Malware

System Security (CM0625, CM0631) 2025-26
Università Ca' Foscari Venezia

Riccardo Focardi
www.unive.it/data/persone/5590470
secgroup.dais.unive.it

Università
Ca'Foscari
Venezia

Definition

NIST SP 800-83

Guide to Malware Incident Prevention and Handling for Desktops and Laptops

Malware (or **malicious code**), is a program that is *covertly inserted* into another program with the intent to:

- **destroy** data
- **run** destructive or intrusive programs
- **compromise** the confidentiality, integrity, or availability of the victim's data, applications, or operating system

⇒ One of the most widespread threats

Malware classification

Propagation mechanism:

- infection of existing executable/interpreted content
- exploitation of vulnerabilities
- social engineering

Payload actions:

- **corruption** of system / data
- theft of a **service**
- theft of **information**
- **stealthing**

Malware can be:

- ***Parasitic*** vs. ***self-contained***
- ***Replicating*** vs. ***non-replicating***

Attack kits

Toolkits for the deployment of malware attacks (since 2000s)

- variety of **propagation** methods
- variety of **payload** “modules”
- **customizable** with last 0-day vulnerabilities

Also known as **crimeware**

⇒ Enlarge the population of malware attackers

Examples:

Zeus crimeware toolkit (2007): **bank** malware that can attack credentials, tamper with on-line bank operations

Angler exploit kit (2013): exploits Flash and browser vulnerabilities to propagate

⇒ Malware as a **service**!

Advanced Persistent Threat (APT)

Attacks to **selected targets** that are persistent and stealthy

Advanced: wide variety of intrusion techniques and (custom) malware

Persistent: over an extended period, so to maximize damage

Threat: attacker's intent to compromise the selected targets

Examples:

- Theft of **intellectual property**
- Theft of **government data**
- Physical disruption of **critical infrastructures**

Propagation mechanisms

(malware classification)

1. **Infection**
2. Exploitation
3. Social engineering

Viruses

Computer Virus: category of malware that infects other programs

Note: word *Virus* is often used to refer to malware, in general

- First computer virus: early 1980s
- Like biological viruses, computer viruses replicate by attaching their **code** to other programs (**code** is like virus **DNA**)

Viruses inherits **privileges** from the infected program

⇒ With no access control it would be possible to infect **any** executable in the system

Access control & **least-privilege** limit a lot the infection of executables

⇒ **Macro viruses** (documents)

Virus structure and lifecycle

Viruses have three components:

- **Infection mechanism**: replicates and spread the virus
- **Trigger**: the condition that activates the payload, also known as **logic bomb**. Can be a date, a configuration, an event
- **Payload**: what the virus does, besides spreading

Virus lifecycle:

1. **Dormant** phase: virus is idle waiting to be activated
2. **Propagation** phase: virus copies into other programs
3. **Triggering** phase: virus becomes active
4. **Execution** phase: payload is executed. Ex.: message on the screen, destruction of data, ...

Macro virus

A virus that attaches itself to **documents** and uses the **macro programming capabilities** of the document's application to execute and propagate [NISTIR 7298]

Examples: Microsoft Office documents and PDF documents

- repetitive tasks, dynamic content, form validation, ...

An **increasingly popular** threat:

1. Platform **independent**
2. Documents are the most **popular** form of information getting into a system
3. Documents are often **shared**
4. Documents are **writable** by users (programs usually are not)
5. Macro viruses are **simpler** than traditional executable viruses

Case study: Melissa macro virus

Released in 1999, targeting Microsoft **Word** and spreading through **Outlook**

Word macros were executed when a document was opened, created, closed

Word macros could **read**, **write** files and **call other applications**

Melissa was activated when the document was **opened** (code)

1. Disable Macro menu and security features (**stealthy**)
2. If called from document: copy into global template (**propagate**)
3. If called from global template copy into the document (**infect**)
4. Use Outlook to attach to 50 emails infected documents (**propagate**, only once: **stealthy**)
5. if minutes==day of month add a Simpson quote (**trigger+payload**)

Concealment strategies

Encrypted: virus is encrypted apart from a small fraction of code that decrypts the virus and execute it

- **random key** ⇒ no fixed pattern

Stealthy: code mutation (polymorphic/metamorphic), compression or rootkits, that we will discuss later

Polymorphic: copies with same functionality but different code

- adding, permuting instructions
- use encryption and then mutate just the decryption code

Metamorphic: mutates itself so to make detection harder. Can also mutate behaviour

Propagation mechanisms

(malware classification)

1. Infection
2. **Exploitation**
3. Social engineering

Worms

Computer Worm: a program that propagates on hosts and systems

- each infected host serves as an **automated launching pad** for attacks on other machines

Worm programs exploit **software vulnerabilities** in client or server programs to gain access to each new system

Worms **scans the network** to look for possible targets

Possible strategies are:

- Scanning hosts in a predefined “hit-list”
- Scanning hosts related to the infected ones
- Scanning the local subnetwork

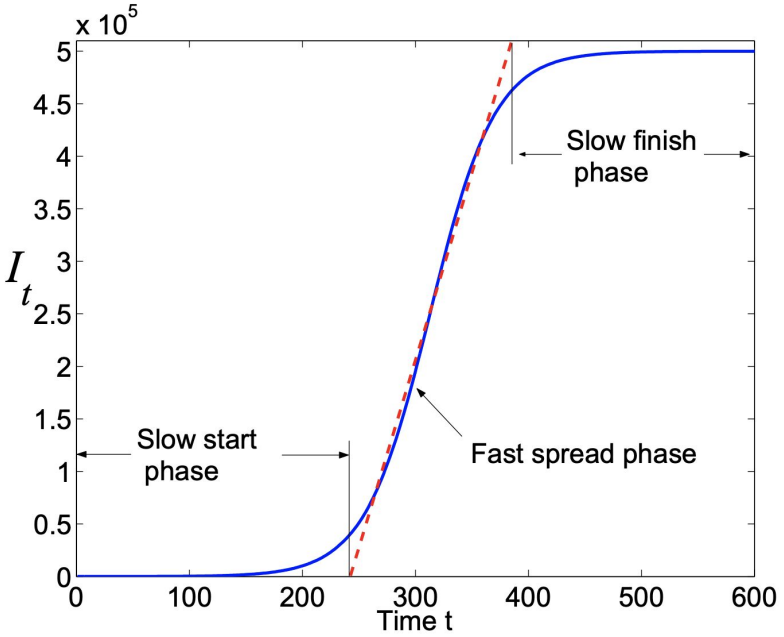
Worm propagation model [Zou'05]

Simple **epidemic model**:

$$\frac{dI_t}{d_t} = \beta I_t [N - I_t]$$

- β is the pairwise infection rate
- N is the number of hosts
- I_t is the number of infected hosts at time t

⇒ Catch in the **slow start phase**!



[Zou'05] Zou, C., et al. "The Monitoring and Early Detection of Internet Worms." *IEEE/ACM Trans. on Networking*, October 2005.

Case study: the Morris worm (1998)

Target: UNIX systems

Host discovery: examining system tables that declared

- trusted hosts
- users' mail forwarding files
- user's remote accounts

… and checking the **status** of network connections

For each discovered host, the worm tried a number of **methods for gaining access**:

- **Crack** the local password file
- **Vulnerability** in the UNIX "finger" protocol
- **Vulnerability** in the sendmail process

⇒ Once in, it could install/run the worm on the new host

Brief history of worm attacks (1)

Melissa (1998): virus and worm in one package

- Opening attachment **propagated** worm by email and virus into documents
- 1999: new version exploiting visual basic scripting in emails: **no need to open** the attachment!
- **Three days** to infect **~100K** computers

Code Red (2001): exploited a **vulnerability** in Microsoft Internet Information Server (**IIS**)

- Phase 1: was only spreading
- After trigger, **distributed DoS** attack on government sites
- **~360K** servers in **14 hours**

Code Red II (2001): also installed a ***backdoor*** for remote execution

Brief history of worm attacks (2)

Sobig.F (2003): exploited proxy servers to turn them into **spam engines**

- **> 1M hosts** of in **24 hours**

Mydoom (2004): mass-mailing e-mail worm

- replicated **~1000 times/minute**
- **100M** infected messages in **36h**
- **exploited IE** to install a backdoor

Samy (2005): the first Web worm, onto MySpace (details here)

Conficker (2008): one of the largest worm infection ever

- exploited vulnerabilities in Windows systems
- **millions of computers** including government, business and home computers **>190 countries**

Brief history of worm attacks (3)

Stuxnet (2010): targeting Industrial Control Systems (ICS)

- exploiting **0-day** vulnerabilities
- first **Cyberwarfare** weapon ever
- targeting the Iranian nuclear program

⇒ Worm induced **stealthy failures** on the centrifuges for uranium enrichment

Flame (2012): Cyber-espionage on Middle-Eastern countries exploiting advanced vulnerabilities

- **MD5 collisions** using a new attack! (see the paper)

WannaCry (2017): vulnerability in the SMB file sharing of Windows

- encrypting files and asking for a **ransom**