



Malware Taxonomy

Gergely Erdélyi – Senior Manager, Anti-malware Research

Definition of Malware

“Software specifically designed to harm the user’s computer or data.”

MALicious soft**WARE**

Terminology: Categories

Category specifies by which process the malware is handled:

Clean:	Not malware
Hoax:	Hoax emails with fake virus alerts and similar
Malware:	Malicious software
Phishing:	Phishing emails
Riskware:	Potentially unwanted software
Spam:	Unsolicited bulk email
Spyware:	Software that invades the user's privacy
Malformatted:	Broken, corrupt files

Terminology: Malware Types

Type specifies the distinguishing malicious features of the sample:

Virus:	Self-replicating (most often refers to parasitic infectors)
Worm:	Self-replicating, stand-alone malware
Backdoor:	Allows unauthorized access to compromised computers
Exploit:	Exploits a software vulnerability to gain authorized access
Trojan:	Non-replicating, deceiving software with hidden functionality
Rootkit:	Stealth, actively hiding software
HackTool:	Exploiting, attack and scanning tools
Spyware:	Software that invades the user's privacy

Terminology: Platforms

Platforms specifies the software or hardware platform the malware executes on:

W32: 32-bit Windows platforms (Win32)

W64: 64-bit Windows platforms (Win64)

Linux: Linux platform

OSX: Apple Mac OS X

JS: JavaScript

X97M: VBA macros for Excel 97 or later versions

SymbOS: Symbian OS

Infection Vectors

Boot Sector: Infecting boot sector or Master Boot Record

File infection: Parasitic infectors

Macros: Macro viruses, type of parasitic infectors

Email: Email worms, spam, phishing

File shares: Parasitic infectors, worms

Network: Network worms, through vulnerabilities

IRC: Internet Relay Chat

P2P networks: IM, Kazaa, etc.

Bluetooth: Worms for mobile devices

Web Apps: Using cross-site scripting vulnerabilities

Other Malware Features

- Multi partite:** Infects several objects (files _and_ boot sector)
- Multi-part:** Malware with several components that work together
- Polymorphic:** Contains a changing encryption layer
- Metamorphic:** Morphs the actual code at each infection
- Stealth:** Actively trying to conceal its presence (a.k.a. rootkit)
- EPO:** Entry Point Obfuscator
- Resident:** After initial start it stays active in memory

Possible Symptoms of Infection

- Unexpected system behaviour
- System instability
- Unknown new executables on the computer
- Unexpected network traffic
- Bounces of infected emails
- Alerts from security software (firewall, antivirus heuristics)
- Money missing from your bank account / credit card
- FBI knocking on your door

Payloads

There have been different trends in malware payloads:

- Non-destructive (funny message, author showing off)
- Destructive (corrupting files, full hard drive)
- Commercial / criminal intent

Example Payloads:

- Displaying messages, pictures or animations
- Overwriting of files or disk sectors
- Monitoring / keylogging / data theft
- Backdoor / remote control functionality
- Attack drone / proxy functionality