İTÜ
Computer Security

Malicious Software (Malware)

Dr. Şerif Bahtiyar

bahtiyars@itu.edu.tr

Fall 2015

Before Starting

Home Depot: Malware hits 56 million payment cards

http://www.clickondetroit.com/consumer/home-depot-malware-hits-56-million-payment-cards/28138354

Before Starting

Medical devices vulnerable to hackers

http://www.bbc.com/news/technology-34390165

Before Starting

Chinese smartphones mount massive web attack

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

Outline

- Introduction to Malicious Software
- Propagation
- Payload
- Countermeasures

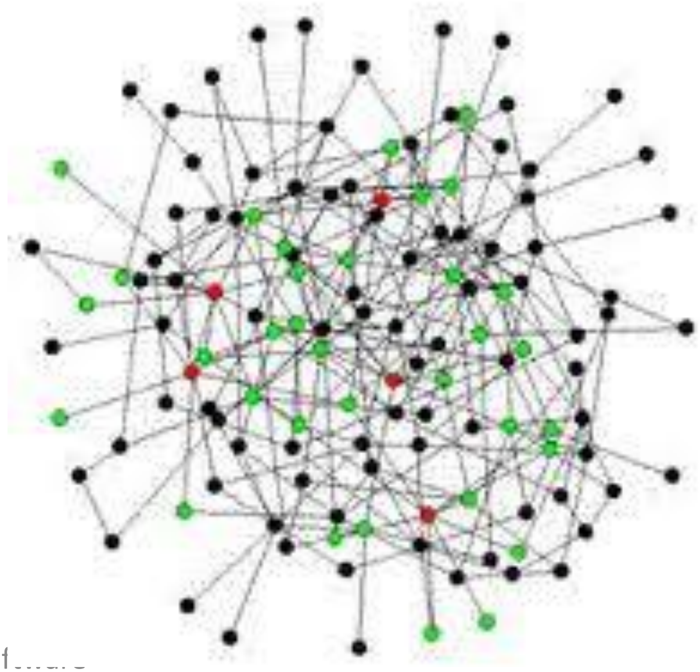
Introduction to Malicious Software

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.

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, …



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.

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 crimeware toolkit is a prominent example of such attack kit)
- Attack sources
  - Changes from being individuals to more organized attack sources, such as politically motivated attackers.

Propagation (Infected Content - Viruses)

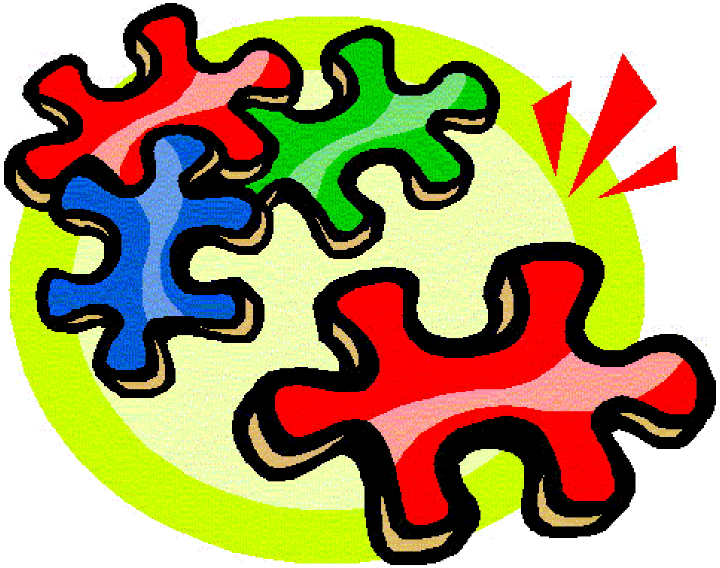
- A computer virus is a piece of software that can infect other programs, or intended type of executable content, by modifying them.
  - First appear in early 1980s
  - Brian virus seen in 1986 was the first to target MSDOS and resulted in a significant number of infections.

- 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.

Propagation (Infected Content - Viruses)

A virus has three components (parts)

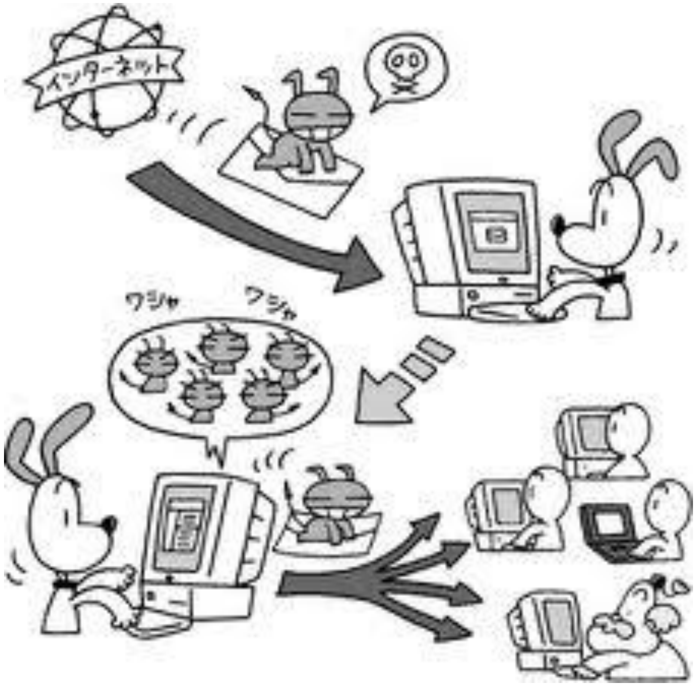
- Infection mechanism (also known as infection vector)
- Trigger (sometime known as logic bomb)
- Payload (what the virus does)



Propagation (Infected Content - Viruses)

Phases of virus during lifetime (4 phases)

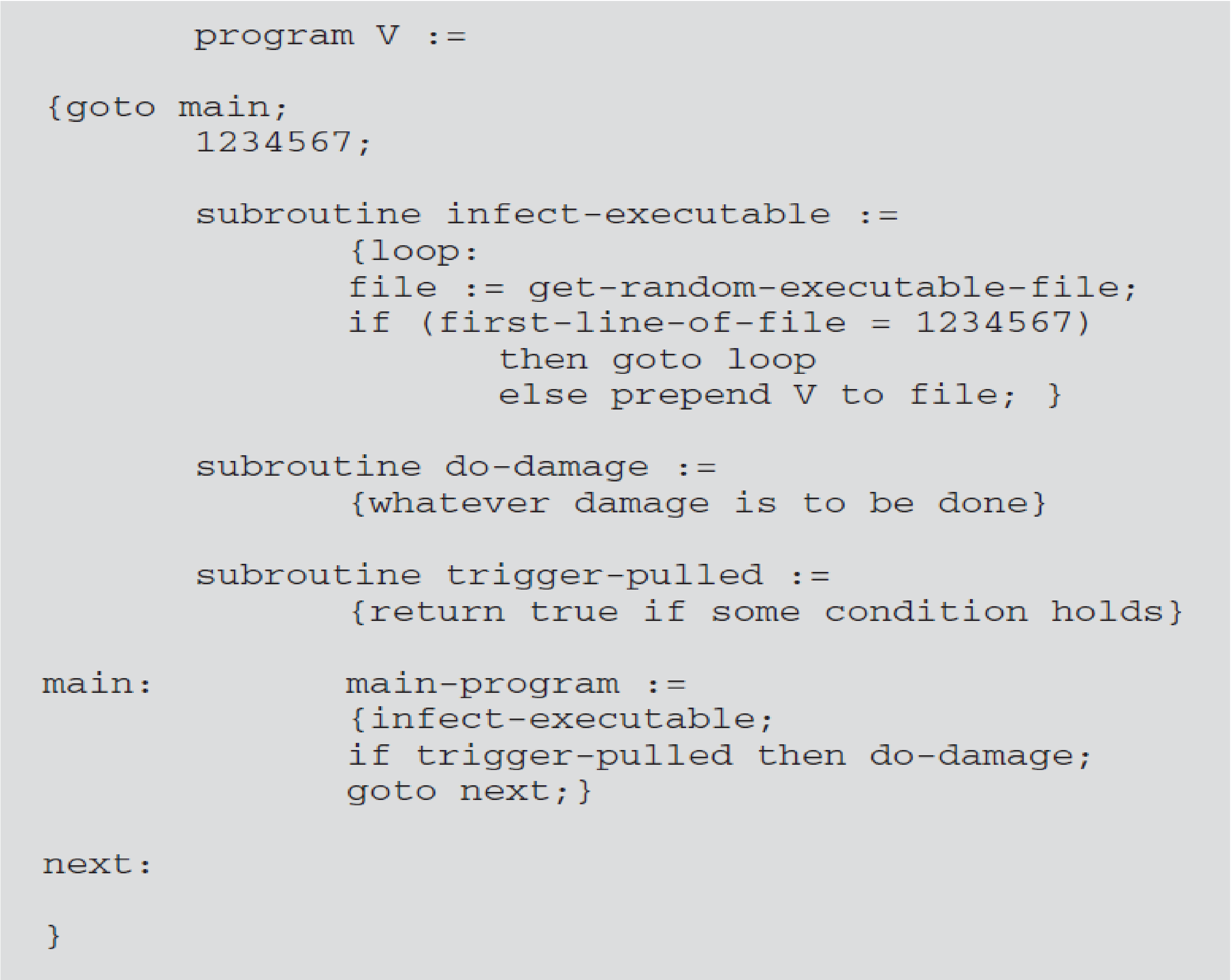
- Dormant phase (virus is idle)
- Propagation phase (copy itself into other programs)
- Triggering phase (virus is activated)
- Execution phase (function is performed)



Propagation (Infected Content - Viruses)

Code of virus

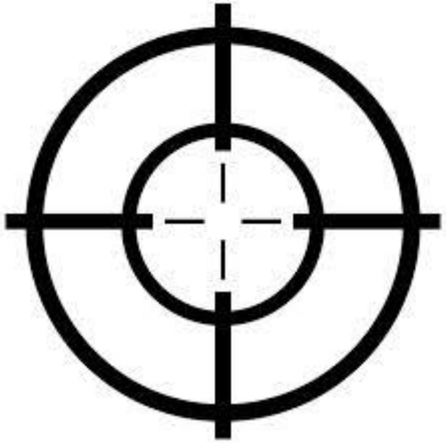
***Source**: COMPUTER SECURITY PRINCIPLES AND PRACTICE, 2nd Edition, William Stallings and Lawrie Brown*



```
      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:

}
```

Propagation (Infected Content - Viruses)

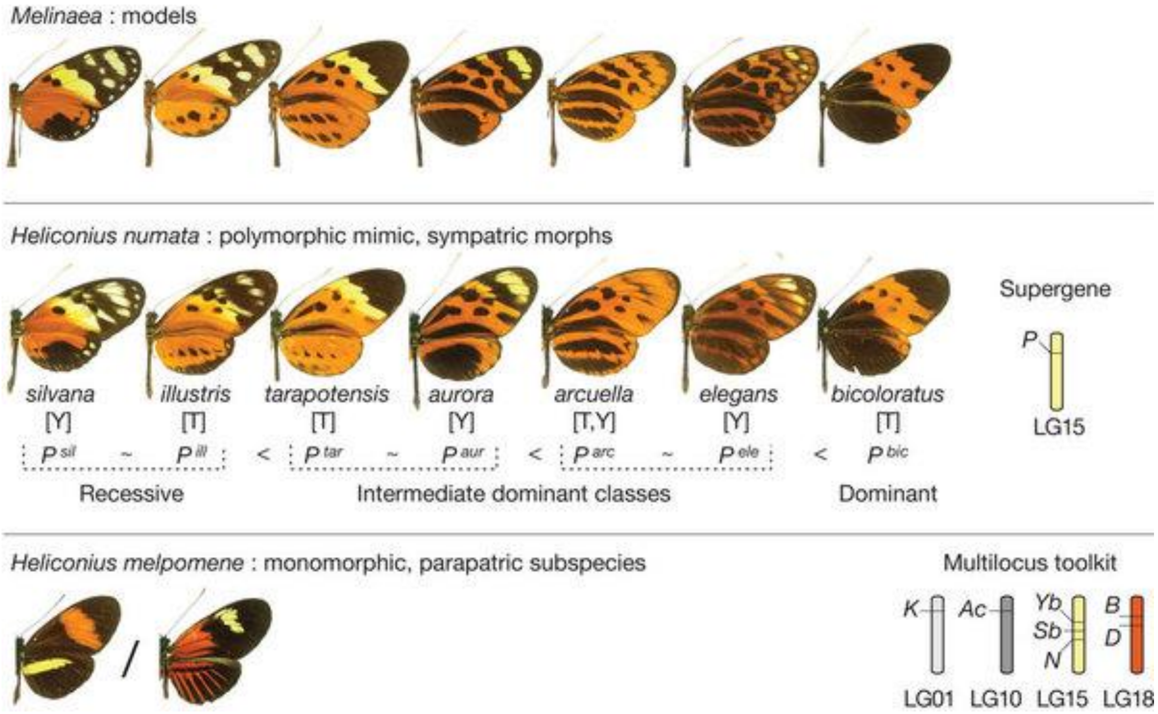
- Virus Classification by target
  - Boot sector infector
  - File infector
  - Macro virus
  - Multipartite virus



- Virus classification by concealment
  - Encrypted
  - Stealth
  - Polymorphic
  - Metamorphic

Propagation (Infected Content - Viruses)

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


Melinaea : models
Heliconius numata : polymorphic mimic, sympatric morphs
silvana
[Y]
illustris
[T]
tarapotensis
[T]
aurora
[Y]
arcuella
[T,Y]
elegans
[Y]
bicoloratus
[T]
P sil ~ P ill < P tar ~ P aur < P arc ~ P ele < P bic
Recessive
Intermediate dominant classes
Dominant
Supergene
P
LG15
Heliconius melpomene : monomorphic, parapatric subspecies
Multilocus toolkit
K
Ac
Yb
Sb
N
B
D
LG01
LG10
LG15
LG18

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 changes its behavior as well as its appearance.

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.

Propagation (Vulnerability Exploit - Worms)

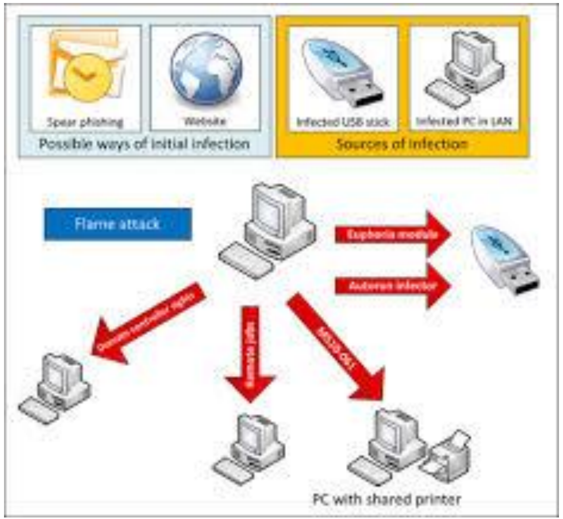
- Worm programs exploit software vulnerabilities in client or server programs to gain access .

***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.

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.

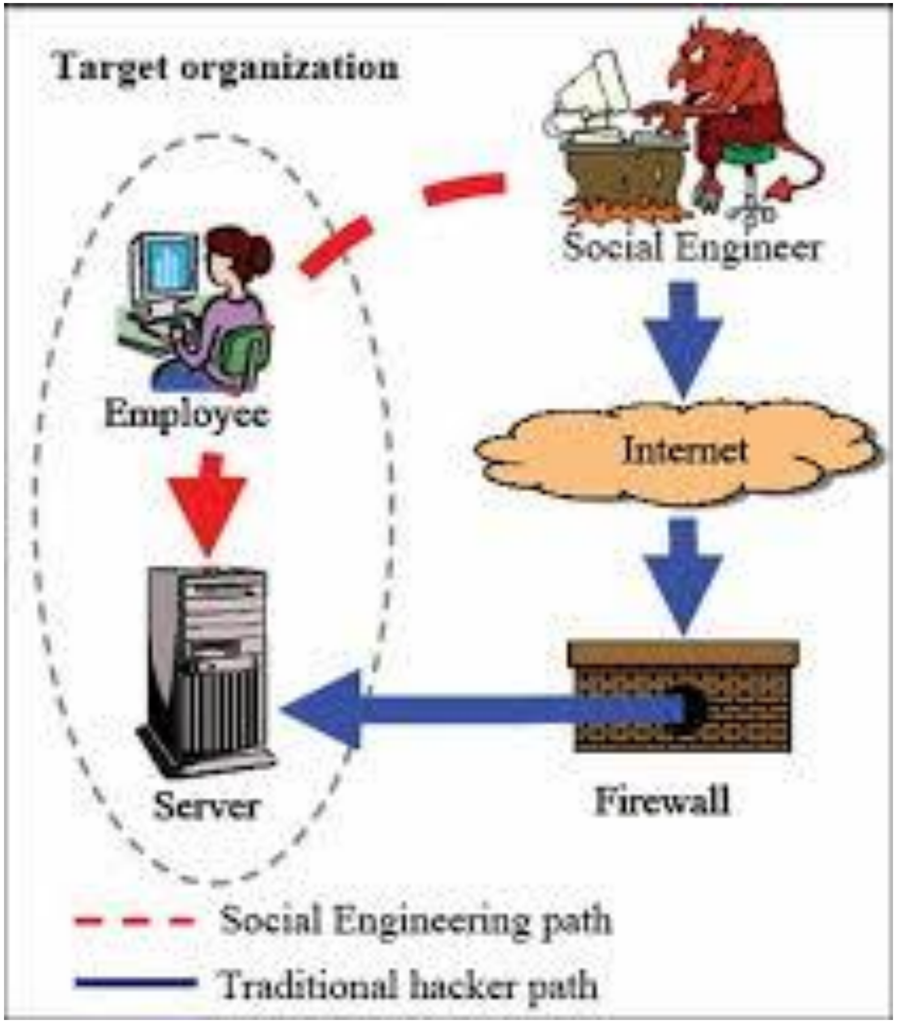
Propagation (Vulnerability Exploit - Worms)

- 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

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

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



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
  - ….

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.

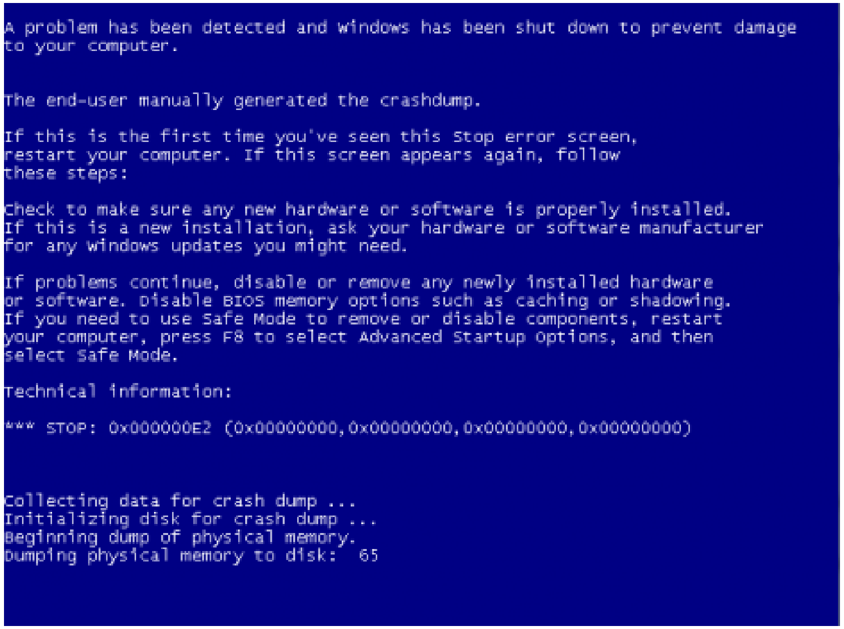
- Trojan horse programs can be used to accomplish functions indirectly that the attacker could not accomplish directly.

Propagation - Summary

- Infected Content
- Vulnerability Exploit
- Social Engineering

Payload (System Corruption)

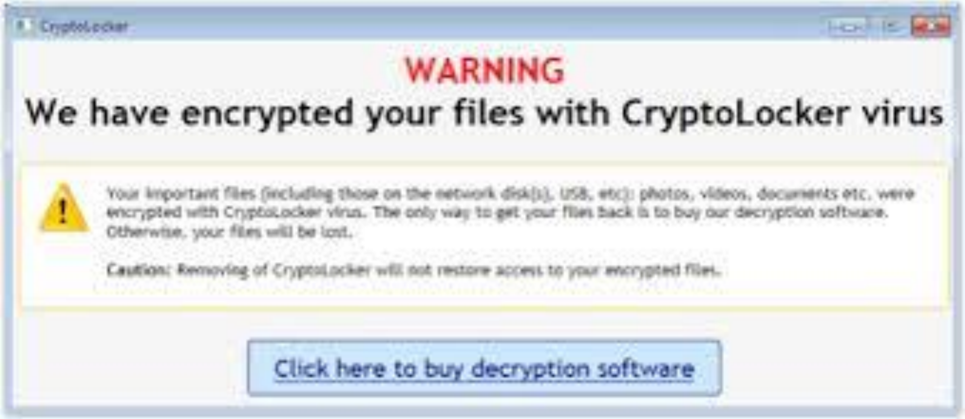
- Once malware is active on the target system, the next concern is what actions it will take on this system. A payload does the action.
  - Data destruction
  - Physical damage
- All actions target the integrity of the computer system's software or hardware, or of the user's data.
- Ransomware encrypts the user's data, and demands payment in order to access the key needed to recover this information.



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.


The end-user manually generated the crashdump.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x00000000,0x00000000,0x00000000,0x00000000)



Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  65
```

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…



WARNING

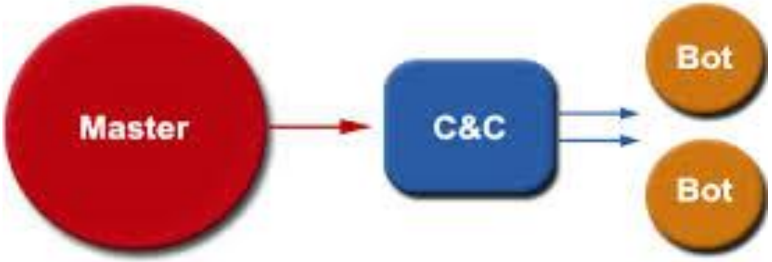
We have encrypted your files with CryptoLocker virus

Your important files (including those on the network disk(s), USB, etc): photos, videos, documents etc. were encrypted with CryptoLocker virus. The only way to get your files back is to buy our decryption software. Otherwise, your files will be lost.

Caution: Removing of CryptoLocker will not restore access to your encrypted files.

Payload (Attack Agent – Zombie, Bots)

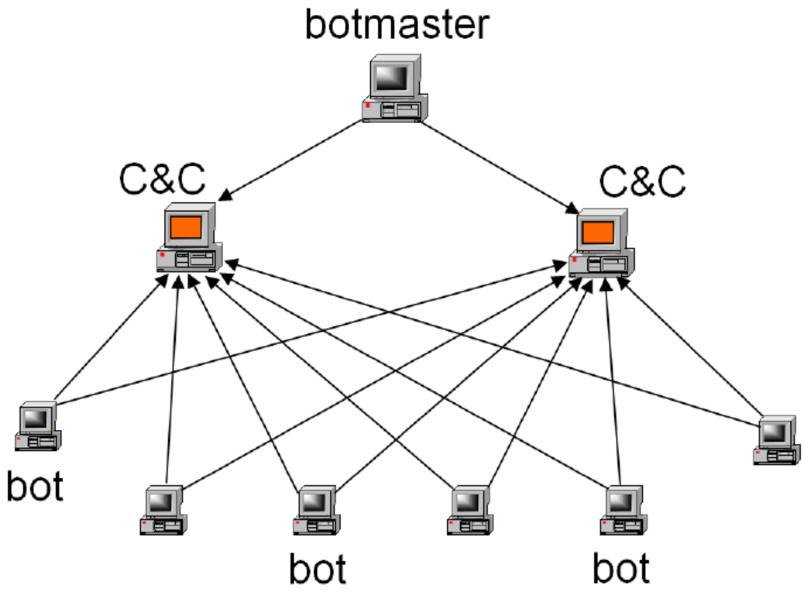
- A bot (robot), zombie, or drone subverts the computational and network resources of the infected system for use by the attacker.
- The bot is typically planted on hundreds or thousands of computers belonging to unsuspecting third parties.
- Some use of bots
  - Distributed denial-of-service attacks
  - Spamming
  - Sniffing traffic
  - Keylogging
  - Spreading malware



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

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.

Payload
Information Theft – Keyloggers, Phishing, Spyware

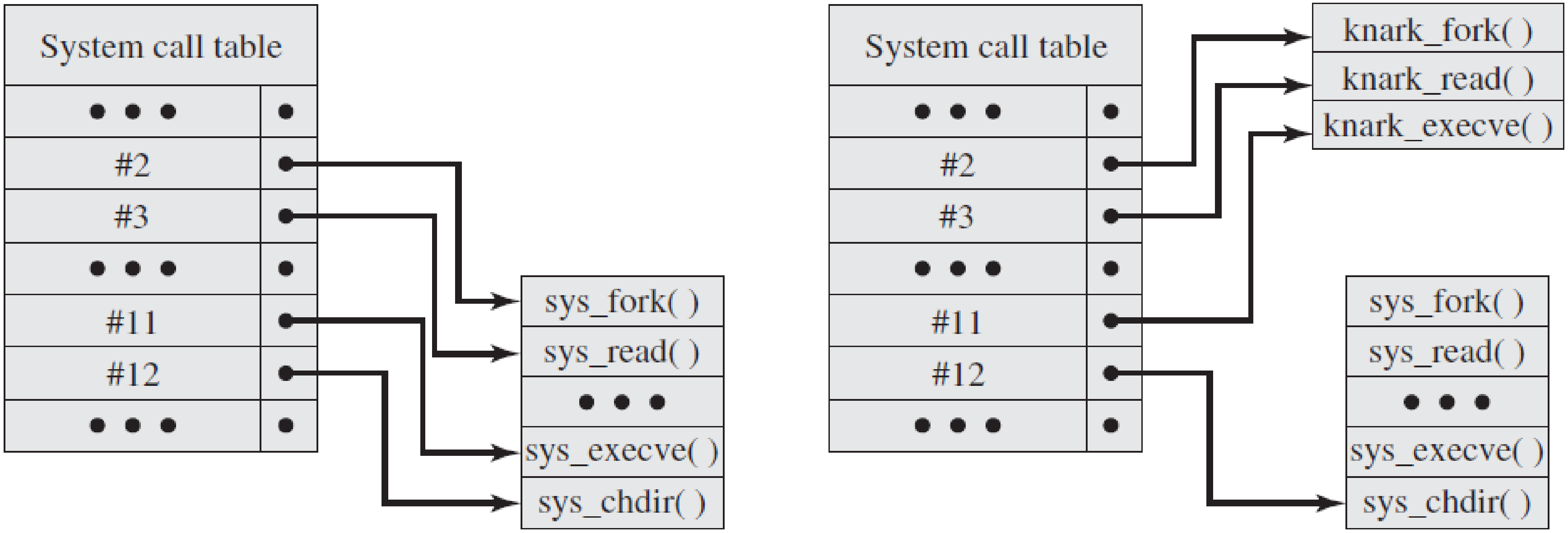
- Payloads where the malware gathers data stored on the infected system for use by the attacker.
- These attacks target the confidentiality of information.
- A keylogger captures keystrokes on the infected machine to allow an attacker to monitor the sensitive information.
- A spyware subverts the compromised 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.

Payload (Stealthing – 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.

Payload (Stealthing – 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.



(a) Normal kernel memory layout

(b) After knark install

Figure 6.5 System Call Table Modification by Rootkit

Payload - Summary

- System corruption
- Attack agent
- Information theft
- Stealth

Countermeasures

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

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.

Countermeasures

- Host-based scanner: Used on each end system.
- Generations of anti-virus software:
  - 1st: simple scanners (requires malware signature to identify the 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.

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

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.

- Perimeter scanning approaches
  - Ingress monitors: monitor incoming traffic
  - Egress monitors: monitor outgoing traffic

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)

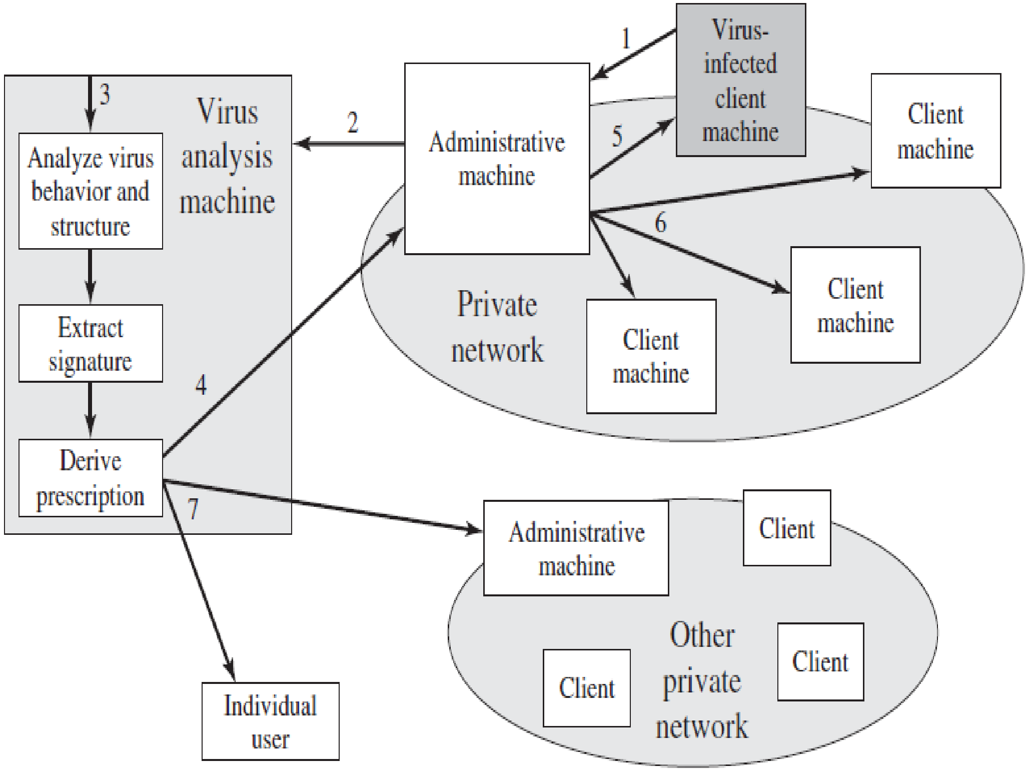
Countermeasures

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.



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