Information Security

CS3002

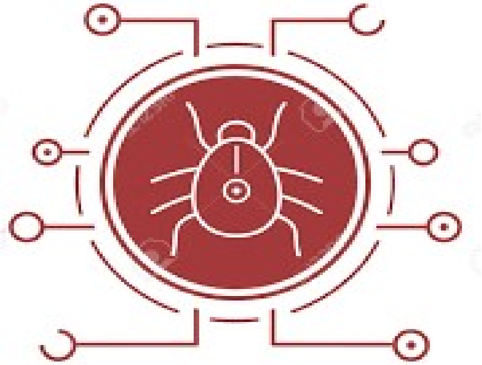
Lecture 12

5th October 2023

Dr. Rana Asif Rehman

Email: r.asif@lhr.nu.edu.pk

MALWARE



What is a malware ?

- "A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim." (NIST – 2005)
- Also called digital pests

What can it do?

- Damages (Sabotage)
- Disables (Sabotage)
- Takes Control of Flow of Execution or Programs (Hijack)
- Takes Full Control of Computing or Network Device (Hijack)
- Steals Information (Espionage)
- Changes the Information (Attacking Integrity)

Exploits

- **Exploit Code**
  - An exploit is a piece of code or a program that takes advantage of a weakness in an application or system
  - Exploitation Techniques
    - Payloads of the Malware to be delivered
    - Zero-Day Exploits: Unknown Exploits
    - CVE: Common Vulnerabilities and Exposures
    - Can be in any programming language; commonly in C++ and Assembly

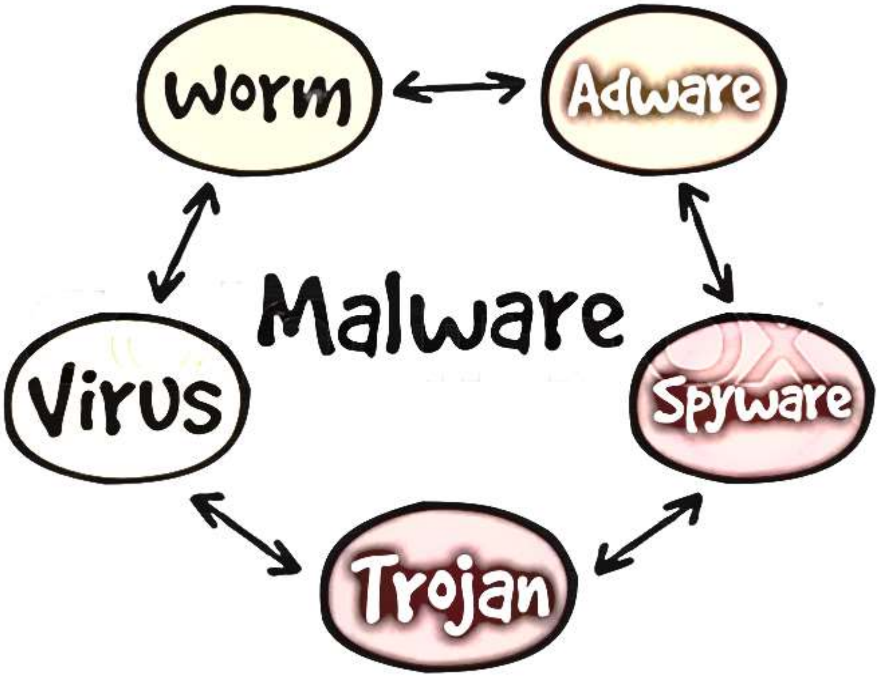
Malware Attack Vector

Attack Vector
Means and Methods through which malware is injected in the computer or network.

- **Common Attack Vectors**
  - Email Attachments
  - Pop-up Windows
  - Web Links
  - Fraud
  - Chat rooms
  - Anti-Viruses
  - Advertisements
  - Instant messages

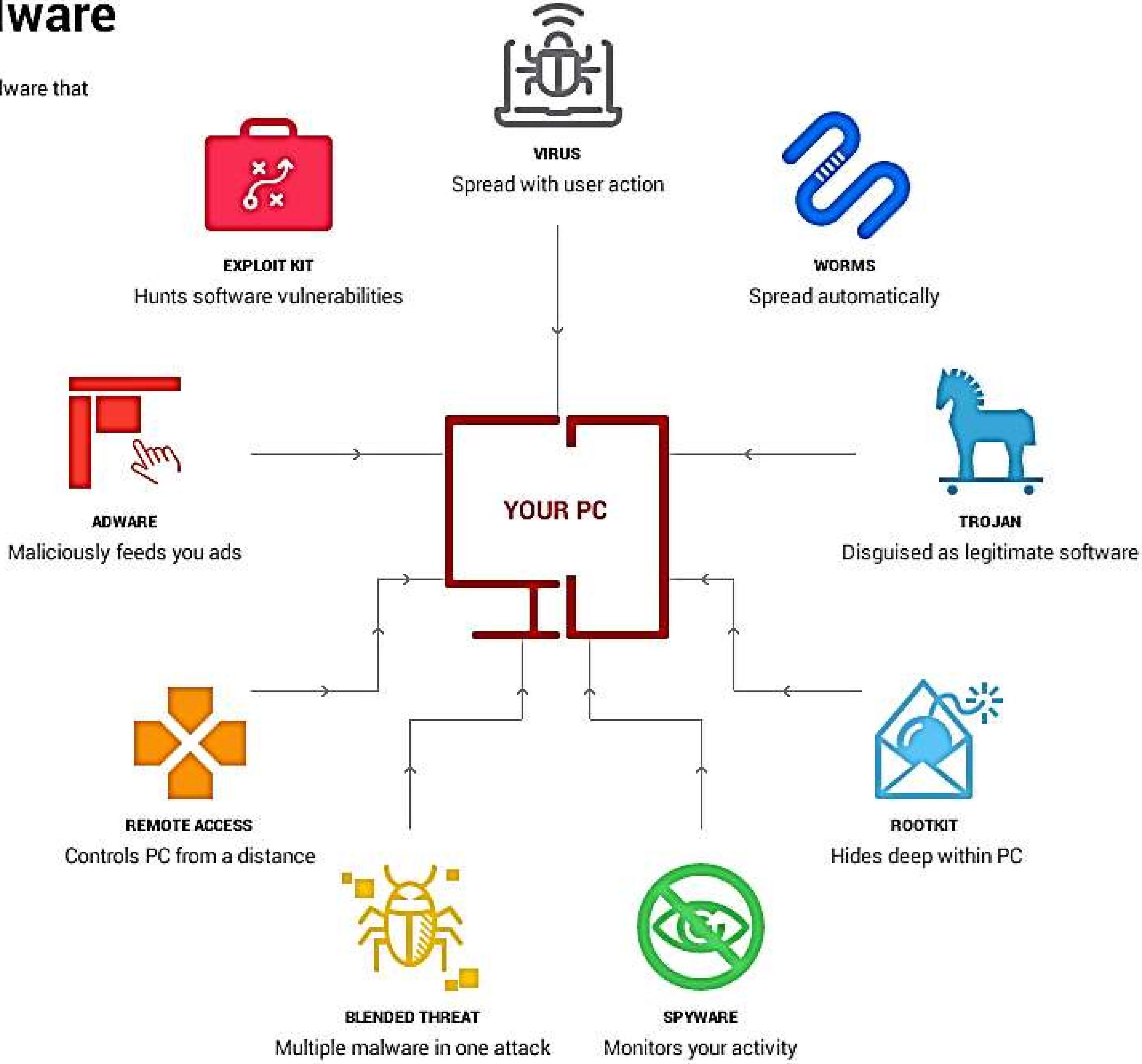
Types of Malware

- **Common Malwares**
  - Viruses
  - Worms
  - Trojans
  - Adware
  - Backdoors
  - Ransomware
  - Spyware
  - Rootkits
  - Bootkits
  - Keyloggers
  - Exploit Kits
  - Logic bomb
  - Zombie
  - Scareware



Types of malware

These are the main types of malware that can be found across the web.



VIRUS
Spread with user action

EXPLOIT KIT
Hunts software vulnerabilities

WORMS
Spread automatically

ADWARE
Maliciously feeds you ads

YOUR PC

TROJAN
Disguised as legitimate software

REMOTE ACCESS
Controls PC from a distance

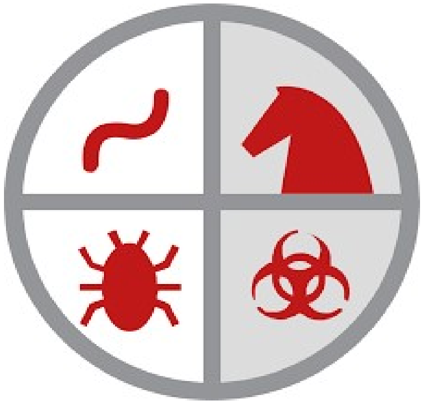
ROOTKIT
Hides deep within PC

BLENDED THREAT
Multiple malware in one attack

SPYWARE
Monitors your activity

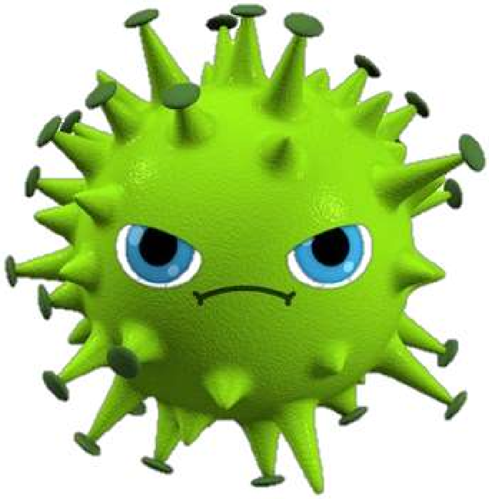
HEIMDAL SECURITY

Types of Malware



- Virus: *attaches itself to a program*
- Worm: *propagates copies of itself to other computers*
- Logic bomb: *“explodes” when a condition occurs*
- Trojan horse: *fakes/contains additional functionality*
- Backdoor (trapdoor): *allows unauthorized access to functionality*
- Spyware: used to spy on victim’s activities on a system and also for stealing sensitive information of the client.
- Ransom-ware: steals some functionality and returns after a ransom is paid
- Scare-ware: users are tricked by scaring and motivated to perform some action. E.g. buying a software license
- Key-loggers: *capture keystrokes*
- Browser hijacker: modifies a web browser's settings without a user's permission, to inject unwanted advertising into the user's browser
- Zombie: *software on infected computers that launch attack on others*

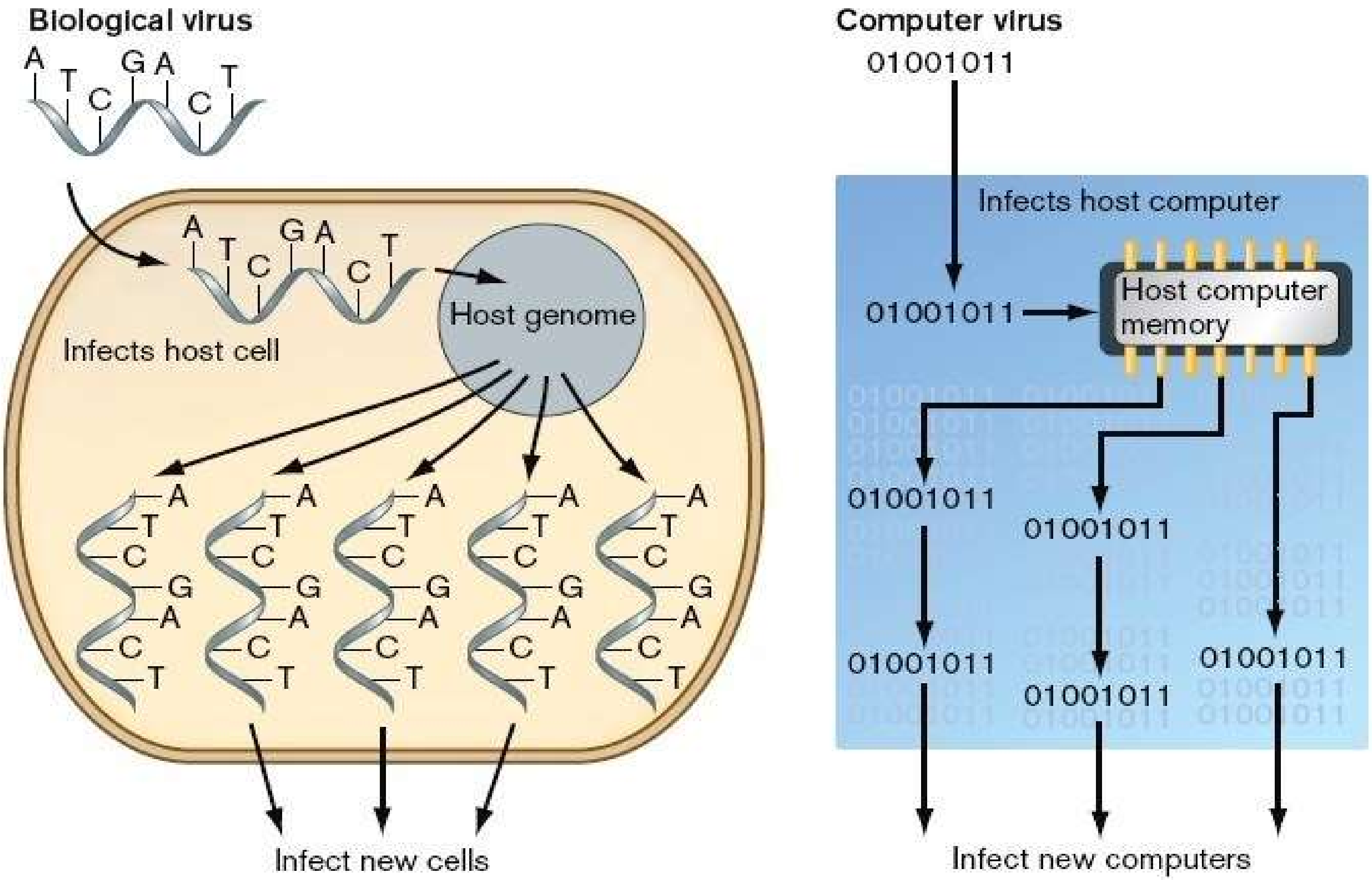
VIRUS



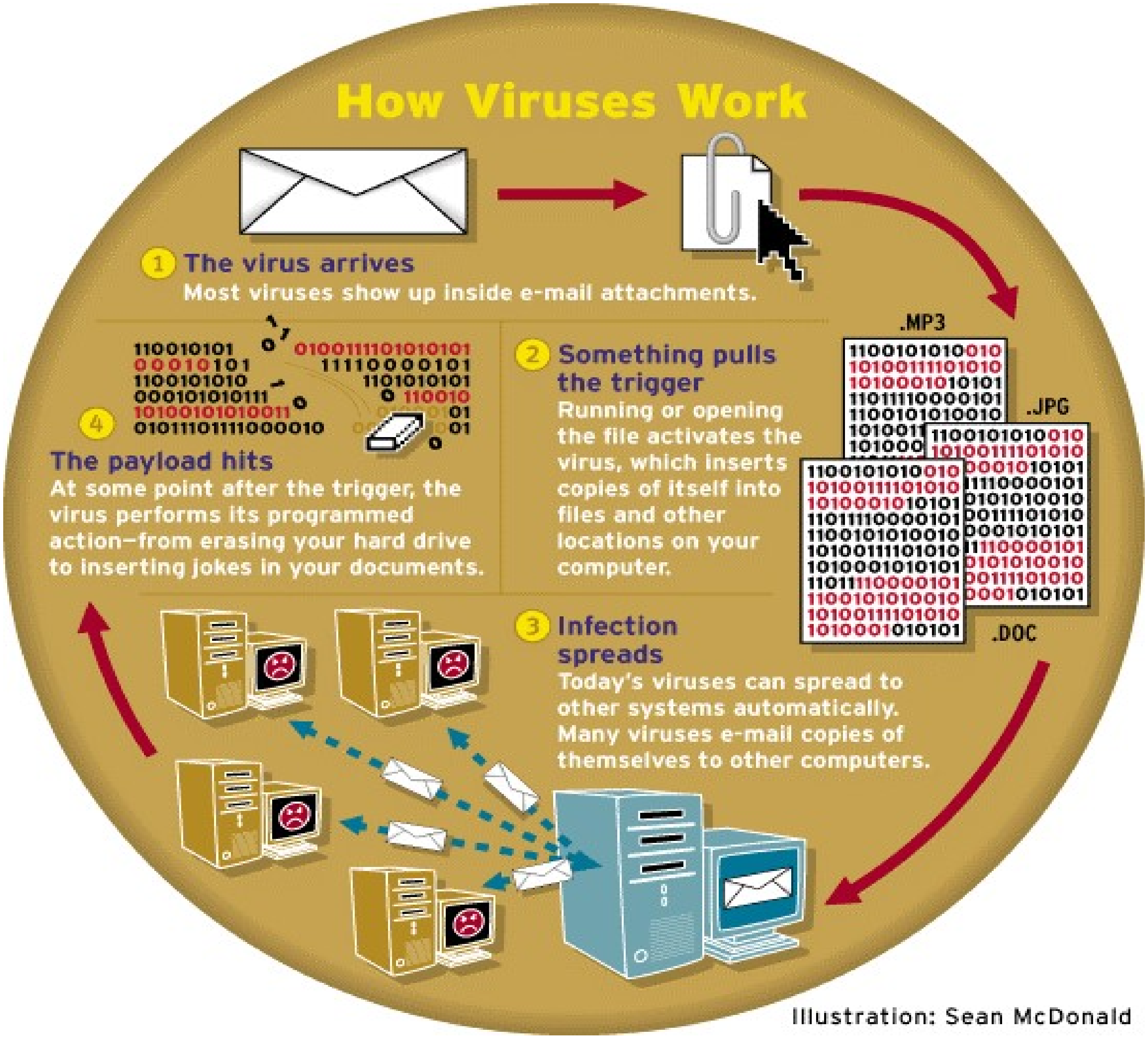
What is a Virus ?

- *A program that can infect other programs by modifying them to include a, possibly evolved, version of itself (*Fred Cohen 1983*)*
  - It executes secretly when host program is run
- Inserts copies of itself into host programs/data files
- Requires user interaction
- Often specific to operating system and hardware
  - taking advantage of their details and weaknesses

Virus


Biological virus
A T C G A C T
Infects host cell
Host genome
A T C G A C T
Infect new cells
Computer virus
01001011
Infects host computer
01001011
Host computer memory
01001011
01001011
01001011
01001011
01001011
Infect new computers

Virus



How Viruses Work

1 The virus arrives

Most viruses show up inside e-mail attachments.

2 Something pulls the trigger

Running or opening the file activates the virus, which inserts copies of itself into files and other locations on your computer.

3 Infection spreads

Today's viruses can spread to other systems automatically. Many viruses e-mail copies of themselves to other computers.

4 The payload hits

At some point after the trigger, the virus performs its programmed action—from erasing your hard drive to inserting jokes in your documents.

Illustration: Sean McDonald

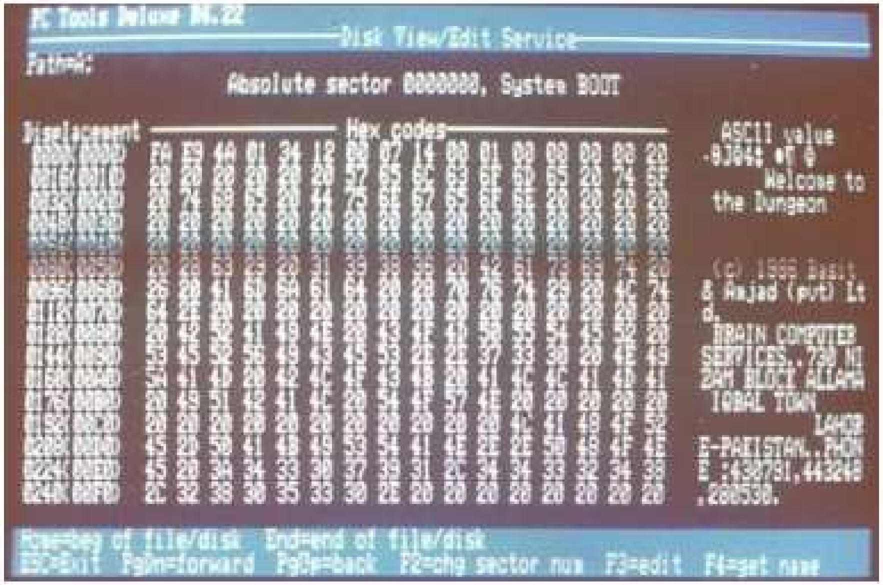
Virus

- Famous viruses
  - Brain Virus – 1986
  - Michelangelo Virus – 1991
  - Melissa Virus – 1999
  - Love Bug Virus – 2000
  - Palm Virus – 2000
  - Anna Kournikova Virus – 2001

Brain-Virus

BRAIN -The first computer Virus was created by two brothers from Lahore in 1986.

Basit Farooq & Amjad Farooq



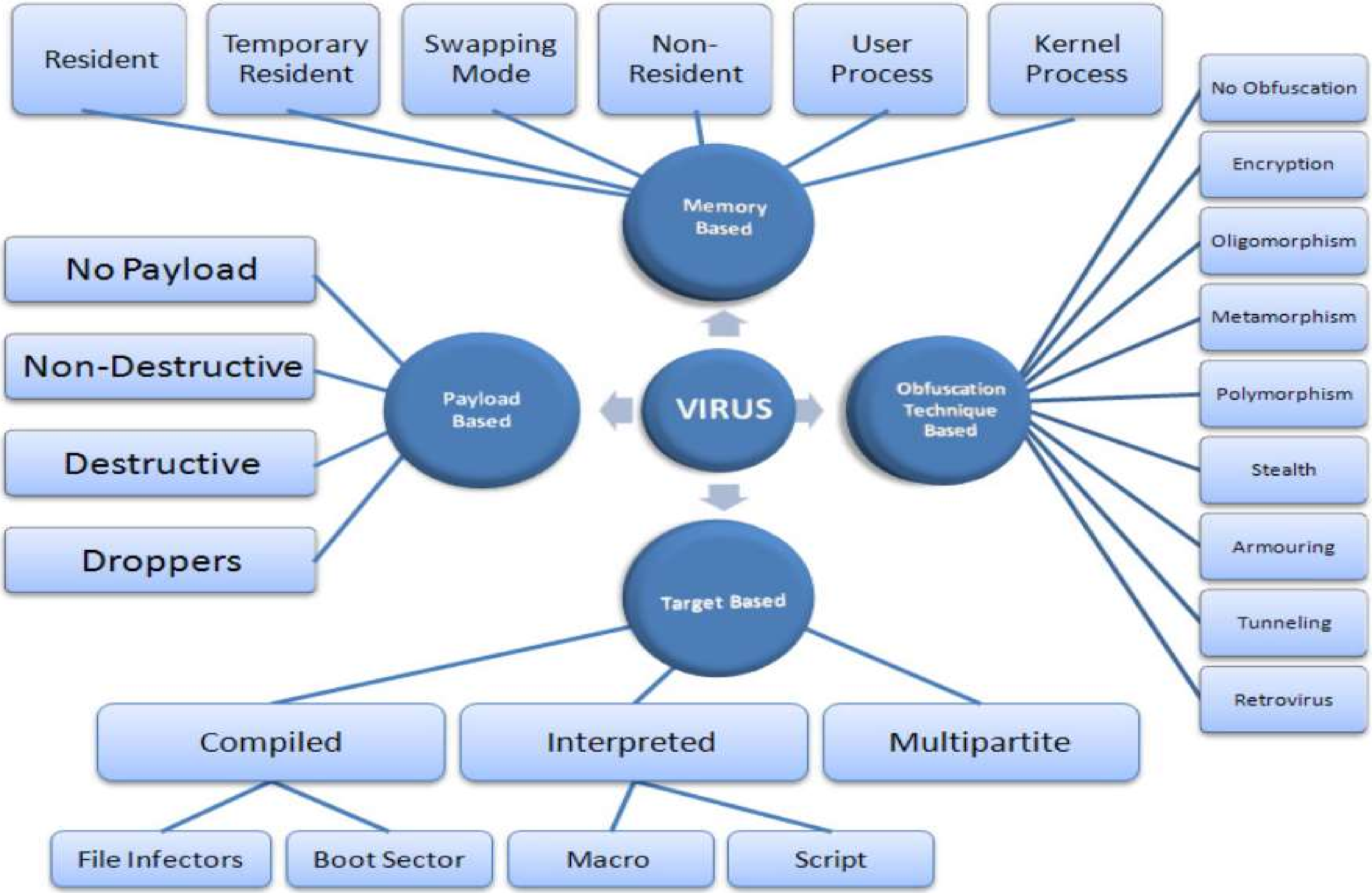
```
PC Tools Deluxe R4.22
                         Disk View/Edit Service
Path=A:
                 Absolute sector 0000000, System BOOT

Displacement  ----------- Hex codes -----------------------  ASCII value
0000(0000)  FA E9 44 01 34 12 00 07 14 00 01 00 00 00 00 20  .9J4 ♦T ☺
[illegible]                                                      Welcome to
[illegible]                                                  the Dungeon
[illegible]
[illegible]
[illegible]                                                   (c) 1986 Basit
[illegible]                                                  & Amjad (pvt) Lt
[illegible]                                                  d.
[illegible]                                                   BRAIN COMPUTER
[illegible]                                                  SERVICES..730 NI
[illegible]                                                  ZAM BLOCK ALLAMA
[illegible]                                                   IQBAL TOWN
[illegible]                                                            LAHOR
[illegible]                                                  E-PAKISTAN..PHON
[illegible]                                                  E :430791,443248
0240(00F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20  ,280530.

Home=beg of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

https://www.youtube.com/watch?v=lnedOWfPKT0&ab_channel=F-Secure

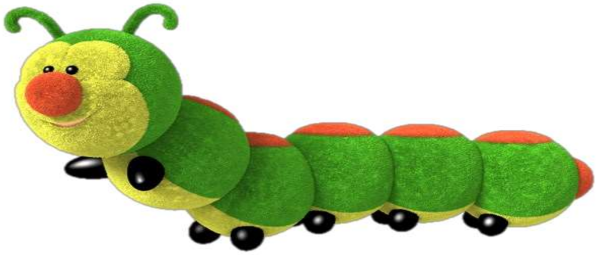
Classification of Virus

- Classification of viruses can be done as follows:
  - Memory Based
    - How they live (stay) in memory
  - Target Based
    - How they spread to others
  - Obfuscation Technique Based
    - What they do to hide
  - Payload Based
    - What they do after infection

Virus classification (detail self-study)



WORM



WORM

- **Self-replicating** computer programs
  - **Spreads** fast from one computer to another computer through the **network**.
  - **Spreads** though **exploiting vulnerabilities** in software **without user intervention**.
  - Does **not need host file** to attach to.
  - Mostly Consumes computer memory, processor and network bandwidth.
  - Usually non-destructive,
  - **Does not infect** other files
  - Most **worms** deliver **backdoors** to allow remote attacker control target machine (bot)

WORM

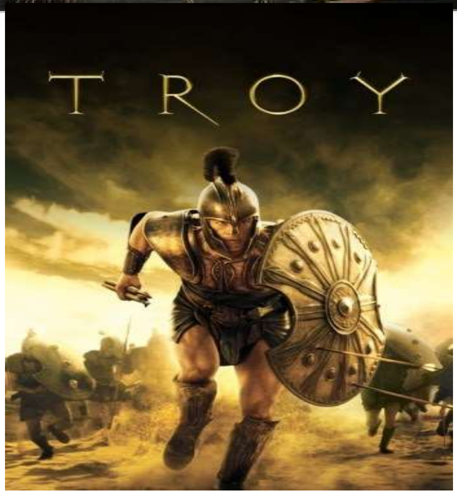
- Famous worms
  - Morris Worm – 1988
  - Code Red Worm– 2001
  - SQL Slammer Worm – 2003
  - Blaster Worm – 2003
  - Conficker Worm – 2008
  - Stuxnet Worm – 2005 – 2010

TROJAN HORSE

Trojan Horse

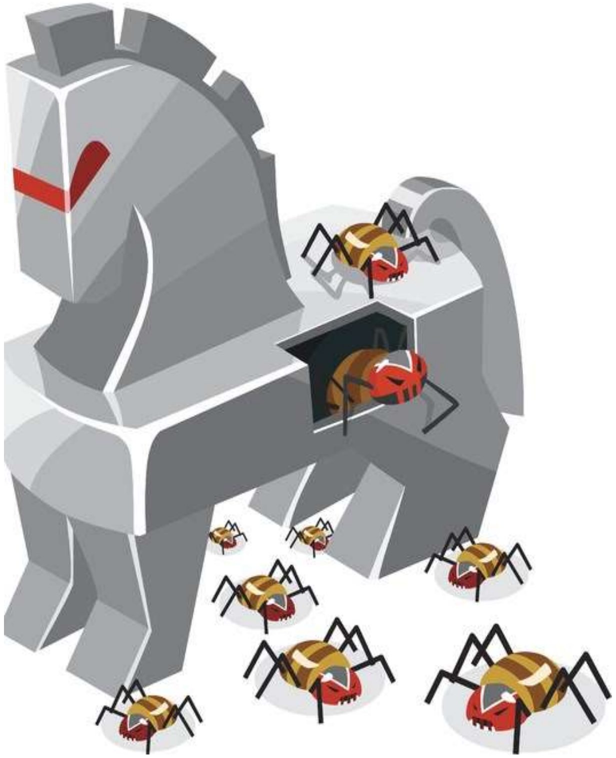
Names after **Wooden Horse** used in **Trojan Wars** between **Greeks** and **Persians.**

- **Disguised** as **innocent / useful** program
- **Non-Self-Replicating**
- **Opens a backdoor** for external attacker to infiltrate the host computer & network.
- **Monitors** the victim activity, **steals** and **transfers** information to the attacker.
- **Delivers** malicious program to the host computer.
- Need user action to activate.


TROY

Trojan Horse

- Famous Trojan Horses
  - Netbus – 1998
  - Sub7 – 1999
  - Back Orifice – 1998
  - Y3K Remote Admin Tool – 2000
  - Beast – 2002
  - Bifrost Trojan – 2004
  - DarkComet – 2008-2012
  - Blackhole exploit kit – 2012
  - Gh0st RAT – 2009
  - MegaPanzer BundesTrojaner – 2009

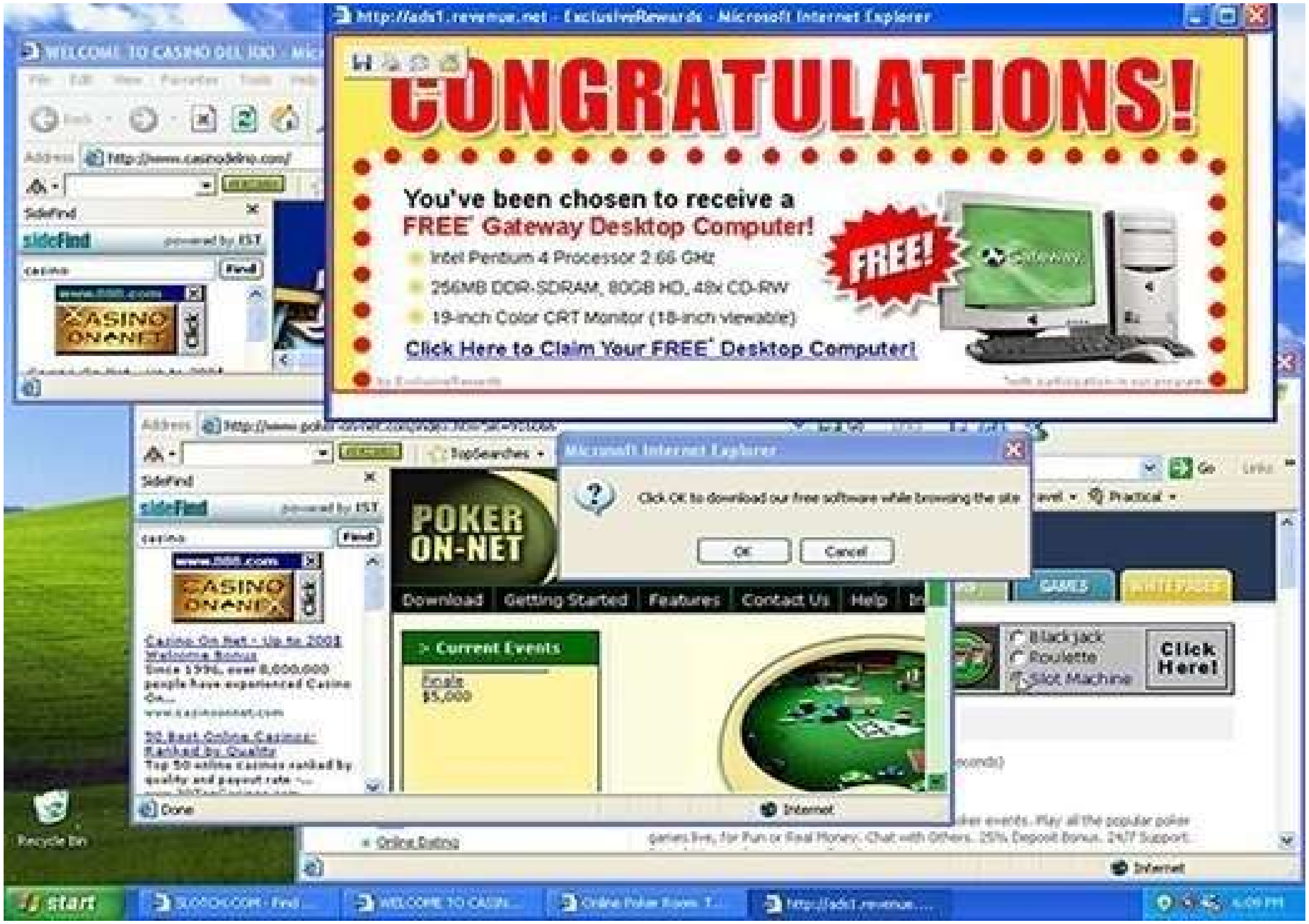


ADWARE

Adware

- Malicious software that presents unwanted advertisement as pop-up windows.
  - Mostly irritating and in some cases a threat.
  - Pop-up window sometimes un-closeable.
  - Hide as cookies or temporary internet files.
  - Also prevalent in Android systems

Adware



http://ads1.revenue.net - ExclusiveRewards - Microsoft Internet Explorer

CONGRATULATIONS!

You've been chosen to receive a FREE* Gateway Desktop Computer!

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

Click Here to Claim Your FREE* Desktop Computer!

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

OK Cancel

Adware

SPYWARE

Spyware

Designed to collect user data without the user’s knowledge or approval.

- Installed automatically or manually through virus, worm or Trojan horse
- Gathers information about you, your browsing and Internet usage habits, as well as other sensitive data.
- Runs quietly in the background for other malicious activities

Spyware

Spyware's malicious activities:

- Capturing keystrokes
- Screen shots
- Authentication credentials
- Personal email addresses
- Web form data
- Internet usage information
- Credit card numbers

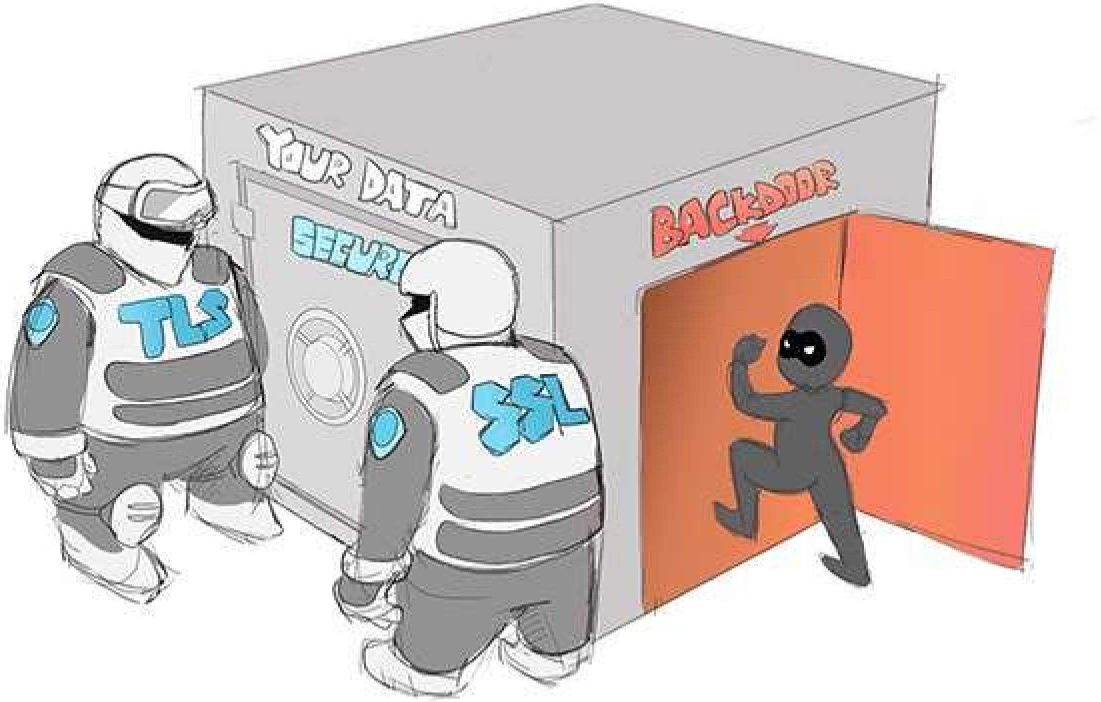
Types of Spywares:

- Password Stealers
- Banking Trojans
- Infostealers
- Keyloggers

BACKDOOR

Backdoor

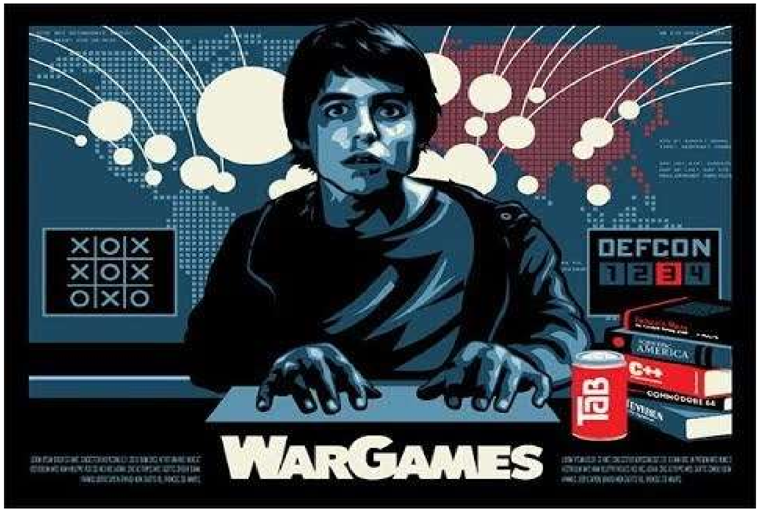
- Enables an attacker to bypass normal authentication to gain access to compromised system.



Backdoor

Means to access a computer system or encrypted data that bypasses the system's customary security mechanisms.

- Sometimes used for remote troubleshooting
- Used for spamming and spying
- Example: Backdoors in free software (file converter), Remote Access Trojan (RAT)

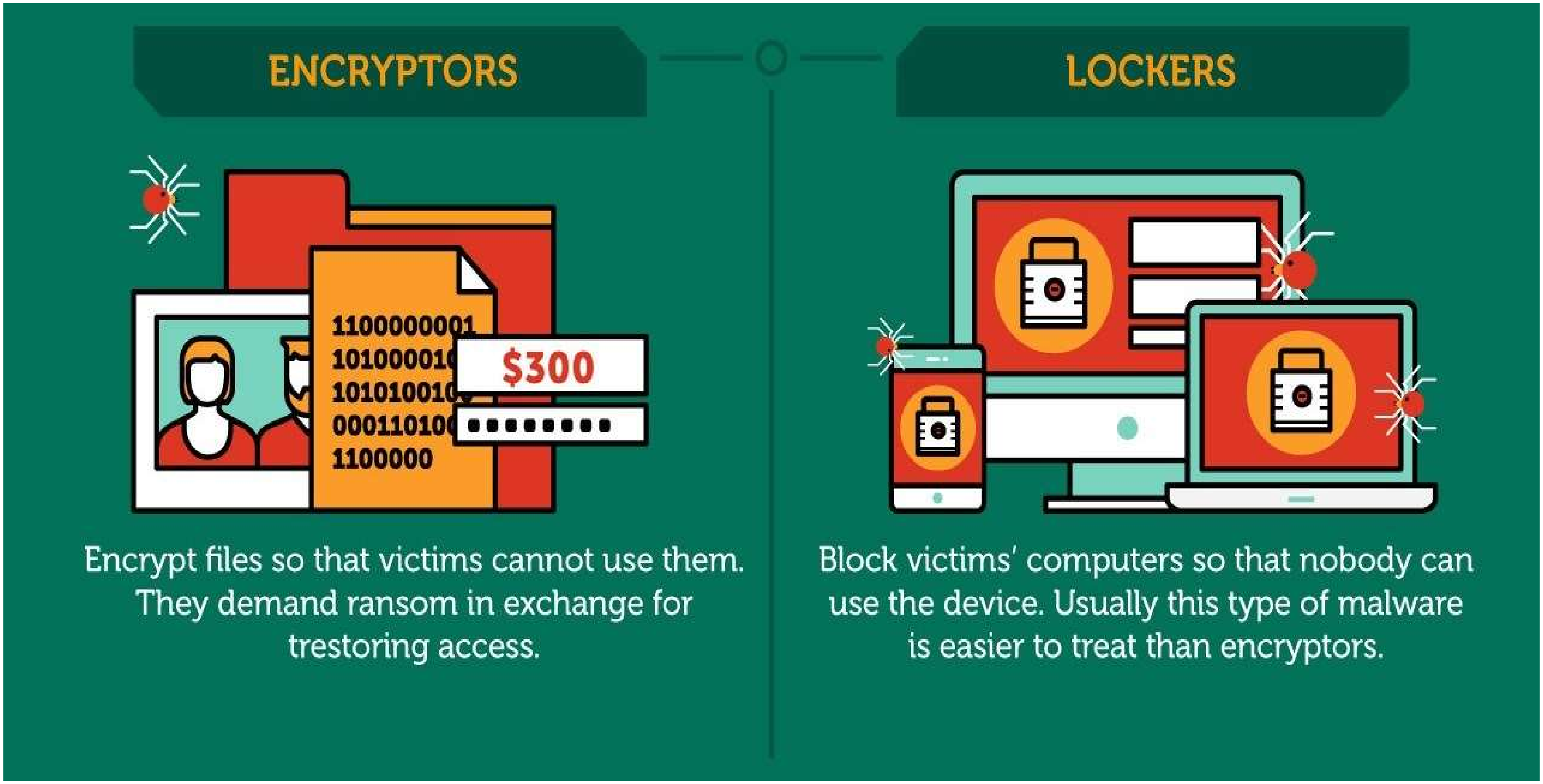


RANSOMWARE

Ransomeware

- Ransom malware
  - – Prevents users from accessing their system or personal files and demands ransom payment in order to regain access.
  - – Threatens to publish the victim's data or perpetually block access to it unless a ransom is paid

Ransomeware



ENCRYPTORS

Encrypt files so that victims cannot use them. They demand ransom in exchange for trestoring access.

LOCKERS

Block victims' computers so that nobody can use the device. Usually this type of malware is easier to treat than encryptors.

ROOTKITS

Rootkits

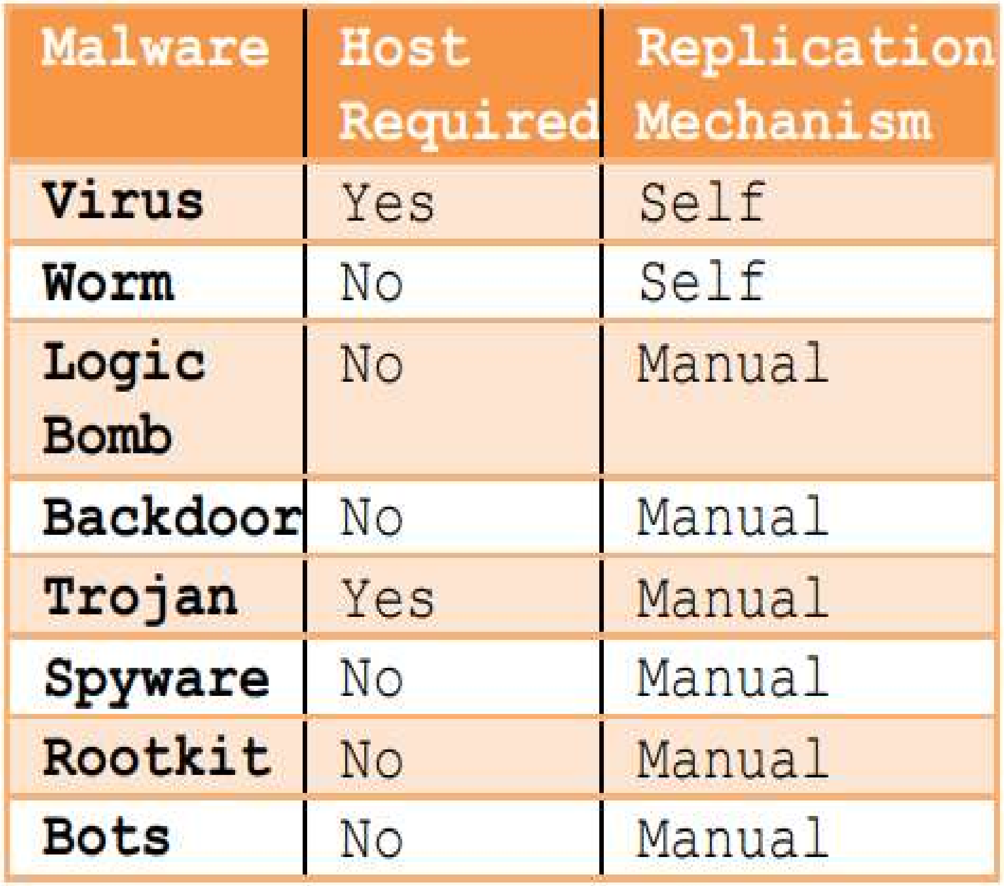
Malware that provides privileged (root-level) access to the computer.

- Can subvert anti-virus protections or other security mechanisms.
- Hides its existence deep within OS.
- Masquerades as some legitimate application
- Hides presence of other malware like virus, worm, trojan
- Avoid detection for long period of time.

Bootkits

- Rootkit variants
  - Designed to modify the boot loader (*the low-level software that runs before the OS loads*)
  - Attacks specific location of Hard Drive known as Boot Sector.
  - Commonly used to attack computers protected by Full Disk Encryption.
  - Loads into memory after getting access to Boot Sector of bootable Hard Disk.
  - Corrupts Master Boot Record (MBR) or File Allocation Table (FAT)

Malware Properties



Malware	Host Required	Replication Mechanism
Virus	Yes	Self
Worm	No	Self
Logic Bomb	No	Manual
Backdoor	No	Manual
Trojan	Yes	Manual
Spyware	No	Manual
Rootkit	No	Manual
Bots	No	Manual

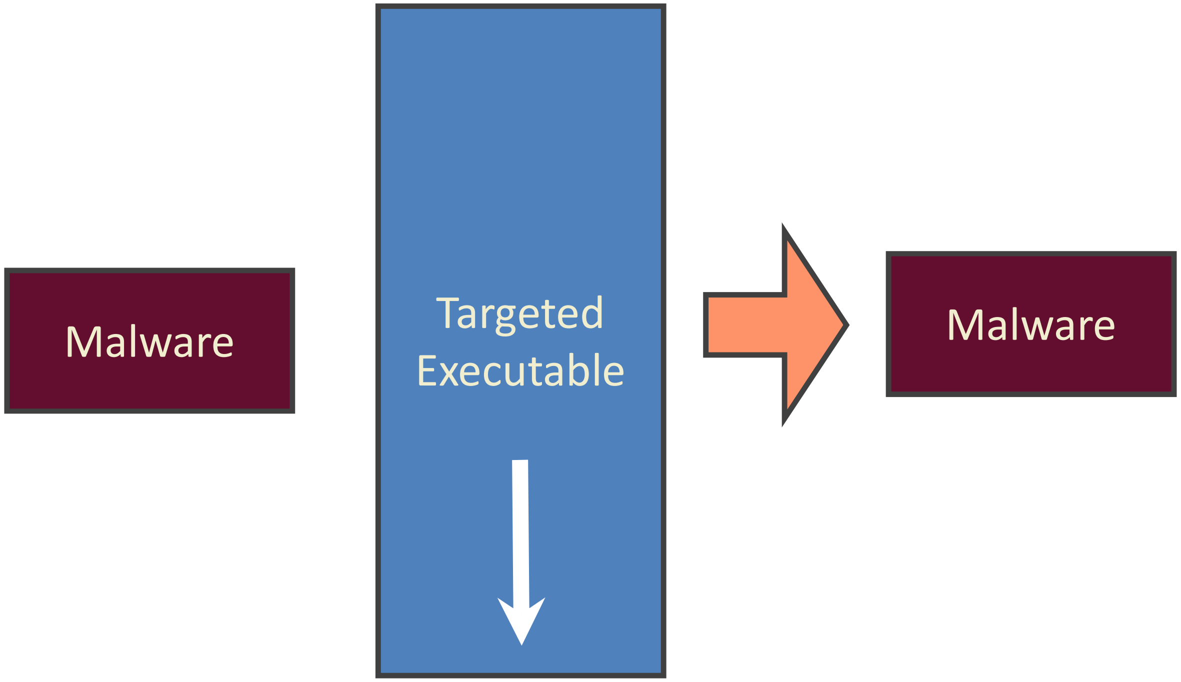
- Host required: malware needs user interaction

What they Infect?

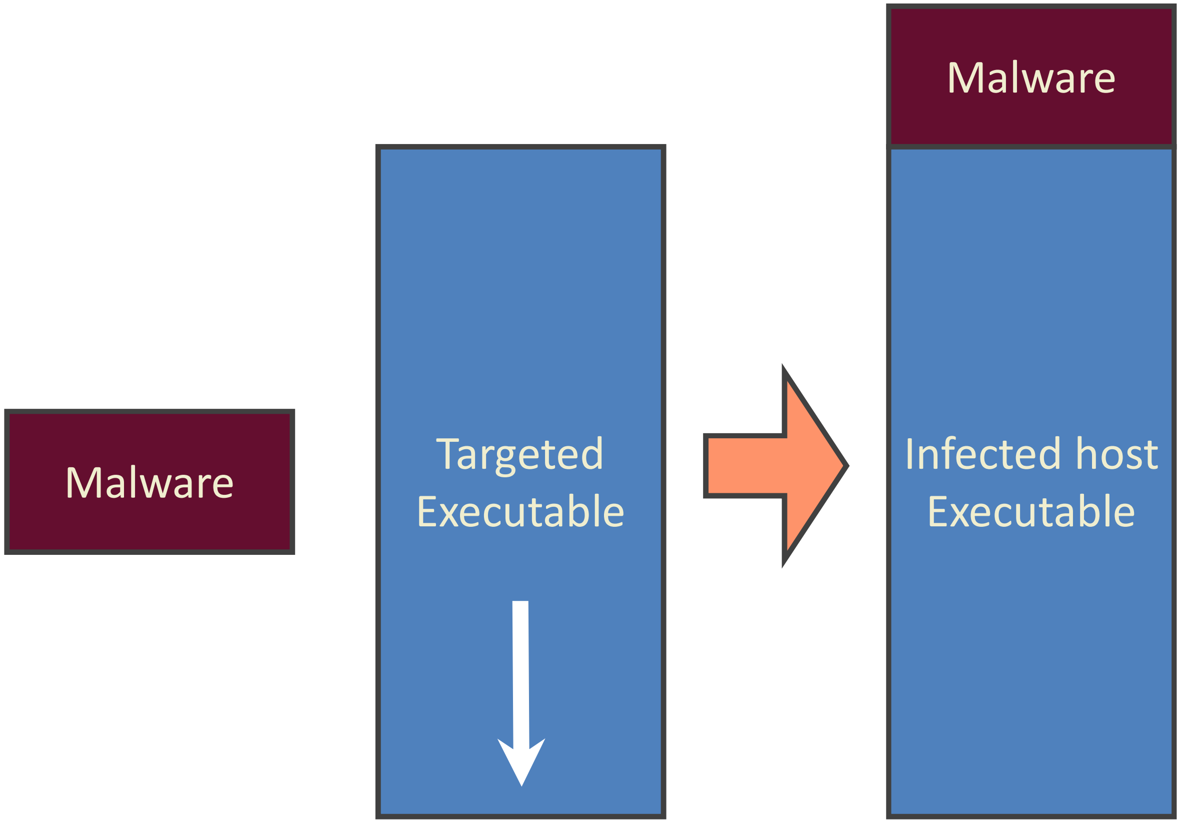
- Executable
- Interpreted file
- Kernel
- Service
- MBR (Master Boot Record)
- Hypervisor

Overwriting Malware

- After infection, it will effectively destroy the original program code by overwriting data in the system's memory.



Pre-pending Malware



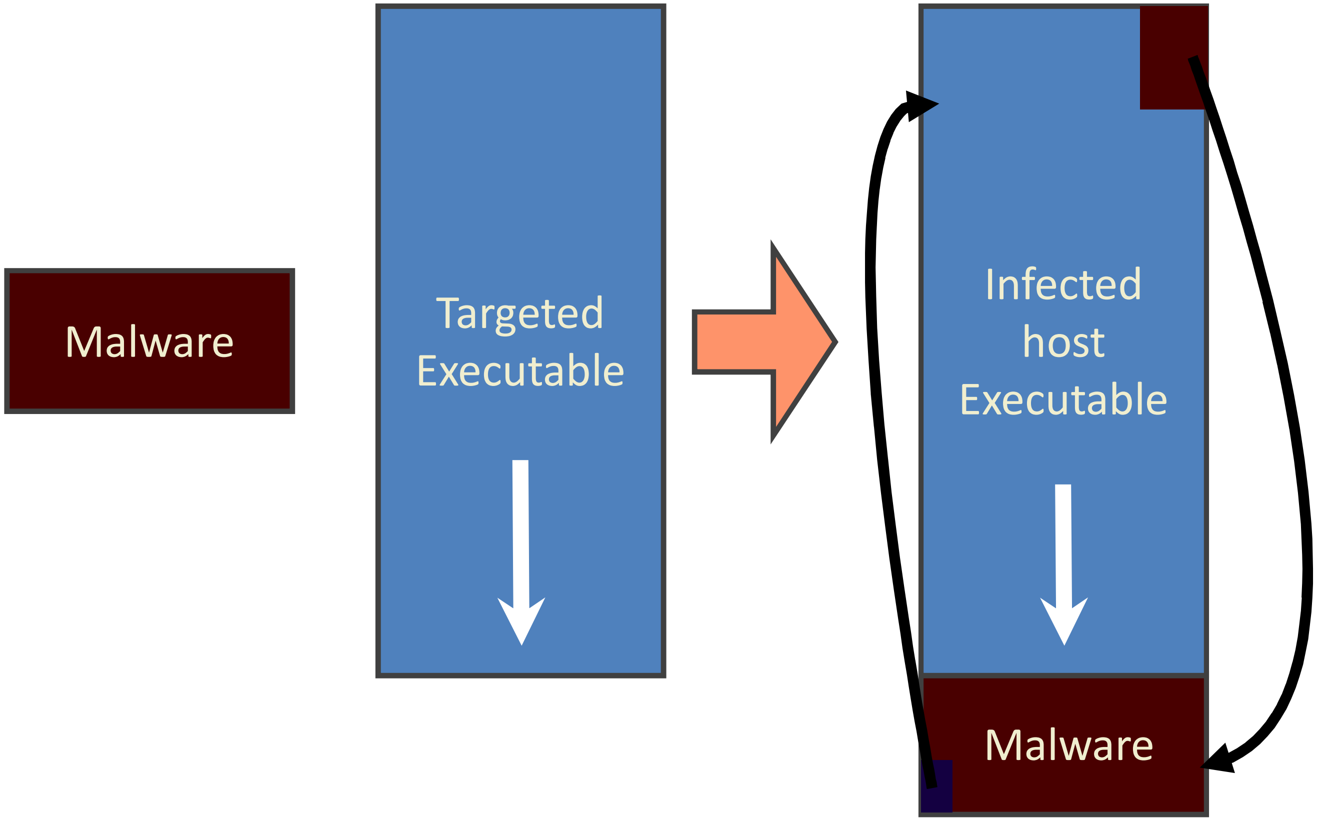
Malware

Targeted Executable

Malware

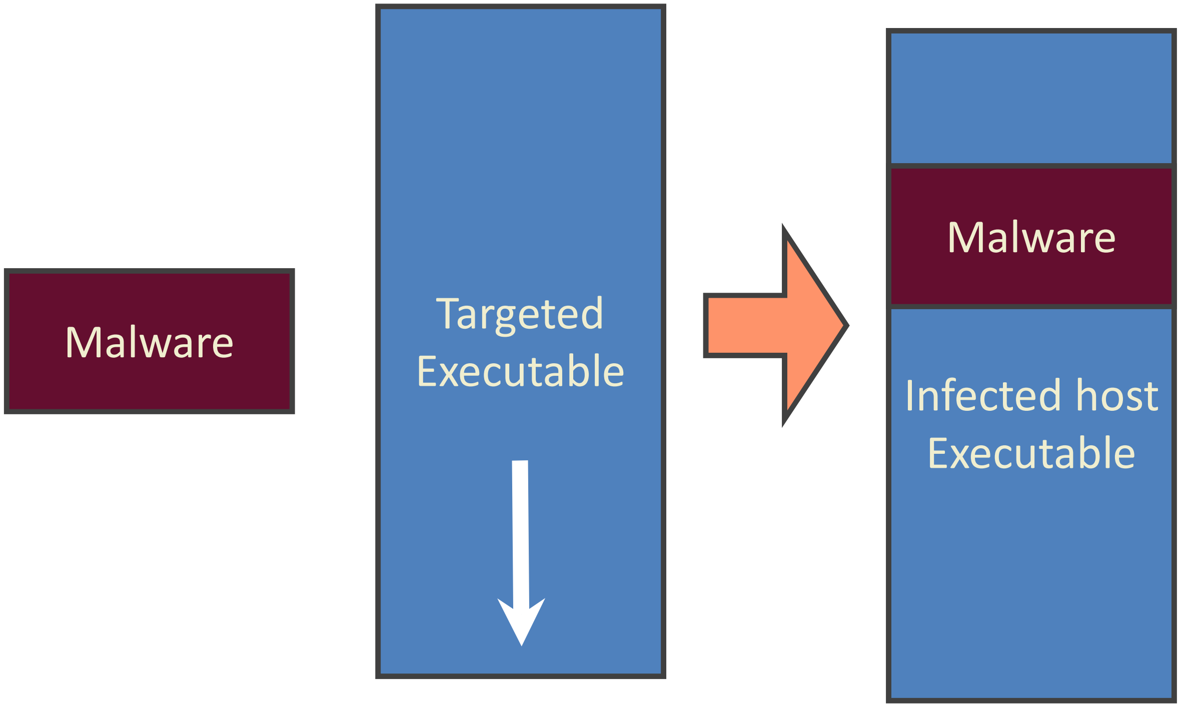
Infected host Executable

Appending Malware

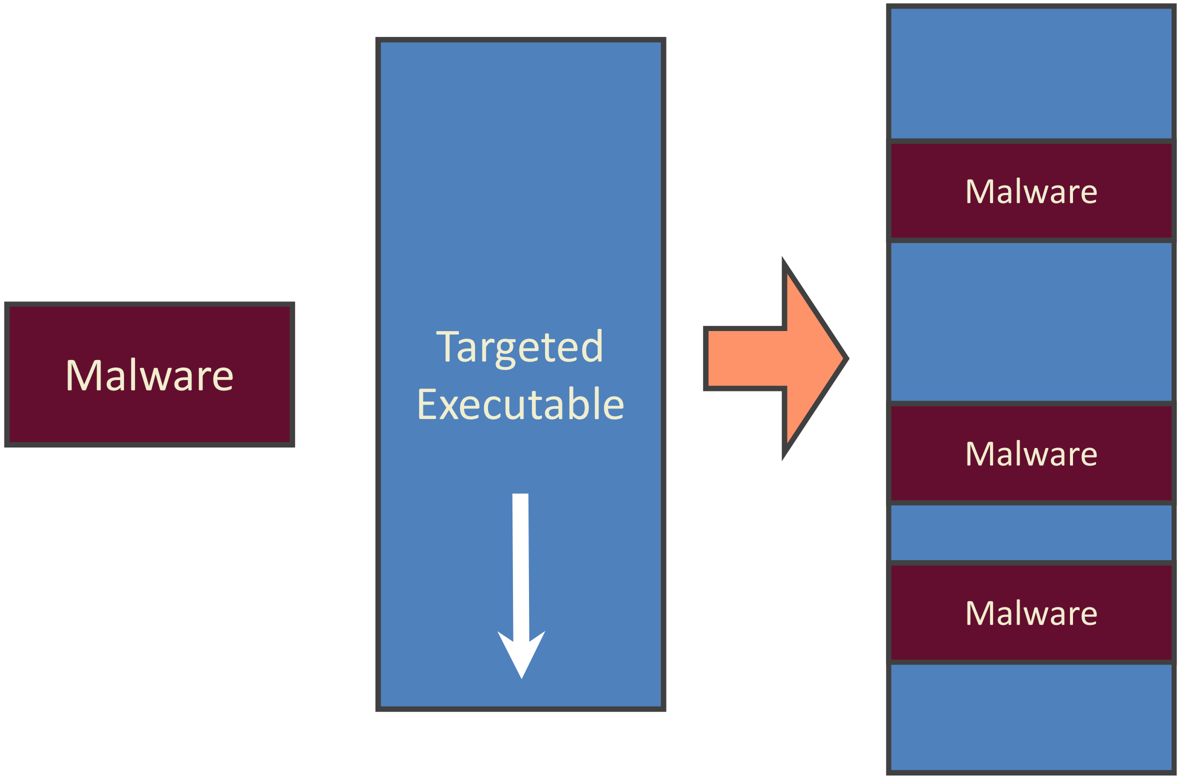


Cavity Malware

- Some malwares can infect files without increasing their sizes or damaging the files by overwriting unused areas of executable files. These are called cavity viruses.
- For example, the CIH virus, or Chernobyl Virus which infects Portable Executable files.



Multi-Cavity Malware



Malware Analysis

- Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware. (wikipedia)

- Three typical use cases
  - Computer Security incident management
  - Malware research
  - Indictor of compromise extraction

- Types
  - Static
  - Dynamic

Why analyze Malware?

- To assess damage
- To discover indicators of compromise
- To determine sophistication level of an intruder
- To identify a vulnerability
- To catch the “bad guy”
- To answer business related questions
  - How long has it been here, spreads on its own? Etc.
- To answer technical questions
  - Date of installation, compilation, persistence mechanism, network or host based indicators

1. Static Analysis

- Analysis in which code is not executed
- “Dead” code is read and understood
- Also referred to as: code analysis
- Requires peeking into the code using a hex editor, unpacking and performing string searches.
- Disassembling the malware. Disassemblers take machine code to higher-level code
  - IDA Pro
- Static analysis is safer
- Malware files are fingerprinted before analysis. Just in case malware analysis is being expected by the (malware) developer.
- Virus scan
  - PEiD, Caprica6 tool can tell you about “packed” code

2. Dynamic Analysis

- Conducted by observing and manipulating malware as it runs
- Needs a safe environment to analyze (run) the code
  - Sandboxed environment.
- Requires monitoring the system
  - Registry files activity
  - File and process/system level activity
  - Network level activity
- Some tools
  - Wireshark
  - SysInternals process monitor
  - Netstat or ResMon in Windows can be used
- Requires analysis while the code is being run using tools like WinDbg

Static vs Dynamic Analysis

- Static: Dissecting code via different resources without executing
- Dynamic: Behavioral analysis is performed by executing the malware.
- Static is much slower (and exhaustive at times) as compared to dynamic.
- Static is far safer than dynamic.
- Static doesn’t (necessarily) need a sandboxed environment while dynamic does.

Malware defenses (1)

- Detection: once the infection has occurred, determine that it has occurred and locate the malware

- Identification: once detection has been achieved, identify the specific malware that has infected a program

- Removal: once the specific malware has been identified, remove the malware from the infected program and restore it to its original state

Malware defenses (2)

- The first generation scanner
  - Malware signature (bit pattern)
  - Maintains a record of the length of programs
- The second generation scanner
  - Looks for fragments of code (neglect unnecessary code)
  - Checksum of files (integrity checking)
- The third generation scanner
  - Identify a malware by its actions
- The fourth generation scanner
  - Include a variety of anti-malware techniques

Malware defenses (3)

- Malware-specific detection algorithm
    - Deciphering
    - Filtering
- Collection method
    - Using honeypots
- Analyze program behavior
    - Network access
    - File open
    - Attempt to delete file
    - Attempt to modify the boot sector

How to prevent them?

- Simple! Learn about security (Not so simple)
- Use a secure Operating systems
- Use secure browsers and plugins/extensions
- And update/patch regularly
- Install anti-virus (maybe?)
- Avoid torrents
- Surf secure websites
- Don’t download what you don’t understand/need
- Use Instant Messaging apps carefully
- Keep backups

How to prevent them?

- Don’t install software that you don’t need or remove after one time use(worms!).
- Install software carefully. Unnecessary bundles gets installed
- Open email attachments with caution
- Monitor the performance of your pc regularly
- Keep frequent restore points and restore your pc if you think you executed a virus/worm/trojan
- Avoid unlicensed software installation
- Layers of authorization for installation of new tools/software

How to prevent them?

Two layers:

- Personal vigilance (First layer)
  - Knowing what to do and what to install
  - Understanding of the system and security
  - Strong passwords (password checkers)

- Protective tools (Second layer)
  - Effective and enough prevention tools
  - They are never enough