

NOREA Factsheet Malware

Definition:

Malware, short for malicious software, is software (i.e. code, script, active content) designed to without consent:

- disrupt or deny computer operation;
- gather sensitive (intellectual property, vital/sensitive, classified) information;
- gain unauthorized access to computer systems;
- other abusive behavior.

Malware includes:

- Viruses
- Worms
- Trojan horses
- Spyware
- Adware
- Scareware
- Crimeware
- Keyloggers
- Ransomware
- Rootkits

Malware could include specific:

- Firmware
- Hardware

Recent Discovery: Chinese Chips in use by military containing a backdoor (May 28th 2012)

We (Cambridge University researcher) scanned the silicon chip in an affordable time and found a previously unknown backdoor inserted by the manufacturer. This backdoor has a key, which we were able to extract. If you use this key you can disable the chip or reprogram it at will, even if locked by the user with their own key. This particular chip is prevalent in many systems from weapons, nuclear power plants to public transport. In other words, this backdoor access could be turned into an advanced Stuxnet weapon to attack potentially millions of systems. The scale and range of possible attacks has huge implications for National Security and public infrastructure.

Malware is also known as computer contaminant.

Introduction:

The first malware were viruses, i.e. programs that replicate itself and spread accordingly. Viruses almost always corrupt or modify files on a target computer. Worms are similar to viruses, they self-replicate as viruses do, but they do not attach themselves to existing computer programs. Worms generally disrupt network operations, for example by consuming a significant portion of bandwidth. Trojans are programs that masquerade within other programs, causing unwanted results when executed. Rootkits are specialized Trojans designed to subvert operating systems and hide their presence.

Trojans make up more than 60% of all malware.

Malware is often executed directly on the internal networks, at times giving the adversary complete control over internal systems at the targeted organization using the malware's command and control (C&C) interface. In addition, malware incidents are expensive and the most frequent type of incidents occurring to organizations. Existing practices and measures to tackle malware as IDS/IPS, endpoint anti-malware, firewalls are necessary but insufficient to detect and block modern threats and protects sensitive information.

Generally seen, there are two techniques for host based AV products to detect malware: Signature-based and behavioral based. The more generalized the detection mechanism become, the more likely false-positives are to occur.

Top 5 Malware risks/effects/consequences:

1. (Industrial) Espionage, leakage of intellectual property, vital /sensitive or classified information;
2. Loss of Competitive Advantage;
3. Reputational Damage;
4. Economic damage (both direct and indirect costs);
5. Loss of control of infrastructure and authorisation management.

Significant Malware Cases

- **RSA**
On March 17, 2011, approximately a month after announcing its CyberCrime Intelligence Service, RSA disclosed that it had been hacked. The attack targeted RSA's two-factor authentication products. The attack compromised RSA Security's network of about 40 million tokens and involved the use of stolen SecurID information to launch an attack on a key RSA Security customer, Lockheed Martin, the US defence contractor.
- **Diginotar**
The company DigiNotar B.V. provides digital certificate services; it hosts a number of Certificate Authorities (CA's). Certificates issued include default SSL certificates, Qualified Certificates and PKIoverheid (Government accredited) certificates. On the evening of Monday August 29th 2011 it became public knowledge that a rogue *.google.com certificate was presented to a number of Internet users in Iran. This false certificate had been issued by DigiNotar B.V. and was revoked that same evening.
- **Stuxnet**
Stuxnet is a computer worm discovered in June 2010. It initially spreads via Microsoft Windows, and targets Siemens industrial software and equipment. While it is not the first time that hackers have targeted industrial systems, it is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit.
- **Hydraq / Aurora**
A hack attack that targeted Google in December 2009 also hit 33 other companies, including financial institutions and defense contractors, and was aimed at stealing source code from the companies, say security researchers at iDefense. The hackers used a zero-day vulnerability in Adobe Reader to deliver malware to many of the companies and were in some cases successful at siphoning the source code they sought, according to a statement distributed by iDefense, a division of VeriSign. Trojan.Hydraq itself is very much a standard backdoor Trojan. Considering the efforts that the attackers put into staging the attack as a whole, the end malware is not so sophisticated. It doesn't use any anti-debugging or anti-analysis tricks. It just uses some basic obfuscation in the form of spaghetti code on some of its components.
- **Zeus**
Zeus is a Trojan horse that steals banking information by Man-in-the-browser keystroke logging and Form Grabbing. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009, security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com,

Cisco, Amazon, and BusinessWeek. In the Netherlands different banks like Rabobank, ING, SNS, ABN AMRO were affected by the ZeuS malware.

- Other Cases
Other significant malware cases include: Titan Rain, Nitro, Duqu, Bredolab / Oficla, Nightdragon

Malware, Lessons Learned:

- Being the victim of a hacker is a certainty
- Cybercrime requires a 24X7 radar, following two tracks:
 - Technical:
 - Improved network monitoring & logging 24X7 all IT systems;
 - All malware detection events should be sent to a central compartmented enterprise anti-malware administration tools and event log servers;
 - Analyst and incident response capacity is available.
 - Organisational:
 - a flexible security organisation is available;
 - capable to respond and analyse adequately on suspicious incidents and attacks and new or prospective threats and follows recent developments, whitepapers, factsheets, newsgroups on malware;
 - The security organisation implemented a well followed and up to date security awareness program.
- The operation, the accuracy and adequacy of the security organisation itself is being under constant review, and audited periodically
 - Review of central logging analysis (Indicators, Abnormalities) -webserver, ids logging, fw logging, dns logging, virusscan client and server logging, mail logging, mobile device logging, logging of compartmented systems
 - Review the quality of security controls (for instance testing malware ids signatures and polymorphic code)
 - Problemanalysis vs. "Whac a Mole"
- Executing a risk and security assessment is a necessity and should be executed periodically:
 - It's necessary to identify and classify information;
 - Conduct vulnerability assessment across the IT infrastructure;
 - Assess and identify possible adversaries and their respective capabilities;
 - Determine what information should be kept in isolated compartments;
 - Determine the strategy to protect the information;
 - Determine the measures to be taken in every aspect of the IT infrastructure (defense-in-depth)
- For the day to day operation, and due to continuous technological developments, it's necessary that the organization has an in-depth knowledge regarding:
 - IT infrastructure
 - Data storage, processing and distribution
 - In generic: granted autorisations and more specific on superusers/admins: who/when/where
 - Implemented counter-measures, these should be under constant reconsideration
- Developments in Sourcing, Cloud and BYOD within organization is a growing point of attention due to:
 - Loss of control on information and hardware and the difficulty to have a proper and legally accepted detection mechanism.
- Frameworks / Standards
 - Most frameworks/standards have measures for known threats
 - Most frameworks/standards do mainly focus on internal threats
 - Frameworks are minimal baselines, they don't cover and follow the fast technological developments
 - Frameworks will never touch every detail and finesse of any possible threat

- Frameworks rarely or at cursory address penetration testing
- Frameworks do not consider creativity of cybercriminals
- Most frameworks do not consider the obligation to review the implementation of prescribed measures

Top 5 recommendations for the IT Auditor:

1. The Information, the IT infrastructure, and all it's components, of organisations are targets of cybercriminals, as a consequence IT auditors are inherently part of this cyber spectrum.
2. Auditors have an good knowledge of continuous technological developments on cybercrime and ICT security. When there is a lack of knowledge in an to be audited technology they know where to find the right people to support the auditing.
3. An auditor is proactively when needed as an advisor on to be implemented measures.
4. Auditors do realize that malware-countermeasures like virusscanning, IDS/IPS, f/w's and logging are minimal standards. Additional measures, like mentioned in this sheet should be taken, but a 100% warranty against every kind of malware can't be given.
5. Penetration testing is taking into consideration before audits are executed.

Links / Sources:

In a daily changing environment it's very hard to conclude with a definitive correct and complet list of valuable links, the links presented here are intended solely to give a useful list of documentation.

SANS Institute (<http://www.sans.org>)

- Bypassing Malware Defenses, Morton Christiansen, 7-5-2010 (testing and understanding the efficiency and configurations of malware defense systems is of uttermost importance)
http://www.sans.org/reading_room/whitepapers/malicious/bypassing-malware-defenses_33378
- SANS Institute's Consensus Audit Guidelines http://www.sans.org/critical-security-controls/cag3_1.pdf
- Assessing Outbound Traffic to Uncover Advanced Persistent Threat
<http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf>

Govcert / NCSC

- www.govcert.nl/binaries/live/govcert/hst%3Acontent/english/service-provision/knowledge-and-publications/trend-reports/trend-report-2010/trend-report-2010/govcert%3AdocumentResource/govcert%3Aresource
- Pentesting www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/whitepapers/pentesten-doe-je-zo/pentesten-doe-je-zo/govcert%3AdocumentResource/govcert%3Aresource (in Dutch only)

PCI (Payment Card Industry)

- https://www.pcisecuritystandards.org/security_standards/prioritized.php
- Pentesting
https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf

CPNI (UK Center for the Protection of National Infrastructure)

- <http://www.cpni.gov.uk/advice/infosec/>
- http://www.cpni.gov.uk/documents/publications/2010/2010nov-understanding_electronic_attack-compromise_on_corpnet_report.pdf?epslanguage=en-gb

Wikipedia:

Computer viruses

http://en.wikipedia.org/wiki/Computer_virus

Worms

http://en.wikipedia.org/wiki/Computer_worm

Trojan horses

http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29

Spyware

<http://en.wikipedia.org/wiki/Spyware>

Adware

<http://en.wikipedia.org/wiki/Adware>

Scareware

<http://en.wikipedia.org/wiki/Scareware>

Crimeware

<http://en.wikipedia.org/wiki/Crimeware>

Rootkits

<http://en.wikipedia.org/wiki/Rootkit>

Keyloggers

<http://en.wikipedia.org/wiki/Keylogger>

Ransomware

http://en.wikipedia.org/wiki/Ransomware_%28malware%29

Hardware – Malware

http://www.cl.cam.ac.uk/~sps32/sec_news.html#Assurance

Significant Cases:

RSA

- <http://isc.sans.edu/diary.html?storyid=10609>
- <http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers/>
- http://www.huffingtonpost.co.uk/andrew-kemshall/the-rsa-security-breach-1_b_1344643.html

Diginotar

- <http://www.govcert.nl/english/service-provision/knowledge-and-publications/dossier-diginotar>
- www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf
- https://docs.google.com/document/d/1kLBonTqidEMYwQqz2wGKSP-vUoDi0MZmERN-zQ-f8Bl/edit?hl=en_GB&pli=1
- <http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/factsheet-fraudulently-issued-security-certificate-discovered.html>

Stuxnet

- <http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/facsheet-vulnerability-in-windows-stuxnet.html>
- <http://en.wikipedia.org/wiki/Stuxnet>

Hydraq / Aurora

- <http://www.wired.com/threatlevel/2010/01/google-hack-attack/>
- <http://www.secureworks.com/research/blog/research/20913/>

Zeus

- http://www.cpni.gov.uk/documents/publications/2010/2010019-phishing_pharming_guide.pdf
- <http://www.enisa.europa.eu/activities/application-security/smartphone-security-1/app-kill-switch-the-last-line-of-defence>
- http://www.enisa.europa.eu/activities/application-security/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware/at_download/fullReport