Windows και Διαδίκτυο

Ζητήματα ασφαλείας

ΜΔΕ Διδακτική της Βιολογίας & Νέες Τεχνολογίες
Ανδρέας Αθανασόπουλος

Κακόβουλο λογισμικό

(Malicious software)

Σκοπός

- Χρήση πόρων του ΗΥ (σε συνδυασμό με άλλους) για παράνομες ενέργειες
  - Επιθέσεις σε Server (DoS attack)
  - Παραβίαση κωδικών
- Αλίευση δεδομένων (κωδικών, διευθύνσεων e-mail, αριθμών πιστωτικών καρτών ή τραπεζικών λογαριασμών)
- Διασκέδαση.

Τρόποι μόλυνσης

- Επιθέσεις από το (δια)δίκτυο με εκμετάλλευση κενών ασφαλείας του ΛΣ ή εγκατεστημένων προγραμμάτων
- Πρόσθετα και εκτελέσιμα σε παραποιημένες ιστοσελίδες
- Είσοδος με συνημμένα σε e-mail
- Είσοδος μέσω μονάδων μνήμης (δισκέτες, CD/DVD, USB stick).

Virus (ιός)

- Είναι ενσωματωμένος στον κώδικα άλλου λογισμικού
- Ενεργοποιείται από κάποιο γεγονός (trigger)
- Εκτελεί το έργο του
- Αναπαράγεται (μέσω φορέα)
- Είδη: macro, bootsector, program, polymorphic, stealth, parasitic, armored, multipartite.

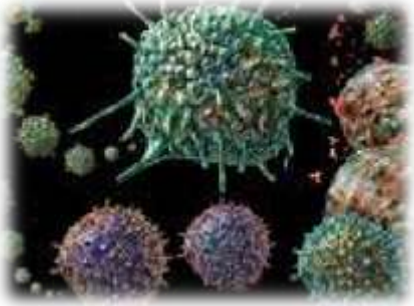
Worm (Αναπαραγωγός)

- Αυτοτελές πρόγραμμα (Δεν είναι ενσωματωμένος στον κώδικα άλλου)
- Αυτοαναπαράγεται
- Χρησιμοποιεί κενά ασφαλείας ή Κερκόπορτες (Backdoors) για να «μολύνει» κάποιο σύστημα.

Trojan horse (Δούρειος ίππος)

- Εμφανίζεται ως χρήσιμο πρόγραμμα, αλλά (παράλληλα ή αποκλειστικά) εκτελεί το ανεπιθύμητο έργο του (αλλαγή ρυθμίσεων ασφαλείας του προσβεβλημένου ΗΥ)
- Επικοινωνεί με τον δημιουργό ή αποστολέα του
- Δεν αυτοαναπαράγεται
- Ο προσβεβλημένος ΗΥ («zombie») κατόπιν πιθανόν αξιοποιείται ως μέλος ενός botnet.

Rootkit



- Τμήμα κώδικα που εκτελείται πριν φορτωθεί το ΛΣ
- Τρέχει με δικαιώματα διαχειριστή -αλλάζει τα δικαιώματα χρηστών
- Μπορεί να ενσωματωθεί σε πρόγραμμα που συνοδεύει υλικό
- Εντοπίζεται πολύ δύσκολα
- Συγκεντρώνει και στέλνει πληροφορίες του χρήστη εν αγνοία του, πχ ιστοσελίδες που επισκεφθήκαμε, πλήκτρα που πατήσαμε.

Spyware, Adware

- Κατασκοπευτικό λογισμικό (Spyware)
  - Συχνά συνδυασμένο με άλλο (κανονικό) πρόγραμμα που κατεβάζουμε
  - Συγκεντρώνει και στέλνει πληροφορίες του χρήστη εν αγνοία του, πχ ιστοσελίδες που επισκεφθήκαμε, πλήκτρα που πατήσαμε
- Λογισμικό με διαφημίσεις (Adware)
  - Παραλλαγή του παραπάνω
  - Pop-up ή περιοχή με διαφήμιση.

Ανεπιθύμητη αλληλογραφία (unsolicited mail, spam)

- Συχνά για προώθηση πωλήσεων ή διαφήμιση με τη λογική της πυραμίδας
- Όχι βλαβερό με την αυστηρή έννοια
- Μπορεί ωστόσο να αξιοποιηθεί για παραπλάνηση του παραλήπτη παραπέμποντάς τον σε ιστοσελίδες που συλλέγουν προσωπικά δεδομένα (phishing).

Μελέτη περίπτωσης: Ιός CIH

- **Τύπος:** Παρασιτικός ιός
- **Παραλλαγές :** PE_CIH, SPACEFILLER, CHERNOBYL, TSHERNOBYL, TSERNOBYL, VIN32, CIHV.
- **Τρόποι μετάδοσης :** Προσβάλλει εκτελέσιμα αρχεία των Windows 9X. Μετά την εκτέλεση του μολυσμένου αρχείου, παραμένει στη μνήμη και μολύνει τα αρχεία των προγραμμάτων που βρίσκονται υπό εκτέλεση.
- **Ενέργειες :** Ο ιός επανεγγράφει (με τυχαία δεδομένα) τα δεδομένα που περιέχονται στους τομείς του σκληρού δίσκου, ξεκινώντας από τον τομέα εκκίνησης. Παράλληλα, προσπαθεί να αλλοιώσει και το BIOS
- **Τρόποι ενεργοποίησης :** Ενεργοποίηση στις 26/4 ή 26/6 ή στις 26 κάθε μήνα.

Μελέτη περίπτωσης: Ιός ILoveYou

- **Τύπος:** Μακροϊός
- **Παραλλαγές:** VBS/Loveletter.b, VBS/Loveletter.c, VBS/Loveletter.d κλπ. και Love Bug, Very Funny, Love Letter και Mothers Day.
- **Τρόποι μετάδοσης:** Αποτελείται από κώδικα VBScript. Χρησιμοποιεί τις εφαρμογές e-mail (που υποστηρίζουν VBScript) και αποστέλλει e-mails σε όλες τις διευθύνσεις του βιβλίου διευθύνσεων του χρήστη. Το θέμα, τα περιεχόμενα και τα επισυναπτόμενα αρχεία του e-mail ποικίλλουν. Μολύνει συστήματα Windows 9X/NT και αρχεία με συγκεκριμένες καταλήξεις, όπου αντικαθιστά τον κώδικα με τον δικό του.
- **Ενέργειες:** Εγκαθίσταται από το διαδίκτυο και εκτελεί το πρόγραμμα WIN-BUGSFIX.exe, το οποίο ανιχνεύει συνθηματικά χρηστών των Windows και τα αποστέλλει σε συγκεκριμένη ηλεκτρονική διεύθυνση.
- **Τρόποι ενεργοποίησης:** Τοποθετεί τη διαδρομή του WIN-BUGSFIX.exe στο μητρώο (registry), ώστε να ενεργοποιείται σε κάθε επανεκκίνηση του συστήματος.

Μελέτη περίπτωσης: αναπαραγωγός NetSky

- **Τύπος:** αναπαραγωγός (worm)
- **Παραλλαγές:** W32/Netsky.c@MM, Win32.Netsky.C, W32/Netsky-C, WORM_NETSKY.C, I-Worm.Moodown.c, I-Worm.NetSky.c, W32/Netsky.C.worm
- **Τρόποι μετάδοσης:** Χρησιμοποιεί τη δική του μηχανή SMTP για να στείλει τον εαυτό του στις e-mail διευθύνσεις που βρίσκει, σαρώνοντας τους σκληρούς δίσκους και άλλους οδηγούς (drives). Το θέμα, τα περιεχόμενα και τα επισυναπτόμενα αρχεία του e-mail ποικίλλουν. Μολύνει συστήματα Windows 9x/NT
  - Αποφεύγει (!) την αποστολή σε διευθύνσεις που περιέχουν τα αλφαριθμητικά: icrosoft, antivi, ymantec, spam, avp, f-secur, itdefender, orman, cafee, aspersky, f-pr, orton, fbi, abuse. Επίσης, προσπαθεί να απενεργοποιήσει τον αναπαραγωγό mydoom
- **Ενέργειες:** Ψάχνει στους οδηγούς C:έως Z:για ονόματα φακέλων που περιέχουν "shar"και αντιγράφει τον εαυτό του σε αυτούς με το όνομα WINLOGON.EXE
- **Τρόποι ενεργοποίησης:** Τοποθετεί τη διαδρομή του WINLOGON.EXE στο μητρώο (registry), ώστε να ενεργοποιείται σε κάθε επανεκκίνηση του συστήματος.

Κακόβουλο λογισμικό - σύνοψη

Virus	Κώδικας που εκτελείται εν αγνοία του χρήστη. Είναι ενσωματωμένο στον κώδικα λογισμικού – φορέα. Ενεργοποιείται από κάποιο εξωτερικό γεγονός και αναπαράγεται προστιθέμενο στον κώδικα κανονικών προγραμμάτων	Love Bug virus Πχ: love-letter-for-you.txt.vbs
Worm	Παρόμοιο με ιό αλλά αυτοτελές – δεν απαιτεί ενσωμάτωση σε φορέα	Nimda. Διάδοση μέσω δικτύων και ομαδικής αλληλογραφίας
Trojan	Εμφανίζεται ως χρήσιμο πρόγραμμα, αλλά εκτελεί (και) ανεπιθύμητο έργο. Δεν αναπαράγεται	Remote access Trojan Πχ: SubSeven malware application
Spyware	Κακόβουλο λογισμικό που κατεβάζουμε εν αγνοία μας από κάποια ιστοσελίδα ή εγκαθιστούμε σε συνδυασμό με άλλο λογισμικό	Internet Optimizer (ή αλλιώς DyFuCA)
Rootkit	Σχεδιασμένο να πάρει τον έλεγχο του ΗΥ αποκτώντας δικαιώματα διαχειριστή	Boot loader rootkits Πχ: Evil Maid Attack
Spam	Κατάχρηση της ηλεκτρονικής αλληλογραφίας ή του instant messaging	Phishing identity theft e-mails Lottery scam e-mails

Πηγή: D. L. Prowse, CompTIA Security+ SY0-201 Cert Guide

Αντιμετώπιση

Στρατηγικές αντιμετώπισης ιομορφών

- **Πρόληψη**: Προλαμβάνει τη μόλυνση από ιομορφικό λογισμικό (πχ. διαχειριστικά μέτρα, ενημέρωση χρηστών)
- **Ανίχνευση**: Ανιχνεύει τη μόλυνση από ιομορφικό λογισμικό (πχ. ανιχνευτές ιών)
- **Αντιμετώπιση**: Επαναφέρει το σύστημα στην αρχική του κατάσταση (πχ. χρήση αντιγράφων ασφαλείας).

Πρακτικά μέτρα

- Εγκατάσταση & συχνή ενημέρωση antivirus & antispyware
- Εγκατάσταση / ενεργοποίηση firewall
- Κωδικός wpa2 στο ασύρματο δίκτυο
- Χρήση Wi-Fi hotspot μόνο σε ανάγκη
- Περιήγηση μόνο σε ασφαλείς ιστοσελίδες
- Όχι εκτέλεση (διπλό κλικ) ύποπτων συνημμένων σε e-mail
- Όχι αποδοχή εγκατάστασης αμφίβολης προέλευσης προσθέτων (plug-in) και „tools"
- Ακραία λύση: Χρήση Linux κ.α. κλώνων Unix αντί Windows.

Μέτρα ειδικά για τα Windows

- Ενεργοποίηση αυτόματων ενημερώσεων των Windows και τελευταίων εκδόσεων των προγραμμάτων
- Είσοδος στα Windows ως χρήστης με περιωρισμένα δικαιώματα
- Ενεργοποίηση εμφάνισης καταλήξεων αρχείων
- Χρήση πληκτρολόγιου οθόνης (⊞+R→ osk) όταν πληκτρολογούμε κρίσιμα δεδομένα
- Virtualization

Προστασία στο Διαδίκτυο

- Ενεργοποίηση φίλτρου ανεπιθύμητης αλληλογραφίας της υπηρεσίας e-mail
- Όχι προεπισκόπηση των μηνυμάτων
- Τελευταίες εκδόσεις των περιηγητών
- Προτιμότεροι οι λιγότερο διαδεδομένοι (Opera, Safari, Chrome)
- Πρόσθετα προειδοποίησης ύποπτων ιστοσελίδων (WOT, McAfee SiteAdvisor κ.ά.)
- Περιήγηση ως χρήστης με περιωρισμένα δικαιώματα.

Προγράμματα προστασίας από κακόβουλο λογισμικό

- Δωρεάν προστασία από ιούς (και μερικώς και από τα υπόλοιπα):
  - Antivir www.free-av.de/
  - Avast www.avast.com/
  - AVG antivirus www.grisoft.com , http://free.avg.com/
  - MS Security essentials www.microsoft.com/security_essentials/.

Προγράμματα προστασίας από κακόβουλο λογισμικό

- Δωρεάν προστασία από spyware κλπ:
  - Spybot Search & Destroy http://www.safer-networking.org/
  - Adaware http://www.lavasoft.de/
  - Windows defender http://www.microsoft.com/windows/products/winfamily/defender/default.mspx
- Δωρεάν θυρωρός (firewall):
  - Zone Alarm http://www.avast.com/
  - Ashampoo firewall http://www.ashampoo.com
  - Windows firewall (από το SP2 και μετά).

Επιδιόρθωση Windows

Προσβολή από κακόβουλο λογισμικό, κολλήματα μετά από εγκατάσταση προγραμμάτων ή οδηγών συσκευών, BSOD, μη εκκίνηση Windows

Πρόληψη

- Δεν εγκαθιστούμε προγράμματα που δεν είναι απολύτως απαραίτητα
- Δοκιμές λογισμικού σε virtual system
- Χρονοπρογραμματισμένα αντίγραφα ασφαλείας των αρχείων μας σε άλλο σκληρό ή οπτικούς δίσκους
- Δημιουργούμε περιοδικά αντίγραφα (images) και του ΛΣ
- Τα έγγραφά μας σε διαφορετικό διαμέρισμα (καλύτερα: δίσκο) από το ΛΣ.

Αν τα Windows εκκινούν

- **F8** αμέσως μετά το BIOS & πριν το „Starting Windows"
  - **Ασφαλής λειτουργία** (safe mode) →αναίρεση προβλήματος (απεγκατάσταση προγράμματος/ συσκευής/ οδηγού συσκευής, απενεργοποίηση αυτόματης εκκίνησης – msconfig) ή
  - **Τελευταία γνωστή** κανονική εκκίνηση (Last known…)
- **Επαναφορά συστήματος** (System restore)
  - Βοηθήματα → Εργαλεία συστήματος
  - Δημιουργία σημείων επαναφοράς και χειροκίνητα.

Αν τα Windows δεν εκκινούν

- Αντιγραφή προσωπικών αρχείων με χρήση Linux Live CD
- Εκτέλεση επιδιόρθωσης ή επαναφοράς μέσα από την κονσόλα αποκατάστασης (για έμπειρους)
- Επαναφορά system partition από αρχείο image
  - Δεν περιλαμβάνεται στα Windows XP / Vista
  - Αποθήκευση αντιγράφου σε άλλο δίσκο.

Προγράμματα δημιουργίας αντιγράφων διαμερίσεων δίσκου

- Εμπορικά
  - Norton Ghost
  - Acronis TrueImage
- Δωρεάν
  - DriveImage XML
  - Seagate – Acronis Max Blast και DiscWizard
  - Paragon Backup & Recovery
  - EASEUS Todo-Backup.

Πηγές

- Γκρίτζαλης Δ. *Ιομορφικό Λογισμικό* Παρουσιάσεις παραδόσεων ΕΑΠ v. 1.1/2005
- Κάτσικας Σ. *Ασφάλεια Υπολογιστών* ΕΑΠ 2001
- D. L. Prowse *CompTIA SecurityPlus SY0-201 Cert Guide*, Pearson 2010