Malicious Software
Group: 5

Infomation
Security

Abdul Aziz (18701032)

Mohsin Hossain (18701057)

Rofiqul Islam (17701101)

Md.Akram Hossain (18701071)

Badhan (18701038)

Md. Abdulla Al Mottalib Ashraf (17701095)

Md. Hasin Arman (18701070)

Muhammad Amjad Hossain Surat(18701062)

August 11,2022

OUTLINE

- Defining malware
- Viruses and worms
- Virus anti detection and worm-spreading techniques
- Stealth: Trojan Horses, Backdoors, Key loggers and Rootkits
- Rootkit details: installation, object modification, hijacking
- Ransomware, botnets and other beasts
- Social engineering and categorizing malware

DEFINING MALWARE

- What is malware?
- How does malware get into devices?
- What makes malware hard to detect?
- How installation of malware be prevented?

VIRUS AND WORMS

- **Virus**
  - A virus is a malicious executable code attached to another executable file that can be harmless or can modify or delete data.
  - The main objective of viruses is to modify the information.
  - Antivirus software is used for protection against viruses.
  - Viruses generally comes from the shared or downloaded files.
  - It needs human action to replicate. Its spreading speed is slower as compared to worms.
- **Worms**
  - Worms are similar to a virus but it does not modify the program.
  - It replicates itself more and more to cause slow down the computer system. Worms can be controlled by remote.
  - The main objective of worms is to eat the system resources.
  - Worms generally comes from the downloaded files or through network connection

VIRUS ANTI DETECTION

1. Virus with encrypted body

- Uses fixed mapping(X-OR with fixed string)
- The decryption key is changed for each new infection

2. Polymorphic Virus

- Self encrypting virus, a mutation engine generates random decryption routine
- Decryption routine is varies from infection to infection

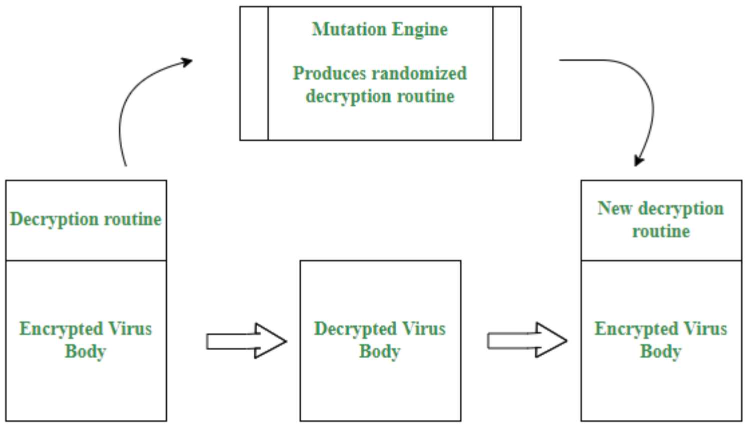
3. Metamorphic virus

- Use no encryption
- Per infection virus rewrite its own code
- Mutation both body and mutation engine, body polymorphic

4. Virus with external decryption key

- The decryption key is stored external to the virus itself

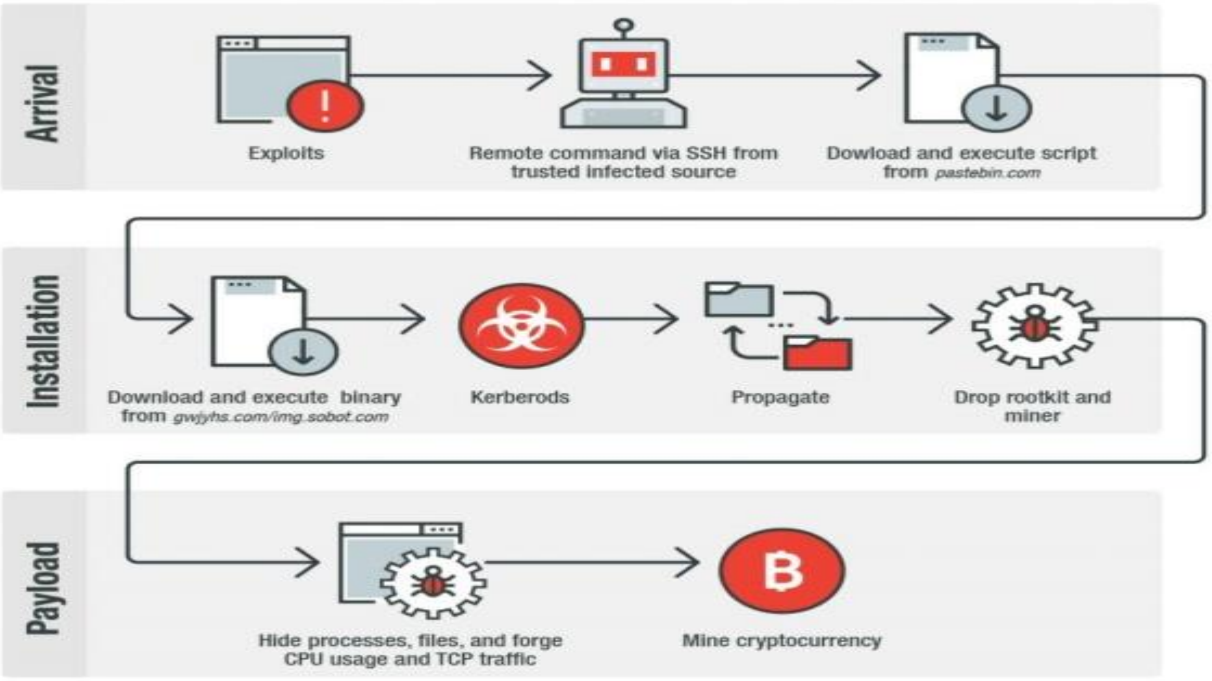
Working of Polymorphic Virus:

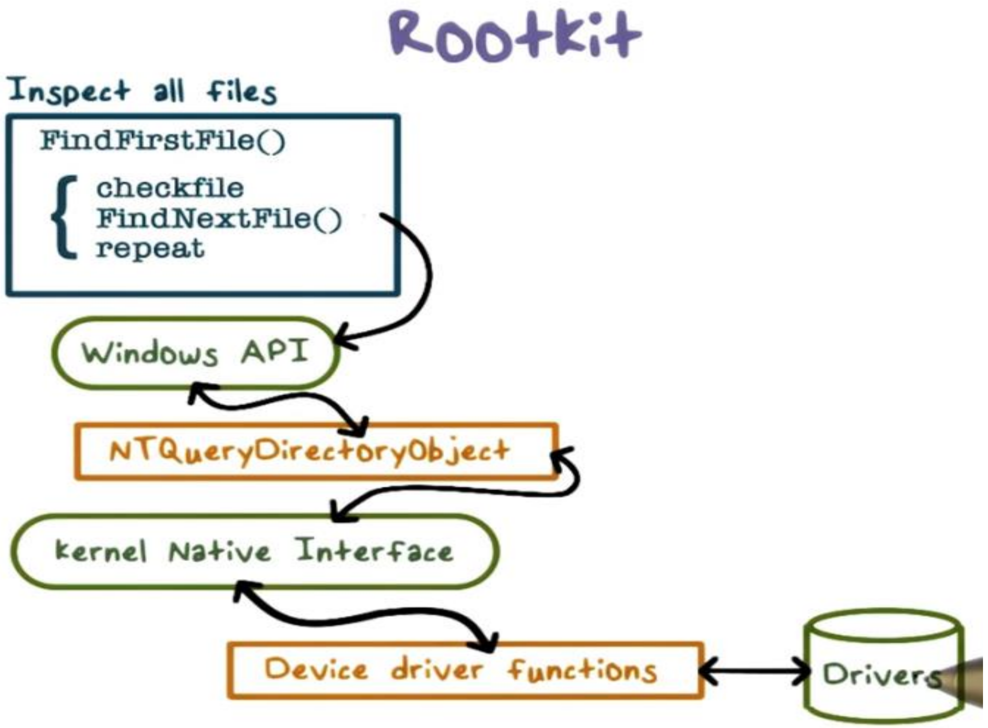


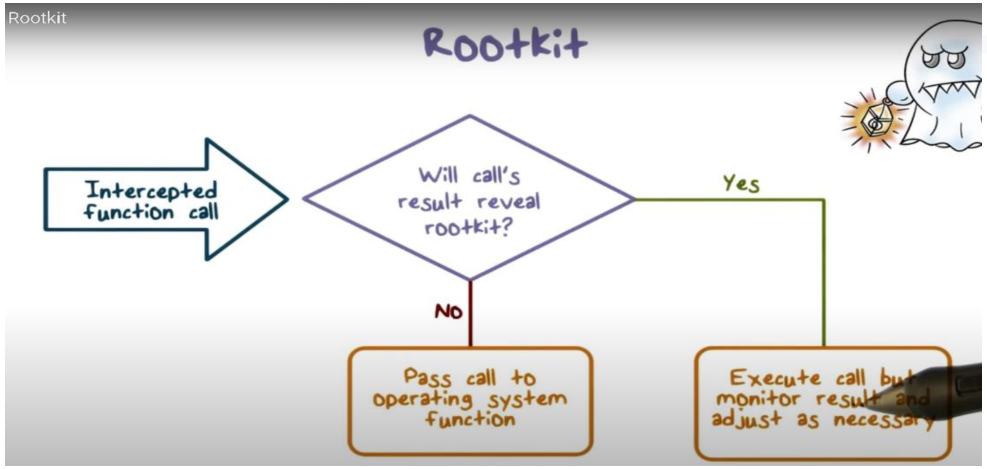
STEALTHY OF TROJAN HORSE,BACKDOOR,KEYLOGGERS AND ROOTKITS

- **Trojan Horse**
  - History of Greek mythology and troy city war.
  - type of malware that downloads onto a computer disguised as a legitimate program
  - Embedded to other software like as games software, emails and web sites link etc.
  - Surveillance to the computer and send the data continuously into the hacker
  - Trojan scanner or malware detection software
- **Backdoor Virus**
  - Malware to specify allow of unauthorized user to bypass security such username and password
  - Hidden entrance door into application, network or computer
  - Attacker can access after removing the virus or malware
  - Strong password, anti-malware virus and firewalls
- **Key loggers**
  - Malicious form of software that secretly install, tracks your own keyboard and send sensitive information to the hacker
  - Download or install when visiting sites
  - Antivirus, virtual keyboards ,firewalls and 2 factor authentication
- **Rootkits**
  - Collection of malicious software enables root access of os and install special program of hackers
  - Administration access. Create ,delete or modify the file
  - Bios program can be infected
  - Anti-virus , malware removal software etc

ROOTKIT ARRIVAL, INSTALLATION AND PAYLOAD


Arrival
Exploits
Remote command via SSH from trusted infected source
Dowload and execute script from pastebin.com
Installation
Download and execute binary from gwjyhs.com/img.sobot.com
Kerberods
Propagate
Drop rootkit and miner
Payload
Hide processes, files, and forge CPU usage and TCP traffic
Mine cryptocurrency



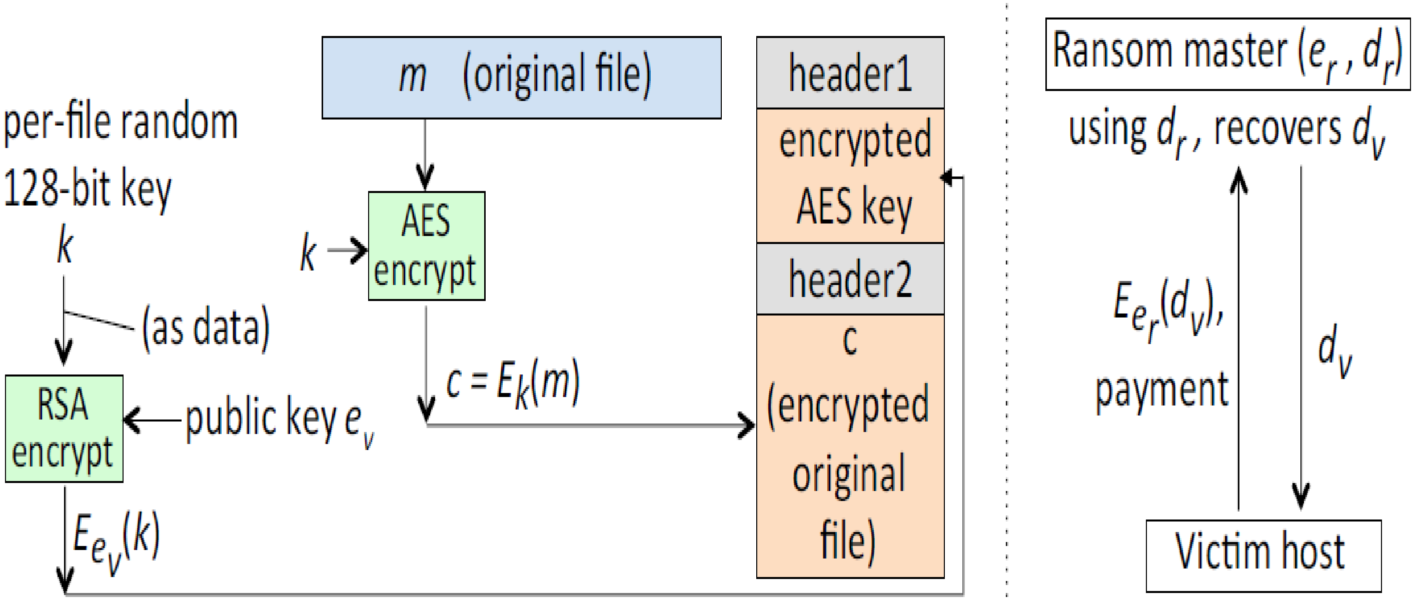

Rootkit
Rootkit
Intercepted function call
Will call's result reveal rootkit?
Yes
No
Pass call to operating system function
Execute call but monitor result and adjust as necessary

RANSOMWARE, BOTNETS AND ZOMBIES.

- Ransomware
  - ✓ Crypto
  - ✓ Locker
- Botnet
  - ✓ Shellcode
  - ✓ Bot and Botnet
- Logic Bomb

Ransomware master public key e_r used to encrypt d_v to $E_{e_r}(d_v)$

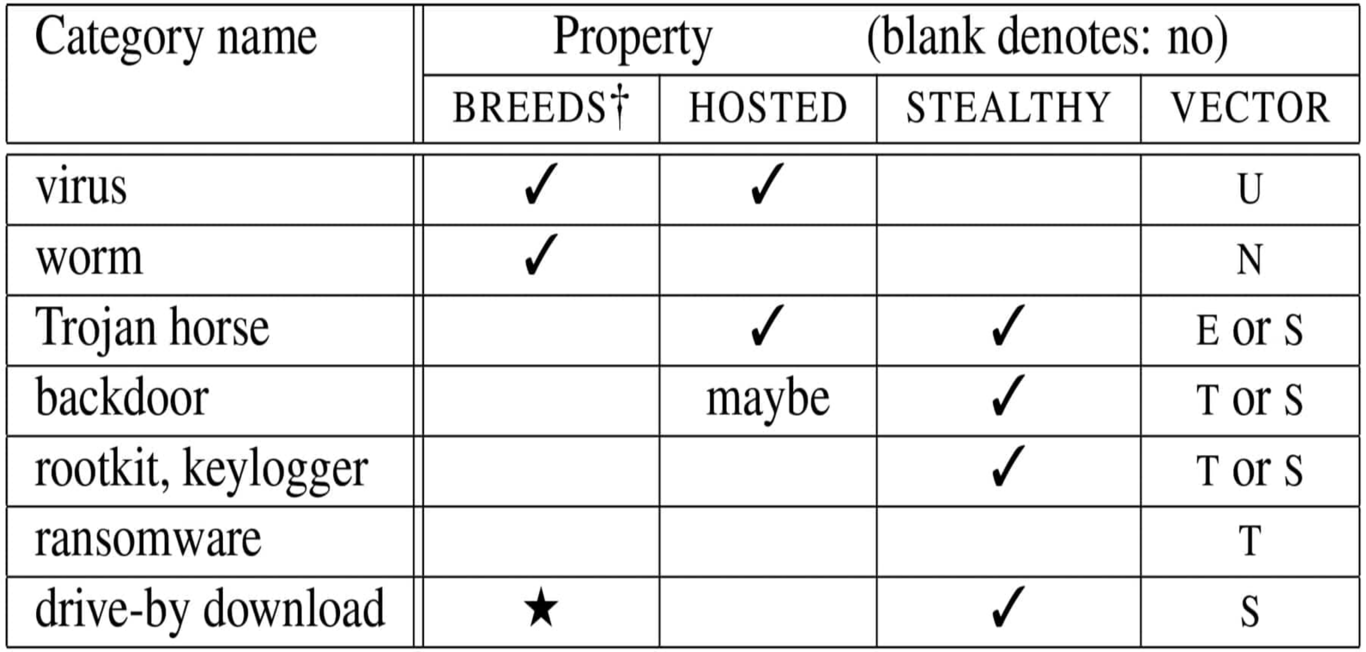
Per-victim (public, private) key pair (e_v , d_v) generated on victim host



SOCIAL ENGINEERING AND CATEGORIZING MALWARE

- Social Engineering Attacks may trick users into one-step download, installation and execution of malware
- **MALWARE CLASSIFICATION BY OBJECTIVE**
  - Image to host and its data.
  - Data theft.
  - Direct financial gain.
  - Ongoing surveillance.
  - Spread of malwares
  - Control of resources

Rahim.jpg.exe



Category name	Property		(blank denotes: no)	
	BREEDS†	HOSTED	STEALTHY	VECTOR
virus	✓	✓		U
worm	✓			N
Trojan horse		✓	✓	E or S
backdoor		maybe	✓	T or S
rootkit, keylogger			✓	T or S
ransomware				T
drive-by download	★		✓	S

- **MALWARE CLASSIFICATION BY TECHNICAL PROPERTIES**
  - Does it breed (self-replicate)?
  - Does it require a host program, as a parasite does?
  - Is it covert (stealthy), taking measures to evade detection and hide its functionality?
  - By what vector does infection occur?
  - Automatically over networks or with user help?
  - If the latter, does it involve social engineering to persuade users to take an action triggering installation (even if as simple as a mouse click on some user interfaces)? Does it enlist the aid of an insider (with privileges beyond that of an external party)?
  - Is it transient (e.g., active content in HTML pages) or persistent (e.g., on startup)?

Thank you