











Fact sheet: Malware










Malware, short for malicious software, is software (i.e. code, script, active content) designed to trigger 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 is also known as computer contaminant, and includes:

-  *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.
-  *Ransomware* is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.
-  Other: Spyware, Adware, Scareware, Crimeware, Keyloggers.

Key developments and trends related to Malware

-  More than 357 million new unique pieces of malware discovered by Symantec in 2016
-  In 2016 the average identities exposed per breach was 927.000
-  Phishing rate increased with 41 percent in 2016 compared to 2015
-  A new zero-day vulnerability was discovered on average each week in 2015, an increase of 125 percent from the year before
-  Ransomware continues to evolve. Crypto-ransomware (encrypting files) pushes the less damaging locker-style ransomware (locking the computer screen) out of the picture. Crypto-style ransomware grew 35 percent in 2015
-  Spear-phishing campaigns targeting employees increased 55 percent in 2015
-  Major security vulnerabilities in 75% of popular websites put us all at risk
-  Email Malware Rate overall (2016), 1 in 131
-  New Android Mobile malware variants (2015), up with 77 percent

Key considerations on Malware resilience

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.

Procedural:

- 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;
- A well followed and up to date security awareness program is implemented.

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, virus scan client and server logging, mail logging, mobile device logging, logging of compartmented systems
- Review the quality of security controls (e.g. testing malware ids signatures and polymorphic code)
- Problem analysis 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 authorisations and more specific on super users/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.

Key focus areas for the IT auditor:

- ☐ The Information, the IT infrastructure, and all its components, of organisations are targets of cybercriminals, as a consequence IT auditors are inherently part of this cyber spectrum.
- ☐ Auditors have a good knowledge of continuous technological developments with regard to Information Security.
- ☐ An auditor is proactively when needed as an advisor on to be implemented measures.
- ☐ Auditors do realize that malware-countermeasures like virus scanning, IDS/IPS, f/w's and logging are minimal standards. Additional measures, like mentioned in this sheet should be taken.
- ☐ Penetration testing is taking into consideration before audits are executed.

References and external links:

In a daily changing environment it's very hard to conclude with a definitive correct and complete 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) www.sans.org/reading_room/whitepapers/malicious/bypassing-malware-defenses_33378
 - SANS Institute's Consensus Audit Guidelines www.sans.org/critical-security-controls/cag3_1.pdf
 - Assessing Outbound Traffic to Uncover Advanced Persistent Threat www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf
- ☐ Nationaal Cyber Security Centrum <https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2016/1/CSBN2016.pdf>
- ☐ National Institute of Standards and Technology <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- ☐ PCI (Payment Card Industry) www.pcisecuritystandards.org/security_standards/prioritized.php
https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf
- ☐ CPNI (UK Center for the Protection of National Infrastructure) www.cpni.gov.uk/documents/publications/2010/2010nov-understanding_electronic_attack-compromise_on_corpnet_report.pdf?epslanguage=en-gb
- ☐ Symantec, Internet Security Threat Report, volume 22, april 2017: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>