COMMAND.COM διότι οι χρήστες εκείνη την περίοδο το παρακολουθούσαν πολύ. Ανακαλύφθηκε τέλος στο Πανεπιστήμιο της Ιερουσαλήμ από τον Yisrael Adai και έτσι πήρε έτσι το όνομα ιός Jerusalem. Καθώς λοιπόν συνέβαιναν όλα αυτά ο ιός Stoned στην Νέα Ζηλανδία δημιουργείται από ένα φοιτητή στο Πανεπιστήμιο του Wellington και είναι πολύ αποτελεσματικός. Μια φορά στις οκτώ όταν γινόταν εκκίνηση από μία μολυσμένη δισκέτα έγραφε το μήνυμα «ο υπολογιστής σου είναι τώρα μαστουρωμένος», και έτσι έλαβε το όνομα Stoned. Ο συγκεκριμένος ιός λόγω της αυτοάμυνας του με τον πολλαπλασιασμό του στο τομέα μνήμης λέγεται ότι ήταν ένας από τους πιο διαδεδομένους ιούς στον κόσμο, με πολλά ξεσπάσματα μέχρι και το 1993. Θεωρούταν απίθανο ο ιός Stoned να γίνει σπάνιος λόγω του βαθμού εξάπλωσής του. Στην συνέχεια, ένας Γερμανός προγραμματιστής έφτιαξε τον ιό Cascade ένα δύσκολα αντιμετωπίσιμο ιό διότι δεν επέτρεπε την αποκρυπτογράφηση του κώδικα του και έτσι δεν μπορούσε ν' αντιμετωπιστεί εύκολα. [36]

Το 1988 ο αναπαραγωγός Morris εξαπλώνεται μέσω του Internet σε όλο τον κόσμο, ξεκινώντας με 600 υπολογιστές στις Ηνωμένες πολιτείες που βρέθηκαν σε πλήρη παράλυση.[37]

[36] http://users.uoa.gr/~nektar/science/technology/a_brief_history_of_viruses.htm , 05/04/2015

[37] http://scholar.google.gr/scholar_url?url=http://arxiv.org/pdf/1302.5392&hl=el&sa=X&scisig=AAGBfm22e2pB2g3ZJprOl5pCZaXz83R5SA&nossl=1&oi=scholarr&ei=XhEQVdWQLtbgatmsgtgG&ved=0CB4QgAMoADAA , 4/4/2015

Το 1990 ο Mark Washborn, δουλεύοντας σε μια ανάλυση κακόβουλου Λογισμικού, δημιούργησε τον πρώτο πολυμορφικό ιό «χαμαιλέοντα» με όνομα 1260. Επίσης το 1990 έχουμε την δημιουργία ιών στην Βουλγαρία από τον γνωστό Dark Avenger. Οι ιοί του Dark Avenger έφεραν στην επιφάνεια δυο νέες ιδέες. Η πρώτη ιδέα είναι η «Γρήγορη Μόλυνση(Fast infector)», δηλαδή αν ο ιός βρίσκεται στην μνήμη τότε μόλις κάποιος για παράδειγμα άνοιγε ένα αρχείο για ανάγνωση, η μόλυνση ξεκινούσε. [38]

Μετά μερικά χρόνια, το 1992, έχουμε τον Michelangelo που όπως και ο ιός Jerusalem, είναι μια λογική βόμβα που δρούσε στα γενέθλια του γνωστού ζωγράφου Μιχαήλ Άγγελου δηλαδή στις 6 Μαρτίου. Έκανε επανεγγραφές τους πρώτους εκατό τομείς του σκληρού δίσκου και δεν επέτρεπε την εκκίνηση του υπολογιστή, σβήνοντας και τον πίνακα κατανομής αρχείων. Την ίδια χρονιά εμφανίστηκαν και άλλοι ιοί με πιο σημαντικούς τους Vsign, Walker, Ambulance και Casino, οι οποίοι επηρέαζαν τον τομέα εκκίνησης χρησιμοποιώντας ένα οπτικό μέσο που χαρακτήριζε το όνομα του καθενός. Επιπλέον έσβηναν τον πίνακα κατανομής αρχείων όταν ο χρήστης έσβηνε τον υπολογιστή. Όλοι οι παραπάνω ιοί μεταδίδονταν με την βοήθεια αρχείων.

Το 1994 έχουμε τη πρώτη παραπλανητική πληροφόρηση (hoax) για τον ιό GoodTimes, ο οποίος δεν υπήρχε απλά το emailπου τον μετέφερε λέγεται ότι προήλθε από το CultoftheDeadCowσαν μια άσκηση για να αποδείξουν την ευπιστία τους ως αυτοαποκαλούμενοι «ειδικοί» στο Internet.

Το 1999 το κακόβουλο λογισμικό αναβαθμίζεται και εξαπλώνεται περισσότερο μέσω του Internet και στους υπολογιστές της Microsoft.

[38] http://users.uoa.gr/~nektar/science/technology/a_brief_history_of_viruses.htm , 05/04/2015

Κακόβουλο λογισμικό όπως τον ιό Happy99, τον αναπαραγωγό Melissa και τον αναπαραγωγό Kak εξαπλώνονται αυτήν την περίοδο στα συστήματα της Microsoft μέσω του Internet. Επίσης αναπτύσσονται και λογισμικά RAT(RemoteAdmistrationTools) όπως το BackOrifice στο οποίο υπάρχει μια διαμάχη στο αν θεωρείται κακόβουλο λογισμικό διότι μπορούσε να επιτρέψει έλεγχο χωρίς να γίνεται αντιληπτό από το χρήστη και γι' αυτό θεωρείται και ως κερκόπορτα αλλά και ως τρωικός ίππος.

Ακριβώς το επόμενο χρόνο το 2000 εμφανίστηκε ο αναπαραγωγός/ιός (διότι οι γνώμες διίστανται) με όνομα ILOVEYOU στις 5 Μαΐου από έναν Φιλιπινέζο φοιτητή. Ο αναπαραγωγός αυτός μέσα σε λίγες μόνο ώρες μόλυνε εκατομμύρια υπολογιστές παγκοσμίως. Λέγεται ότι είναι ένας από τους πιο βλαβερούς αναπαραγωγούς που υπήρξαν ποτέ. Έπειτα, στις 28 Ιουνίου, έχουμε την εμφάνιση του ιού Pikachu, ο οποίος απευθυνόταν σε παιδιά. Μεταφερόταν μέσω email με τίτλο "PikachuPokemon" και παρακινούσε τα παιδιά ότι τα επέλεξε από εκατομμύρια άλλους. Μαζί με το email αυτό ως συνημμένο υπήρχε το pikachupokemon.exe το οποίο μόλις ενεργοποιούνταν μετά από μια επανεκκίνηση ζητούσε από το χρήστη να σβήσει όλα τα αρχεία των Windows με αποτέλεσμα να σβήνει εντελώς το λογισμικό. Αυτό μόλυνε τα Windows 95, 98 και Me.[39]

Το 2001 εμφανίστηκαν τα λογισμικά CodeRed, Ninda, Aliz, BadtrausII τα οποία εντόπιζαν αδυναμίες στα λογισμικά. Λόγω αυτών των επιδημιών άλλαξε ουσιαστικά το πρόσωπο της Ασφάλειας Υπολογιστών (ComputerSecurity) και ήταν σταθμός ανάπτυξης κακόβουλου λογισμικού για τα επόμενα χρόνια. Επιπλέον το 2001 ήταν η χρονιά που πρωτοεμφανίστηκαν τα chat-roomsτης ICQ και του MSN Messenger απ' όπου και γινόταν μεταφορά κακόβουλου κώδικα. Επιπλέον αυτή τη

[39]http://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms, 4/4/2015

χρονιά έκανε την εμφάνισή του ο αναπαραγωγός με όνομα Anna Kournikova, ο οποίος όπως ο προγενέστερος αναπαραγωγός ILOVEYOU, αναπαραγόταν μέσω της αποστολής ηλεκτρονικών μηνυμάτων. Το μήνυμα αυτού του αναπαραγωγού έλεγε ότι περιείχε μια φωτογραφία της γνωστής παίκτριας του τένις Anna Kournikova. Αυτό που περιείχε όμως ήταν ένα πρόγραμμα το οποίο ανάγκαζε τον υπολογιστή να στέλνει μηνύματα στις επαφές του. Προγραμματίστηκε από τον Jande Wit έναν εικοσάχρονο φοιτητή χρησιμοποιώντας μια γεννήτρια δημιουργίας αναπαραγωγών(worm generator). [40]

Το 2002 ο ιός Smile γράφτηκε σε συμβολική γλώσσα του οποίου ο κώδικας είχε μεταμορφωτικές ιδιότητες και άλλαζε ανάλογα με τις πληροφορίες που λάμβανε από τον υπολογιστή τον οποίο μόλυνε. Η κερκόπορτα και τρωικός ίππος Beastείναι ένα RAT που αναπτύσσεται πρώτη φορά σε κώδικα γραμμένο σε Delphi από τον Tatayeto 2002. Υπάρχει μια φήμη ότι ο ιός Beast μολύνει όλες τις εκδόσεις των Windows. Στις 7 Μαρτίου του ίδιου έτους ο αναπαραγωγός Mylife έστελνε κακόβουλα email για να αναπαραχθεί στον κατάλογο στο Microsoft Outlook του χρήστη ο οποίος μολύνθηκε πρώτος.[41] Τέλος το 2002 εμφανίστηκε η κερκόπορτα και τρωικός ίππος OptixPro, τα οποία είναι επίσης προγράμματα RAT αλλά είναι πιο θανάσιμα θα λέγαμε από τα υπόλοιπα και μπορούσαν να απενεργοποιήσουν το τείχος προστασίας και όποιο πρόγραμμα υπήρχε που στρεφόταν ενάντια στο κακόβουλο λογισμικού.

Το 2003 έχουμε την πρώτη μεγάλη παραγωγή κακόβουλου λογισμικού. Αρχικώς έχουμε την εμφάνιση του αναπαραγωγού SQLSlammer ή αλλιώς Shapphire που επιτίθεται στις αδυναμίες του

[40] http://news.softpedia.com/news/Kournikova-Worm-Celebrates-10th-Anniversary-183904.shtml 14/5/2015

[41] http://en.wikipedia.org/wiki/Mylife_(computer_worm) 12/4/2015

Microsoft SQLServer και αναπαράγεται πάρα πολύ γρήγορα συντρίβοντας το Ιντερνέτ μέσα σε δεκαπέντε λεπτά από την κυκλοφορία του.[42]Έπειτα έχουμε το τρωικό ίππο Graybird ο οποίος μόλις ενεργοποιηθεί κατεβάζει κρυφά αρχεία από το Internet. Θεωρείται επίσης και ως κερκόπορτα.[43] Έπειτα έχουμε τη κερκόπορτα και τρωικό ίππο ProRat το οποίο είναι κι αυτό ένα πρόγραμμα RAT. Στην συνέχεια έχουμε τον αναπαραγωγό Blaster ο οποίος εξαπλώθηκε τον Αύγουστο του 2003 και μόλυνε υπολογιστές με λειτουργικό σύστημα Windows XP και Windows 2000.[44]Λύση για τον Blaster υπήρξε ο αναπαραγωγός Welchia(Nachi) το οποίο έσβηνε τον Blaster και έπειτα κατέβαζε ένα patch ασφάλειας για την αποφυγή επιπλέον προσβολών από τον Blaster αλλά δημιουργούσε δικτυακά προβλήματα στον χρήστη.[45]Επιπλέον αυτή την χρονιά έχουμε και το spyware CoolWebSearch το οποίο αλλάζει την αρχική σελίδα του Internet Explorer σε coolwebsearch.com αλλά υπάρχουν και διάφορες παραλλαγές του που επηρεάζουν και άλλα προγράμματα περιήγησης. Έπειτα παρουσιάστηκεο αναπαραγωγός Sobig, ο οποίος είχε πολλές παραλλαγές με πιο διαδομένη την παραλλαγή του με όνομα Sobig.F το οποίο αναπαρήγαγε τον εαυτό του αποστέλλοντας αυτόκλητα email (spam) σε διευθύνσεις που έβρισκε στον υπολογιστή.[46] Στην συνέχεια έχουμε άλλον ένα αναπαραγωγό τον Swen ο οποίος ερχόταν ως ένα μήνυμα από το Windows Update για αναβάθμιση του συστήματος. Αυτό που έκανε όμως ήταν να απενεργοποιεί το τείχος προστασίας και να αναπαράγεται μέσω email και μέσω P2P δίκτυα όπως το Kazaa. Μπορεί επίσης να αναπαραχθεί και μέσω IRC και μέσω ομάδων ενημέρωσης

[42]http://archive.wired.com/wired/archive/11.07/slammer.html , 14/04/2015

[43]http://www.symantec.com/security_response/writeup.jsp?docid=2003-040217-2506-99 , 14/04/2015

[44]http://en.wikipedia.org/wiki/Blaster_(computer_worm) , 14/04/2015

[45]http://www.giac.org/paper/gcih/517/welchia-worm/105720 , 14/04/2015

[46]http://en.wikipedia.org/wiki/Sobig . 14/04/2015

(newsgroups). [47] Στην συνέχεια ο αναπαραγωγός Sober κάνει την πρώτη εμφάνιση του στα συστήματα Windows, όπως και τα προηγούμενα αναπαράγεται μέσω αποστολής ηλεκτρονικών αυτόκλητων μηνυμάτων. Αναβαθμίστηκε έως και το 2005 με ονομασίες όπως Sober.L, Sober.T, Sober.X.[48] Έπειτα έχουμε την οικογένεια αναπαραγωγών Agobot γνωστή και ως Gaobot, με την πρώτη έκδοση γραμμένη από τον γερμανό προγραμματιστή Axel "Ago" Gembe.[49]Το ίδιο έτος έχουμε επίσης και την πρώτη εμφάνιση του αναπαραγωγού Mimail, ο οποίος έστελνε μαζικά ηλεκτρονική μηνύματα. Τέλος έχουμε τον αναπαραγωγό Bolgi ο οποίος εκμεταλλευόταν μια αδυναμία υπερχείλισης buffer στα Windows.

Το 2004 αρχικά εμφανίζεται ο αναπαραγωγός Bagle που κάνει μαζική αποστολή μηνυμάτων και επηρεάζει όλες τις εκδόσεις των Windows. Ο αναπαραγωγός αυτός είχε 28 παραλλαγές, τον BagleA, τον BagleB κτλ. Στην συνέχεια έχουμε τον αναπαραγωγό L10n ή αλλιώς Lion που επηρέαζε τους υπολογιστές της Linux 6.2 και 7.0 που εκμεταλλευόταν μια υπερχείλιση buffer στο BIND DNS εξυπηρετητή και ήταν βασισμένο σε ένα παλιότερο αναπαραγωγό με το όνομα Ramen. [50] Στην συνέχεια κάνει την εμφάνισή του ο αναπαραγωγός MyDoom ο οποίος λέγεται ότι είναι ο πιο γρήγορος μαζικός αποστολέας που υπήρξε ποτέ. Υπήρξε ως παραλλαγή του Mimail γι' αυτό και ονομάζεται διαφορετικά Mimail.R , αλλά οι αναλύσεις που έγιναν έδειξαν πως έχει μεν κάποια σχέση αλλά δεν υπήρξε κάποια οριστική κατάληξη όσον αφορά τους δημιουργούς αυτών των δύο κακόβουλων λογισμικών.[51] Έπειτα η οικογένεια αναπαραγωγών Netsky αποκαλύπτεται. Οι αναφορές παραθέτουν το

[47] http://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/worm_swen.b , 14.04/2015

[48] https://www.opendemocracy.net/media-edemocracy/spam_2535.jsp , 14/04/2015

[49] http://en.wikipedia.org/wiki/Agobot . 14/04/2015

[50] https://www.sans.org/search/results , 15/04/2015

[51] http://en.wikipedia.org/wiki/Mydoom , 15/04/2015

γεγονός ότι τον Ιούνιο του 2004 είχε τις περισσότερες παραλλαγές, 29 σε αριθμό, με τον προαναφερθέντα αναπαραγωγό Bagle να έχει 28 και τον Mydoom να έχει 10.[52]Ένας αρκετά διάσημος αναπαραγωγός ήταν ο Witty που εμφανίστηκε τον Μάρτιο του 2004. Όταν ο αναπαραγωγός μόλυνε έναν υπολογιστή έσβηνε ένα τυχαίο κομμάτι του σκληρού δίσκου, κάνοντας συνήθως τον υπολογιστή αχρησιμοποίητο. Ήταν από τους πρώτους μαζικούς αναπαραγωγούς που είχε ένα καταστροφικό φορτίο. Λέγεται ότι αποτελούσε την πιο γρήγορη ανταπόκριση σε αδυναμία που εκδηλώθηκε από την ISS, σε μόλις μία ημέρα. Επίσης επισυνάπτεται ότι μπορεί μεν να μην εξαπλώθηκε πολύ αλλά εξαπλώθηκε σε χρήστες που έκαναν κάτι παραγωγικό για την Υπολογιστική Ασφάλεια Συστημάτων σε εταιρίες.[53] Στην συνέχεια οαναπαραγωγός Sasser εκμεταλλεύτηκε την αδυναμία των Windows XP με την διεπαφή LSASS (Local Security Authority Subsystem Service). Ο αναπαραγωγός αυτός προξένησε πολλές διαταραχές όπως την διακοπή των δορυφορικών επικοινωνιών του πρακτορείου ειδήσεων AgenceFrance-Presse(AFP) αλλά και την Αμερικανική αεροπορική εταιρία Delta Airlines που έπρεπε να ακυρώσει αρκετές πτήσεις γιατί τα υπολογιστικά συστήματα είχαν κατακλυστεί από τον αναπαραγωγό αυτόν. Ο γερμανός φοιτητής πληροφορικής Sven Jaschan κατηγορήθηκε γι αυτόν το αναπαραγωγό, όπως και για τον Netsky.[54] Στην συνέχεια έχουμε και την εμφάνιση του πρώτου αναπαραγωγού για κινητά τηλέφωνα του Cabir και επηρέαζε συστήματα της SymbianOS, ο οποίος μεταφερόταν με Bluetooth. Επιπλέον έχουμε το Nuclear το οποίο είναι μια κερκόπορτα ή τρωικός ίππος που εμφανίστηκε στις 16 Αυγούστου και επηρέαζε την οικογένεια συστημάτων της

[52]http://en.wikipedia.org/wiki/Netsky_(computer_worm) 15/04/2015

[53]http://www.caida.org/research/security/witty/ 15/04/2015

[54]http://www.sophos.com/en-us/press-office/press-releases/2004/05/va_sasserarrest.aspx 15/04/2015

Windows NT. Την ίδια περίοδο εμφανίζεται και ένας τρωικός ίππος ο Vundo ο οποίος προκαλούσε την εμφάνιση παραθύρων και διαφήμιζε ψεύτικα προγράμματα antispyware. Επίσης προκαλούσε τη μη λειτουργία ιστοσελίδων που περιλάμβαναν την Google και το Facebook. Αυτή την περίοδο επίσης ανακαλύπτεται και η οικογένεια τρωικών ίππων και κερκοπορτών Bifrost το οποίο έχει 10 παραλλαγές οι οποίες μολύνουν τα Windows από την έκδοση των 95 έως και τα Windows 7. Όσον αφορά τις δυνατότητες του, ο Bifrost επιτρέπει στον επιτιθέμενο να εκτελέσει συμβολικό κώδικα με αποτέλεσμα ο έλεγχος του υπολογιστή να περνά στα χεριά αυτού που το έστειλε. Τέλος, έχουμε τον πρώτο γνωστό αναπαραγωγό που δρούσε στο Internet και εκμεταλλευόταν την αδυναμία στο phpBB της Google για να βρίσκει τους στόχους του.

Το 2005 αρχικά εμφανίστηκαν οι αναπαραγωγοί Zotob και Rbot που προκάλεσαν αναταραχές στις Ηνωμένες Πολιτείες και έψαχναν αδυναμίες στο συστήματα των Windows 2000 και όταν προσβάλλονταν επέτρεπαν στον επιτιθέμενο να τα ελέγχει.[55]Στη συνέχεια το rootkit προστασίας αντιγραφής των μουσικών CD της SonyBMG αποκαλύπτεται. Το rootkit αυτό δημιουργεί αδυναμίες στους υπολογιστές τις οποίες μπορούσαν να εκμεταλλευτούν κακόβουλα λογισμικά. Στα τέλη του 2005 έχουμε τον τρωικό ίππο Zlob το οποίο έδειχνε πως ήταν μία απαραίτητη κωδικοποίηση για βίντεο στην μορφή ενός στοιχείου της ActiveX.

Το 2006 η λογική βόμβα Nyxem αποκαλύπτεται. Μεταφερόταν με την μαζική αποστολή email και το φορτίο δεδομένων του ενεργοποιούνταν κάθε 3η ημέρα κάθε μήνα. Αυτόν τον χρόνο επίσης εμφανίστηκε ο πρώτος τρωικός ίππος για Mac, με το όνομα Leap. Από την άλλη, όμως, ο Leap δεν ήταν και τόσο επιβλαβείς στους χρήστες της Mac. Στην συνέχεια,έχουμε την πρώτη εμφάνιση του ιού Brontok που ξεκίνησε

[55]http://www.nytimes.com/2005/08/17/technology/17virus.html?_r=0 , 15/04/2015

στην Ινδονησία. Ο ιός αυτός μπορεί να ήταν ένα παράδειγμα ηλεκτρονικού ακτιβισμού(Hacktivism). Επίσης, ο ιός είχε 10 παραλλαγές. Στην συνέχεια υπάρχει η οικογένεια κακόβουλου λογισμικού Stration η οποία ξεκίνησε με έναν αναπαραγωγό ο οποίος εκτός από το ότι αναπαραγόταν με την μαζική αποστολή ηλεκτρονικών μηνυμάτων, κατέβαζε και άλλες παραλλαγές του ίδιου αναπαραγωγού που φτιάχνονται περίεργα μέσα σε 30 λεπτά, και απενεργοποιούσε την ασφάλεια του συστήματος.[56] Επίσης αυτή την χρονιά υπήρχε παραπλανητική πληροφόρηση(hoax) για τον ιό OlympicTorch, που μεταφερόταν μέσω email για να παραπλανεί τον κόσμο ότι ο σκληρός δίσκος τους θα γύριζε τόσο γρήγορα που θα έπιανε φωτιά.[57]

Το 2007 εμφανίστηκε το Storm Worm το οποίο είναι μια κερκόπορτα αλλά και τρωικός ίππος ο οποίος τοποθετούσε τον υπολογιστή τον οποίο μόλυνε σ' ένα botnet που έφτασε από ένα σε δέκα εκατομμύρια υπολογιστές παγκοσμίως και ελεγχόταν για προσωπικά στοιχεία όπως πιστωτικές κάρτες.[58] Δεν έκανε όμως μόνο αυτό αλλά τοποθετούσε και ένα rootkit το Win32.agent.dh.[59] Έπειτα, ο τρωικός ίππος με το όνομα Zeus προσπαθεί να κλέψει τραπεζικές πληροφορίες με την καταμέτρηση και καταγραφή των πλήκτρων που γράφει ο χρήστης.[60] Τέλος σ' αυτόν τον χρόνο έχουμε το Cutwail botnet το οποίο είχε αναπτυχθεί με την διάδοση του κακόβουλου λογισμικού με το ίδιο όνομα το όποιο κατέβαζε τον Zeus αλλά και πολλά Fake AntiVirus (FakeAV)αν ο χρήστης διάβαζε τα μηνύματα που του αποστέλλονταν από το botnet.Την ίδια χρονιά

[56]http://en.wikipedia.org/wiki/Stration 15/04/2015

[57]https://www.sophos.com/en-us/threat-center/threat-analyses/hoaxes/virus-hoax/olympic.aspx 15/04/2015

[58]http://news.bbc.co.uk/2/hi/technology/6278079.stm 16/04/2015

[59]http://en.wikipedia.org/wiki/Storm_Worm 16/04/2015

[60]http://en.wikipedia.org/wiki/Zeus_(malware) 16/04/2015

αναπτύχθηκε ραγδαία και το Pushdo botnet το οποίο οφείλεται για μεγάλη διάδοση των spam.

Το 2008 αρχικώς έχουμε την εμφάνιση ενός τρωικού ίππου του Mocmex ο οποίος βρέθηκε σε μία ψηφιακή κορνίζα τον Φεβρουάριο. Ήταν ο πρώτος σοβαρός τρωικός ίππος σε μια ψηφιακή κορνίζα. Οι ύποπτοι για τον ιό αυτόν βρέθηκαν σε μια ομάδα στην Κίνα.[61] Στην συνέχεια το Torpig είναι ένας τρωικός ίππος , ο οποίος απενεργοποιεί τα αντιβιοτικά προγράμματα. Επιτρέπει σε άλλους να ελέγχουν τον υπολογιστή, αλλάζει δεδομένα, κλέβει προσωπικά στοιχεία και εγκαθιστά περισσότερα κακόβουλα λογισμικά στον υπολογιστή.[62] Έπειτα το Win32.Ntldrbot ή αλλιώς Rustock.C, ένα rootkit το οποίο έφτιαχνε bot για την διάδοση αυτόκλητων μηνυμάτων το οποίο παρέμενε κρυφό από τον Οκτώβριο του 2007 το λιγότερο, αποκαλύπτεται και εξοντώνεται στις 6 Μάιου του 2008.[63] Στην συνέχεια έχουμε άλλο ένα RAT ή τρωικό ίππο το οποίο ονομάζεται Bohmini.A. Το Bohmini.A εκμεταλλεύεται τις αδυναμίες στο AdobeFlash 9.0.115 με το InternetExplorer 7.0 και το Firefox 2.0 στα Windows XP με Service Pack 2. Τον Ιούλιο του 2008 το Bohmini.A ξεκίνησε να εξαπλώνεται με κακόβουλη διαφήμιση (malvertising) μέσω του Facebook. Στην συνέχεια έχουμε έναν αναπαραγωγό που προσβάλει όλα τα είδη συστημάτων, Windows, MacOS, Linux. Αυτός ο αναπαραγωγός προσέβαλε χρήστες του Facebook, Skype, Yahoo Messenger και ιστοσελίδων όπως Gmail. Επίσης προσβάλει και χρήστες του Myspace, Friendster, Twitter, και μπορεί τέλος να μεταφέρεται και μέσω χρηστών ενός τοπικού δικτύου.[64] Αυτό που κάνει ο Koobface είναι να κλέβει

[61] http://www.seattlepi.com/business/article/Chinese-PC-virus-may-have-hidden-agenda-1264738.php , 16/04/2015

[62] http://windowssecrets.com/top-story/dont-be-a-victim-of-sinowal-the-super-trojan/ , 16/04/2015

[63] http://www.pr.com/press-release/84130 , 16/04/2015

[64] http://en.wikipedia.org/wiki/Koobface , 16/04/2015

δεδομένα όπως κωδικούς και ονόματα χρηστών σε γνωστές ιστοσελίδες και να δημιουργεί με τους προσβλημένους υπολογιστές ένα botnet με το οποίο και να τους ελέγχει. Επίσης γίνεται έλεγχος για την έκδοση του Koobface και αναβαθμίζεται αυτόματα.[65]Στην συνέχεια έχουμε την οικογένεια αναπαραγωγών Conficker. Αρχικώς, ο Conficker είναι συνδυασμός πολλών παρελθοντικών τεχνικών οι οποίες συνδυάστηκαν σε έναν ενιαίο κακόβουλο λογισμικό το οποίο προσέβαλε υπολογιστές της Microsoft.[66] Προξένησε εκατομμύρια εισβολές παγκοσμίως μέχρι και σε κυβερνητικούς οργανισμούς εκτός από τις εταιρίες και τους προσωπικούς υπολογιστές που προσβλήθηκαν.[67]

Το 2009 τον Ιούλιο έχουμε τις ψηφιακές επιθέσεις ενάντια σε κυβερνητικές, ενημερωτικές, και οικονομικές ιστοσελίδες στην Νότια Κορέα και στις Ηνωμένες Πολιτείες. Αυτές οι επιθέσεις σκόπευαν στην δημιουργία ενός botnet και να κάνει τους υπολογιστές τους να υπερφορτωθούν λόγω της μαζικής εισροής στη ροή της ηλεκτρονικής κυκλοφορίας, το οποίο αλλιώς λέγεται επίθεση DDoS(Distributed Denial-of-Service). Αυτές οι επιθέσεις έγιναν σε τρία στάδια. Αρχικά, το πρώτο κύμα επιθέσεων έγινε στις 4 Ιουλίου (Ημέρα της Ανεξαρτησίας) στις Ηνωμένες Πολιτείες και στην Νότια Κορέα. Σύμφωνα με τα αρχεία καταγραφής που βρέθηκαν στους μολυσμένους υπολογιστές, ο στόχος ήταν 27 ιστοσελίδες. Το δεύτερο κύμα επιθέσεων έγινε στις 7 Ιουλίου και επηρέασε την Νότια Κορέα. Ανάμεσα στις ιστοσελίδες ήταν και αυτές του Μπλε Οίκου, του Υπουργείου Άμυνας και πολλές άλλες. Το τρίτο κύμα επιθέσεων έγινε στις 9 Ιουλίου και εκτός από όλα τα προηγούμενα έγιναν εισβολές και σε τράπεζες στην Νότια Κορέα αλλά στην Αμερική είχαν

[65]http://www.infowar-monitor.net/reports/iwm-koobface.pdf , 16/04/2015

[66]http://www.nytimes.com/2009/01/23/technology/internet/23worm.html?_r=0 16/04/2015

[67]http://en.wikipedia.org/wiki/Conficker , 16/04/2015

προετοιμαστεί για αυτό το τρίτο κύμα επιθέσεων και δεν προκλήθηκαν πολλές βλάβες όπως με τα άλλα δύο κύματα επιθέσεων[68] που προξένησαν μόνο αναστάτωση και δεν είχαν ως στόχο την κλοπή δεδομένων.[69]Αυτό τον χρόνο έχουμε επίσης τον αναπαραγωγό Daprosyo οποίος μεταφέρεται με USB drives και μέσω email. Στόχος του ήταν να υποκλέψει κωδικούς και άλλα δεδομένα που εισάγονταν μέσω πληκτρολογίου και αναπαραγόταν μέσω του τοπικού δικτύου ή αποστέλλοντας τον εαυτό του σε άλλους υπολογιστές μέσω αυτόκλητων ηλεκτρονικών μηνυμάτων.[70] Ο Τρωικός ίππος Spyeye δημιουργείται και χρησιμοποιείται για την κλοπή τραπεζικών κωδικών.,

Το 2010 αρχικά υπάρχει ο αναπαραγωγός Waledac, ο οποίος δημιούργησε ένα botnet με 90.000 υπολογιστές που αποσκοπούσε στην αποστολή αυτόκλητων ηλεκτρονικών μηνυμάτων. Όμως, η Microsoft κατάφερε να κλείσει τους υπολογιστές που έκαναν τον έλεγχο του botnet με αποτέλεσμα να σώσει πάρα πολλούς υπολογιστές.[71]Στην συνέχεια εμφανίστηκε ο τρωικός ίππος Alureon σε μια αναβαθμισμένη μορφή, ο οποίος λειτουργούσε κατεβάζοντας ένα «αυτόκλητο» λογισμικό ασφαλείας το οποίο σταματούσε σημαντικές λειτουργίες στον υπολογιστή.[72] Επιπλέον, ο τρωικός ίππος Stuxnet εμφανίζεται και πολιορκεί τα συστήματα SCADA τα οποία ήταν τοποθετημένα σε πυρηνικούς αντιδραστήρες στο Ιράν. Θεωρείται επίσης ότι ο εν λόγω τρωικός ίππος αν ενεργοποιηθεί μπορεί να επιτελέσει επαναπρογραμματισμό στους υπολογιστές αυτούς και μ' αυτό τον τρόπο να γίνουν αυτά που θέλησε ο δημιουργός του. Αυτός ο τρωικός ίππος είναι

[68]http://en.wikipedia.org/wiki/July_2009_cyber_attacks 17/04/2015

[69]http://www.csmonitor.com/World/Asia-Pacific/2009/0709/p06s23-woap.html , 17/04/2015

[70]http://www.threatexpert.com/report.aspx?md5=7c6a5c18801938867644c861ebfdf0b8 , 17/04/2015

[71]http://www.theregister.co.uk/2010/03/16/waledac_takedown_success/ ,

[72]http://en.wikipedia.org/wiki/Alureon,18/04/2015

ένα από τα πρώτα κύματα της ψηφιακής τρομοκρατίας.[73] Ο αναπαραγωγός «Here you have» κάνει την εμφάνιση του. Ο συγκεκριμένος αναπαραγωγός μεταφέρεται μέσω email με το θέμα να λέει «Ορίστε(Here you have)» και εξαπλώνεται μέσω της αποστολής στις επαφές του χρήστη στο Outlook. Τέλος ο ιός Kenzero εμφανίστηκε. Μεταφερόταν μέσω των δικτύων peer to peer(P2P) και έπαιρνε το ιστορικό περιήγησης του μολυσμένου χρήστη και το ανέβαζε στο Internet.

Το 2011 αρχικώς, ο τρωικός ίππος Spyeye σε συνδυασμό με τον Zeus του 2007 καταλαμβάνει τις κινητές συσκευές και λαμβάνει πληροφορίες για τραπεζικούς λογαριασμούς.[74] Στην συνέχεια το κακόβουλο λογισμικό AntiSpyware2011 το οποίο είτε ερχόταν μέσω Trojan στο μολυσμένο υπολογιστή ή εγκαθίσταντο μόνο του χωρίς παρεμβολή του χρήστη.. Αυτό το λογισμικό απενεργοποιούσε ότι πρόγραμμα αντιμετώπισης κακόβουλου λογισμικού υπήρχε και απενεργοποιούσε την διαχείριση εργασιών(TaskManager) και ζητούσε την αναβάθμιση του σε pro μέσα σε λίγα λεπτά λειτουργίας επισημαίνοντας ότι ο υπολογιστής είναι γεμάτος spyware.[75]Επιπλέον ο αναπαραγωγός Morto επιτίθεται στα συστήματα με αδύναμους κωδικούς[76], και έπειτα προσπαθεί να επικοινωνήσει με το domain του hacker ο οποίος το δημιούργησε. Αν αποτύχει παραμένει αδρανές μέχρι να μπορέσει να αποκτήσει επικοινωνία. [77] Στην συνέχεια εμφανίστηκε το ZeroAccess ένα rootkit αλλά και έπειτα τρωικός ίππος το οποίο στόχο έχει να μαζέψει χρήματα χρησιμοποιώντας 2 τεχνικές το "Bit coin mining" και "Click Fraud".[78]Τέλος ο αναπαραγωγός Duqu αναλύεται

[73]http://www.telegraph.co.uk/technology/news/8021102/Stuxnet-virus-worm-could-be-aimed-at-high-profile-Iranian-targets.html, 18/04/2015

[74]http://www.theregister.co.uk/2011/01/25/spyeye_zeus_merger/ 18/04/2015

[75]http://www.precisesecurity.com/rogue/xp-anti-spyware-2011 19/04/2015

[76]http://blog.appriver.com/2011/08/morto-worm-spreads-to-weak-systems/ 19/04/2015

[77]http://blog.imperva.com/2011/09/morto-post-mortem-a-worm-deep-dive.html 19/04/2015

[78]http://en.wikipedia.org/wiki/ZeroAccess_botnet 19/04/2015

από την CrySyS και η έρευνα καταλήγει στο συμπέρασμα ότι ο Duqu έχει κοινά χαρακτηριστικά με τον αναπαραγωγό Stuxnet, και όπως κι αυτός, επιλέγει τους στόχους του.[79]

Το 2012, ο Flame είναι μια κερκόπορτα, τρωικός ίππος που έχει χαρακτηριστικά αναπαραγωγού και μπορεί να χαρακτηριστεί ως πολυμορφικός ιός. Η CrySyS του Πανεπιστήμιου Τεχνολογίας της Βουδαπέστης σε μια ανάλυση που έκανε τον χαρακτήρισε ως το πιο περίπλοκο κακόβουλο λογισμικό που υπήρξε ποτέ. Είχε κάποιες ομοιότητες με τον Stuxnet του 2011. Αρχικά χρησιμοποιήθηκε για κατασκοπεία στον κυβερνοχώρο στις χώρες της Μέσης Ανατολής και έπειτα εξαπλώθηκε στον υπόλοιπο δυτικό κόσμο.[80] Στην συνέχεια άλλος ένας πολυμορφικός ιός που εμφανίστηκε σ' αυτό το έτος είναι ο Shamoon, ο οποίος στόχο είχε τις εταιρίες παραγωγής ενέργειας.[81] Αρχικά χτύπησε την εταιρία Saudi Aramco, μια εταιρία παραγωγής πετρελαίου και φυσικού αερίου που βρίσκεται στην Σαουδική Αραβία. [82] Η λειτουργία του ήταν «να ρίχνει, να καθαρίζει και να αναφέρει» όπως γράφει το Digital Journal. Επίσης αναφέρει ότι «ο λόγος του ότι φτιάχτηκε ένα κακόβουλο λογισμικό που κάνει αχρησιμοποίητους τους υπολογιστές που μολύνει είναι ακόμα ασαφές.»[83]Επιπλέον ένας τρωικός ίππος ο NGRBot αποκαλύπτεται. Ο NGRBot καλύπτεται σε ένα email με θέμα Skype. Αν ο χρήστης ενεργοποιήσει το επισυναπτόμενο εκτελέσιμο αρχείο τότε το κακόβουλο λογισμικό ενεργοποιείται και παρακολουθεί το ιστορικό του χρήστη με αποτέλεσμα να κλέβει αριθμούς πιστωτικών καρτών και

[79] http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf 19/04/2015
[80] http://www.crysys.hu/skywiper/skywiper.pdf 20/04/2015
[81] http://en.wikipedia.org/wiki/Shamoon#cite_note-Iran_Malware-9 20/04/2015
[82] http://en.wikipedia.org/wiki/Saudi_Aramco 20/04/2015
[83] http://www.digitaljournal.com/article/331033 20/04/2015

κωδικούς αλλά και ονόματα χρηστών από γνωστές ιστοσελίδες. Τέλος αυτά τα στοιχεία πωλούνται σε πολλές σκιώδεις ιστοσελίδες. [84]

Το 2013 εμφανίζεται ο πρώτος Ransomware ο Cryptorlocker. Ο Cryptorlocker λειτουργούσε κρυπτογραφώντας τα αρχεία του μολυσμένου υπολογιστή και ζητούσε χρήματα για την αποκρυπτογράφηση τους. [85] Τέλος το Zeus Gameover ένας τρωικός ίππος ο οποίος μεταφερόταν μέσω του Cutwail botnet, ο οποίος έκλεβε δεδομένα όπως ο ομώνυμος του Zeus, λέγεται όμως ότι επίσης οφείλεται στη διάδοση του Cryptorlocker.

Το 2014 η Synatrec ανακαλύπτει το μεταλλασσόμενο τρωικό ίππο Regin (Warior Pride), παραλλαγές του οποίου είχαν εμφανιστεί από το 2003. Λέγεται πως είχε συγκεκριμένους στόχους και δεν εξαπλωνόταν πέρα από αυτούς. Για το κακόβουλο αυτό λογισμικό οφείλεται η κατασκοπευτική εταιρία GCHQ και λέγεται ότι χρησιμοποιούνταν για κατασκοπευτικούς λόγους μόνο. Σκοπός του λογισμικού ήταν να κατεβάζει τον εαυτό του και να κάνει τον υπολογιστή να μπλοκάρει ελάχιστα ώστε να μην γίνεται αντιληπτό από τα προγράμματα antivirus. Επίσης παρακολουθούσε τις κινήσεις στον υπολογιστή που είχε προσβάλει.[86] Τέλος αυτόν τον χρόνο παρατηρήθηκε και ένα σφάλμα στον OpenSSL κώδικα το οποίο έλαβε το όνομα Heartbleed, λόγω του γεγονότος ότι αξιοποιούσε το Heartbeat, ένα κομμάτι κώδικα. Αυτό που έκανε το σφάλμα είναι να επιτρέπει στους hackers να λαμβάνουν μεγάλο μέρος πληροφορίας ακόμα και τα προσωπικά κλειδιά των χρηστών του OpenSSL.

Έως και σήμερα το κακόβουλο λογισμικό έχει αναπτυχθεί και έχει διδάξει την προσοχή στις αδυναμίες που μπορεί να έχει ένα υπολογιστικό

[84] http://www.enigmasoftware.com/ngrbot-removal/ 20/04/2015
[85] http://www.snopes.com/computer/virus/Cryptorlocker.asp 23/04/2015
[86] https://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/ 29/04/2015

σύστημα. Όμως πάντα θα υπάρχουν αδυναμίες που δεν θα ‘χουν καλυφθεί ως τώρα γι’ αυτό και πρέπει να υπάρχει εγρήγορση διότι κάποιοι θα εκμεταλλευτούν τις αδυναμίες αυτές προς όφελος τους.

2 Ιομορφικό Λογισμικό

Στο δεύτερο κεφάλαιο αυτής της πτυχιακής γίνεται αναφορά στο ιομορφικό λογισμικό και θα αναλυθεί στα περαιτέρω είδη αυτής της κατηγορίας κακόβουλου λογισμικού.

Όπως αναφέρει ο Lincoln Spector της PCWorld, «η λέξη ιός χρησιμοποιείται για να περιγράψει κάθε τύπο κακόβουλου λογισμικού. Βέβαια λανθασμένα, διότι δεν είναι κάθε είδος κακόβουλου λογισμικού ένας ιός. Οι πραγματικοί ιοί υπήρξαν διαδεδομένοι την δεκαετία του 1980 και του 1990, όταν πρωτοεμφανίστηκαν οι προσωπικοί υπολογιστές, και ο λόγος του ότι είναι τόσο σπάνιοι είναι διότι οι επιτιθέμενοι βρήκαν καλύτερους τρόπους για την διάδοση κακόβουλου κώδικα. Και επειδή δεν υπήρχε ο όρος κακόβουλο λογισμικό(malware) γι' αυτό και οι άνθρωποι από τότε αποκαλούσαν κάθε είδος κακόβουλο λογισμικό, έναν ιό, πράγμα που ισχύει ακόμα και σήμερα. Γι' αυτό και πολλές εταιρίες λένε ότι το αντιβιοτικό τους πρόγραμμα λέγεται antivirus.»[87]

Επιστημονικά όμως, σύμφωνα με τον Ηλιάδη, «ένας ιός θεωρείται τμήμα λογισμικού που ενσωματώνεται στο κώδικα ενός προγράμματος που αποκαλείται ξενιστής., και αναπαράγεται με την αντιγραφή του εαυτού του σε άλλους ξενιστές.»

Σύμφωνα με τον ίδιο, «οι διαφορές μεταξύ ιομορφικού και άλλων τύπων κακόβουλου λογισμικού είναι όσον αφορά την πιθανότητα μόνιμης βλάβης για τους ιούς πιο χαμηλή σε σχέση με τους υπόλοιπους τύπους μη-ιομορφικού λογισμικού όπου η βλάβη είναι μη προβλέψιμη. Όσον αφορά την αναπαραγωγή ο ιός αναπαράγεται μόνος του ενώ τα υπόλοιπα κακόβουλα λογισμικά χρειάζονται ανθρώπινη παρέμβαση. Η

[87] http://www.pcworld.com/article/2048261/understanding-tech-language-the-difference-between-malware-and-a-virus.html 1/7/2015

πιθανότητα για επεισόδια σε μεγάλη κλίμακα από την πλευρά των ιών είναι υψηλή, ενώ από την πλευρά των άλλων τύπων λογισμικού είναι χαμηλή εκτός και αν πρόκειται για διαδεδομένο λογισμικό. Τα επίπεδα δυσκολίας εντοπισμού είναι από την πλευρά των ιών χαμηλά ενώ από την πλευρά των άλλων τύπων λογισμικού υψηλή.»[88]

Όσον αφορά τον τρόπο ενεργοποίησης του ιομορφικού λογισμικού, σύμφωνα με τον Hardikar, «αν εκτελεσθεί ένα αρχείο που έχει μέσα στον κώδικά του κώδικα ιού, τότε ο ιός ενεργοποιείται.»[89]

Βέβαια, σύμφωνα με τον Ηλιάδη, «ένα χαρακτηριστικό των ιών είναι το ότι εκτελούνται στο παρασκήνιο. Ο κύκλος ζωής ενός ιού περιλαμβάνει τρία στάδια: την φάση επώασης, φάση αναπαραγωγής και τέλος φάση ενεργοποίησης και εκτέλεσης. Όσον αφορά την πρώτη, ο ιός παραμένει ανενεργός στο υπολογιστικό σύστημα. Εκτελείται από κάποιο γεγονός και την έλευση κάποιας χρονικής στιγμής, θυμίζοντας λογική βόμβα. Η φάση αυτή δίνει στον ιό την δυνατότητα να αναμένει τις κατάλληλες συνθήκες για την ενεργοποίηση του και να παραμένει απαρατήρητος από τα προγράμματα ανίχνευσης ιών. Βέβαια υπάρχουν περιπτώσεις ιών που δεν κάνουν χρήση της φάσης επώασης αλλά ενεργοποιούνται αμέσως μόλις βρεθεί ο κατάλληλος ξενιστής που θα επιτρέψει την αναπαραγωγή τους.»

Το δεύτερο στάδιο, που όλοι οι ιοί περνούν, θεωρείται ως ένα από τα ιδιαίτερα χαρακτηριστικά τους, η αναπαραγωγή. Στην διάρκεια της αναπαραγωγής ο ιός χρησιμοποιώντας προγράμματα ξενιστές,

[88]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[89]Hardikar, Amman, MALWARE 101, Viruses,SANSInstitute,Seattle, 2008. Available at: https://www.sans.org/reading-room/

αντιγράφει τον εαυτό του.[90] Ο Hardikar αναφέρει ότι δεν είναι μόνο τα προγράμματα που αναπαράγουν τους ιούς αλλά και τα αρχεία ξενιστές.[91]

«Τελευταίο στάδιο», σύμφωνα με τον Ηλιάδη, «η φάση Ενεργοποίησης κατά την οποία, ο ιός εκτελεί μια σειρά ενεργειών με πιθανές επιβλαβείς συνέπειες για το υπολογιστικό σύστημα που τον φιλοξενεί.»[92] Σύμφωνα με τον Hardikar οι επιπτώσεις που μπορεί να έχει ένας ιός είναι να καταστρέφει συγκεκριμένους τύπους αρχείων, είτε με το να διαγράφει το περιεχόμενό τους είτε με το να κρυπτογραφεί το περιεχόμενο τους μ' ένα τυχαίο κλειδί και να αλλοιώνει τους τομείς εκκίνησης, τα μεταδεδομένα, ή τους πίνακες αρχείων του συστήματος,[93]

Βέβαια ο ιός διατηρεί συγκεκριμένες υπορουτίνες ήτοι την υπορουτίνα αναζήτησης, την υπορουτίνα αντιγραφής και την υπορουτίνα κατά του εντοπισμού. Όσον αφορά την υπορουτίνα αναζήτησης, αυτή αφορά στην αναζήτηση από τον ιό για κατάλληλα προγράμματα ξενιστές τα οποία μπορούν να προβληθούν με το τμήμα του κώδικα του. Επιπλέον η υπορουτίνα αντιγραφής περιλαμβάνει την αντιγραφή του ιού σε ξενιστές που ανακαλύφθηκαν από την υπορουτίνα αναζήτησης. Τέλος η υπορουτίνα κατά του εντοπισμού είναι αυτή που παραμετροποιεί τις άλλες δύο υπορουτίνες έτσι ώστε να μην γίνονται αντιληπτές από αντιβιοτικά προγράμματα. [94]

---

[90]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[91]Hardikar, Amman, MALWARE 101, Viruses,SANSInstitute,Seattle, 2008. Available at: https://www.sans.org/reading-room/

[92]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[93]Hardikar, Amman, MALWARE 101, Viruses,SANSInstitute,Seattle, 2008. Available at: https://www.sans.org/reading-room/

[94]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

2.1 Τρόπος Έρευνας

Για τον έλεγχο των ιων σε αυτή την πτυχιακή χρησιμοποιήθηκε η τεχνική του sandboxing δηλαδή του ελέγχου λειτουργίας κακόβουλου λογισμικού σε ελεγχόμενες εικονικές μηχανές (virtual machines). Αν και αρκετά επικίνδυνος για τον υπολογιστή που κάνει αυτή την ανάλυση, ο τρόπος αυτός δίνει την δυνατότητα να γίνει έλεγχος σε πραγματικές συνθήκες. [95]

Το κακόβουλο λογισμικό που χρησιμοποιήθηκε προήλθε από το VXHeaven, αλλά λόγω προβλημάτων της ιστοσελίδας (http://vxheaven.org/), υπήρξε ανάγκη για κατέβασμα μιας βάσεως δεδομένων με κακόβουλο λογισμικό εώς και το 2010 με AcademicTorrent από την ιστοσελίδα: (http://academictorrents.com/details/34ebe49a48aa532deb9c0dd08a08a017aa04d810/tech&dllist=1)

Αν και χρονοβόρο λόγω μεγάλης ποσότητας υλικού και δυσκολίας όσον αφορά στο άνοιγμα της βάσεως δεδομένων που έπαιρνε πολύ χρόνο παρόλη την τοποθέτηση μεγάλων δυνατοτήτων στο VM, όπως και στην χρήση των αρχείων κακόβουλου λογισμικού, η έρευνα επέφερε καρπούς όπως φαίνεται παρακάτω στις αναλύσεις που έγιναν με αυτή την μέθοδο, λόγω όμως του γεγονότος ότι πολλές φορές τα ιομορφικά λογισμικά δεν λειτουργούσαν, δεν χρησιμοποιήθηκε παντού. Έτσι, έγινε χρήση των αναλύσεων του κακόβουλου λογισμικού από ιστοσελίδες γνωστών αντιβιοτικών προγραμμάτων. Βεβαίως όσο αφορά το DOS ιομορφικό λογισμικό οι αναλύσεις πάρθηκαν από βιβλιογραφική έρευνα μόνο.

Στην συνέχεια γίνεται αναφορά στους τύπους κακόβουλου λογισμικού.

[95] http://labs.lastline.com/different-sandboxing-techniques-to-detect-advanced-malware , 19/08/2015

2.2 Κατηγορίες Ιομορφικού Λογισμικού

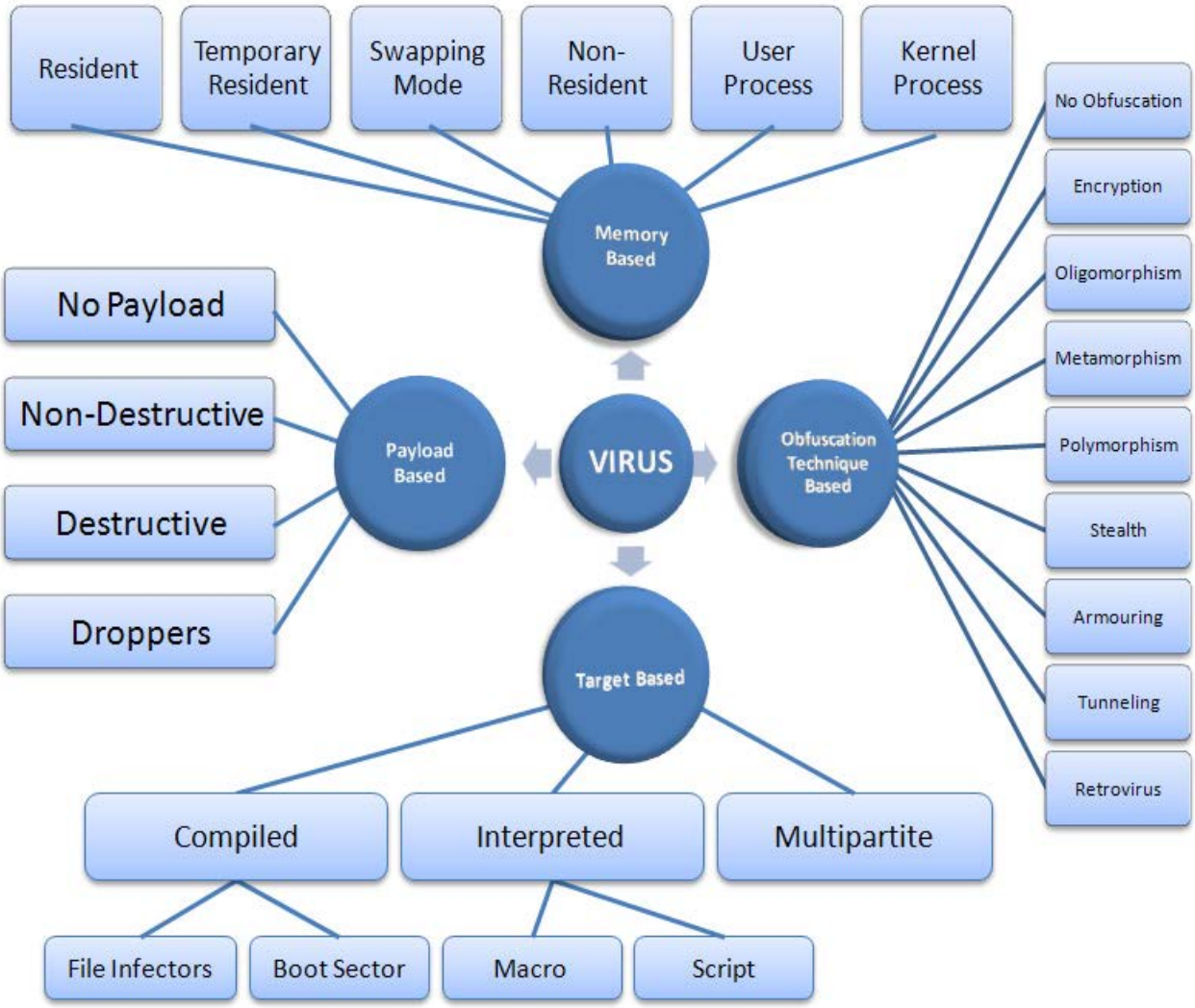
Αρχικά ο Hardikar αναφέρει πως για να κατηγοριοποιήσουμε τους ιούς θα αναφερθούμε σε ιούς που βασίζονται στην μνήμη του υπολογιστή, αυτούς που βασίζονται στον στόχο τους, αυτούς που χρησιμοποιούν διαφορετική τεχνική συσκότισης, και αυτούς που σχετίζονται στην σειρά ενεργειών.(Εικόνα 7)[96]

Ο Ηλιάδης από την δική του πλευρά συγκεκριμενοποιεί τις παραπάνω κατηγορίες και χωρίζει τους ιούς σε ιούς τομέα εκκίνησης, παρασιτικούς, πολυμερείς ιούς, κρυφούς, κρυπτογραφημένους, πολυμορφικούς, ρετρο-ιούς, ιούς που διαγράφουν τμήμα του ξενιστή και τέλος τους μακρό ιούς.[97]

Στην συνέχεια θα γίνει αναφορά σε κάθε κατηγορία σύμφωνα με το πρότυπο του Ηλιάδη και θα αναφερθούν τεχνικές αναλύσεις με παραδείγματα.

[96]Hardikar, Amman, MALWARE 101, Viruses,SANSInstitute,Seattle, 2008. Available at: https://www.sans.org/reading-room/

[97]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.



Εικόνα 7 Διαχωρισμός Ιομορφικού Λογισμικού

2.2.1 Ιοί τομέα εκκίνησης(BootSectorviruses)

Ο Ηλιάδης αναφέρει: «Οι ιοί τομέα εκκίνησης αντικαθιστούν τις υπάρχουσες ρουτίνες στον τομέα εκκίνησηςενός δίσκου τοποθετώντας τις σ' άλλο τμήμα του και έτσι μπορούν να τις ανακαλέσουν, αφού εκτελεσθούν οι ίδιοι πρώτα. Επιπλέον λόγω του μικρού χώρου του τομέα εκκίνησης οι ιοί εγγράφουν μόνο μια ρουτίνα εκκίνησης του ιού και αφήνουν το υπόλοιπο κύριο τμήμα του σε άλλον τομέα του σκληρού δίσκου. Τέλος αναφέρει ότι πολλές φορές παραμένουν στην μνήμη όταν ενεργοποιηθούν(memoryresident) έτσι ώστε να εκτελέσουν το στόχο τους και να διατηρήσουν τον έλεγχο του συστήματος με τέτοιο τρόπο ώστε να μην γίνονται αντιληπτοί από αντιβιοτικά προγράμματα.»[98]

Ένα παράδειγμα ιού τέτοιου τύπου είναι ο Boot.Cidex. Ο ιός αυτός μολύνει έναν υπολογιστή πακετάροντας τον εαυτό του με torrentκαι αρχεία από διάφορες ιστοσελίδες διαμοιρασμού αρχείων. Μπορεί επιπλέον να κρύβεται ως ένα νόμιμο πρόγραμμα από μια χαμηλά ελεγχόμενη πηγή. Επιπλέον μπορεί να είναι συνημμένο σε κάποιο ηλεκτρονικό μήνυμα. Μπορεί επίσης να χρησιμοποιήσει και κοινωνικά δίκτυα παριστάνοντας ότι είναι ένα μήνυμα ότι νίκησε ο χρήστης σε κάποιο διαγωνισμό, κλπ. Επίσης μπορεί να διαμοιρασθεί με την χρήση ιστοσελίδων επίθεσης.

Όσον αφορά την λειτουργία του, αυτό που κάνει μόλις ενεργοποιηθεί είναι να πολλαπλασιάσει τις διεργασίες και συγκεκριμένα τη διεργασία explorer.exeκάνοντας τον υπολογιστή να χάσει όλη την μνήμη RAM οδηγώντας σε επανεκκίνηση. Μόλις ο χρήστης ξανανοίξει τον υπολογιστή μέχρι και σε ασφαλή λειτουργία, αυτό θεωρείται και το

[98]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

πιο ανησυχητικό ότι τότε ο ιός που βρίσκεται στον τομέα εκκίνησης θα ενεργοποιηθεί προκαλώντας το ίδιο αποτέλεσμα μέχρι να καταστρέψει τον μολυσμένο υπολογιστή. [99]

Άλλες πηγές δείχνουν ότι ο ιός μοιάζει πολύ με τον Boot.Cidox , πράγμα που τον κάνει να απενεργοποιεί το τείχος προστασίας και το αντιβιοτικό πρόγραμμα παραμένοντας κρυμμένος στην μνήμη του υπολογιστή. Έτσι επιτρέπει σε άλλα κακόβουλα λογισμικά να εισέλθουν στον υπολογιστή. Τέλος κλέβει και προσωπικά δεδομένα.[100]

[99] http://www.enigmasoftware.com/bootcidex-removal/ 20/07/2015
[100] http://guides.yoosecurity.com/boot-cidex-removal-guide , 20/07/2015

2.2.2 Παρασιτικοί ιοί(Parasitic viruses)

Οι παρασιτικοί ιοί αν και θεωρούνται από τα μη επιτυχημένα κακόβουλα λογισμικά, λόγω του σχετικά εύκολου εντοπισμού τους, αποτελούν το πιο διαδεδομένο τύπο ιού στο Διαδίκτυο. Σύμφωνα με τον Ηλιάδη, «ο Παρασιτικός Ιός προσαρτάται στον κώδικα ενός εκτελέσιμου αρχείου είτε στην αρχή του κώδικα, είτε στην μέση, είτε στο κέντρο. Έτσι το μέγεθος του αρχείου αυξάνεται ανάλογα με το μέγεθος του ιού.»[101]

Θα γίνει αναφορά στον παρασιτικό ιό Datacrime. Αν και παλιός είναι ένα παράδειγμα διότι τοποθετούνταν στον κώδικα εκτελέσιμων αρχείων και εμφάνιζε ένα μήνυμα κάθε φορά που ο χρήστης έτρεχε το μολυσμένο πρόγραμμα αν και δεν προξένησε μεγάλο πρόβλημα από την άλλη δημιούργησε υστερία τον χρόνο κυκλοφορίας του το 1989 στην πλατφόρμα DOS.

Ο ιός έμπαινε στο μολυσμένο σύστημα με την μεταφορά ενός αρχείου και την εκτέλεση του. Όταν ένα μολυσμένο αρχείο εκτελεσθεί ο ιός ψάχνει να βρει στους διαθέσιμους δίσκους με την σειρά C: , D: , A: ,B: για αρχεία με κατάληξη .com. Αποφεύγει αρχεία με το «D» σαν το έβδομο γράμμα, έτσι ώστε να αποφύγει την μόλυνση του COMMAND.COM. Ο Ιός μολύνει ένα αρχείο .com κάθε φορά που ο χρήστης ανοίγει ένα από τα αρχεία που είχε ήδη μολύνει ο ιός. Ο ιός αντικαθιστά τα πρώτα 3 bytes από το μολυσμένο πρόγραμμα τα οποία οδηγούν στο σώμα του ιού, το οποίο μεταφέρεται στο τέλος του μολυσμένου αρχείου. Τα 3 αρχικά bytes βρίσκονται μέσα στο σώμα του ιού. Αν ένα μολυσμένο αρχείο ανοιχθεί στις 13 Οκτωμβρίου και έπειτα τότε ο ιός εμφανίζει το κρυπτογραφημένο μήνυμα: "DATACRIMEVIRUS' 'RELEASED MARCH 1989". Στην συνέχεια

[101]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

διαγράφει τα πρώτα 9 τμήματα του σκληρού δίσκου. Βέβαια υπάρχουν πολλά σφάλματα στον κώδικα της διαγραφής (Formatting Function)[102].

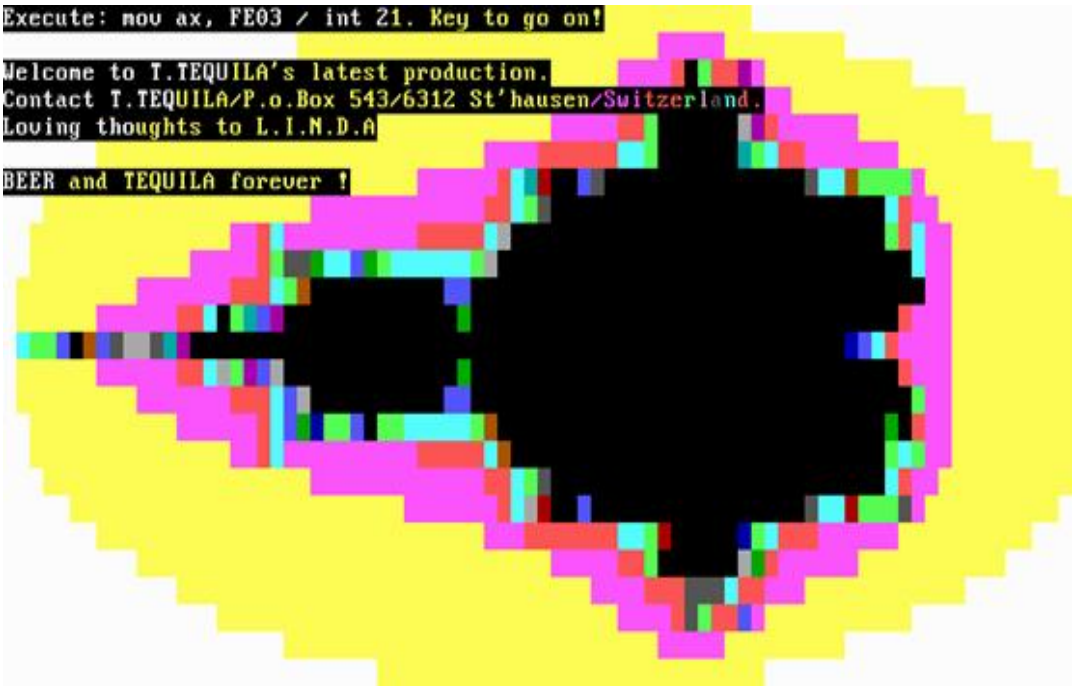
[102]http://virus.wikia.com/wiki/Datacrime

2.2.3 Πολυμερείς Ιοί(Multipartite Viruses)

Οι ιοί αυτής της κατηγορίας συνδυάζουν τις τεχνικές των δύο παραπάνω τύπων ιομορφικού λογισμικού. Παρασιτικοί, όταν μολύνουν εκτελέσιμα αρχεία και ιοί τομέα εκκίνησης, όταν μολύνουν τον τομέα εκκίνησης. [103]

Ένα παράδειγμα ιού αυτού του είδους είναι ο ιός Tequila, ο οποίος εμφανίστηκε το 1991 για συστήματα της DOS. Αυτό που έκανε ο συγκεκριμένος ιός όταν εκτελούνταν ένα αρχείο που τον περιείχε, ήταν να μολύνει τον κεντρικό τομέα εκκίνησης(Master Boot Record). Στην συνέχεια ο ιός μειώνει το μέγεθος του διαχωρισμού του δίσκου κατά 6 τομείς και τοποθετεί τον κώδικα του σε τομείς που είναι εκτός του διαχωρισμού. Όταν ο δίσκος εκκινηθεί, ο ιός διαμένει στην κύρια μνήμη. Όταν τα αρχεία .exeεκτελεσθούν τότε ο ιός τοποθετεί τα 2468 bytes του κώδικα του σ' αυτά. Δεν μολύνει αρχεία με τα γράμματα «sc» και «v». Αυτό το κάνει βέβαια για να αποφύγει την μόλυνση των αντιβιοτικών προγραμμάτων. Ο ιός εμφανίζει το παρακάτω μήνυμα μαζί με ένα φράκταλ όπως βλέπουμε παρακάτω:

[103]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.



Εικόνα 8 Ιός Tequila

Επίσης ο συγκεκριμένος ιός έχει πολλούς τρόπους να προστατεύει τον εαυτό του από τον εντοπισμό και την αποσυναρμολόγηση. Ο κώδικας του περιέχει πολλές άχρηστες εντολές για να μπερδέψει κάποιον που τον αποσυναρμολογεί. Επίσης χρησιμοποιεί χρονικές σφραγίδες(timestamps) για να δηλώσει πότε μόλυνε ένα συγκεκριμένο αρχείο και τοποθετεί τα δευτερόλεπτα στο αδύνατο νούμερο 62. Χρησιμοποιεί αυτήν την σφραγίδα για να υπολογίσει πότε θα αφαιρέσει τα 2468 Bytes από το μέγεθος του αρχείου, όταν ο χρήστης χρησιμοποιήσει την εντολή DIR.

Ο συγκεκριμένος ιός επεκτάθηκε πολύ στην Ευρώπη. Δύο άτομα, 18 και 21 ρωτήθηκαν από την Ελβετική αστυνομία για τον ιό το 1993. Ο ιός Tequila ήταν κοινός και στην Νότια Αφρική.

2.2.4 Κρυφοί Ιοί (Stealth Viruses)

Ως κρυφοί αναφέρονται οι ιοί που κρύβουν την μόλυνση που προκαλούν στα αρχεία με διάφορους τρόπους ώστε να μην γίνονται αντιληπτοί από αντιβιοτικά προγράμματα.

Σύμφωνα με τον Ηλιάδη, «Κάθε ιός κάνει κάποιες αλλαγές στα αρχεία ή τομείς εκκίνησης που προσβάλλει. Αυτές οι αλλαγές γίνονται αντιληπτές από τα αντιβιοτικά προγράμματα που τηρούν αρχείο με αθροίσματα ελέγχου(checksums) όλων των αρχείων που περιέχονται σε ένα υπολογιστικό σύστημα. Όταν ένα αντιβιοτικό πρόγραμμα αυτού του τύπου εκτελείται, συγκρίνει τα αθροίσματα ελέγχου των αρχείων στο δίσκο με τα αθροίσματα ελέγχου που είχε υπολογίσει στον προηγούμενο έλεγχο.

«Οι κρυφοί ιοί αποκτούν έλεγχο των κλήσεων συστήματος που αφορούν την πρόσβαση σε αρχεία. Μ' αυτό τον τρόπο αποκρύπτουν από τα αντιβιοτικά προγράμματα το γεγονός ότι ένα αρχείο έχει μολυνθεί.» [104]

Τεχνικά, σύμφωνα με την Kaspersky:«Ένας κρυφός ιός μπορεί να μολύνει το σύστημα με διάφορους τρόπους. Για παράδειγμα, όταν ένας χρήστης κατεβάσει ένα κακόβουλο συνημμένο αρχείο, ή εγκαταστήσει ένα κακόβουλο λογισμικό που παριστάνει ότι είναι ένα νόμιμο πρόγραμμα από μια ιστοσελίδα, είτε με το να χρησιμοποιεί μη πιστοποιημένα προγράμματα γεμάτα κακόβουλο λογισμικό. Όπως και με τους άλλους ιούς, ο κρυφός ιός έχει την δυνατότητα να ελέγχει πάρα πολλές κλήσεις συστήματος. Όταν οι υπόλοιποι τύποι ιών πραγματοποιούν τέτοιες διεργασίες, τα αντιβιοτικά προγράμματα μπορούν να εντοπίσουν το κακόβουλο λογισμικό, οι Κρυφοί Ιοί όμως

[104]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

έχουν την δυνατότητα να παραμένουν ενεργητικά στην αφάνεια. Αυτό το καταφέρνουν είτε μεταφέροντας τον εαυτό τους μακριά από το αρχείο που μολύνθηκε, σε κάποιον άλλο σκληρό δίσκο, αφήνοντας ένα καθαρό αρχείο. Επίσης οι Κρυφοί Ιοί μπορούν να αποκρύπτονται αλλάζοντας το μέγεθος του αρχείο που μολύνθηκε.» [105]

Ως παράδειγμα θα αναφέρω στην κατηγορία ιών Xorer. Ένας από αυτούς τους ιούς ήταν ο Xorer.X που εμφανίστηκε το 2007. Φέτος, το 2015, υπάρχει χαμηλή πιθανότητα να μολυνθεί κανείς από τέτοιου είδους κακόβουλο λογισμικό.

Ο Xorer.Χλοιπόν, είναι ένας ιός prepender, δηλαδή η ρουτίνα μόλυνσης του δεν αφορά απευθείας τροποποίηση του ξενιστή-προγράμματος , και τοποθέτηση του κώδικα του σ' αυτό, αλλά προσάπτει όλο το εκτελέσιμο αρχείο ως overlaytου. Αναζητεί τους ξενιστές/εκτελέσιμα αρχεία σε όλους τους σκληρούς δίσκους. Στην συνέχεια όταν εντοπίσει το αρχείο δημιουργεί ένα αντίγραφο του αρχείου με κατάληξη .pif και το αρχικό τους όνομα. Ταυτόχρονα, τοποθετεί τον κώδικά του στο μολυσμένο πρόγραμμα που αντέγραψε και εγράφει και τον κώδικα του αρχείου στο τμήμα με τους πόρους στο κώδικα του τοποθετώντας 8 bytesστο overlay του ιού. Αυτός ο ιός επιπλέον κλέβει το εικονίδιο του προγράμματος ξενιστή, έτσι ώστε να μην υπάρχουν διαφορές μεταξύ του αρχικού και του μολυσμένου αρχείου. Βέβαια κάνοντας τα παραπάνω το μολυσμένο αρχείο έχει αυξηθεί σε χωρητικότητα κατά 64 KBσε σχέση πάντα με το αρχικό.

Όταν, αρχικά, εκτελείται, ο ιός κάνει εκτέλεση του ξενιστή, τοποθετώντας το αρχικό του εκτελέσιμο πρόγραμμα, σαν ένα κρυφό αρχείο, με όνομα [αρχικό-όνομα-προγράμματος].~tmp. Όταν ο ξενιστής

[105] http://usa.kaspersky.com/internet-security-center/definitions/stealth-virus#.VcelmjYVjml , 08/08/2015

σταματήσει την εκτέλεση του, ο ιός προσπαθεί να μολύνει το αρχείο συστήματος %System%\Drivers\Isass.exe.Αν επιτύχει θα κάνει εκτέλεση του νέου μολυσμένου αρχείου και θα συνεχίσει με την σειρά ενεργειών εκεί. Αν αποτύχει θα υποθέσει ότι μόλυνε το σύστημα και ότι είναι ενεργό στην μνήμη.

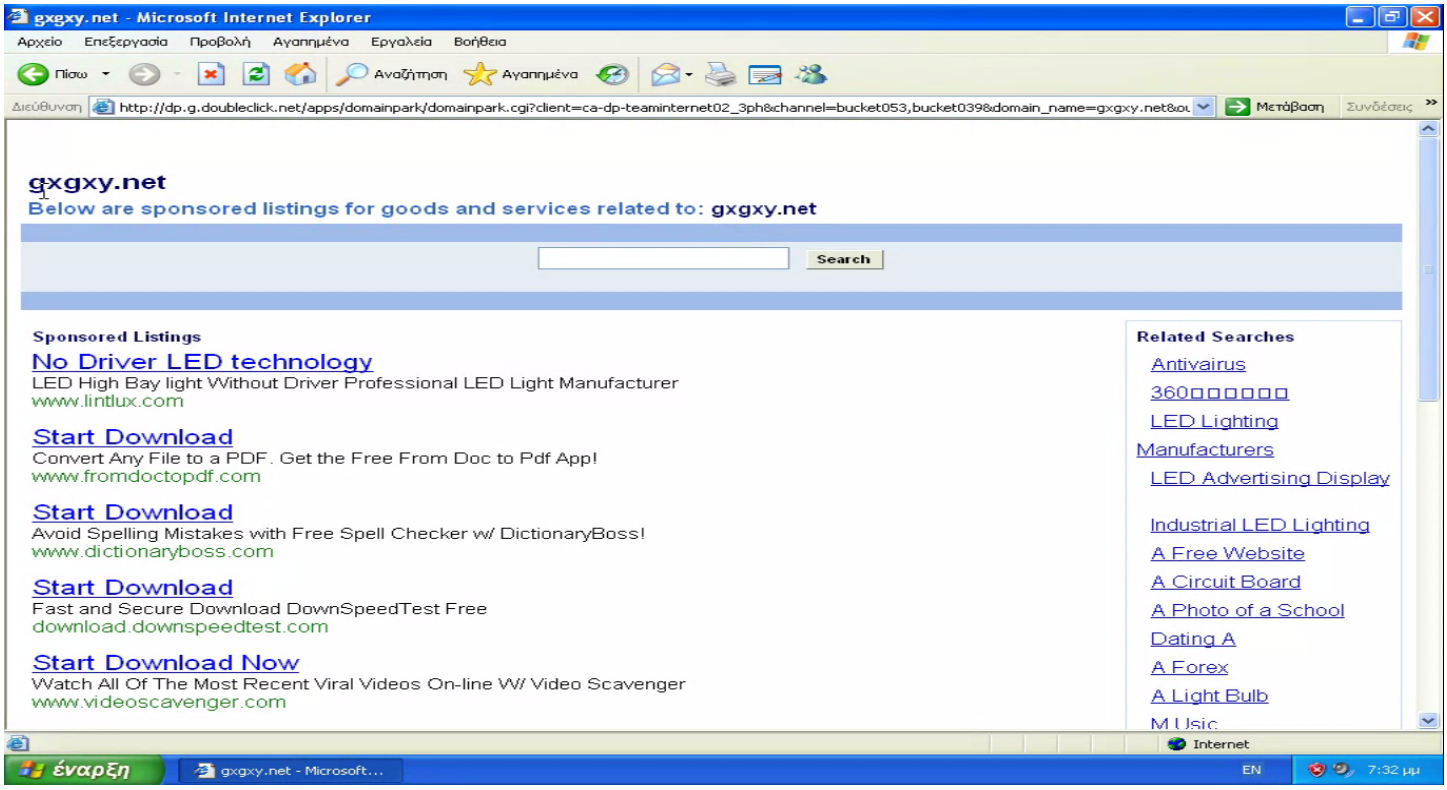
Όταν το νέο μολυσμένο αρχείο εκτελεσθεί, ο ιός τοποθετεί τέσσερις χρονοδιακόπτες. Ο πρώτος εκτελείται κάθε 1 δευτερόλεπτο, και είναι υπεύθυνος για συνεχή παρακολούθηση για την ύπαρξη του αρχείου του ιού στην τοποθεσία Documents and Settings\[όνομα χρήστη]\StartMenu\Programs\Startup\~.pif. Αν το αρχείο δεν υπάρχει, είτε δεν το έφτιαξε ακόμα, ή σβήστηκε` σε κάθε περίπτωση, το ξανάδημιουργεί. Επιπλέον απαριθμεί τους δίσκους και τοποθετεί μέσα στο καθένα, ένα αντίγραφο του εαυτού στο root με όνομα "pagefile.pif" και ένα "autorun.inf" που θα το σημαδεύει. Αυτός ο χρονοδιακόπτης θα ενεργοποιεί και την ρουτίνα μόλυνσης που συζητήθηκε προηγουμένως.

Ο δεύτερος χρονοδιακόπτης ενεργοποιείται κάθε 15 δευτερόλεπτα, με τον ιό να παρατηρεί αν υπάρχει κάποιο παράθυρο ανοιχτό που το όνομα της κλάσης του είναι IEFrame (το οποίο ανήκει στο InternetExplorer) και αν το βρει στέλνει διαφημίσεις με κακόβουλο περιεχόμενο.

Ο τρίτος χρονοδιακόπτης, ο οποίος ενεργοποιείται κάθε δυόμιση ώρες, κάνει ότι ακριβώς και ο δεύτερος με μόνη διαφορά ότι θα ξεκινά την διεργασία του Internet Explorer από μόνο του στέλνοντας κακόβουλο διαφημιστικό περιεχόμενο.

Τέλος, ο τέταρτος χρονοδιακόπτης ενεργοποιείται όταν έχουν πράξει οι προηγούμενοι έστω μία φορά, και κάνει ότι ακριβώς και ο τρίτος μόνο που η χρονική διάρκεια στην οποία δρα είναι κάθε λεπτό.[106]

[106] https://thepiratebay.gd/torrent/7066921/Vx_heavens_collection(all), 17/08/2015



Εικόνα 9 από VM (Virtual Machine) Δεύτερος χρονοδιακόπτης

2.2.5 Κρυπτογραφημένοι Ιοί(Encryptedviruses)

Αυτός ο τύπος ιών χρησιμοποιεί κρυπτογραφία στον κώδικα του, μόλις μολύνει ένα σύστημα «μεταμορφώνει» το κώδικα του από κρυπτογραφημένο σε μη και τον εκτελεί.

Σύμφωνα με τον Ηλιάδη: «Ορισμένα αντιβιοτικά προγράμματα προσπαθούν να ανιχνεύσουν την ύπαρξη ιών συγκρίνοντας τον κώδικα στα αρχεία που ελέγχουν με ακολουθίες κώδικα που ανήκουν σε ήδη ταυτοποιημένους ιούς.»

Βέβαια ο παραπάνω τρόπος σφάλει και έτσι ο Ηλιάδης συνεχίζει: «Οι Κρυπτογραφημένοι ιοί(EncryptedViruses) αποφεύγουν την ανίχνευση από τα προαναφερθέντα αντιβιοτικά προγράμματα, κρυπτογραφώντας μεγάλο τμήμα του ιού, αφήνοντας σε νη κρυπτογραφημένη μορφή μόνο μια απλή ρουτίνα αποκρυπτογράφησης και ένα τυχαίο κλειδί κρυπτογράφησης.»[107]

Ο Ευγένιος Κωνσταντίνου αναφέρει ότι: « Μία από τις πρώτες και πιο εύκολες μεθόδους που οι προγραμματιστές ιών χρησιμοποίησαν για να κρύψουν την λειτουργικότητα ενός ιομορφικού κώδικα ήταν η κρυπτογραφία. Συνήθως ένας κρυπτογραφημένος ιός αποτελείται από δύο μέρη: τον κώδικα αποκρυπτογράφησης και τον κρυπτογραφημένο κώδικα. Ο κώδικας αποκρυπτογράφησης ενεργοποιείται όταν ένα μολυσμένο πρόγραμμα εκτελείται και αποκρυπτογραφεί τον κώδικα του ιού.»[108]

Ο πρώτος ιός που χρησιμοποίησε τέτοιου είδους τεχνική ήταν ο Cascade ο οποίος χρησιμοποιούσε ένα αρκετά περίπλοκο για την εποχή του αλγόριθμο. Περιλάμβανε XOR-ing σε κάθε byte δύο φορές με

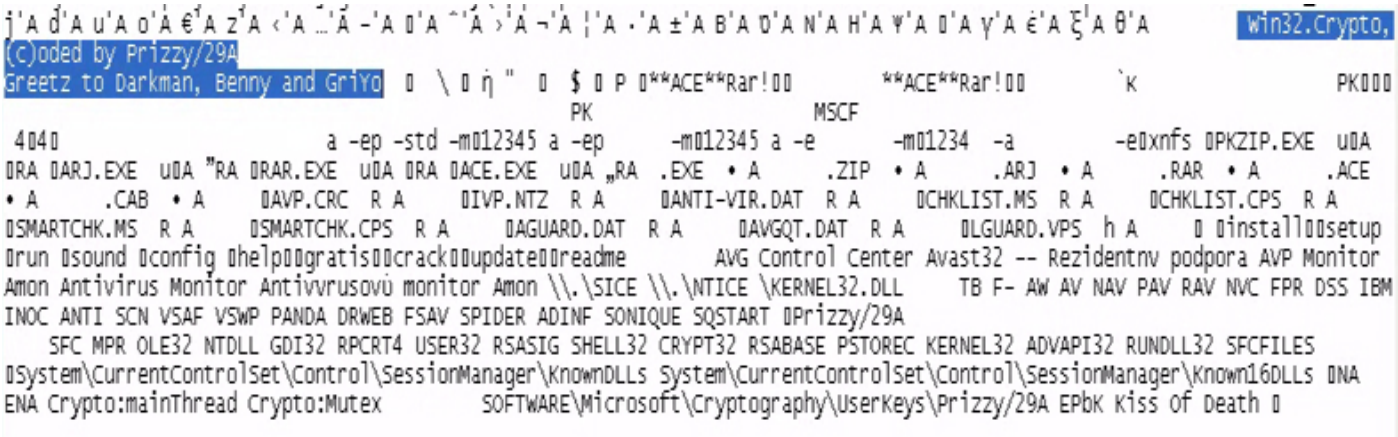
[107]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[108]Konstantinou, Evgenios,Metamorphic Virus: Analysis and Detection, Royal Holloway University of London, London, 2008. Available at: https://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-02.pdf/

μεταβλητές τιμές, μία από αυτές που βασίζεται στο μέγεθος του προγράμματος.[109]

Θα γίνει ανάλυση του ιού Crypto, ενός ιού Win32 , ο οποίος αρχικά μολύνει αρχεία PE(Portable Executable), τοποθετώντας τον κώδικά του στο τέλος του κώδικα του εκτελέσιμου αρχείου σε κρυπτογραφημένη μορφή. Επιπλέον αυτός ο ιός μπορεί να μεταλλάσσεται perse και είναι δύσκολο να εντοπιστεί. Το μέγεθος τουαρχικού ιού είναι 20 KB δηλαδή ο Cryptoγια ιός είναι μεγάλου μεγέθους.

Όταν ένα μολυσμένο αρχείο εκτελεσθεί, ο ιός μολύνει το KERNEL32.DLL στο κατάλογο \Windows. Είναι σημαντικό να τονισθεί ότι ο ιός δεν είναι κρυπτογραφημένος όταν μολύνει αυτό το αρχείο και έτσι η λογική του μπορεί να κατανοηθεί με οποιοδήποτε εργαλείο εμφάνισης(viewing tool). Μολυσμένα αρχεία KERNEL32.DLL περιείχαν τη σειρά κείμενο: «Win32.Crypto, (c)oded by Prizzy/29A Greetz to Darkman, Benny and GriYo Kiss Of Death», όπως βλέπουμε στην φωτογραφία 10 από το VM.



Εικόνα 10 από VM(Virtual Machine) Μολυσμένο Kernel32 (Κώδικας Ιού)

[109]Skualson , 1990

Όμως έτσι ώστε να ενεργοποιηθεί το συγκεκριμένο αρχείο, ο ιός δημιουργεί ένα δικό του αρχείο με όνομα wininit.ini το οποίο δρομολογεί στα Windows μια διεργασία στην επόμενη εκκίνηση του υπολογιστή για το συγκεκριμένο αρχείο.Όταν ο υπολογιστής ενεργοποιηθεί ξανά με το μολυσμένο KERNEL32.DLL ο κώδικας του ιού ενεργοποιείται και ο ιός προσπαθεί να μολύνει 20 αρχεία στην εκκίνηση του υπολογιστή και επίσης ελέγχει για γνωστά αρχεία archivesκαι τα μολύνει με την χρήση διαθέσιμων συστημάτων archives όπως PKZIP.EXE, ARJ.EXE, RAR.EXE και ACE.EXE. Ο ιός τοποθετεί τα μολυσμένα αρχεία στα archives που βρήκε προηγουμένως. Εκτός από τ' ότι είναι ένας κρυπτογραφημένος ιός, αποτελείται και από στοιχεία συμπεριφοράς ρετρο-ιού για τους οποίους θα μιλήσουμε στην συνέχεια αναλύοντας περεταίρω το προηγούμενο παράδειγμα. [110]

[110]http://www.symantec.com/security_response/writeup.jsp?docid=2000-121515-4637-99&tabid=2 25/08/2015

2.2.6 Ρετρο-Ιοί(Retroviruses)

Σύμφωνα με τον Ηλιάδη: «Πρόκειται για τους ιούς που προσπαθούν να ανιχνεύσουν την ύπαρξη αντιβιοτικών προγραμμάτων , και να τα καταστήσουν αναποτελεσματικά. Οι Ρετρο-Ιοί εκμεταλλεύονται συγκεκριμένες στιγμές κατά τις οποίες τα αντιβιοτικά προγράμματα είναι ευάλωτα , όπως π.χ. κατά την διάρκεια ενημέρωσης των αντιβιοτικών προγραμμάτων στην επόμενη έκδοση τους.»[111]

Οι Ρετρο-Ιοί λοιπόν βασιζόμενοι στο βιολογικό όρο «ρετρο-ιός», είναι ιοί οι οποίοι αναζητούν ένα αντιβιοτικό πρόγραμμα σ' ένα υπολογιστή και του επιτίθενται. Ένας Ρετρο-Ιός θα προσπαθήσει να απενεργοποιήσει και να μολύνει το αντιβιοτικό πρόγραμμα για να αποφύγει την ανίχνευση στο υπολογιστικό σύστημα. Επίσης τους αποκαλούν με τον όρο« anti-antivirusvirus», αντί-αντιβιοτικός ιός.[112]

Το παράδειγμα που τέθηκε στο κεφάλαιο 2.1.5 με τον ιό Crypto θα αναλυθεί περεταίρω σ' αυτό το κεφάλαιο. Ο Crypto λοιπόν δίνει προσοχή σε συγκεκριμένα debuggers λογισμικών. Σβήνει αρχεία δεδομένων αντιβιοτικών προγραμμάτων και απενεργοποιεί τις αντιβιοτικές λειτουργίες ορισμένων προγραμμάτων (archiving).

Τεχνικά, ο ιός τοποθετεί στο στόχαστρο του τα παρακάτω αρχεία αντιβιοτικών προγραμμάτων:

- AVP.CRC
- IVP.NTZ
- ANTI-VIR.DAT
- CHKLIST.MS
- SMARTCHK.MS
- SMARTCHK.CPS

---

[111]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[112]http://www.webopedia.com/TERM/R/retrovirus.html (27/08/2015)

- AGUARD.DAT
- AVGQT.DAT,
- LGUARD.VPS

Ο Crypto επιπλέον έχει δυνατότητες αποφυγής. Αρχικά αποφεύγει την μόλυνση γνωστών αντιβιοτικών προγραμμάτων ή προγράμματα που κάνουν συχνά αθροίσματα ελέγχου. Επιπλέον ο ιός θα αποφεύγει τα αρχεία που αρχίζουν από:

- TB
- F-
- AW
- AV
- NAV
- PAV
- RAV
- NVC
- FPR
- DSS
- IBM
- INOC
- ANTI
- SCN
- VSAF
- VSWP
- PANDA
- DRWEB
- FSAV
- SPIDER
- ADINF

- SONIQUE
- SQSTART

Τέλος ο ιός επίσης ελέγχει ώστε να μην μολύνει αρχεία που παρακολουθούνται από το σύστημα για αλλαγές.[113]

[113] όπως και παραπάνω

2.2.7 Πολυμορφικοί Ιοί(PolymorphicViruses)

Οι Πολυμορφικοί Ιοί αποτελούν μια αναβαθμισμένη μορφή των Κρυπτογραφημένων Ιών (Κεφ. 2.1.5). Σύμφωνα με τον Ηλιάδη: « Στη περίπτωση των Κρυπτογραφημένων ιών, η ρουτίνα αποκρυπτογράφησης παραμένει σε μη κρυπτογραφημένη μορφή, σε αντίθεση με το υπόλοιπο τμήμα του ιού που κρυπτογραφείται με τυχαίο κλειδί. Τα αντιβιοτικά προγράμματα που ανιχνεύουν ιούς με βάση ακολουθίες κώδικα ταυτοποιημένων ιών μπορούν να εντοπίσουν έναν κρυπτογραφημένο ιό , ανιχνεύοντας το υπολογιστικό σύστημα για τις προαναφερθείσες ρουτίνες αποκρυπτογράφησης.»[114]

Στην συνέχεια, ο Κωνσταντίνου αναφέρει: «Ένας Πολυμορφικός Ιός είναι ένα ιός που παίρνει πολλές μορφές. Οι Πολυμορφικοί Ιοί μπορεί να μεταλλάξουν τους decryptors τους σε μεγάλο αριθμό διαφορετικών περιπτώσεων που παίρνουν εκατομμύρια διαφορετικές μορφές. Χρησιμοποιούν τη μηχανή μεταλλάξεων(mutation engine) τους για να δημιουργήσουν μια καινούρια ρουτίνα αποκρυπτογράφησης κάθε φορά που μολύνουν ένα πρόγραμμα. Η καινούρια ρουτίνα αποκρυπτογράφησης θα έχει ακριβώς την ίδια λειτουργία, αλλά η σειρά εντολών μπορεί να είναι εντελώς διαφορετική».[115]

Επιπλέον ο Ηλιάδης αναφέρει ότι: «Οι Πολυμορφικοί Ιοί αποτελούνται από Κρυπτογραφημένους Ιούς οι οποίοι μεταβάλλουν την ρουτίνα αποκρυπτογράφησης μετά από κάθε προσβολή αρχείου ξενιστή. Με αυτόν τον τρόπο, οι Πολυμορφικοί Ιοί αποφεύγουν την ανίχνευση από αντιβιοτικά προγράμματα που χρησιμοποιούν ακολουθίες κώδικα

[114]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[115] Konstantinou, Evgenios, Metamorphic Virus: Analysis and Detection, Royal Holloway University of London, London, 2008. Available at: https://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-02.pdf/

ταυτοποιημένων ιών , με μεγαλύτερη επιτυχία σε σύγκριση με τους Κρυπτογραφημένους ιούς.»[116]

Ως παράδειγμα θα τεθεί ο ιός Win32.Driller, ο οποίος είναι ένας παρασιτικός, υπερβολικά πολυμορφικός και ιός που κατοικεί στην μνήμη για κάθε διεργασία του. Ο ιός μολύνει PE εκτελέσιμα αρχεία με καταλήξεις .EXE, .SCR, .CPL, μόλις εκτελεσθεί. Ο ιός παραμένει στην μνήμη του συστήματος ως ένα κομμάτι του μολυσμένου ξενιστή/προγράμματος, και παίρνει έλεγχο των λειτουργιών KERNEL και παρεμβαίνει σε 15 από αυτές: αναζήτηση αρχείων, άνοιγμα , αντιγραφή , αποκοπή/μετακίνηση αρχείων κτλ. Όταν ένα PE εκτελέσιμο πρόγραμμα χρησιμοποιήσει μία από τις παραπάνω λειτουργίες/εντολές συστήματος ο ιός το μολύνει. Σαν αποτέλεσμα, ο ιός θα μολύνει όλα τα PE εκτελέσιμα αρχεία και ο ιός θα παραμείνει ενεργός μέχρι να κλείσει το πρόγραμμα/ξενιστής. Στην διάρκεια της μόλυνσης ο ιός κρυπτογραφεί το 8K κώδικα του και τοποθετείται στο τέλος του κώδικα του αρχείου. Ο ιός στην συνέχεια διαβάζει το 8K κώδικα του μολυσμένου αρχείου και το κρυπτογραφεί τοποθετώντας το στο τέλος μετά τον κώδικα του. Στο κενό που δημιουργείται από την μετακίνηση του κώδικα τοποθετείται μια ρουτίνα αποκρυπτογράφησης του κεντρικού πολυμορφικού κώδικα του ιού. Το παραπάνω φαίνεται στο σχήμα:

Συνήθως το πολυμορφικό σύστημα (Polymorphic Engine) του ιού κολλάεικαι ο ιός δεν μπορεί να αποκρυπτογραφήσει τον κώδικα του εμφανίζοντας ένα μήνυμα σφάλματος του ξενιστή/προγράμματος.

Τις Παρασκευές και βασιζόμενο και στην ημερομηνία ο ιός αντικαθιστά την αρχική σελίδα του MS Internet Explorer και του Netscape Navigator με την ιστοσελίδα: «http://www.thehungersite.com».

[116]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

Ο ιός περιέχει το παρακάτω κείμενο «πνευματικής ιδιοκτησίας»:

«[Virus TUAREG by The Mental Driller|29A]

- This virus has been designed for carrying the TUAREG engine -- » [117]

[117] https://archive.is/20140702092942/https://www.securelist.com/en/descriptions/70544/Virus.Win32.Driller , 25/09/2015

2.2.8 Ιοί που διαγράφουν τμήμα του ξενιστή(FileOverwriters)

Αυτό το είδος ιών είναι το πιο εύκολα αντιληπτό από λογισμικά προστασίας, διότι εκτός από το να μολύνουν τα αρχεία και να τα αφήνουν ανέπαφα όπως οι Παρασιτικοί Ιοί (Κεφ.2.1.2), οι Ιοί που διαγράφουν τμήμα του ξενιστή σβήνουν τμήμα ή ολόκληρο το αρχείο που προσβάλουν.

Σύμφωνα με τον Ηλιάδη: «Υπάρχει όμως και η κατηγορία Ιών που διαγράφουν τμήμα του ξενιστή (Overwriters) ή και όλα τα περιεχόμενα του ξενιστή. Αυτό τους καθιστά ιδιαίτερα ανιχνεύσιμους από αντιβιοτικό λογισμικό.»[118]

Ως παράδειγμα θα θέσω τον ιό LoveLetter που κάποιοι θεωρούν και ως αναπαραγωγό. Πρωτοεμφανίστηκε το 2000 και με πάρα πολλές παραλλαγές υφίσταται και ως σήμερα. «Ο κίνδυνος μόλυνσης είναι χαμηλός επιπέδου 2» ,σύμφωνα με την Synatrec.

Ο ιός εισέρχεται στο σύστημα με email που έχει θέμα «ILOVEYOU». Τοκείμενοτουμηνύματοςείναιωςεξής: «Kindly check the attached LOVE LETTER coming from me».

Το επισυναπτόμενο αρχείο φαίνεται να είναι ένα αρχείο .txt αλλά πίσω από αυτό κρύβεται ένα εκτελέσιμο αρχείο Visual Basic .vbs. Μόλις το αρχείο εκτελεσθεί, ο χρήστης δεν λαμβάνει καμία ειδοποίηση και έτσι ο ιός τοποθετείται στις παρακάτω τοποθεσίες:

- %System%\Mskernel32.vbs
- %System%\LOVE-LETTER-FOR-YOU.TXT.vbs
- %Windows%\Win32dll.vbs

Στην συνέχεια , ο ιός ελέγχει αν υπάρχει στο υπολογιστή το αρχείο Win-bugsfix.exe στο φάκελο %System% και αν δεν υπάρχει τοποθετεί ως

[118]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

αρχική σελίδα μια τοποθεσία που κατεβάζει το Win-bugsfix.exe. Αν το αρχείο υπάρχει τότε ο ιός δημιουργεί ένα SubKey στο Registry:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX

Μόλις γίνει επανεκκίνηση και όταν το αρχείο αυτό εκτελεσθεί ο ιός τοποθετεί στον Internet Explorer μια κενή σελίδα ως αρχική.

Για κάθε δίσκο συμπεριλαμβανομένων και δίσκων δικτύου, ο ιός αναζητεί αρχεία με κατάληξη .vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .mp3 και .mp2. Στην συνέχεια ο ιός επικαλύπτει τα αρχεία που βρήκε και τα αντικαθιστά με τον εαυτό του δίνοντας τους το ίδιο όνομα. Για παράδειγμα μια φωτογραφία με όνομα «Τοπίο.jpg» θα μετατραπεί σε «Τοπίο.vbs» και το αρχικό αρχείο θα διαγραφθεί. Για τα αρχεία με κατάληξη .mp2 και .mp3 ο ιός κάνει μια εξαίρεση και απλά κρύβει τα αρχεία και τοποθετεί αντίγραφα του εαυτού του στην θέση τους, αλλά έτσι τα αρχεία αυτά δεν χάνονται απλά εάν ο χρήστης έχει τις default ρυθμίσεις στον υπολογιστή του δεν θα του εμφανίζονται τα αρχεία.

Ο λόγος που αυτός ο ιός θεωρείται αναπαραγωγός έγκειται στο γεγονός ότι χρησιμοποιεί το ηλεκτρονικό ταχυδρομείο και το mIRC για να αναπαραχθεί. Αρχικώς χρησιμοποιεί κλήσεις MAPI(Message Application Programming Interface) για να εισβάλει στο ηλεκτρονικό ταχυδρομείο του προγράμματος Microsoft Outlook και δημιουργεί μηνύματα τα οποία στέλνει σε όλους τους παρευρισκόμενους στο κατάλογο διευθύνσεων του χρήστη. Για να βεβαιωθεί ο ιός ότι έχει στείλει τα μηνύματα σε όλους μία φορά ο ιός ελέγχει το Microsoft Registry. Όσον αφορά το mIRC , δημιουργεί ένα αρχείο Script.ini στο φάκελο του προγράμματος mIRC. Το script αυτό στέλνει το αρχείο LOVELETTERFORYOU.HTM σε άλλους χρήστες στο chatroom και έτσι επιτρέπει την αναπαραγωγή του.

Τέλος αφήνει το αρχείο LOVELETTERFORYOU.HTM στο φάκελο Windows\%System32%.

2.2.9 Μακρο-Ιοί(MarcoViruses)

Ως τους πιο πλέον διαδεδομένους ιούς, αναφέρονται οι Μακρο-Ιοί, οι οποίοι μπορούν να προσβάλλουν όλα τα λειτουργικά συστήματα που χρησιμοποιούν προγράμματα με μακροεντολές.

Όπως αναφέρει ο Ηλιάδης: «Μακρο-Ιοί είναι οι Ιοί που αποτελούνται από μια ακολουθία εντολών, η οποία διερμηνεύεται (interpreted) αντί να εκτελείται(executed).» [119]

Σύμφωνα με τον ορισμό της Kapresky: «Ένας Μακρο-Ιός είναι ένας ιός ο οποίος μεταλλάσει ή αντικαθιστά μια μακροεντολή, η οποία είναι μια σειρά ενεργειών που χρησιμοποιείται από προγράμματα για να εκτελούν συχνές εντολές. Για παράδειγμα, η πράξη "Open Document", που χρησιμοποιείται από πολλά προγράμματα επεξεργασίας κειμένου βασίζετε σε μακροεντολή με αρκετά κρυφά βήματα στην διεργασία αυτή. Οι Μακρο-Ιοί αλλάζουν αυτή την σειρά εντολών, επιτρέποντας τους έτσι να εκτελεστούν όταν εκτελείται η μακροεντολή.» [120]

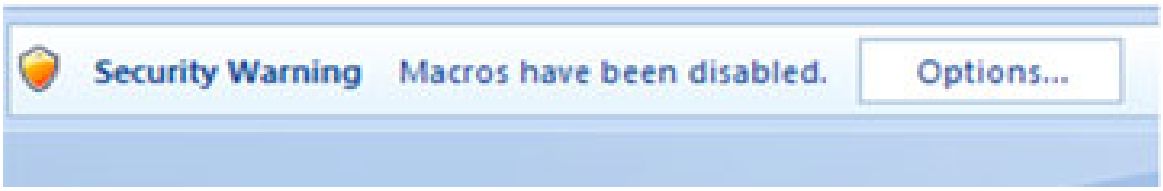
Οι Ιοί αυτής της κατηγορίας μεταφέρονται μέσω ηλεκτρονικού ταχυδρομείου καθώς αρχεία λογισμικού που χρησιμοποιεί μακροεντολές, όπως Microsoft Word, OpenOffice Write και άλλα πολλά, στέλνονται καθημερινά μέσω του συστήματος SMTP, το οποίο αν μολυνθεί όσον αφορά την περιεκτικότητα αρχείων, θα μπορούσε ένας κακόβουλος χρήστης να τοποθετήσει τον Μακρο-Ιό στο αρχείο που αποστέλλεται με μια πολύ απλή εντολή τοποθέτησης στο προσβαλλόμενο εκείνη την στιγμή αρχείο.

Για την τεκμηρίωση της άποψης ότι οι Μακρο-Ιοί είναι ακόμα και σήμερα στο προσκήνιο, ο Szappanos της Sophos αναλύει το γεγονός ότι οι

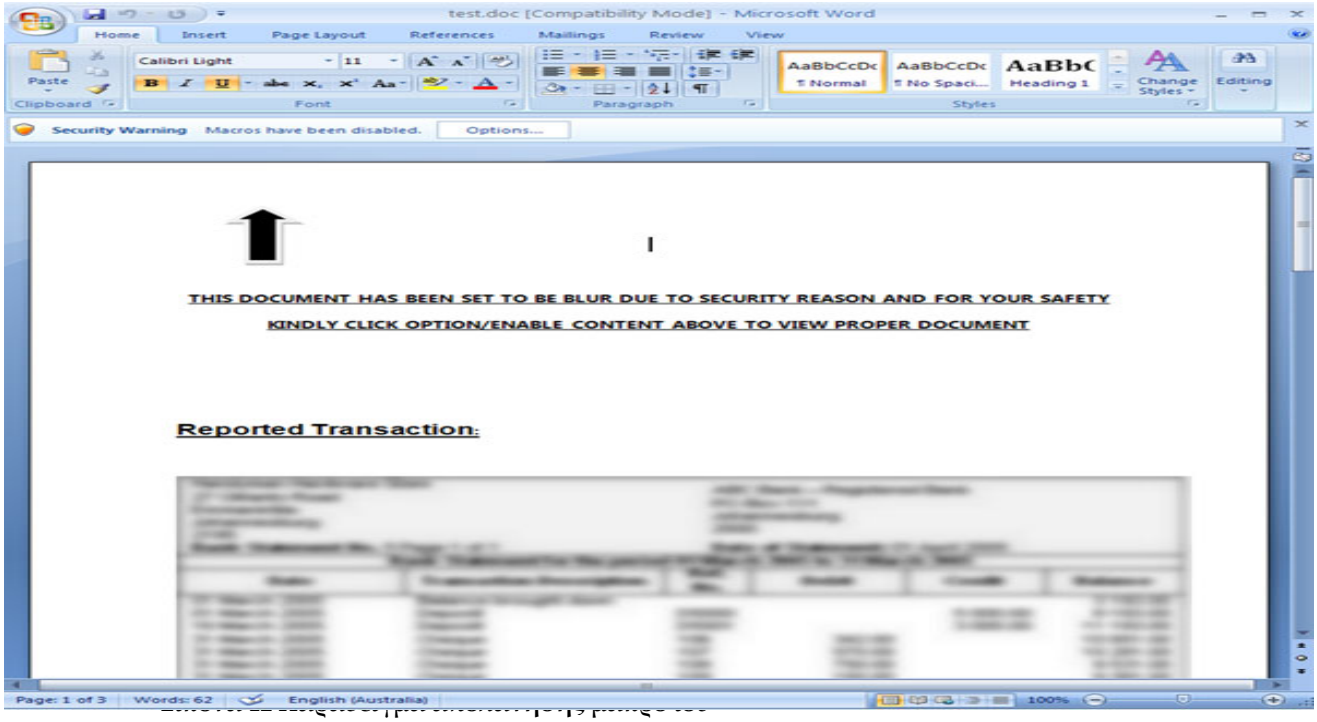
[119]Ηλιάδης, Γιάννης,Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

[120]https://usa.kaspersky.com/internet-security-center/definitions/macro-virus#.VeBDkjYVhhg, 28/08/2015

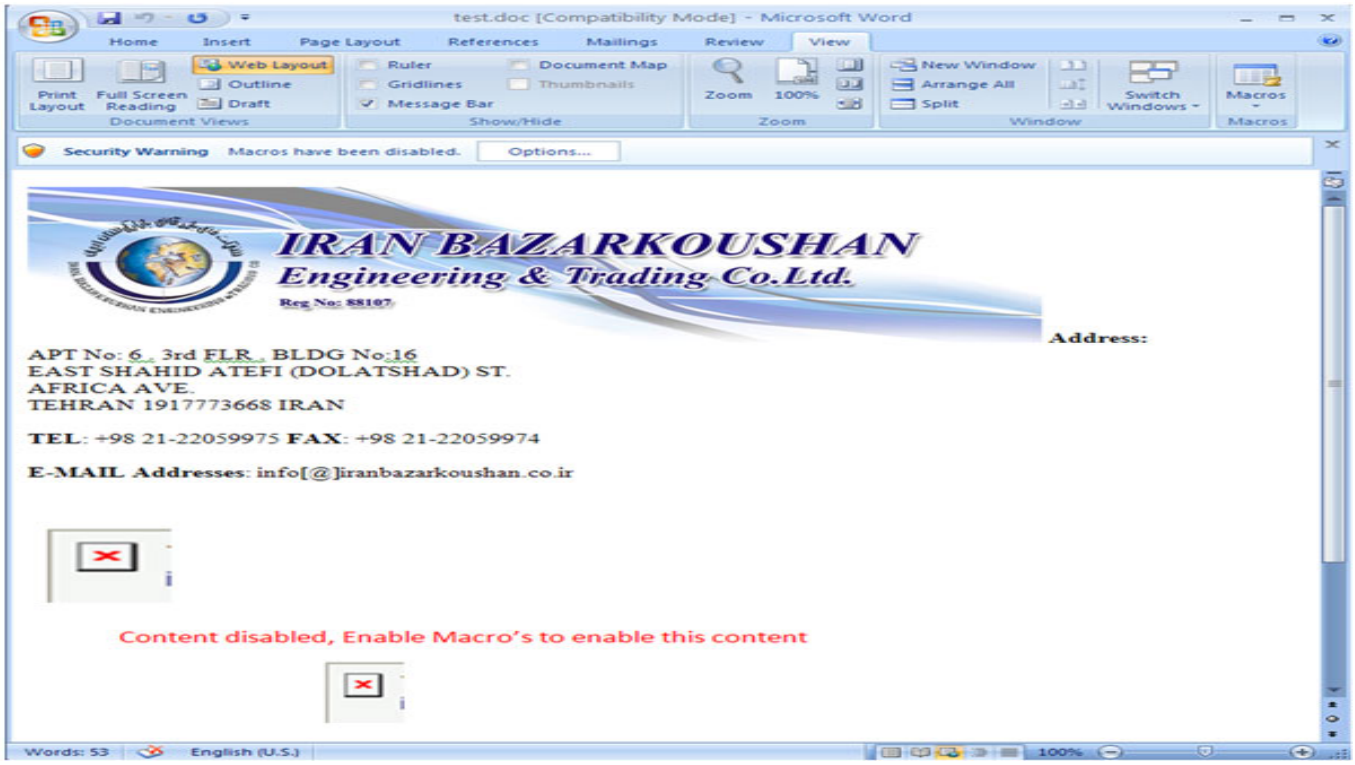
Μακρο-Ιοί μπορεί να ήταν στο προσκήνιο την δεκαετία του 90 αλλά και το 2014 «VBA is not dead». Στο άρθρο με τον ομώνυμο τίτλο ο Szappanos αναφέρει τους νέους τρόπους που οι κακόβουλοι χρήστες εκμεταλλεύονται τους χρήστες του διαδικτύου για να τοποθετήσουν τους Μακρο-Ιούς. Αναφέρει την «Κοινωνική Μηχανική»(Social Engineering). Και ενώ το λογισμικό της Microsoft τοποθετεί προειδοποιήσεις, όπως η παρακάτω(εικόνα 11) οι κακόβουλοι χρήστες έχουν τοποθετήσει οδηγίες για σφάλματα αναφερόμενοι και σε θέματα ασφάλειας, βλέπουμε το βελάκι στην επόμενη εικόνα(εικόνα 12). Κάτι το εξωφρενικό είναι ότι οι χρήστες που λαμβάνουν τέτοιο κακόβουλο λογισμικό είναι πρόθυμοι να παραβιαστεί το σύστημα τους ώστε να λυθεί η περιέργεια τους. (Εικόνα 13).



Εικόνα 11 Security Warning Microsoft Office



Εικόνα 13 Παράδειγμα Μακρό Ιού



Ως παράδειγμα δίδεται οιός Cybernet.A. Ο Ιός αυτός διανέμεται μέσω ηλεκτρονικού ταχυδρομίου με θέμα « You've GOT Mail !!». Το κείμενο του μηνύματος είναι: «Please, saved the document after you read and don't show to anyone else. The document is also VIRUS FREE...so DISREGARD the virus protection warning!!!». Όπως προηγουμένως η αντίληψη της «Κοινωνικής Μηχανικής» σε όλο της το μεγαλείο.

Ο ιός αυτός μολύνει και αρχεία του Word αλλά και του Excel. Για να μολύνει το Excel ο Ιός δημιουργεί ένα αρχείο με όνομα «CyberNET.xls». Επιπλέον ο ιός απενεργοποιεί την προειδοποίηση του Word και του Excel.(Εικόνα 2.5)

Αποστέλλει χρησιμοποιώντας το Microsoft Outlook τα μολυσμένο αρχείο μαζικά σε όλους τις διευθύνσεις του καταλόγου του χρήστη. Έπειτα διαγράφει όλα τα .xl? αρχεία που υπάρχουν στο φάκελο του Excel στην τοποθεσία \Program Files\Microsoft Office\Office\Xlstart. Στην συνέχεια τοποθετεί εκεί το αρχείο CyberNET.xls. Στην συνέχεια διαγράφει το πρότυπο Normal.dot. Επίσης διαγράφει όλα τα αρχεία .do? από τον

φάκελο του Word\Program Files\Microsoft Office\Office\Startup. Τέλος τοποθετεί ένα νέο μολυσμένο αρχείο Normal.dot. Η πολυμορφικότητα έγκειται στο γεγονός ότι ο ιός αλλάζει την ρουτίνα αποκρυπτογράφησης του σε κάθε νέο αρχείο που μολύνει και εκτελεί την σειρά ενεργειών όπως ειπώθηκε προηγουμένως

Όμως δεν τελείωσαν όλα εδώ. Στις 25 Δεκεμβρίου ή 17 Αυγούστου μια καταστροφική σειρά ενεργειών εκτελείται. Ο ιός τοποθετεί τυχαία σχήματα στο αρχείο που εκτελείται. Έπειτα αλλάζει το autoexec.bat και το Config.bat. Το πρώτο αρχείο αντικαθιστάται μ' ένα αρχείο που οι εντολές που περιέχει οδηγούν τον δίσκο σε φορμάρισμα.

Μόλις έχει κάνει όλα τα παραπάνω ο ίός εμφανίζει το μήνυμα:

Assalamualaikum Li Kulli Muslim...Moslem Power Never End...

Nothing Can Stop << CyberNET >> Virus. Your System Has Already Infected!!!

Now...I Am Outta Here...

Μόλις ο χρήστης πατήσει το Ok στο παραπάνω μήνυμα, ο υπολογιστής τερματίζεται. Αν ο χρήστης δοκιμάσει να τον ξανανοίξει ο υπολογιστής δεν θα ανοίγει πλέον.[121]

[121] https://www.f-secure.com/v-descs/cybernet.shtml 01/09/2015

3 Τρόποι αντιμετώπισης και πρόληψης

Στο κεφάλαιο αυτό θα γίνει αναφορά στους τρόπους πρόληψης και αντιμετώπισης για το ιομορφικό λογισμικό που αναλύθηκε επαρκώς στο Κεφάλαιο 2.

Θα γίνει αναφορά σε μεθόδους αντιμετώπισης που αναφέρονται οι εταιρίες αντιβιοτικών προγραμμάτων και σε χειροκίνητους (manual) τρόπους αντιμετώπισης ιομορφικού λογισμικού, οι οποίοι είναι μεν λίγοι αλλά και αξίζει μια αναφορά σ' αυτούς.

Επίσης, το πιο σημαντικό, θα γίνει μια αναφορά σε προτεινόμενους τρόπους πρόληψης του Ιομορφικού Λογισμικού.

Τέλος, θα γίνει μια αναφορά στα παραδείγματα που παρουσιάστηκαν στο προηγούμενο κεφάλαιο και το πώς αυτά αντιμετωπίζονται και αν υπάρχει (ή υπήρχε όσον αφορά τα DOS ιομορφικό λογισμικό) τρόπος πρόληψης αυτών.

3.1 Τρόποι Αντιμετώπισης Κακόβουλου Λογισμικού

Αρχικά θα γίνει αναφορά στο Δίσκο Διάσωσης της Kaspersky, τον οποίο η εταιρία εκδίδει δωρεάν. Βέβαια ο τρόπος χρήσης είναι αρκετά πολύπλοκος για έναν άπειρο χρήστη.

Πρώτον πρέπει ο Δίσκος Διάσωσης να τοποθετηθεί σε μια μονάδα USB ή ένα CD από έναν μη μολυσμένο υπολογιστή.

Στη συνέχεια αν χρησιμοποιείται το USB, πρέπει να ανοιχτεί το Bios Menu του μολυσμένου υπολογιστή. Για να επιτευχθεί αυτό πρέπει ο χρήστης να πατήσει το πλήκτρο DEL ή το F2 όταν ανοίγει ο υπολογιστής. Έπειτα ο χρήστης πρέπει να κατευθυνθεί στη καρτέλα Εκκίνηση(BootTab) και επιλέγει την εκκίνηση από την μονάδα USB. Επιπλέον ο χρήστης πρέπει να ελέγξει στη καρτέλα Επιλογές (SettingsTab) ότι οι επιλογές USB Keyboard Support καιUSB Mouse Support είναι ενεργοποιημένες (Enabled). Μόλις έχει γίνει αυτός ο έλεγχος ο χρήστης αποθηκεύει τις αλλαγές και κλείνει το Bios Menu με το F10. Μόλις το κάνει, ο υπολογιστής ανοίγει άλλη μια φορά με τις καινούριες οδηγίες. Συνεχίζοντας ο χρήστης τοποθετεί το USB στην θύρα και έτσι μόλις ο χρήστης εκκινήσει τον υπολογιστή ξεκινά η διαδικασία.

Μόλις ανοίξει ο υπολογιστής εμφανίζεται στην οθόνη το σήμα της Kaspersky κάτω δεξιά και ζητά από τον χρήστη να πατήσει ένα οποιοδήποτε πλήκτρο στο πληκτρολόγιο, έχοντας και ένα χρονικό διάστημα μέχρι το άνοιγμα του υπολογιστή από τον σκληρό δίσκο.(Εικόνα 14)

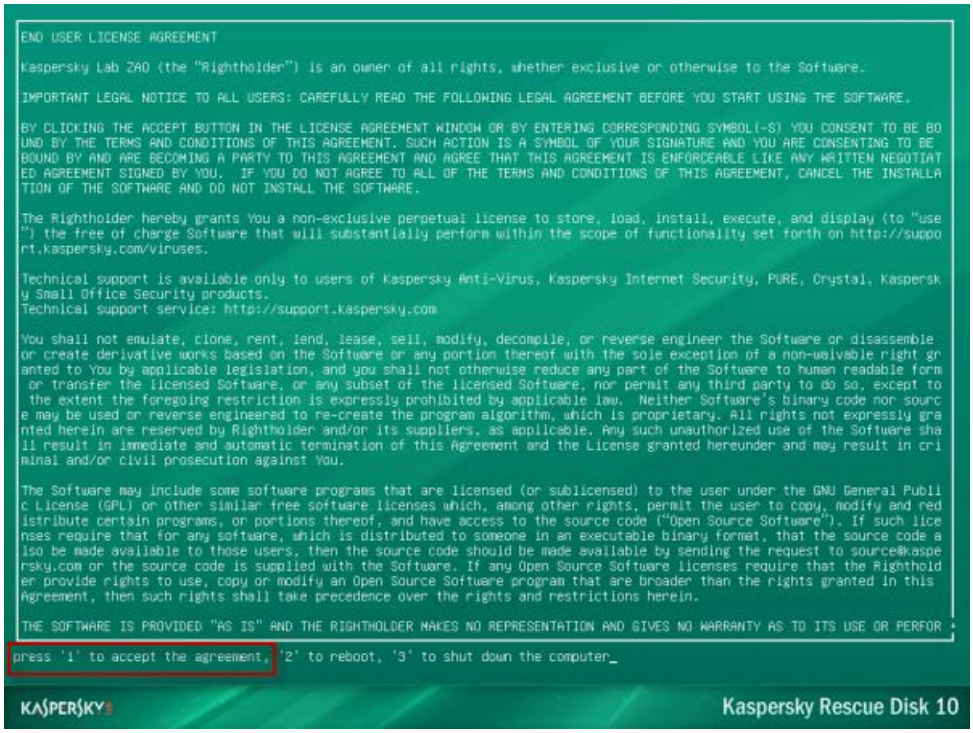
Εικόνα 14ΠρώτηοθόνηKasperskyRescueDisc

Στην συνέχεια, ο χρήστης επιλέγει την γλώσσα που θα χρησιμοποιήσει για το λογισμικό. (Εικόνα 15)

Εικόνα 15 Επιλογή Γλώσσας

Συνεχίζοντας ο χρήστης καλείται να δεχτεί τους όρους χρήσης της εφαρμογής, έχοντας και δύο επιπλέον επιλογές ή επανεκκίνηση (Εικόνα 16) και τέλος να διαλέξει σε ποια λειτουργία θα χρησιμοποιηθεί η εφαρμογή (Εικόνα 17).

Εικόνα 16Άδεια χρήσης προϊόντος(LicenseAgreement)



Εικόνα 17Επιλογή τρόπου χρήσης εφαρμογής(ModeSelect)

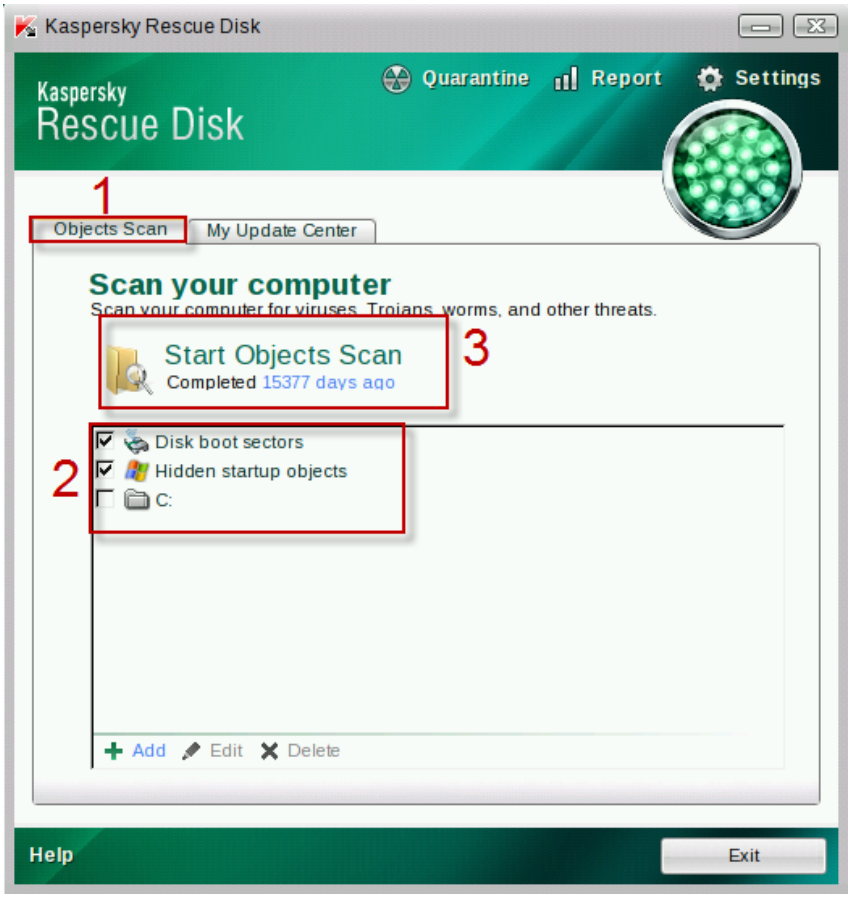
Η ανάλυση που θα γίνει στην συνέχεια αφορά το τρόπο χρήσης με γραφικά(GraphicMode). Αρχικώς, ενεργοποιείται ένα σύστημα σαν την Έναρξη του υπολογιστή μόνο που έχει το σύμβολο  . Μόλις ο χρήστης πατήσει σ' αυτό το σύμβολο εμφανίζεται ένα μενού που περιέχει επιλογές(Εικόνα 18)

Εικόνα 18Επιλογές (Menu Kaspresky)

Ο χρήστης πατάει το πρώτο εικονίδιο με το κείμενο Kaspersky Rescue Disc. Μόλις πατηθεί το εικονίδιο ενεργοποιείται το αντιβιοτικό πρόγραμμα. Έτσι λοιπόν ζητά από τον χρήστη να ελέγξει για ενημερώσεις όπως φαίνεται στην Εικόνα 19.

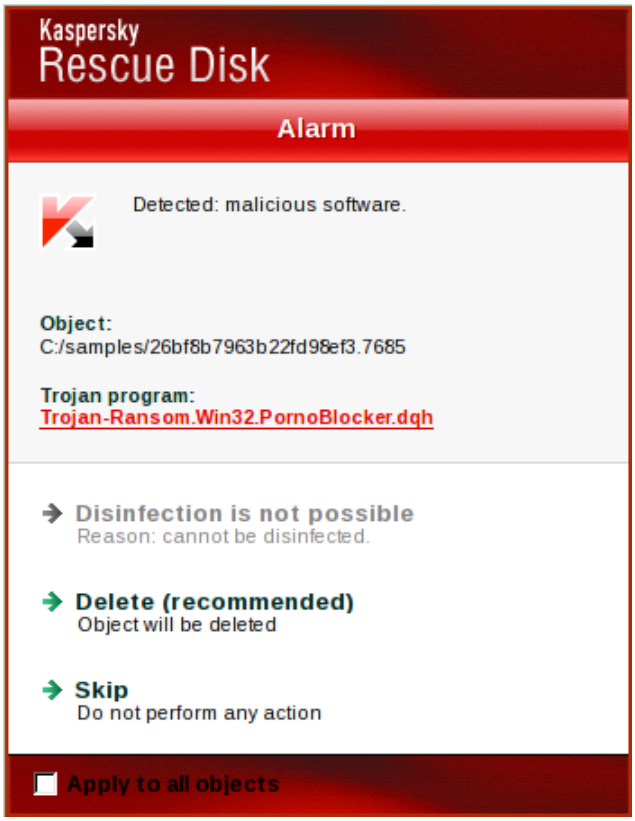
Εικόνα 19 Ενημέρωση Αντιβιοτικού Προγράμματος(Update)

Επιπλέον ο χρήστης με την αλλαγή καρτέλας από το «My Update Center» σε «Objects Scan» επιλέγει ποιους χώρους θέλει να ελέγξει για την ύπαρξη κακόβουλου λογισμικού που υφίσταται στον τομέα εκκίνησης αρχικώς και έπειτα ελέγχει για άλλα είδη κακόβουλου λογισμικού που μπορεί να υπάρχουν στο σύστημα.(Εικόνα 20)



Εικόνα 20 Βήματα για την εκκίνηση έλεγχου(StepsforStartingaScan)

Μόλις τελειώσει ο έλεγχος τότε το αντιβιοτικό πρόγραμμα εμφανίζει τα αποτελέσματα ως αναδυόμενα παράθυρα.(Εικόνα 3.8)

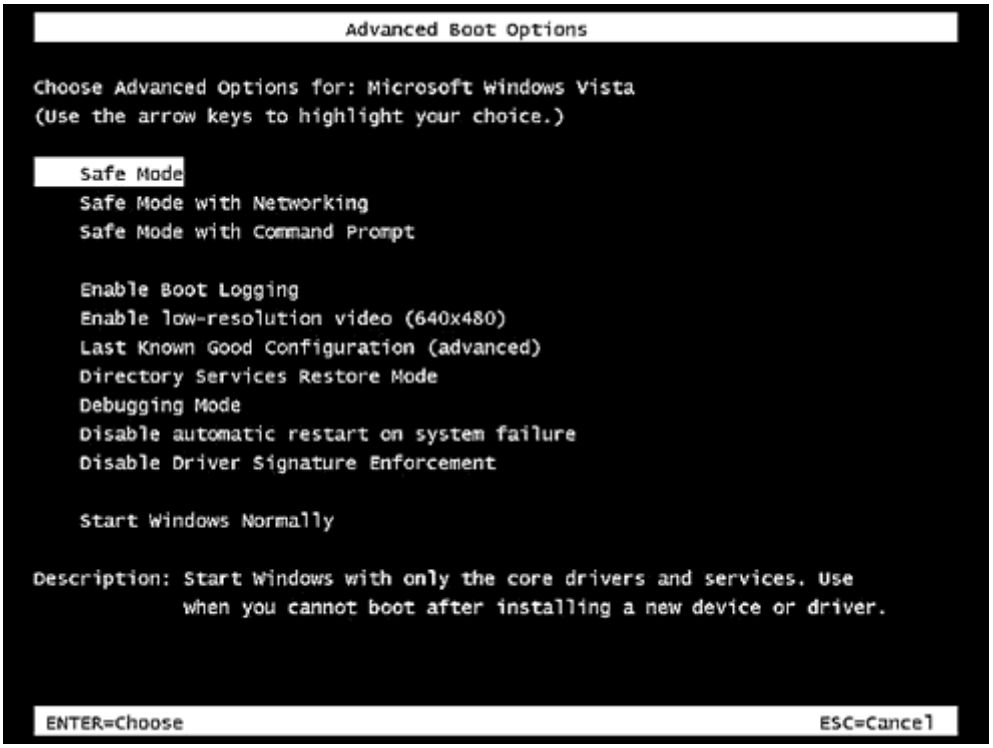


Εικόνα 21 Αναδυόμενο Παράθυρο (Alarm Windows)

Το παραπάνω λογισμικό αποδεικνύει της ύπαρξη ενός τρόπου αντιμετώπισης που νοιάζεται για τον χρήστη και τις επιλογές του και έτσι τον βοηθάει να αντιμετωπίσει όποιο πρόβλημα προήλθε από το κακόβουλο λογισμικό και να συνεχίζει την εργασία του όπως αυτός θελήσει.

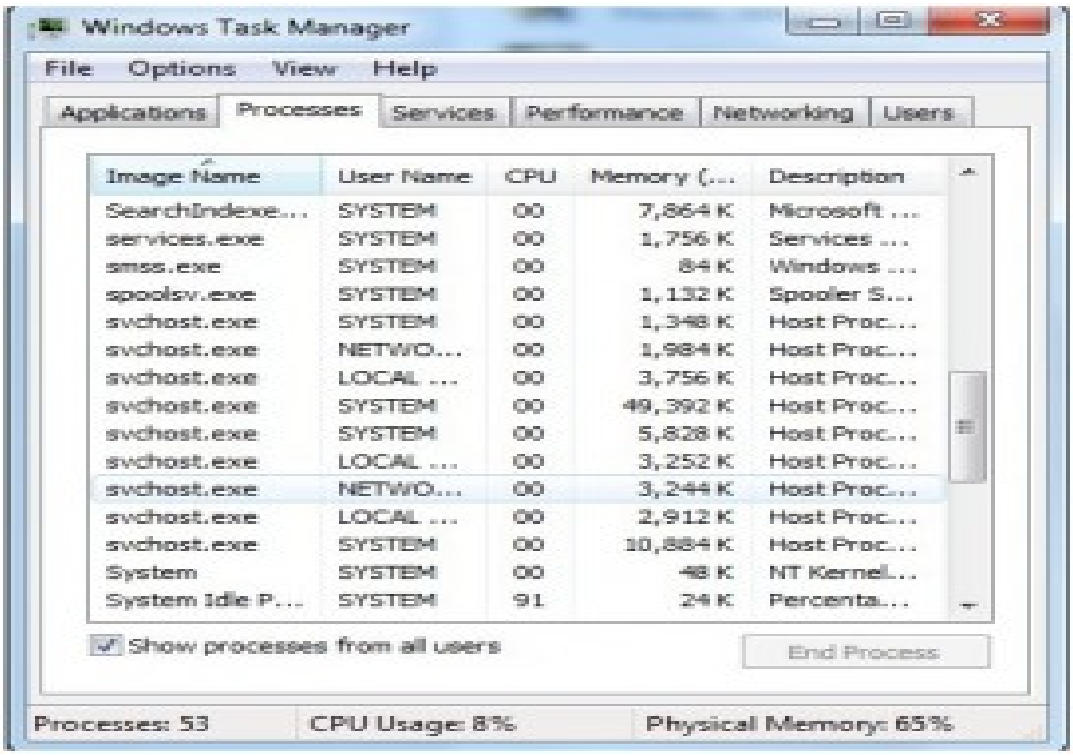
3.1.1 Τρόπος Αντιμετώπισης Boot.Cidex

Ο ιός που αναλύθηκε στο Κεφάλαιο 2.2.1 μπορεί να αντιμετωπιστεί και χειροκίνητα (χωρίς την χρήση ιομορφικού λογισμικού). Αρχικώς ο χρήστης πρέπει να κάνει επανεκκίνηση στο υπολογιστή του κλείνοντας τον από το κουμπί ενεργοποίησης ή πατώντας το πλήκτρο F8 όταν γίνεται εκκίνηση. Μόλις το κάνει εμφανίζεται η οθόνη της εικόνας 3.9(Βήμα 1) .



Εικόνα 22 Επιλογές Προχωρημένης Εκκίνησης (AdvancedBootOptions)

Ο χρήστης σ' αυτό το σημείο πρέπει να πατήσει την δεύτερη επιλογή της Ασφαλής Λειτουργίας με την Χρήση Δικτύου (Safe Mode with Networking). Μόλις ο υπολογιστής ανοίξει ο χρήστης πρέπει να ανοίξει την διαχείριση εργασιών (Task Manager) με την χρήση των πλήκτρων Ctrl+Alt+Delete. Μόλις ανοίξει η διαχείριση εργασιών ο χρήστης πρέπει να κλείσει όλα τα Boot.Cidex που είναι ανοιχτά , όπως φαίνεται στην εικόνα 3.10(Βήμα 2).



Εικόνα 23 Σταματώντας όλα τις διεργασίες του ιού (Ending all Virus Proccesses)

Στην συνέχεια ο χρήστης πρέπει να επιτρέψει την εμφάνιση κρυφών αρχείων (Βήμα 3) και να σβήσει τα αρχεία από τις παρακάτω τοποθεσίες:

- %UserProfile%\Application Data\Microsoft\[random].exe
- %System Root%\Samples
- %User Profile%\Local Settings\Temp
- %Documents and Settings%\All Users\Start Menu\Programs\Boot.Cidex
- C:\Program Files\ Boot.Cidex \license.rtf
- C:\Documents and Settings\All Users\Start Menu\Programs\ Boot.Cidex
- C:\Documents and Settings\All Users\Start Menu\Programs\ Boot.Cidex \License Agreement

Μόλις ο χρήστης σβήσει τα παραπάνω κακόβουλα αρχεία, πρέπει να σβήσει και τις εισαγωγές που έκανε ο ιός στο registry όπως αναγράφονται παρακάτω:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\ Boot.Cidex \DisplayIcon %AppData%\[RANDOM CHARACTERS]\[RANDOM CHARACTERS].exe,0
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\[RANDOM CHARACTERS] %AppData%\[RANDOM CHARACTERS]\[RANDOM CHARACTERS].exe
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Trojan:Win32/Nadeomi.A\DisplayName As Boot.Cidex HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ Boot.Cidex
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ Boot.Cidex \SettingsMngr
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\ Boot.Cidex
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\ Boot.Cidex[122]

Έχοντας πραγματοποιήσει τα παραπάνω ο χρήστης θα έχει απαλλαγεί από αυτό το ιομορφικό λογισμικό.

[122] http://blog.teesupport.com/how-to-remove-boot-cidex-manually-tips-for-boot-cidex-removal-solution/ , 15/09/2015

3.1.2 Τρόπος Αντιμετώπισης Xorer.X

Σύμφωνα με την Ανάλυση που έγινε στοκεφάλαιο 2.2.4 ο ιός Xorer.X είναι Κρυφός Ιός. Επιπλέον, όπως αναλύθηκε στο προηγούμενο κεφάλαιο, ο ιός Xorer.X έχει ακριβώς τον ίδιο τρόπο αντιμετώπισης μόνο που αλλάζουν τα συστατικά που κάθε ιομορφικό λογισμικό χρησιμοποιεί.

Μόλις ο χρήστης λοιπόν ολοκληρώσει τα βήματα 1, 2 & 3, πρέπει να εντοπίσει τα αρχεία του ιού τα οποία είναι:

- <first hard disk:>\037589.log
- <first hard disk:>\pagefile.pif
- <first hard disk:>\netapi000.sys
- %windir%\system32\dnsq.dll
- %windir%\system32\<random numbers>.log
- %windir%\system32\com\lsass.exe
- %windir%\system32\com\smss.exe
- %windir%\system32\com\netcfg.000
- %windir%\system32\com\netcfg.dll
- <first hard disk:>\037589.log - Virus:Win32/Xorer.X
- <first hard disk:>\pagefile.pif - Virus:Win32/Xorer.X
- <first hard disk:>\netapi000.sys - Virus:Win32/Xorer.H
- %windir%\system32\dnsq.dll - Vius:Win32/Xorer.gen!dll
- %windir%\system32\<GetTickCount()>.log - Virus:Win32/Xorer.X
- %windir%\system32\com\lsass.exe - Virus:Win32/Xorer.X
- %windir%\system32\com\smss.exe - Virus:Win32/Xorer.O
- %windir%\system32\com\netcfg.000 - Virus:Win32/Xorer.E
- %windir%\system32\com\netcfg.dll - Virus:Win32/Xorer.E

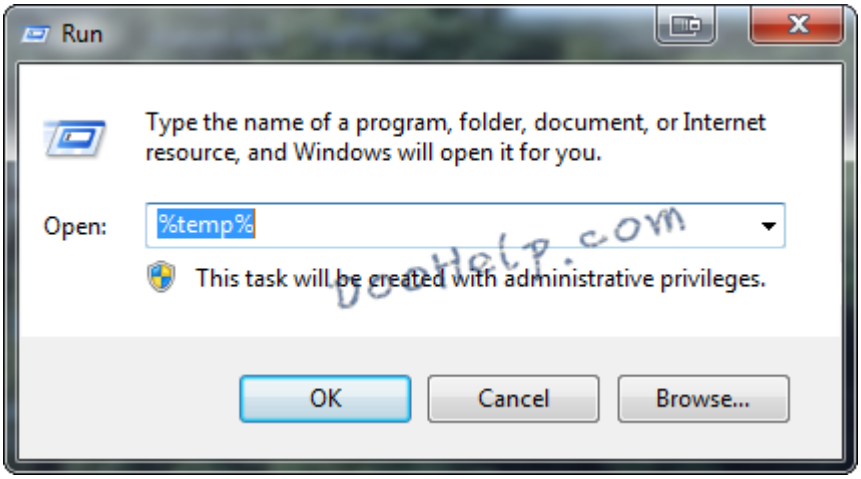
Στη συνέχεια όσον αφορά τον καθαρισμό του Registry αυτός γίνεται με την διαγραφή των εισαγωγών:

- HKLM\SYSTEM\CurrentControlSet\Services\NetApi000
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden
- HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\{4D36E967-E325-11CE-BFC1-08002BE10318}
- HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network\{4D36E967-E325-11CE-BFC1-08002BE10318}
- HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}
- HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}
- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution\Options
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects
- HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run[123]

[123] http://removecomputermalware.blogspot.gr/2012/10/solution-express-how-to-get-rid-of_19.html , 16/09/2015

3.1.3 Τρόπος Αντιμετώπισης Crypto

Σύμφωνα με την ανάλυση που έγινε στο Κεφάλαιο 2.2.5 και Κεφάλαιο 2.2.6 ο ιός Crypto είναι ένας Ρετρο-Ιός και Κρυπτογραφημένος Ιός. Ο τρόπος αντιμετώπισης είναι κατά βάση ίδιος μόνο που ο συγκεκριμένος ιός διατηρεί και προσωρινά αρχεία (TemporaryFiles) τα οποία πρέπει να διαγραφούν από τον χρήστη. Για να γίνει αυτό αφού εκείνος επιτελέσει τα βήματα 1,2,3 με επιτυχία, πρέπει να ανοίξει το παράθυρο εκτέλεσης (Run) και να εκτελέσει το «%Temp%», όπως φαίνεται στην εικόνα 3.11 .



Εικόνα 24 Παράθυρο εκτέλεσης (Run Window)

Σβήνοντας λοιπόν όλα τα προσωρινά αρχεία στην συνέχεια πρέπει να σβηστούν οι εισαγωγές στο Registry οι οποίες είναι:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings "CertificateRevocation" = '1'
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments "SaveZoneInformation" = '0'

Στην συνέχεια με προσοχή πρέπει να σβηστούν και οι εισαγωγές στοRegistryπου περιέχουν τυχαίους αριθμούς και την λέξη RUN από τις τοποθεσίες:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \Current Version
- HKEY_CURRENT_USER\Software\Microsoft\Windows\Curr entVersion
- HKEY_CURRENT_USER\Software\Microsoft\Windows\Curr entVersion\Explorer\Shell Folders Startup="C:\windows\start menu\programs\startup

Στην συνέχεια ο χρήστης για να απαλλαγεί πλήρως από τον Crypto πρέπει να σβήσει τα κρυφά αρχεία που βρίσκονται στις τοποθεσίες:

- %AllUsersProfile%
- %AllUsersProfile%\Programs\{random letters}\
- %AllUsersProfile%\Application Data\~r
- %AllUsersProfile%\Application Data\~dll[124]

[124]http://blog.doohelp.com/get-rid-ofremove-win32cryptor-virus-restore-your-pc/

3.1.4 Τρόπος Αντιμετώπισης Driller(Tuareg)

Ο ιός Driller(Tuareg) που αναλύθηκε στο κεφάλαιο 2.2.7 είναι ένας πολυμορφικός ιός. Ο Τρόπος αντιμετώπισης του δεν διαφέρει των υπολοίπων, έτσι ο χρήστης ακολουθά τα τρία βασικά βήματα 1, 2 & 3.

Στην συνέχεια ο χρήστης πρέπει να σβήσει τα σχετικά αρχεία του ιού από τις τοποθεσίες:

- C:\program files
- %AllUsersProfile%\Application Data\
- %AllUsersProfile%\

Τέλος ο χρήστης πρέπει να σβήσει τις εισαγωγές στο Registryαπό τις τοποθεσίες με τα κλειδιά:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msconfig.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msmpeng.exe
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments "SaveZoneInformation"=1
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msseces.exe "Debugger"="svchost.exe"

3.1.5 Τρόπος Αντιμετώπισης Love.Letter

Ο ιός Love.Letter, που αναλύθηκε στο κεφάλαιο 2.2.8 είναι ένας ιός που διαγράφει τμήμα ή και ολόκληρο τον ξενιστή και τον αντικαθιστά με το αρχείο του κώδικα του.

Για την εξουδετέρωση αυτού του ιού ο χρήστης πρέπει να επιτελέσει τα τρία βήματα και στην συνέχεια να σβήσει τα αρχεία:

- MSKernel32.vbs
- Win32DLL.vbs
- LOVE-LETTER-FOR-YOU.TXT.vbs
- LOVE-LETTER-FOR-YOU.HTM
- WINFAT32.EXE
- Funny Love.vbs
- Funny Love.htm

Στην συνέχεια ο χρήστης πρέπει να σβήσει όλες τις εισαγωγές, που έχουν κατάληξη .VBS, από τα σημεία στο registry:

- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

Έπειτα γίνεται αναφορά για το Windows Scripting Host (WSH) στο οποίο ο χρήστης πρέπει να σβήσει οποιοδήποτε timeout υπάρχει στο σύστημα αυτού του προγράμματος.

Μόλις το επιτελέσει αυτό ο χρήστης πρέπει να αλλάξει την αρχική σελίδα του Internet Explorer σε:

- http://www.symantec.com/avcenter/repair_instruct.html

Συνεχίζοντας ο χρήστης πρέπει να επιστρέψει στο registry και να σβήσει τα κλειδιά WAB εκτός από τα κλειδιά LDAPConnectionTimeout και ServerID.

Έπειτα μόλις επιτελέσει όλα τα παραπάνω βήματα ο χρήστης μπορεί πλέον να βρει τα αρχεία μουσικής (MP2 και MP3) που είχε κρύψει ο ιός και να αλλάξει τις ιδιότητες των αρχείων.

Τέλος ο χρήστης πρέπει να αναζητήσει και να διαγράψει όλα τα αρχεία SCRIPT.INI που ο ιός είχε δημιουργήσει.[125]

[125] ftp://ftp.fisio.cinvestav.mx/Updates/fixes/readmefix.vbs.loveletter.html 29/9/2015

3.2 Τρόποι Πρόληψης

Ο συγγραφέας σ' αυτό το σημείο θα αναφερθεί σε τρόπους πρόληψης που προτείνει ο ίδιος μετά από αρκετά περιστατικά που αντιμετώπισε και πρόλαβε να λύσει πριν την εφαρμογή των σειρών ενεργειών που έχει κάθε κακόβουλο λογισμικό.

Αρχικώς λοιπόν εκτός από την ύπαρξη καλού αντιβιοτικού προγράμματος που θεωρείται ως άμεση λύση αλλά και πρόληψη, ο συγγραφέας προτείνει την ύπαρξη ενός προγράμματος καθαρισμού προσωρινών αλλά και διόρθωσης του registry στο οποίο αναφέρθηκε εκτενέστατα σ' αυτό το κεφάλαιο όπως το λογισμικό CCleaner της Piriform.

Το CCleaner είναι ένα πρόγραμμα βελτιστοποίησης (optimization) του συστήματος και με πολύ απλό χειρισμό μπορεί ο χρήστης να αντιμετωπίσει προβλήματα κολλήματος (lagging) του υπολογιστή αλλά και αντιμετώπισης υπολογιστικών αδιεξόδων και σφαλμάτων (computer crashes & errors).

Μ' αυτόν τον τρόπο ο απλός χρήστης επιτυγχάνει την βελτιστοποίηση της ταχύτητας του υπολογιστή, γρηγορότερη εκκίνηση αλλά και ασφαλέστερο σερφάρισμα (browsing) στο διαδίκτυο.[126]

Όπως έχει διαπιστωθεί από τον συγγραφέα, αυτό το λογισμικό εκτός από τα παραπάνω θετικά αποτελέσματα που δίνει σ' ένα υπολογιστικό σύστημα, πετυχαίνει και την πρόληψη κακόβουλων απειλών αν χρησιμοποιείται σωστά και ταχτικά.

Βέβαια, ο συγγραφέας στηρίζει την άποψη ότι όλα τα λογισμικά έχουν τις αδυναμίες τους άρα δεν μπορεί να υπάρξει ένα πλήρως ασφαλές σύστημα, πρέπει οι χρήστες να βρίσκονται σε επιφυλακή και να περιμένουν το άγνωστο.

[126] https://www.piriform.com/ccleaner , 26/9/2015

4 Συμπεράσματα και προτάσεις έρευνας

Αρχικώς το ιομορφικό λογισμικό Boot.Cidex δεν έχει ως αδυναμία την ασφαλή λειτουργία των συστημάτων Windows αλλά προτείνεται αυτή η λειτουργία για την αντιμετώπιση κακόβουλων λογισμικών. Έπειτα αδύναμο σημείο είναι τα κρυφά αρχεία που δημιουργεί και μπορούν εύκολα να εντοπιστούν από τον χρήστη. Συνεχίζοντας αδυναμία υπάρχει στο Registry όπου το κακόβουλο λογισμικό αφήνει εμφανές άχρηστα στον χρήστη στοιχεία που μπορούν να διαγραφούν στην ασφαλή λειτουργία και βέβαια η αδυναμία όλων σχεδόν των Ιών είναι τα αντιβιοτικά προγράμματα(Πίνακας 1).

Πίνακας1 Αδυναμίες Boot.Cidex

Αδυναμίες Λογισμικού	**Boot Cidex**
Ασφαλή Λειτουργία	
Κρυφά Αρχεία	✓
Registry	✓
Ύπαρξη Προσωρινών Αρχείων	
Αντιβιοτικό Λογισμικό	✓

Το επόμενο ιομορφικό λογισμικό που αναλύθηκε είναι το DOS.CyberCrime το οποίο ως λογισμικό DOS δεν έχει τις αδυναμίες που περιγράψαμε παραπάνω και δεν υπάρχει διαθέσιμη βιβλιογραφική αναφορά για τις αδυναμίες που μπορεί να είχε αλλά διατίθεται και ένας πίνακας παρακάτω:

Πίνακας 2Αδυναμίες DOS.CyberCrime

Αδυναμίες Λογισμικού	**DOS.CyberCrime**

Ασφαλή Λειτουργία	
Κρυφά Αρχεία	
Registry	
Ύπαρξη Προσωρινών Αρχείων	
Αντιβιοτικό λόγισμικό	✓

Συνεχίζοντας έγινε ανάλυση του ιού DOS.Tequila για τον οποίο και πάλι δεν υπήρχαν αδυναμίες εκτός αυτή του αντιβιοτικού λογισμικού που διατίθεται για συστήματα DOS.

Πίνακας 3Αδυναμίες DOS.Tequila

Αδυναμίες Λογισμικού	**DOS.Tequila**
Ασφαλή Λειτουργία	
Κρυφά Αρχεία	
Registry	
Ύπαρξη Προσωρινών Αρχείων	
Αντιβιοτικό λογισμικό	✓

Έπειτα αναλύθηκε το ιομορφικό λογισμικό Xorex.X το οποίο έχει τις ίδιες αδυναμίες με το Boot.Cidex που αναφέρθηκε προηγουμένως.

Πίνακας 4 Αδυναμίες Xorer.X

Αδυναμίες Λογισμικού	**Xorer.X**
Ασφαλή Λειτουργία	✓
Κρυφά Αρχεία	✓
Registry	✓
Ύπαρξη Προσωρινών Αρχείων	
Αντιβιοτικό Λογισμικό	✓

Το επόμενο ιομορφικό λογισμικό το Crypto που περιλαμβάνει μια επιπλέον αδυναμία την ύπαρξη προσωρινών αρχείων στο σύστημα κατά την περίοδο λειτουργίας του, έτσι ώστε και να εντοπιστεί από το αντιβιοτικό λογισμικό να μπορεί να ανακάμψει εάν δεν σβηστούν αυτά τα αρχεία.(Πίνακας 4.5)

Πίνακας 5 Αδυναμίες Crypto

Αδυναμίες Λογισμικού	**Crypto**
Ασφαλή Λειτουργία	✓
Κρυφά Αρχεία	✓
Registry	✓
Ύπαρξη Προσωρινών Αρχείων	✓
Αντιβιοτικό Λογισμικό	✓

Στην συνέχεια ο Driller (Tuareg) έχει όλες τις παραπάνω αδυναμίες εκτός από την ύπαρξη προσωρινών αρχείων στο σύστημα και την αντιμετώπιση σε ασφαλή λειτουργία αν και πάντα προτείνεται να βρίσκεται ο χρήστης σε ασφαλή λειτουργία όταν κάνει αντιμετώπιση κακόβουλων απειλών:

Πίνακας 6 Αδυναμίες Driller (Tuareg)

Αδυναμίες Λογισμικού	**Driller (Tuareg)**
Ασφαλή Λειτουργία	
Κρυφά Αρχεία	✓
Registry	✓
Ύπαρξη Προσωρινών Αρχείων	
Αντιβιοτικό Λογισμικό	✓

Τέλος ο ιός LoveLetter κατέχει όλες τις αδυναμίες που προαναφέρθηκαν αλλά ο συγκεκριμένος ιός εάν εκτελεστεί και

αντιμετωπιστεί δεν σημαίνει πως δεν θα υπάρξουν και απώλειες (JPEG αρχεία κλπ.).

Πίνακας 7 Αδυναμίες Love Letter

Αδυναμίες Λογισμικού	**Love Letter**
Ασφαλή Λειτουργία	✓
Κρυφά Αρχεία	✓
Registry	✓
Ύπαρξη Προσωρινών Αρχείων	✓
Αντιβιοτικό Λογισμικό	✓

Αυτή η έρευνα έδωσε την ελευθερία για ασχολία σε πλαίσια εικονικής υπολογιστικής (virtual computing), ανοίγοντας την μελλοντική σκέψη για επιπλέον ανάπτυξη σε περισσότερα είδη κακόβουλου λογισμικού.

Βιβλιογραφία

Βιβλιογραφικές Αναφορές

Ηλιάδης, Γιάννης,*Ασφάλεια Πληροφοριακών Συστημάτων: Κεφάλαιο 8. Κακόβουλο λογισμικό* , Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.

Hardikar, Amman,*MALWARE 101, Viruses,*SANSInstitute,Seattle, 2008. Available at: https://www.sans.org/reading-room/

Konstantinou, Evgenios,*Metamorphic Virus: Analysis and Detection*, Royal Holloway University of London, London, 2008. Available at: https://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-02.pdf/

Skulason,Fridrik, *1260 - the variable virus*, Virus Bulletin, 1990.

Summers, Rita, *Secure Computing Threats and Safeguards*, McGraw-Hill, 1997.

Διαδικτυακές Αναφορές(Σύμφωνα με εμφάνιση στο κείμενο)

1) http://www.seas.ucla.edu/security/malware.html, 03/03/2015
2) http://www.techopedia.com/definition/4015/malicious-software-malware , 03/03/2015
3) https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101, 10/05/2015
4) http://www.kaspersky.com/internet-security-center/threats/malware-classifications, 10/05/2015
5) http://www.computerhope.com/jargon/b/backdoor.htm, 28/07/2015
6) http://www.itsecurity.com/features/trapdoors-backdoors-103007/, 18/05/2015
7) http://www.sans.edu/research/security-laboratory/article/log-bmb-trp-door#__utma=21257146.1574720757.1433083109.1433083109.1433083109.1&__utmb=21257146.6.9.1433083269726&__utmc=21257146&__utmx=-&__utmz=21257146.1433083109.1.1.utmcsr=(direct)|utmccn=(direct)|ut

mcmd=(none)&__utmv=-&__utmk=151620858 ,21/5/2015

https://www.sans.org/search/results , 01/06/2015

8) http://www.sans.org/security-resources/top15_mal_spyware.php ,01/06/2015
9) http://download.cnet.com/Gator/3000-18501_4-10785.html ,26/07/2015
10) http://download.cnet.com/CWShredder/3000-8022_4-10301587.html ,26/07/2015
11) http://www.downloadcrew.com/article/23452-auslogics_internet_optimizer, 26/07/2015
12) https://www.sans.org/search/results, 01/06/2015
13) https://en.wikipedia.org/wiki/Jerusalem_%28computer_virus%29#Mendoza_.28Jerusalem_Mendoza.29, 10/06/2015
14) https://www.sans.org/search/results , 19/06/2015
15) http://www.trendmicro.com/vinfo/us/security/definition/ransomware, 19/06/2015
16) http://vxheaven.org/lib/pdf/Future%20Trends%20in%20Malicious%20Code%20-%202006%20Report.pdf, 19/06/2015
17) https://blog.cisecurity.org/cis-cyber-alert/, 20/06/2015
18) http://www.pctools.com/security-news/what-is-a-computer-worm/, 29/06/2015
19) https://en.wikipedia.org/wiki/Sobig, 26/07/2015
20) http://jazz.he.fi/jargon/html/W/wabbit.html, 29/06/2015
21) https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101, 29/06/2015
22) http://www.spamlaws.com/zango-adware.html, 29/06/2015
23) https://www.gdata-software.com/security-labs/information/history-of-malware, 04/04/2015
24) http://www.elite-hackers.com/hacking-tools/sub7, 12/04/2015

25) http://users.uoa.gr/~nektar/science/technology/a_brief_history_of_viruses.htm, 05/04/2015

26) http://scholar.google.gr/scholar_url?url=http://arxiv.org/pdf/1302.5392&hl=el&sa=X&scisig=AAGBfm22e2pB2g3ZJprOl5pCZaXz83R5SA&nossl=1&oi=scholarr&ei=XhEQVdWQLtbgatmsgtgG&ved=0CB4QgAMoADAA , 4/4/2015

27) http://users.uoa.gr/~nektar/science/technology/a_brief_history_of_viruses.htm , 05/04/2015

28) http://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms , 4/4/2015

29) http://news.softpedia.com/news/Kournikova-Worm-Celebrates-10th-Anniversary-183904.shtml, 14/5/2015

30) http://en.wikipedia.org/wiki/Mylife_(computer_worm) , 12/4/2015

31) http://archive.wired.com/wired/archive/11.07/slammer.html , 14/04/2015

32) http://www.symantec.com/security_response/writeup.jsp?docid=2003-040217-2506-99 , 14/04/2015

33) http://en.wikipedia.org/wiki/Blaster_(computer_worm) , 14/04/2015

34) http://www.giac.org/paper/gcih/517/welchia-worm/105720 , 14/04/2015

35) http://en.wikipedia.org/wiki/Sobig, 14/04/2015

36) http://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/worm_swen.b , 14.04/2015

37) https://www.opendemocracy.net/media-edemocracy/spam_2535.jsp , 14/04/2015

38) http://en.wikipedia.org/wiki/Agobot , 14/04/2015 https://www.sans.org/search/results , 15/04/2015http://en.wikipedia.org/wiki/Mydoom , 15/04/2015

39) http://en.wikipedia.org/wiki/Netsky_(computer_worm), 15/04/2015

40) http://www.caida.org/research/security/witty/ , 15/04/2015

41) http://www.sophos.com/en-us/press-office/press-releases/2004/05/va_sasserarrest.aspx ,15/04/2015

42) http://www.nytimes.com/2005/08/17/technology/17virus.html?_r=0 , 15/04/2015

43) http://en.wikipedia.org/wiki/Stration , 15/04/2015

44) https://www.sophos.com/en-us/threat-center/threat-analyses/hoaxes/virus-hoax/olympic.aspx , 15/04/2015

45) http://news.bbc.co.uk/2/hi/technology/6278079.stm , 16/04/2015

46) http://en.wikipedia.org/wiki/Storm_Worm , 16/04/2015

47) http://en.wikipedia.org/wiki/Zeus_(malware) , 16/04/2015

48) http://www.seattlepi.com/business/article/Chinese-PC-virus-may-have-hidden-agenda-1264738.php , 16/04/2015

49) http://windowssecrets.com/top-story/dont-be-a-victim-of-sinowal-the-super-trojan/ , 16/04/2015

50) http://www.pr.com/press-release/84130 , 16/04/2015

51) http://en.wikipedia.org/wiki/Koobface , 16/04/2015

52) http://www.infowar-monitor.net/reports/iwm-koobface.pdf , 16/04/2015

53) http://www.nytimes.com/2009/01/23/technology/internet/23worm.html?_r=0 , 16/04/2015

54) http://en.wikipedia.org/wiki/Conficker , 16/04/2015

55) http://en.wikipedia.org/wiki/July_2009_cyber_attacks , 17/04/2015

56) http://www.csmonitor.com/World/Asia-Pacific/2009/0709/p06s23-woap.html , 17/04/2015

57) http://www.threatexpert.com/report.aspx?md5=7c6a5c18801938867644c861ebfdf0b8 , 17/04/2015

58) http://www.theregister.co.uk/2010/03/16/waledac_takedown_success/, 18/04/2015

59) http://en.wikipedia.org/wiki/Alureon , 18/04/2015

60) http://www.telegraph.co.uk/technology/news/8021102/Stuxnet-virus-worm-could-be-aimed-at-high-profile-Iranian-targets.html , 18/04/2015

61) http://www.theregister.co.uk/2011/01/25/spyeye_zeus_merger/ , 18/04/2015

62) http://www.precisesecurity.com/rogue/xp-anti-spyware-2011 , 19/04/2015

63) http://blog.appriver.com/2011/08/morto-worm-spreads-to-weak-systems/, 19/04/2015

64) http://blog.imperva.com/2011/09/morto-post-mortem-a-worm-deep-dive.html , 19/04/2015

65) http://en.wikipedia.org/wiki/ZeroAccess_botnet , 19/04/2015

66) http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf , 19/04/2015

67) http://www.crysys.hu/skywiper/skywiper.pdf , 20/04/2015

68) http://en.wikipedia.org/wiki/Shamoon#cite_note-Iran_Malware-9 , 20/04/2015

69) http://en.wikipedia.org/wiki/Saudi_Aramco , 20/04/2015

70) http://www.digitaljournal.com/article/331033 , 20/04/2015

71) http://www.enigmasoftware.com/ngrbot-removal/ , 20/04/2015

72) http://www.snopes.com/computer/virus/Cryptorlocker.asp , 23/04/2015

73) https://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/ , 29/04/2015

74) http://www.pcworld.com/article/2048261/understanding-tech-language-the-difference-between-malware-and-a-virus.html , 1/7/2015

75) http://labs.lastline.com/different-sandboxing-techniques-to-detect-advanced-malware , 19/08/2015

76) http://www.enigmasoftware.com/bootcidex-removal/ , 20/07/2015

77) http://guides.yoosecurity.com/boot-cidex-removal-guide , 20/07/2015

78) http://virus.wikia.com/wiki/Datacrime , 21/07/2015

79) http://usa.kaspersky.com/internet-security-center/definitions/stealth-virus#.VcelmjYVjmI ,08/08/2015

80) http://www.symantec.com/security_response/writeup.jsp?docid=2000-121515-4637-99&tabid=2 25/08/2015

81) http://www.webopedia.com/TERM/R/retrovirus.html ,27/08/2015

82) https://archive.is/20140702092942/https://www.securelist.com/en/descriptions/70544/Virus.Win32.Driller, 25/09/2015

83) https://usa.kaspersky.com/internet-security-center/definitions/macro-virus#.VeBDkjYVhhg, 28/08/2015

84) https://www.f-secure.com/v-descs/cybernet.shtml, 01/09/2015

85) http://support.kaspersky.com/viruses/rescuedisk/main , 11/09/2015

86) http://blog.teesupport.com/how-to-remove-boot-cidex-manually-tips-for-boot-cidex-removal-solution/, 15/09/2015

87) http://removecomputermalware.blogspot.gr/2012/10/solution-express-how-to-get-rid-of_19.html , 16/09/2015

88) http://blog.doohelp.com/get-rid-ofremove-win32cryptor-virus-restore-your-pc/ , 20/09/2015

89) ftp://ftp.fisio.cinvestav.mx/Updates/fixes/readmefix.vbs.loveletter.html , 29/9/2015

90) https://www.piriform.com/ccleaner, 26/9/2015