İTÜ
Computer Security

Malicious Software (Malware)

Dr. Şerif Bahtiyar

1

Before Starting

US says hackers attacked defense organization, stole sensitive info

https://www.defensenews.com/cyber/2022/10/05/us-says-hackers-attacked-defense-organization-stole-sensitive-info/

2

Before Starting

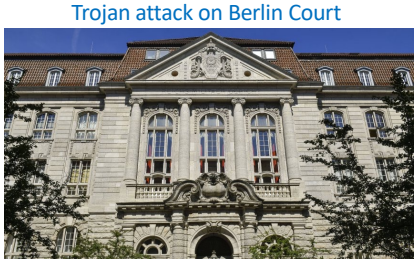
Chinese smartphones mount massive web attack

http://www.bbc.com/news/technology-34379254

3

Before Starting

Trojan attack on Berlin Court



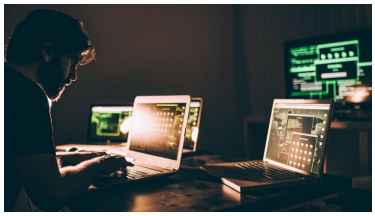
The Berlin Court of Appeal is currently harder to reach for citizens than usual: The employees are struggling with the consequences of a malware infection.

https://www.spiegel.de/netzwelt/web/emotet-berliner-kammergericht-wird-opfer-einer-trojaner-attacke-a-1289919.html

4

Before Starting

Brezilya'nın avcı bankacılık yazılımı dünyaya yayılıyor



https://www.hurriyet.com.tr/teknoloji/brezilyanin-avci-bankacilik-yazilimi-dunyaya-yayiliyor-41658895

5

Outline

- Introduction to Malicious Software
- Advanced Persistent Threat
- Propagation
- Payload
- Countermeasures

6

Introduction to Malicious Software

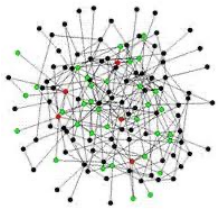
Malicious Software (Malware): A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

7

Introduction to Malicious Software

Propagation (spread)

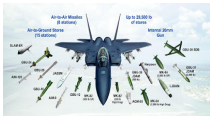
- Propagation mechanisms include infection of existing executable that is subsequently spread to other systems
- Exploit of software vulnerabilities by worms to allow malware to replicate
- Virus, worm, spam, …



8

Introduction to Malicious Software

- Payload (action): Payload of malware performs actions once it reaches a target system.
  - Corruption of system or data files
  - Theft of service in order to make the system a zombie agent of attack as part of a botnet
  - Zombie, bot, keylogger,…



- A blended attack uses multiple methods of infection or propagation, to maximize the speed of contagion and the severity of the attack.

9

Introduction to Malicious Software

- Brief History of Attack Kits
  - Before 1990 : the development and deployment of malware required considerable technical skill
  - 1990-2000: virus creation toolkits
  - 2000-now: more general attack kits

- Crimeware
  - Attack kits that include a variety of propagation mechanisms and payload modules that even novices can combine, select, and deploy. *Zeus, Sakura, Blackhole, and Phoenix are some crimeware toolkits.*
- Attack sources
  - Changes from being individuals to more organized attack sources, such as politically motivated attackers.

10

Advanced Persistent Threat (APT)

- APT is not a new type of malware.
- APT is well-resourced persistent application:
  - Uses many intrusion technologies
  - Many malware
- Usually targets are business and political
- Typically created and used
  - state-sponsored organizations
  - some criminal enterprises
- Stuxnet, Aurora, Duqu,…

11

Advanced Persistent Threat

Differences of Attacks with APT

- Careful target selection
- Persistent
- Often stealthy
- Intrusion efforts over extended periods

12

Advanced Persistent Threat

Characteristics of APT

- Advanced: malware may not necessary advanced, but are carefully selected to compromise the target.
- Persistent: maximize the chance of attack over an extended period.
- Threats: active involvement of people and automated attack tools to maximize the likelihood of successful attack.

13

Propagation

14

Propagation (Infected Content - Viruses)

- A computer virus is a piece of software that can infect other programs, or intended type of executable content, by modifying them.
  - First appear in early 1980s
  - Brian virus seen in 1986 was the first to target MSDOS and resulted in a significant number of infections.

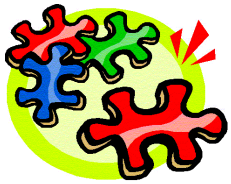
- Viruses dominated the malware scene in earlier years because there was a lack of user authentication and access controls on personnel computer systems at that time.

15

Propagation (Infected Content - Viruses)

A virus has three components (parts)

- Infection mechanism (also known as infection vector)
- Trigger (sometime known as logic bomb)
- Payload (what the virus does)

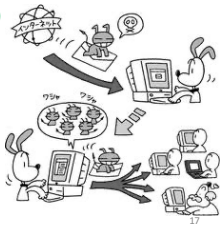


16

Propagation (Infected Content - Viruses)

Phases of virus during lifetime (4 phases)

- Dormant phase (virus is idle) [Not all viruses have this phase!]
- Propagation phase (copy itself into other programs)
- Triggering phase (virus is activated)
- Execution phase (function is performed)



17

Propagation (Infected Content - Viruses)

```
        program V :=
{goto main;
        1234567;
        subroutine infect-executable :=
                {loop:
                file := get-random-executable-file;
                if (first-line-of-file = 1234567)
                        then goto loop
                        else prepend V to file; }
        subroutine do-damage :=
                {whatever damage is to be done}
        subroutine trigger-pulled :=
                {return true if some condition holds}
main:           main-program :=
                {infect-executable;
                if trigger-pulled then do-damage;
                goto next;}
next:
}
```

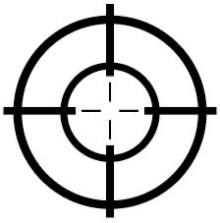
Source: COMPUTER SECURITY PRINCIPLES AND PRACTICE, 2nd Edition, William Stallings and Lawrie Brown

18

Propagation (Infected Content - Viruses)

Virus Classification by Target

- Boot sector infector
- File infector
- Macro virus
- Multipartite virus



There is no single agreed-classification!

19

Propagation (Infected Content - Viruses)

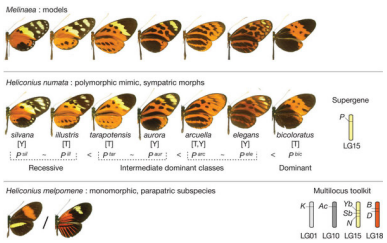
Virus Classification by Concealment

- Encrypted
- Stealth
- Polymorphic
- Metamorphic

20

Propagation (Infected Content - Viruses)

A polymorphic virus creates copies during replication that are functionally equivalent but have distinctly (not fully) different bit patterns.



21

Propagation (Infected Content - Viruses)

- Generating keys and performing encryption / decryption is referred to as the mutation engine.
- The difference between polymorphic and metamorphic viruses is that a metamorphic virus rewrites itself completely at each iteration and may change its behavior as well as its appearance.

22

Propagation (Vulnerability Exploit - Worms)

A worm is a program that actively seeks out more machines to infect, and then each infected machine serves as an automated launching pad for attacks on other machines.

23

Propagation (Vulnerability Exploit - Worms)

- Worm programs exploit software vulnerabilities in client or server programs to gain access .

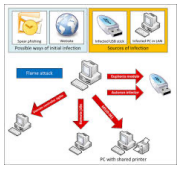
Heartbleed *is a security bug disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited regardless of whether the party using a vulnerable OpenSSL instance for TLS is a server or a client.*

- The first know worm implementation was done in Xerox Palo Alto Labs in early 1980s. It was nonmalicious, searching for idle systems to use to run a computationally intensive task.

24

Propagation (Vulnerability Exploit - Worms)

- A worm may use some of the following ways to access remote systems (propagation ways):
  - Electronic mail or instant messenger facility
  - File sharing
  - Remote execution capability
  - Remote file access or transfer capability
  - Remote login capability



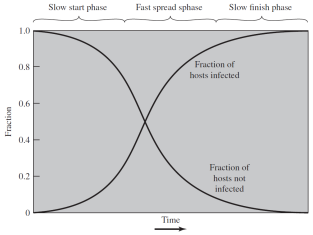
- A worm typically uses the same phases as a computer virus.

25

Propagation (Vulnerability Exploit - Worms)

The classic epidemic models for understanding computer virus and worm propagation behavior.

$$\frac{dI(t)}{dt} = \beta I(t)\, S(t)$$



$I(t)$ = number of individuals infected as of time t
$S(t)$ = number of susceptible individuals (susceptible to infection but not yet infected) at time t
β = infection rate
N = size of the population, $N = I(t) + S(t)$

26

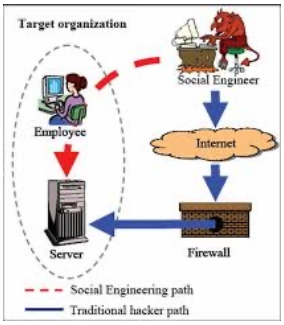
Propagation (Vulnerability Exploit - Worms)

- There are claims that Stuxnet appears to be the first serious use of a cyberwarfare weapon against a nation's physical infrastructure.
- The state of the art in worm technology:
  - Multiplatform
  - Multi-exploit
  - Ultrafast spreading
  - Polymorphic
  - Metamorphic
  - Transport vehicles
  - Zero-day exploit

27

Propagation (Social Engineering – Spam e-mail, Trojans)

Social engineering: Tricking users to assist in the compromise of their own systems or personnel information.



28

Propagation (Social Engineering – Spam e-mail, Trojans)

- Spam: Unsolicited bulk e-mail
- While some spam is sent from legitimate mail servers, most recent spam is sent by botnets using compromised user systems.
  - Advertisement
  - Significant malware carrier
  - Convince the recipient to purchase
  - Phishing attack
  - ….

29

Propagation (Social Engineering – Spam e-mail, Trojans)

- A Trojan horse is a useful, or apparently useful, program or utility containing hidden code that, when invoked, performs some unwanted or harmful function.

- Trojan horse programs can be used to accomplish functions indirectly that the attacker could not accomplish directly.

30

Propagation - Summary

- Infected Content
- Vulnerability Exploit
- Social Engineering

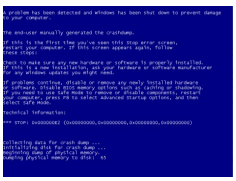
31

Payload

32

Payload (System Corruption)

- Once malware is active on the target system, the next concern is what actions it will take on this system. A payload does the action.
  - Data destruction
  - Physical damage



- All actions target the integrity of the computer system's software or hardware, or of the user's data.

33

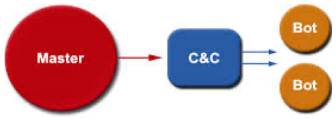
Payload (System Corruption)

- Ransomware encrypts the user's data, and demands payment in order to access the key needed to recover this information.
- CryptoLocker is a ransomware Trojan which targeted MS Windows platforms.
  - Propagated via email attachments and botnets.
  - Payload: encrypt certain types of files with RSA public-keys. Offers to decrypt data if a payment is made…

34

Payload (Attack Agent – Zombie, Bots)

- A bot (robot), zombie, or drone subverts the computational and network resources of the infected system for use by the attacker.

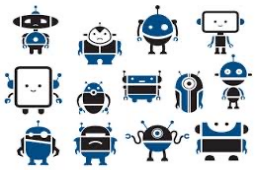


- The bot is typically planted on hundreds or thousands of computers belonging to unsuspecting third parties.

35

Payload (Attack Agent – Zombie, Bots)

- Some use of bots
  - Distributed denial-of-service attacks
  - Spamming
  - Sniffing traffic
  - Keylogging
  - Spreading malware

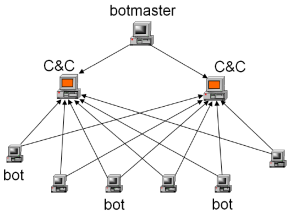


- This type of payload attacks the integrity and availability of the infected system.

36

Payload (Attack Agent – Zombie, Bots)

- Botnet: A collection of bots can act in a coordinated manner.



- Remote control facility: The remote control facility is what distinguishes a bot from a worm. A worm propagates itself and activates itself, whereas a bot is controlled from some central facility, at least initially.

37

Payload
Information Theft – Keyloggers, Phishing, Spyware

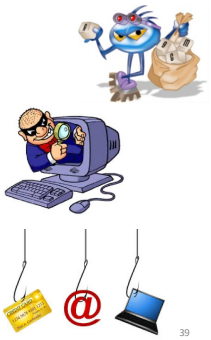
- Payloads where malware gathers data stored on the infected system for use by the attacker.

- These attacks target the confidentiality of information.

38

Payload
Information Theft – Keyloggers, Phishing, Spyware

- A keylogger captures keystrokes on the infected machine to allow an attacker to monitor the sensitive information.
- A spyware subverts the compromised machine to allow monitoring of a wide range of activity on the system.
- A phishing attack exploits social engineering to leverage user's trust by masquerading as communications from a trusted source.



39

Payload (Stealth – Backdoors, Rootkits)

- These payloads hide their presence on the infected system, and provide covert access to that system.
- Attacks the integrity of the infected system.
- A backdoor, also known as a trapdoor, is a secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures.

40

Payload (Stealth – Backdoors, Rootkits)

A rootkit is a set of programs installed on a system to maintain covert access to that system with administrator (or root) privileges, while hiding evidence of its presence to the greatest extend possible.

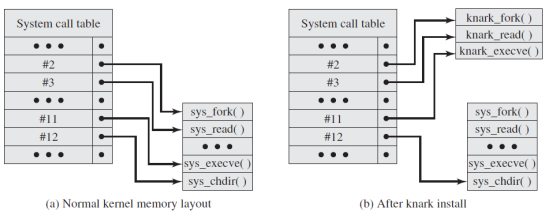


Figure 6.5 System Call Table Modification by Rootkit

41

Payload - Summary

- System corruption
- Attack agent
- Information theft
- Stealth

42

Countermeasures

- The ideal solution is prevention (nearly impossible to achieve).
- If prevention fails, following mitigation options can be used:
  - Detection
  - Identification
  - Removal

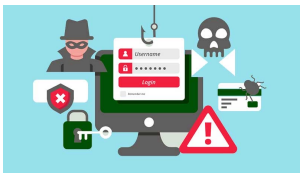
Generally known as anti-virus mechanisms

43

Countermeasures

Four main elements of prevention (NIST SP 800-83):

- Policy
- Awareness
- Vulnerability mitigation
- Threat mitigation



44

Countermeasures

Some requirements for effective malware countermeasures:

- Generality: Should be able to handle a wide variety of attacks.
- Timeliness: Respond quickly.
- Minimal denial-of service costs
- Transparency: Should not require modification to existing system.
- Global and local coverage: Deal with attack sources both from outside and inside of the enterprise network.

45

Countermeasures

- Host-based scanner: Used on each end system.
- Generations of anti-virus software:
  - 1st: simple scanners (requires malware signature to identify malware)
  - 2nd: heuristic scanners (looks for fragments of code, integrity check)
  - 3rd: activity traps (identify malware by its actions)
  - 4th: full-featured protection (uses a variety of anti-virus techniques)

- Generic decryption: Enables the anti-virus program to easily detect even the most complex polymorphic viruses and other malware, while maintaining fast scanning speeds.

46

Countermeasures

Host-based behavior (blocking software)

- It integrates the operating system of a host computer and monitors program behavior in real time for malicious actions.

- Advantage: it can detect modified malware in real time
- Disadvantage: it can cause harm before detection of malware

47

Countermeasures

Spyware detection and removal

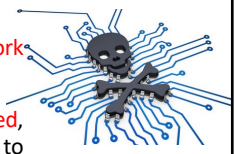
- Spyware uses stealthy techniques.
- The software specializes to remove such malware.
- Complement general anti-virus product.

48

Countermeasures

Rootkit countermeasures

- One of the most difficult malware types to detect, sometimes undetectable.
- Require a variety of host and network level security tools.
- If a kernel level rootkit is detected, the only secure and reliable way to recover is to do an entire new OS install on the infected machine.



49

Countermeasures

Perimeter scanning approaches

- Ingress monitors: monitor incoming traffic
- Egress monitors: monitor outgoing traffic

50

Countermeasures

Worm countermeasures

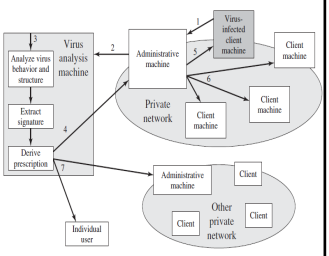
- Signature-based worm scan filtering (vulnerable to polymorphic worms)
- Filter-based worm containment (focus on content rather signature, requires efficient detection algorithms)
- Payload-classification-based worm containment (network-based methods, anomaly detection)
- Threshold random walk scan detection (effective against common behavior of worms, fast)
- Rate limiting (introduce longer delays, not suitable for slow and stealthy worms)
- Rate halting (immediately blocks outgoing traffic when a threshold is exceeded)

51

Countermeasures

Distributed Intelligence Gathering Approaches

- Gathers data from a large number of both host-based and perimeter sensors.
- Digital Immune System:
  Gathers intelligence from many sources, such as Symantec gathers information more than 133 million clients, servers, and gateways.



52

Summary

- Introduce malicious software (malware)
- Malware propagation mechanisms
- Basic operations of viruses, worms, and others
- Categories of malware payloads
- Bots, spyware, and rootkits
- Some malware countermeasures

53