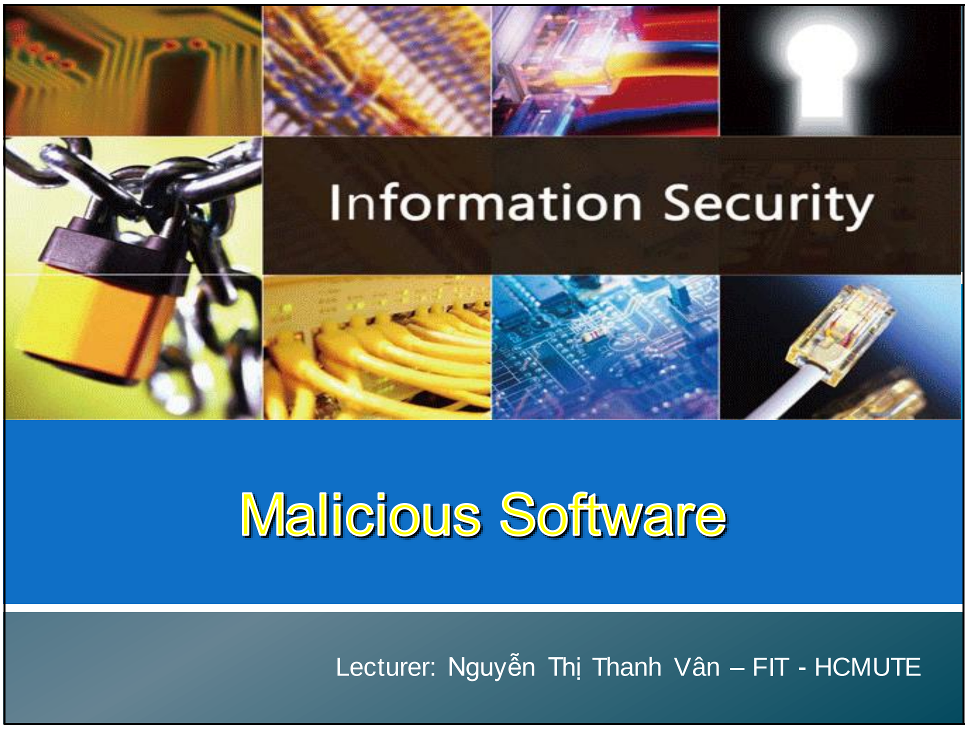
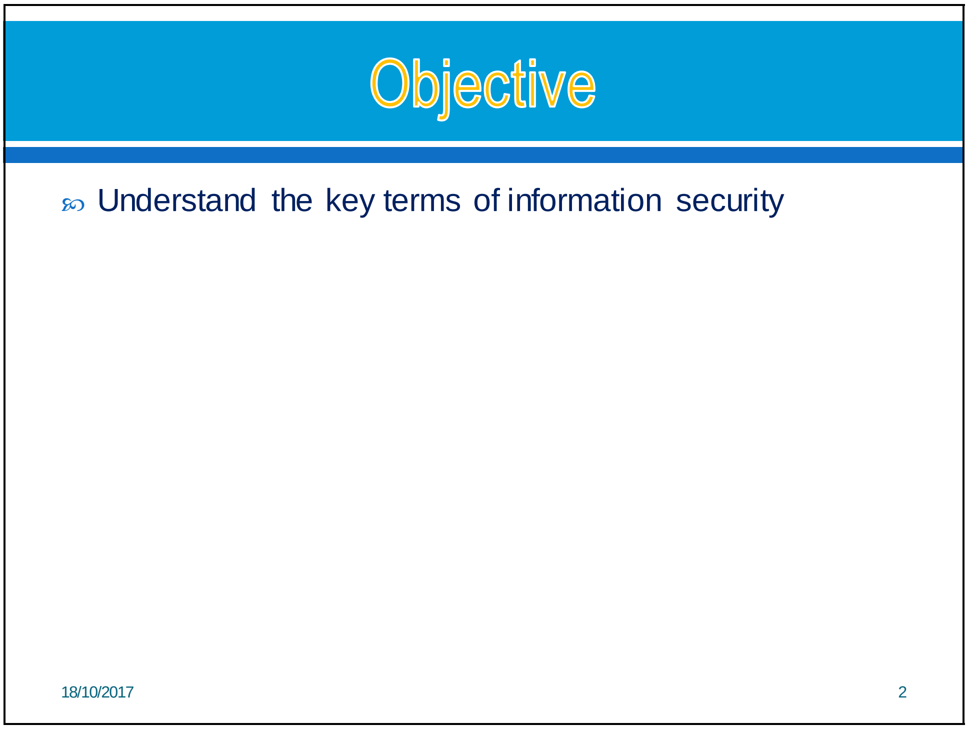


Information Security

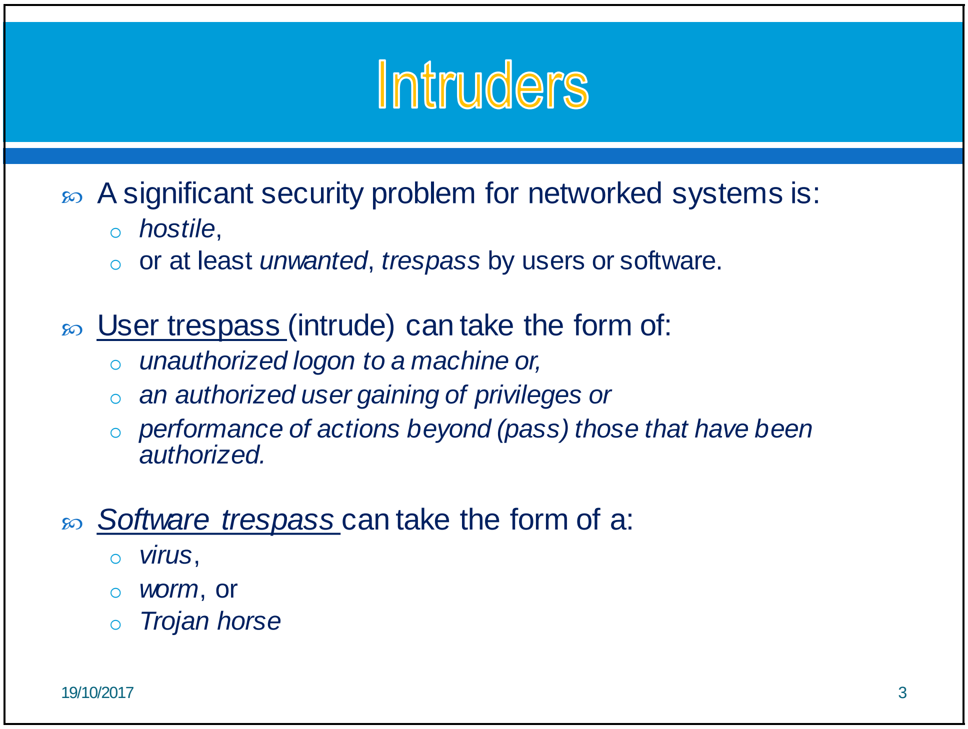
Malicious Software

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE



Objective

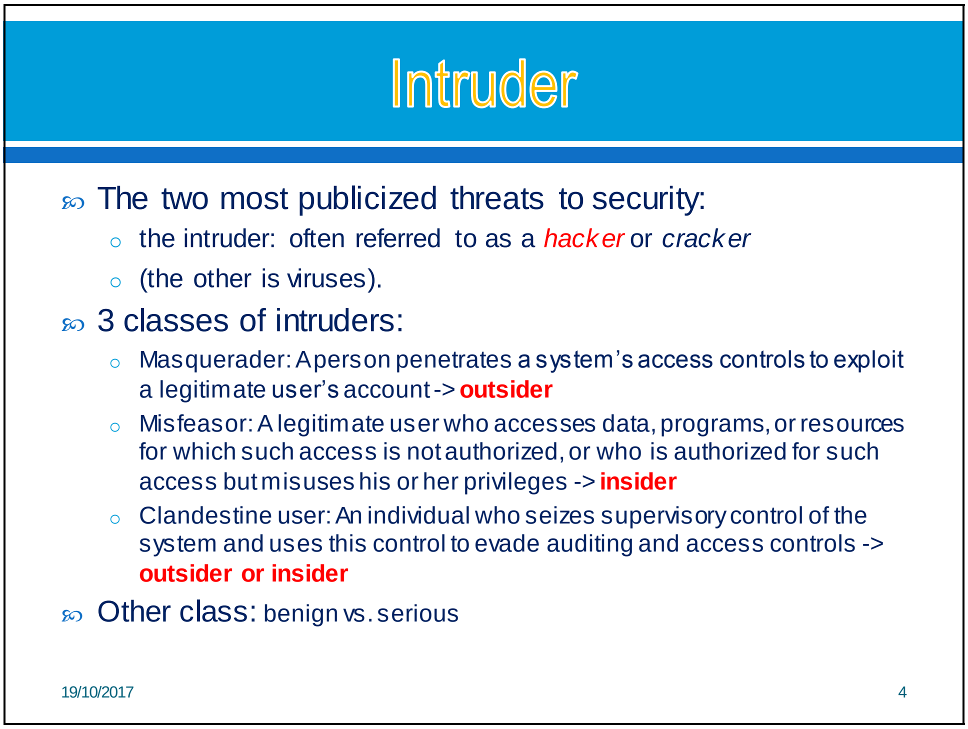
- Understand the key terms of information security



Intruders

- A significant security problem for networked systems is:
  - *hostile*,
  - or at least *unwanted*, *trespass* by users or software.
- User trespass (intrude) can take the form of:
  - *unauthorized logon to a machine or,*
  - *an authorized user gaining of privileges or*
  - *performance of actions beyond (pass) those that have been authorized.*
- *Software trespass* can take the form of a:
  - *virus*,
  - *worm*, or
  - *Trojan horse*

19/10/2017 3



Intruder

- The two most publicized threats to security:
  - the intruder: often referred to as a *hacker* or *cracker*
  - (the other is viruses).
- 3 classes of intruders:
  - Masquerader: A person penetrates a system's access controls to exploit a legitimate user's account -> **outsider**
  - Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges -> **insider**
  - Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls -> **outsider or insider**
- Other class: benign vs. serious

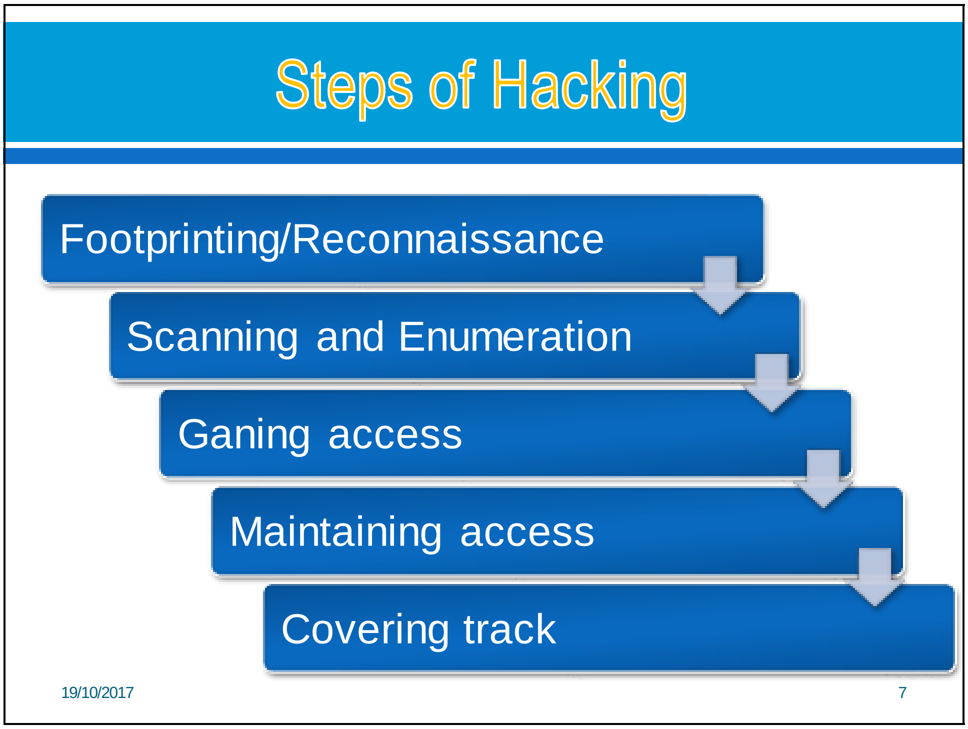
19/10/2017 4

HACKER

Nguyen Thi Thanh Van - Khoa CNTT

Introduction

- *Benign intruders* might <u>be *tolerable*</u>, although they do <u>consume resources and may slow performance</u> for legitimate users.
- However, there is <u>*no way in advance*</u> to know whether an intruder will be *benign* or *harmful*.
- IDSs and IPSs are designed to counter this type of hacker threat.
- One of the results of the growing awareness of the intruder problem has been the establishment of a number of Computer Emergency Response Teams (CERTs).
    - collect / disseminate vulnerability info / responses



Steps of Hacking

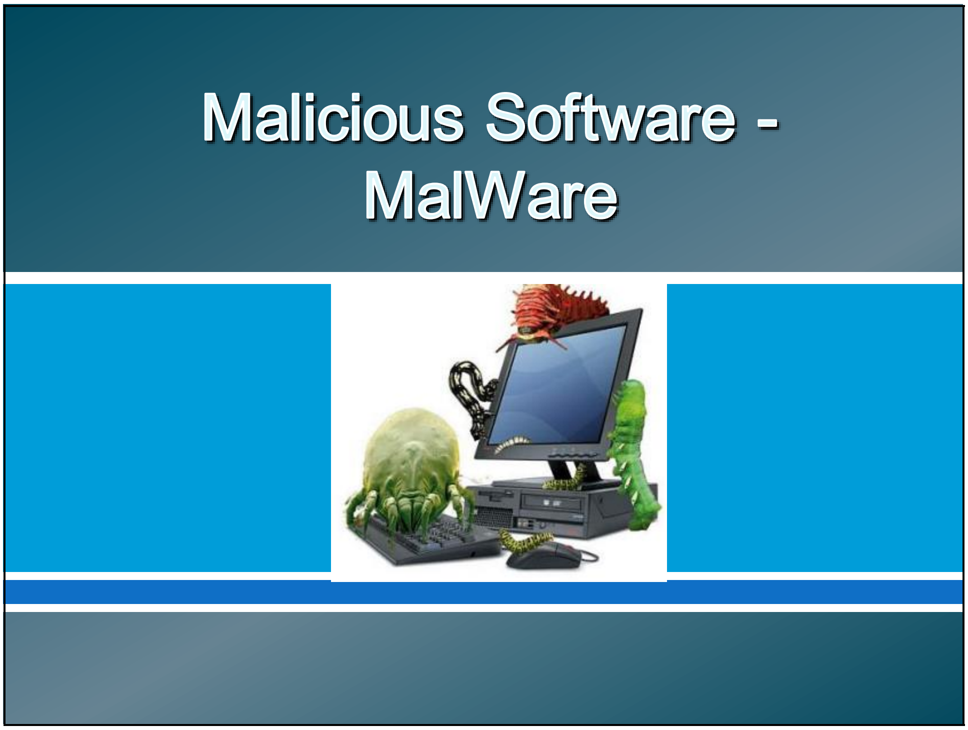
Footprinting/Reconnaissance

Scanning and Enumeration

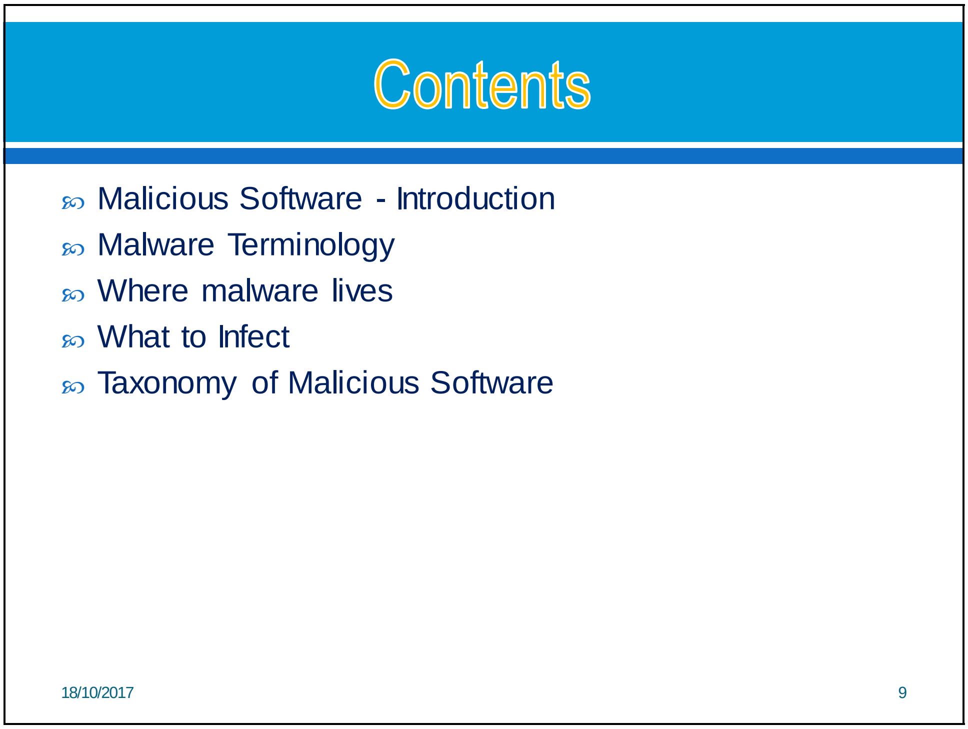
Ganing access

Maintaining access

Covering track

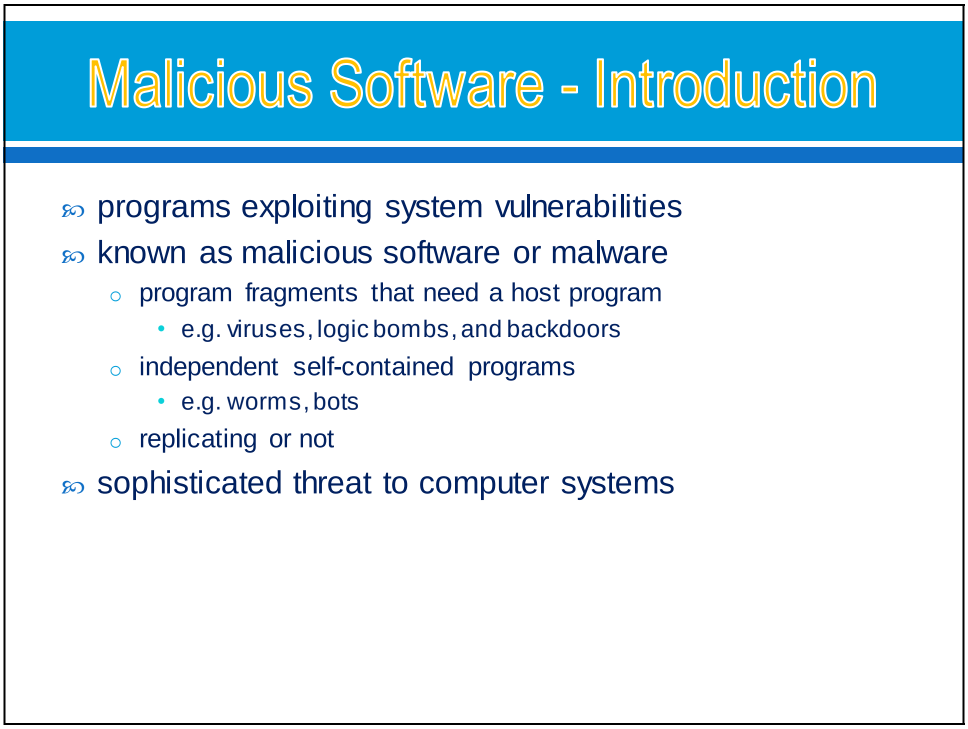


Malicious Software - MalWare



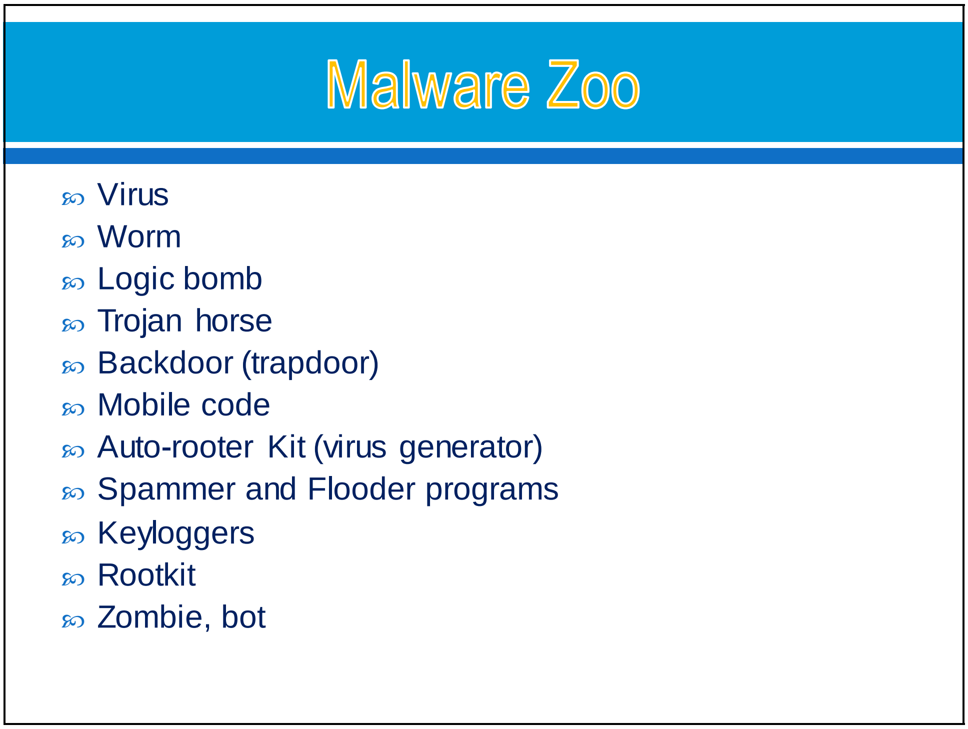
Contents

- Malicious Software - Introduction
- Malware Terminology
- Where malware lives
- What to Infect
- Taxonomy of Malicious Software



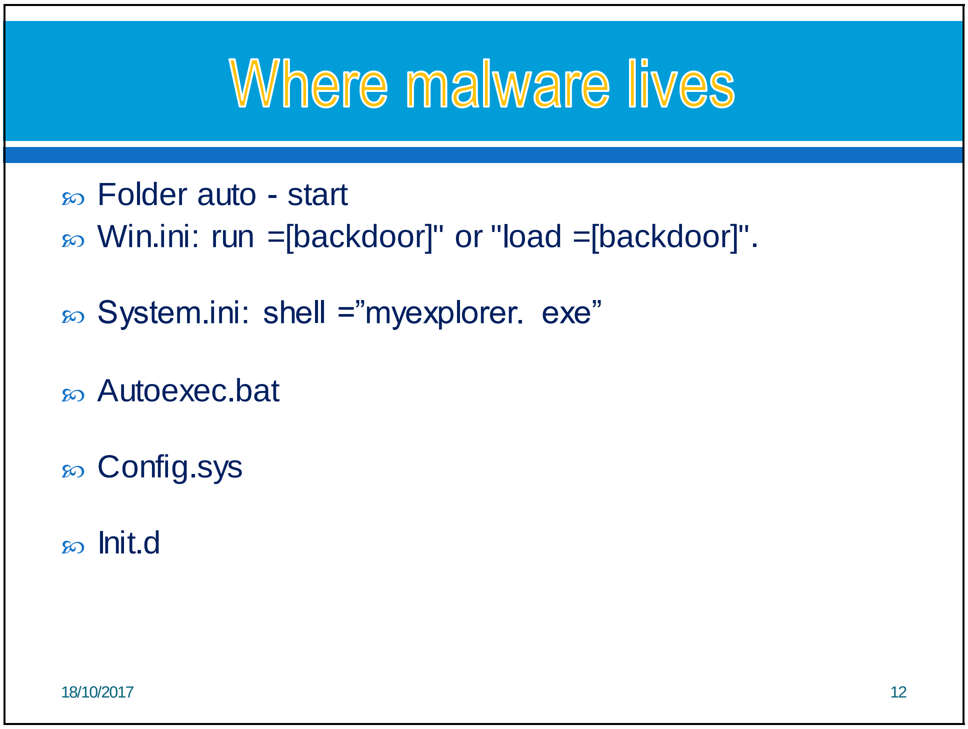
Malicious Software - Introduction

- programs exploiting system vulnerabilities
- known as malicious software or malware
  - program fragments that need a host program
    - e.g. viruses, logic bombs, and backdoors
  - independent self-contained programs
    - e.g. worms, bots
  - replicating or not
- sophisticated threat to computer systems



Malware Zoo

- Virus
- Worm
- Logic bomb
- Trojan horse
- Backdoor (trapdoor)
- Mobile code
- Auto-rooter Kit (virus generator)
- Spammer and Flooder programs
- Keyloggers
- Rootkit
- Zombie, bot



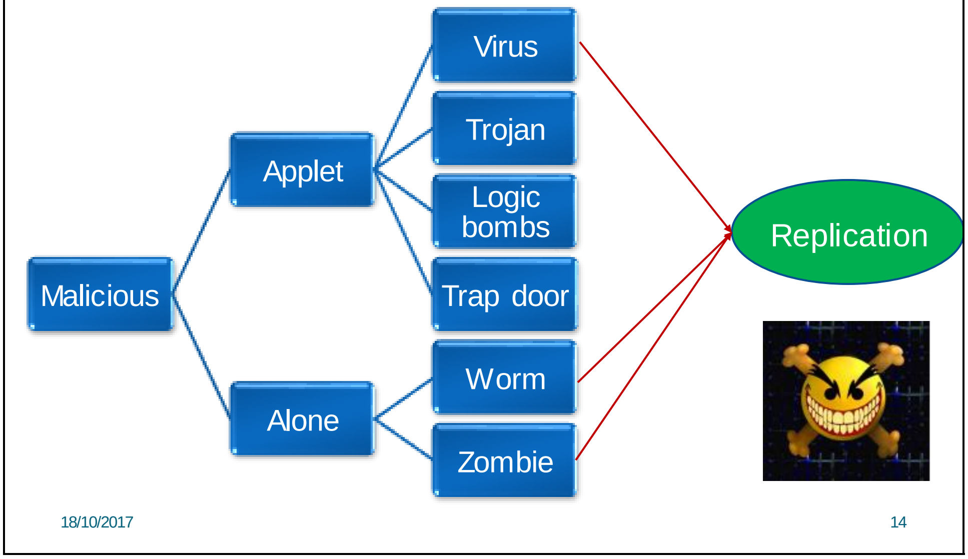
Where malware lives

- Folder auto - start
- Win.ini: run =[backdoor]" or "load =[backdoor]".
- System.ini: shell =”myexplorer. exe”
- Autoexec.bat
- Config.sys
- Init.d

What to Infect

- Executable
- Interpreted file
- Kernel
- Service
- Master Boot Record

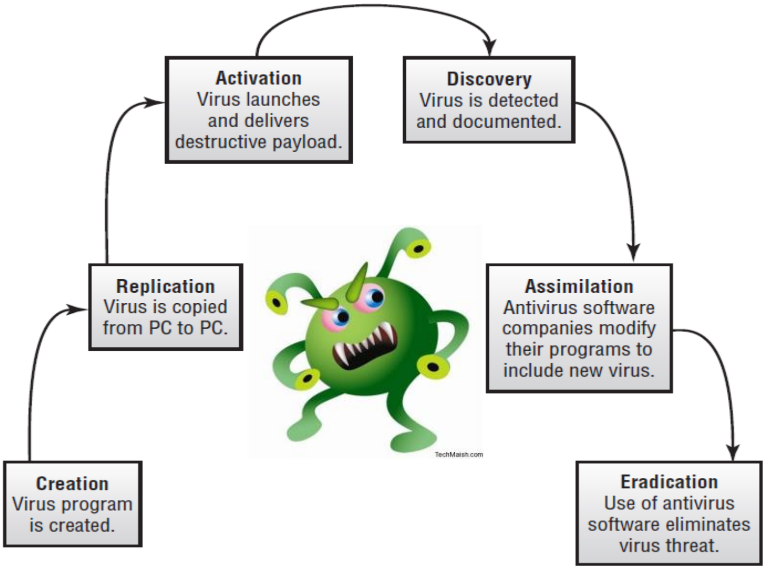
Taxonomy of Malicious Software



Viruses

- piece of software that infects other programs
  - modifying them to include a copy of the virus
  - so it executes secretly when host program is run
- specific to operating system and hardware
  - taking advantage of their details and weaknesses

Virus life cycle



Creation
Virus program is created.

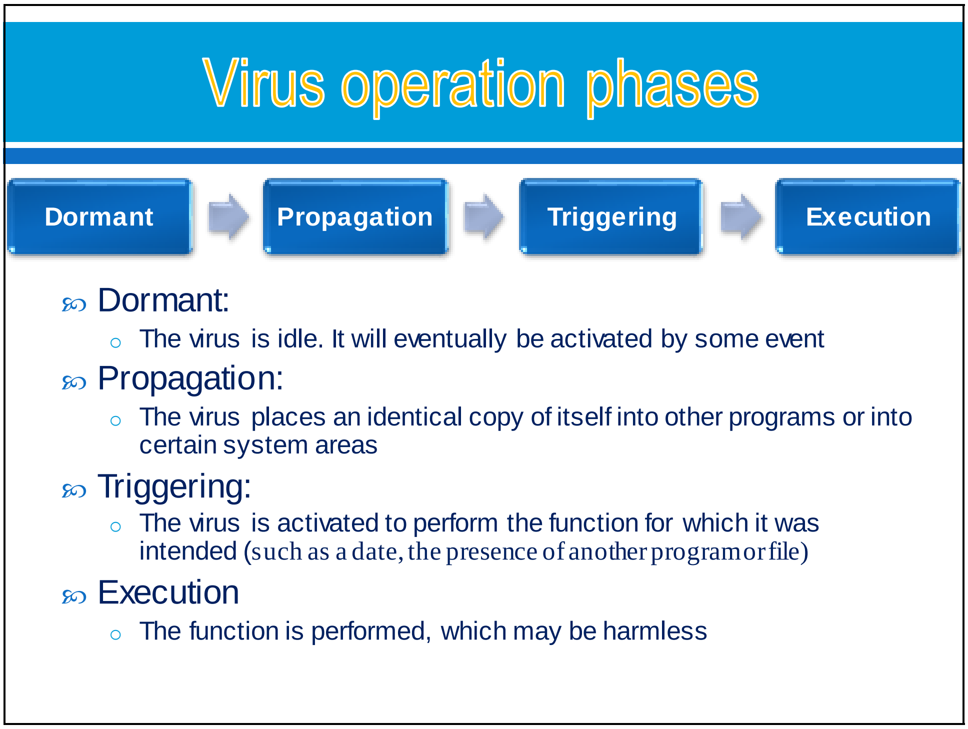
Replication
Virus is copied from PC to PC.

Activation
Virus launches and delivers destructive payload.

Discovery
Virus is detected and documented.

Assimilation
Antivirus software companies modify their programs to include new virus.

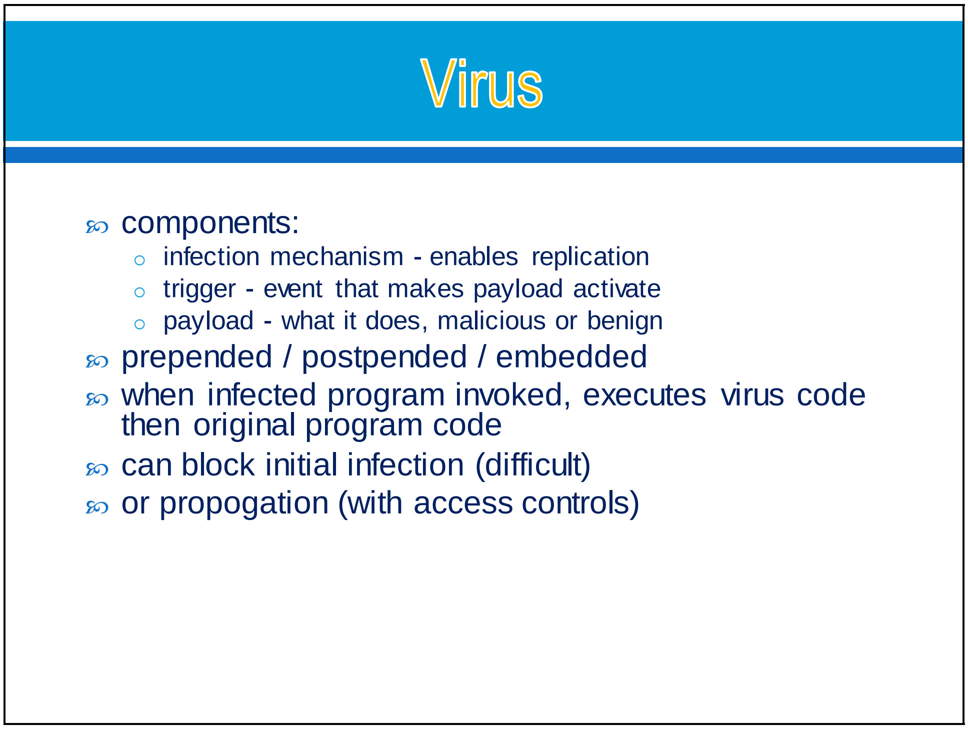
Eradication
Use of antivirus software eliminates virus threat.



Virus operation phases

Dormant → Propagation → Triggering → Execution

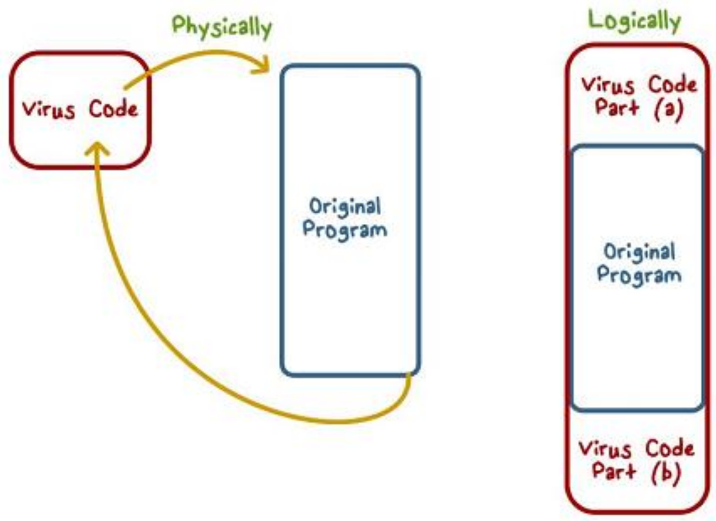
- Dormant:
  - The virus is idle. It will eventually be activated by some event
- Propagation:
  - The virus places an identical copy of itself into other programs or into certain system areas
- Triggering:
  - The virus is activated to perform the function for which it was intended (such as a date, the presence of another program or file)
- Execution
  - The function is performed, which may be harmless



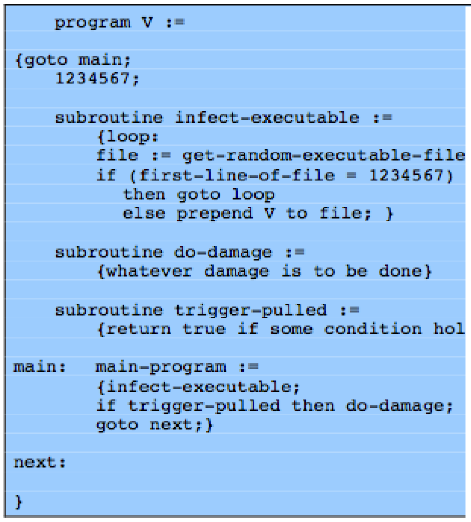
Virus

- components:
  - infection mechanism - enables replication
  - trigger - event that makes payload activate
  - payload - what it does, malicious or benign
- prepended / postpended / embedded
- when infected program invoked, executes virus code then original program code
- can block initial infection (difficult)
- or propogation (with access controls)

Virus Structure



Virus Structure



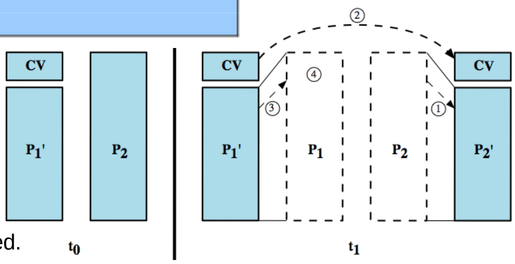
```
    program V :=

{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 hol

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

- Virus V:
  - 1: go to “main” of virus program
  - 2: a special flag (infected or not)
- Main:
  - Find uninfected programs - infect them
  - Do something damaging to the system
  - “Go to“ first line of the host program - do normal work
- Avoid detection by looking at size of program
  • Compress/decompress the host program

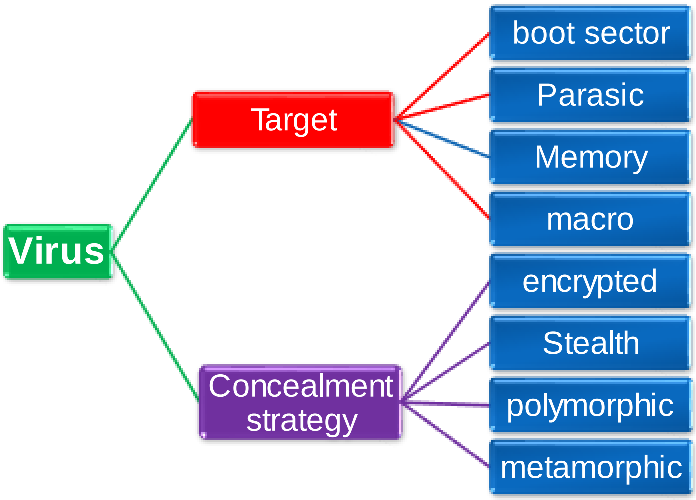
Compression Virus

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
          {loop:
               file := get-random-executable-file;
          if (first-line-of-file = 01234567) then goto loop;
      (1)      compress file;
      (2)      prepend CV to file;
      }

main:   main-program :=
          {if ask-permission then infect-executable;
      (3)      uncompress rest-of-file;
      (4)      run uncompressed file;}
      }
```

P1 is infected with the virus CV,
1. P2 (uninfected) is found, the virus compresses that file to P2'.
2. A copy of the virus is prepended to the compressed program.
3. The compressed version of the original infected program, is uncompressed.
4. The uncompressed program is executed.

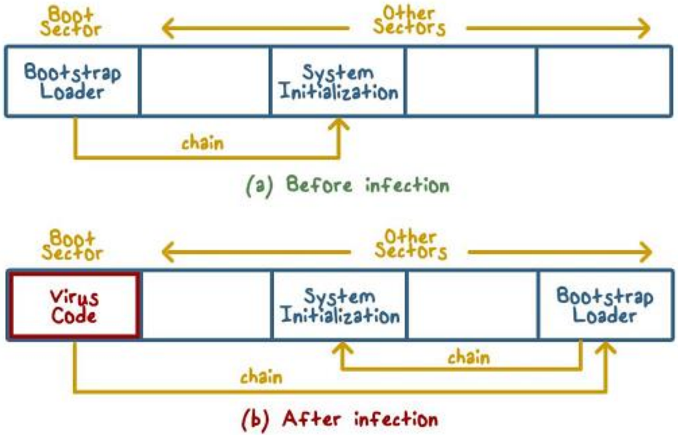


Virus Classification



Virus Classification – Target

- **Boot Sector Virus**: Infects master boot record / boot record (boot sector) of a disk and spreads when a system is booted with an infected disk (original DOS viruses).



(a) Before infection

(b) After infection

Virus Classification – Target

- **Memory-resident Virus**:
  - Reside in RAM
  - is infect running programs
- **Parasic Virus**:
  - Infects executable files.
  - They attach their self to executable files as part of their code.
  - Runs whenever the host program is executed.
-

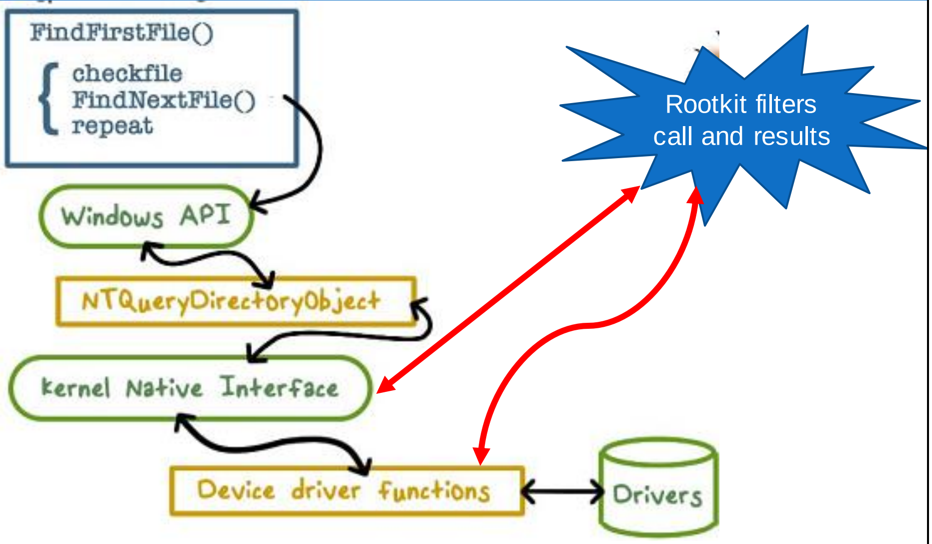
Virus Classification – Target

- **Macro Virus:**
  - became very common in mid-1990s
  - platform independent
  - infect documents (Word or excel files)
  - easily spread
  - often a form of Basic
  - more recent releases include protection
  - recognized by many anti-virus programs

Rootkits

- Resides in operating systems. Modifies OS code and data structure
- set of programs installed for admin access
- may hide its existence
  - difficult to determine that the rootkit is present and to identify what changes have been made
  - disrupting report mechanisms on processes, files, registry entries…
- can be classified on whether survive a reboot and execution mode:
  - Persistent: Activates each time the system boots, store code in a persistent store
  - memory-based: Has no persistent code and therefore cannot survive a reboot
  - user mode: Intercepts calls to APIs and modifies returned results.
  - kernel mode: Can intercept calls to native APIs in kernel mode; may hide the malware process by removing it from the kernel's list of active processes.
- installed by user via Trojan or intruder on system
- range of countermeasures needed

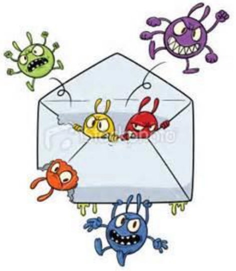
Rootkits

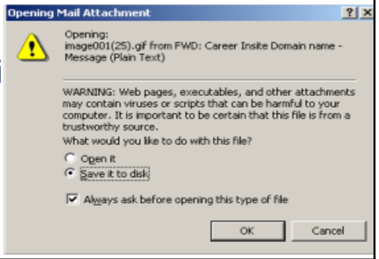


```
FindFirstFile()
  { checkfile
    FindNextFile()
    repeat
```

E-Mail Viruses

- more recent development
- e.g. Melissa
  - exploits MS Word macro in attached doc
  - if attachment opened, macro activates
  - sends email to all on users address list
  - and does local damage
- then saw versions triggered reading email
- hence much faster propagation
- file types should never be opened i
  .E XE, .PIF, . BAT, .VBS, .COM





Opening Mail Attachment

Opening:
image001(25).gif from FWD: Career Insite Domain name - Message (Plain Text)

WARNING: Web pages, executables, and other attachments may contain viruses or scripts that can be harmful to your computer. It is important to be certain that this file is from a trustworthy source.

What would you like to do with this file?

○ Open it
● Save it to disk

☑ Always ask before opening this type of file

Virus Classification - Concealment

- **Encrypted Virus** - A portion of virus creates a random encryption key and encrypts the remainder of the virus. The key is stored with the virus. When the virus replicates, a different random key is generated.
- **Stealth Virus** - explicitly designed to hide from Virus Scanning programs.
- **Polymorphic Virus** - mutates with every new host to prevent signature detection, signature detection is useless.
- **Metamorphic Virus** – Rewrites itself completely with every new host, may change their behavior and appearance.

Virus Countermeasures

- prevention - ideal solution but difficult
- realistically need:
  - detection
  - identification
  - Removal

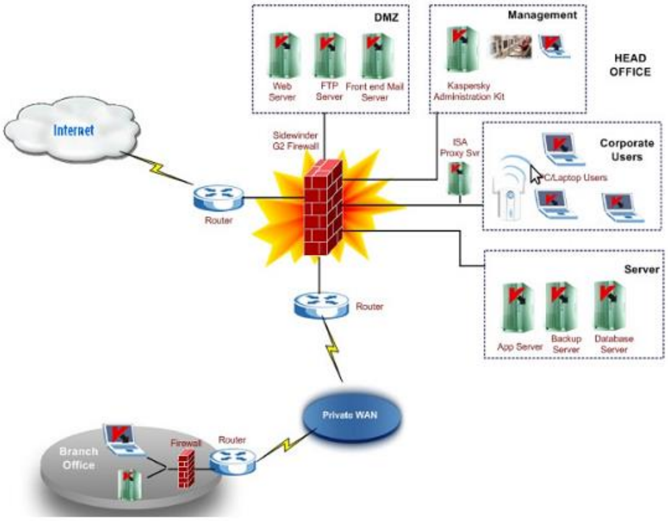
- if detect but can't identify or remove, must discard and replace infected program

Anti-Virus Evolution

- virus & antivirus tech have both evolved
- early viruses simple code, easily removed
- as become more complex, so must the countermeasures
- Generations
  - Scanner:
    - first - signature scanners
    - second - heuristics
  - Real time Monitors
    - third - identify actions
    - fourth - combination packages

Anti-Virus

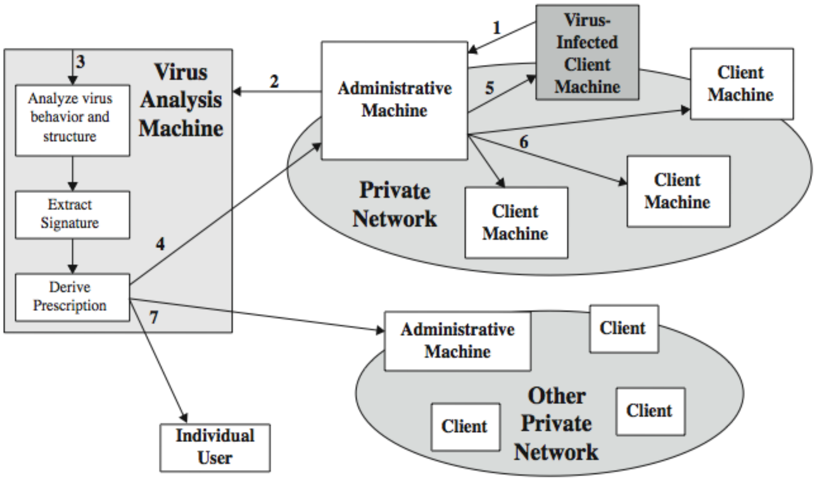
- Kaspersky



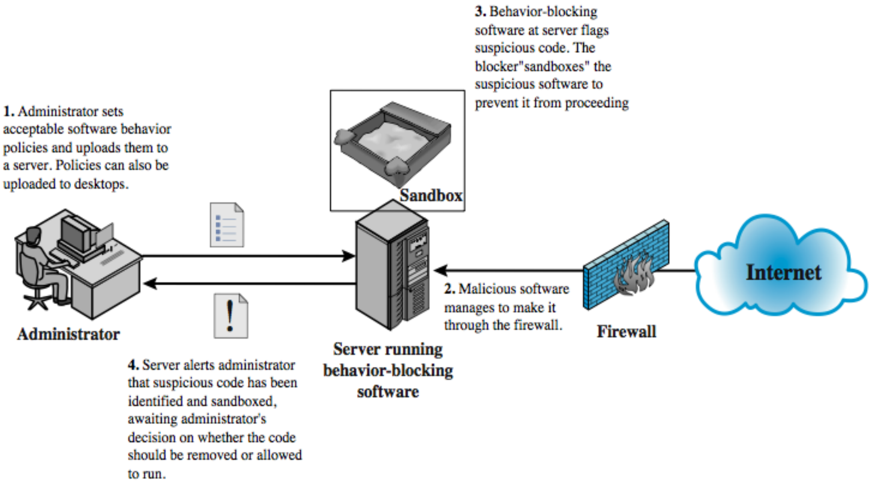
Generic Decryption

- runs executable files through GD scanner:
  - CPU emulator to interpret instructions
  - virus scanner to check known virus signatures
  - emulation control module to manage process
- lets virus decrypt itself in interpreter
- periodically scan for virus signatures
- issue is long to interpret and scan
  - tradeoff chance of detection vs time delay

Digital Immune System



Behavior-Blocking Software



1. Administrator sets acceptable software behavior policies and uploads them to a server. Policies can also be uploaded to desktops.

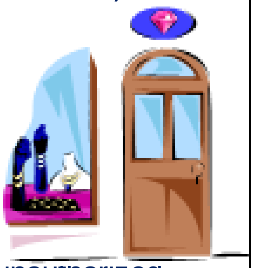
2. Malicious software manages to make it through the firewall.

3. Behavior-blocking software at server flags suspicious code. The blocker"sandboxes" the suspicious software to prevent it from proceeding

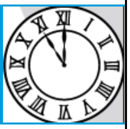
4. Server alerts administrator that suspicious code has been identified and sandboxed, awaiting administrator's decision on whether the code should be removed or allowed to run.

Backdoor or Trap door

- ~~S~~ecret entry point into a program
- Allows those who know access by passing usual security procedures
- Remains hidden to casual inspection
- Can be a new program to be installed
- Can modify an existing program
- Trap doors can provide access to a system for unauthorized procedures
- Very hard to block in O/S

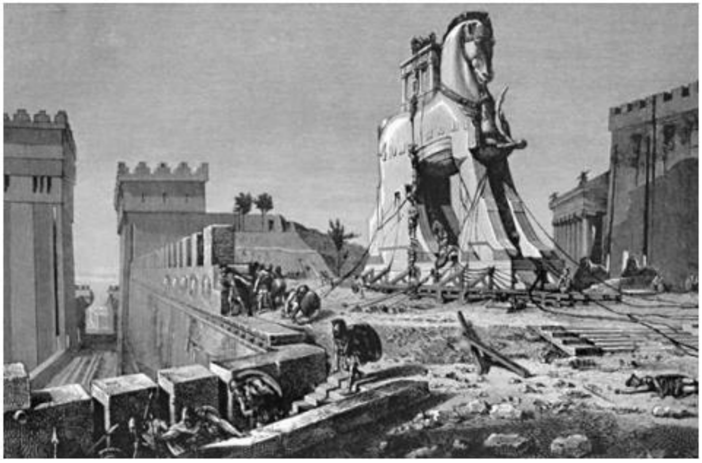


Logic Bomb



- One of oldest types of malicious software
- Piece of code that executes itself when predefined conditions are met
- Logic Bombs that execute on certain days are known as Time Bombs
- Activated when specified conditions met
  – E.g., presence/ absence of some file
  – particular date/ time
  – particular user
- When triggered typically damage system
  – modify/ delete files / disks , halt machine, etc.

Trojan



- the gift horse left outside the gates of Troy by the Greeks, Trojan Horses appear to be useful or interesting to an unsuspecting user, but are actually harmful.

Trojan horse

- **Trojan horse** is a malicious program that is designed as authentic, real and honest software.
- **Common features of Trojan Programs** :

  • Capturing screenshots of your computer.

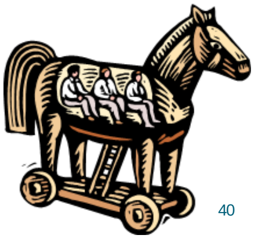
  • Recording key strokes and sending files to the hacker

  • Giving full Access to all your drives and files.

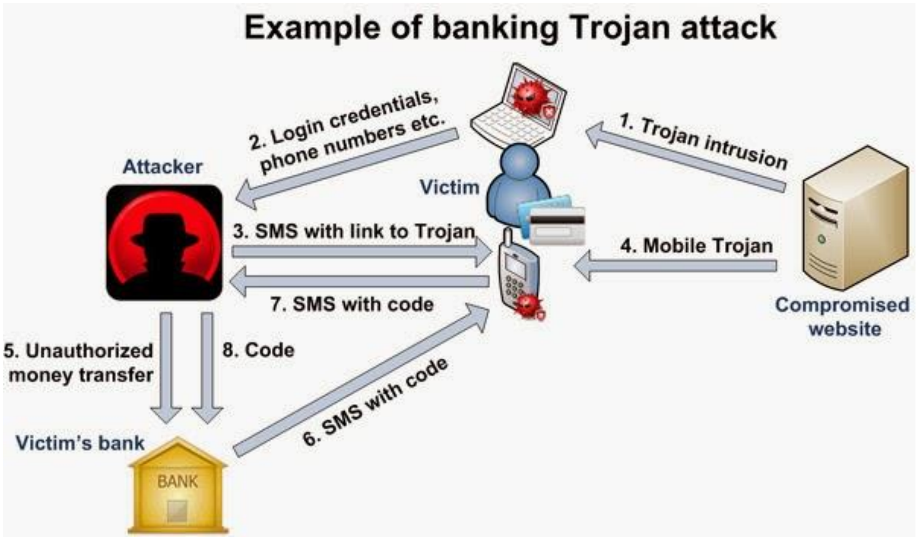
  • Ability to use your computer to do other hacking related activities

Trojan horse

- What Trojan scan do ?
  - Erase or overwrite data on a computer
  - Spread other viruses or install a backdoor. ('dropper'.)
  - Networks of zombie computers in order to launch DoS attacks or send Spam.
  - Logging keystrokes to steal information such as passwords and credit card numbers (known as a key logger)
  - Phish for bank or other account details, which can be used for criminal activities.
  - Or simply to destroy data
  - Mail the password file



Trojan, ex


Example of banking Trojan attack
Attacker
2. Login credentials, phone numbers etc.
Victim
1. Trojan intrusion
3. SMS with link to Trojan
4. Mobile Trojan
7. SMS with code
Compromised website
5. Unauthorized money transfer
8. Code
6. SMS with code
Victim's bank
BANK

Worms

- replicating program that propagates over net
  - using email, remote exec, remote login
- has 4 phases like a virus
- may disguise itself as a system process
- Once active:
  - It can behave as a computer virus or bacteria,
  - Iit could implant Trojan horse programs
  - Perform any number of disruptive or
  - Destructive actions
- The features:
  - Do not require a host application to perform their activities
  - Do not necessarily require any user interaction, direct or otherwise, to function
  - Replicate extremely rapidly across networks and hosts
  - Consume bandwidth and resources

Morris Worm

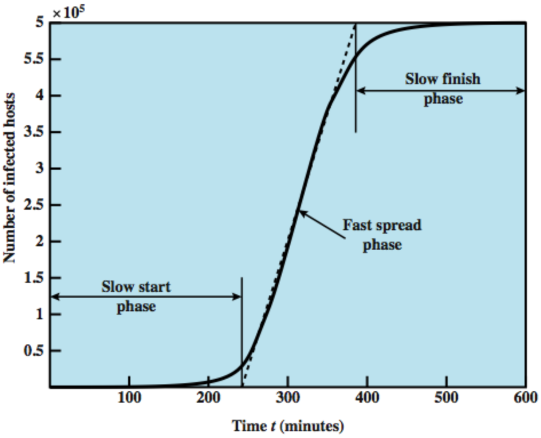
- one of best know worms
- released by Robert Morris in 1988
- various attacks on UNIX systems
  - cracking password file to use login/password to logon to other systems
  - exploiting a bug in the finger protocol
  - exploiting a bug in sendmail
- if succeed have remote shell access
  - sent bootstrap program to copy worm over

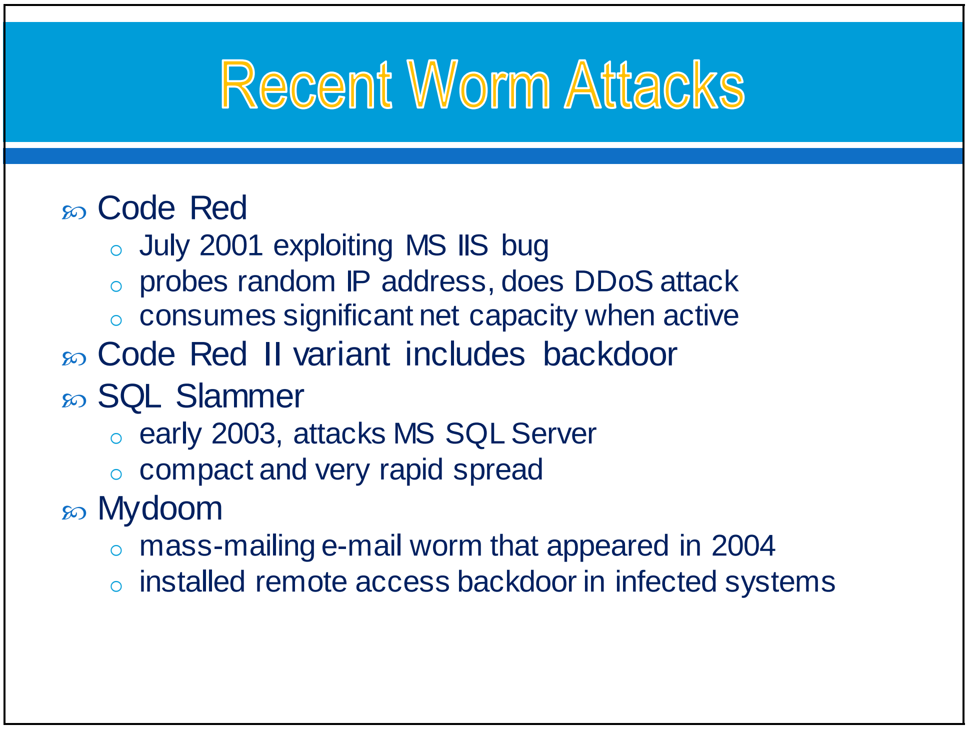
Worm Propagation Model

- The speed of propagation and the total number of hosts infected depend on a number of factors, including
  - the mode of propagation,
  - the vulnerability

  or vulnerabilities exploited,
  - the degree of similarity

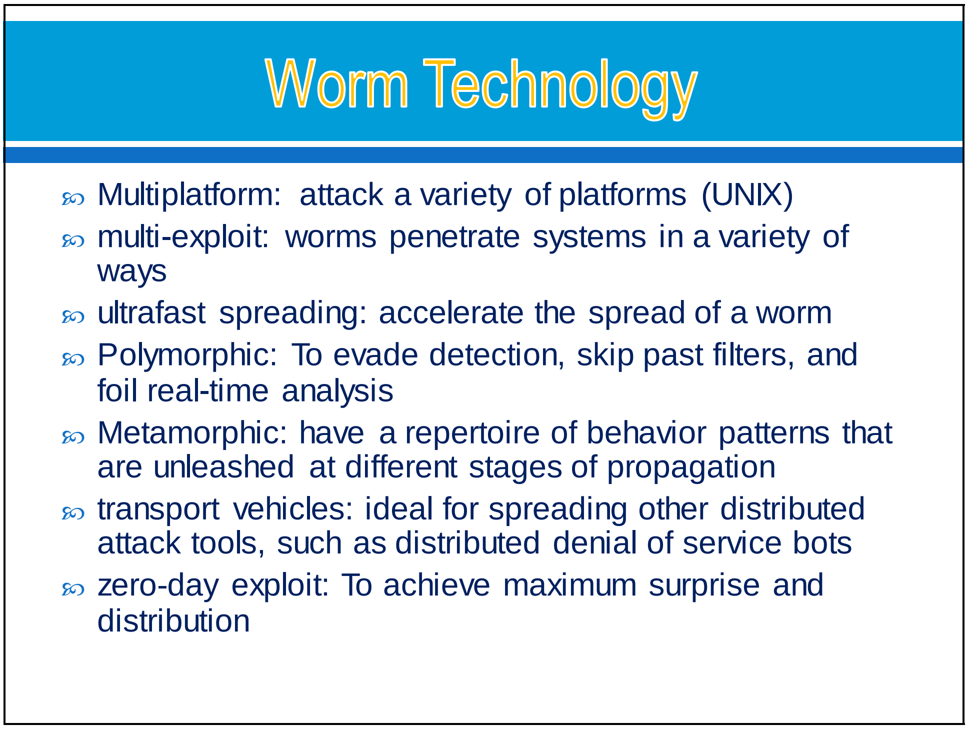
  to preceding attacks.





Recent Worm Attacks

- Code Red
  - July 2001 exploiting MS IIS bug
  - probes random IP address, does DDoS attack
  - consumes significant net capacity when active
- Code Red II variant includes backdoor
- SQL Slammer
  - early 2003, attacks MS SQL Server
  - compact and very rapid spread
- Mydoom
  - mass-mailing e-mail worm that appeared in 2004
  - installed remote access backdoor in infected systems



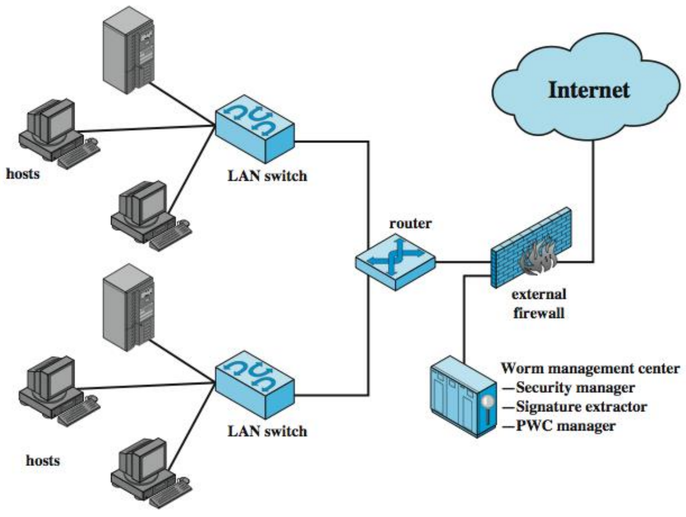
Worm Technology

- Multiplatform: attack a variety of platforms (UNIX)
- multi-exploit: worms penetrate systems in a variety of ways
- ultrafast spreading: accelerate the spread of a worm
- Polymorphic: To evade detection, skip past filters, and foil real-time analysis
- Metamorphic: have a repertoire of behavior patterns that are unleashed at different stages of propagation
- transport vehicles: ideal for spreading other distributed attack tools, such as distributed denial of service bots
- zero-day exploit: To achieve maximum surprise and distribution

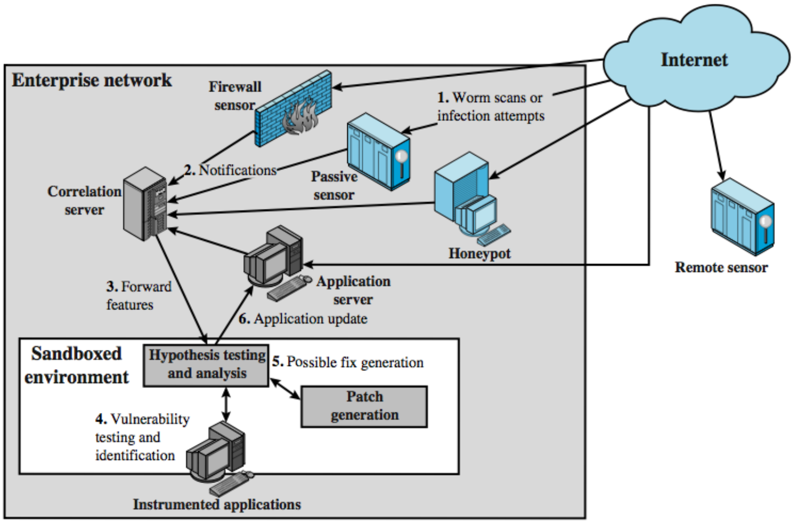
Worm Countermeasures

- overlaps with anti-virus techniques
- once worm on system A/V can detect
- worms also cause significant net activity
- worm defense approaches include:
  - signature-based worm scan filtering
  - filter-based worm containment
  - payload-classification-based worm containment
  - threshold random walk scan detection
  - rate limiting and rate halting

Proactive Worm Containment



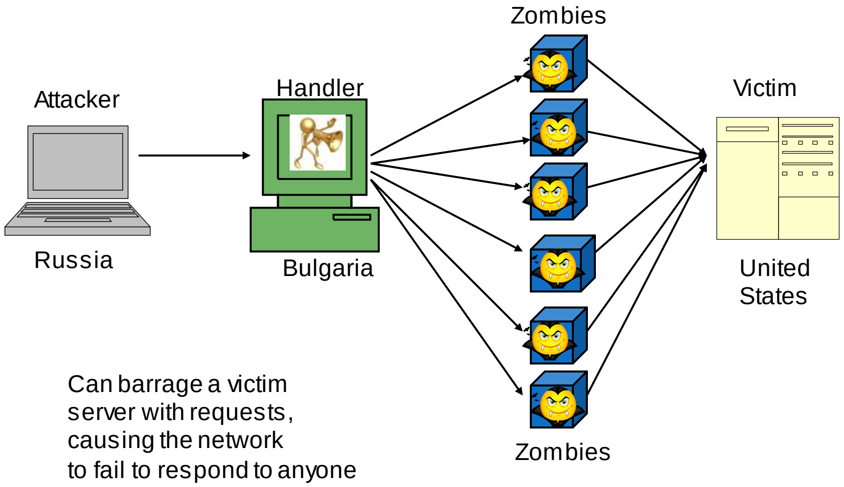
Network Based Worm Defense



Zombie

- The program which secretly takes over another networked computer and force it to run under a common command and control infrastructure.
- Uses it to indirectly launch aNacks, e.g., DDoS, phishing, spamming, cracking
- Difficult to trace zombie’ s creator)
- Infected computers — mostly Windows machines — are now the major delivery method of spam.
- Zombies have been used extensively to send e-mail spam; between 50% to 80% of all spam worldwide is now sent by zombie computers.

Distributed Denial of Service

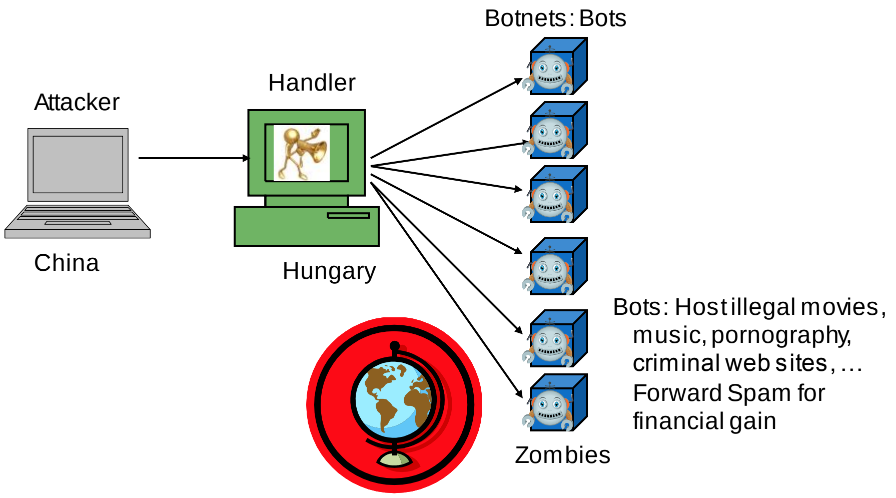


Can barrage a victim server with requests, causing the network to fail to respond to anyone

Bots (zombie, drone)

- Bot: a program secretly takes over hundreds or thousands of computer then uses that computer to launch attacks that are difficult to trace to the bot's creator.
- Botnet: The collection of bots
- Botnet has characteristics:
    - the bot functionality
    - remote control facility
        - via IRC/HTTP etc
    - spreading mechanism
        - attack software, vulnerability, scanning strategy
- various counter-measures applicable
- Some uses of bots include:
    - DDoS attacks, spamming, sniffing traffic, keylogging, spreading new malware, installing advertisement add-ons .

Botnets



Attacker

China

Handler

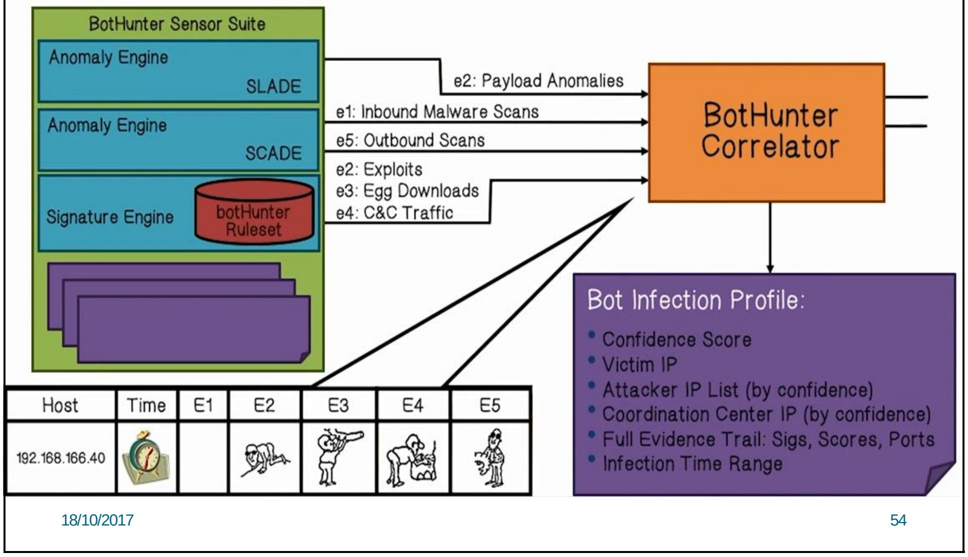
Hungary

Botnets: Bots

Zombies

Bots: Host illegal movies,
music, pornography,
criminal web sites, …
Forward Spam for
financial gain

BotHunter Architecture



BotHunter Sensor Suite

Anomaly Engine
SLADE

Anomaly Engine
SCADE

Signature Engine
botHunter Ruleset

e2: Payload Anomalies

e1: Inbound Malware Scans

e5: Outbound Scans

e2: Exploits
e3: Egg Downloads
e4: C&C Traffic

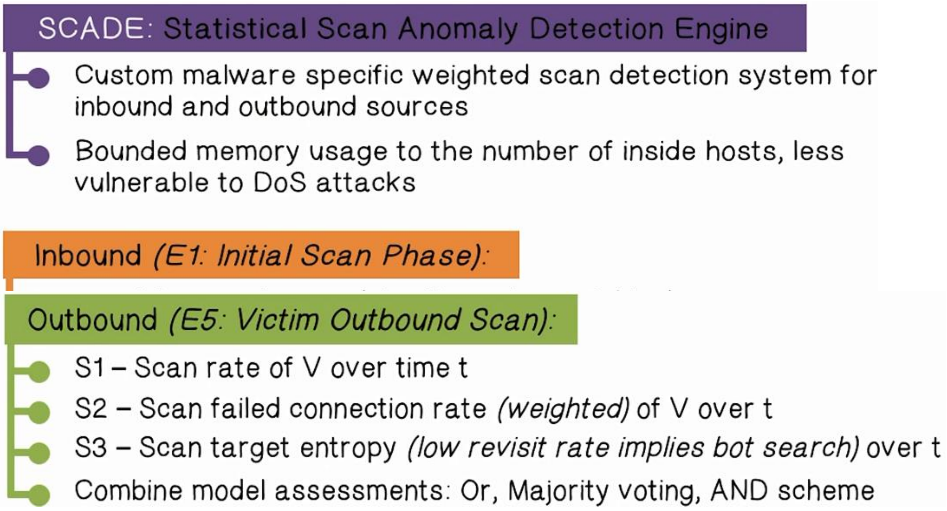
BotHunter Correlator

Host	Time	E1	E2	E3	E4	E5
192.168.166.40						

Bot Infection Profile:

- Confidence Score
- Victim IP
- Attacker IP List (by confidence)
- Coordination Center IP (by confidence)
- Full Evidence Trail: Sigs, Scores, Ports
- Infection Time Range

BotHunter Architecture: SCADE



SCADE: Statistical Scan Anomaly Detection Engine

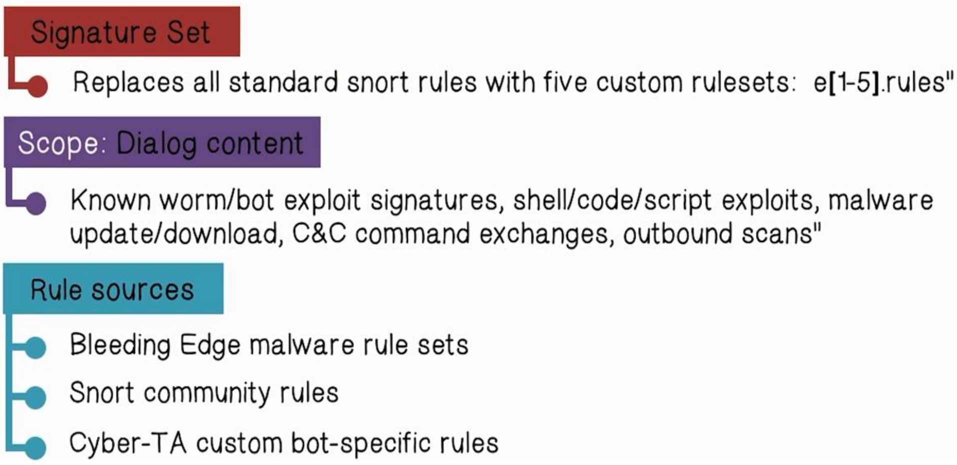
- Custom malware specific weighted scan detection system for inbound and outbound sources
- Bounded memory usage to the number of inside hosts, less vulnerable to DoS attacks

Inbound *(E1: Initial Scan Phase)*:

Outbound *(E5: Victim Outbound Scan)*:

- S1 – Scan rate of V over time t
- S2 – Scan failed connection rate *(weighted)* of V over t
- S3 – Scan target entropy *(low revisit rate implies bot search)* over t
- Combine model assessments: Or, Majority voting, AND scheme

Signature engine



Signature Set

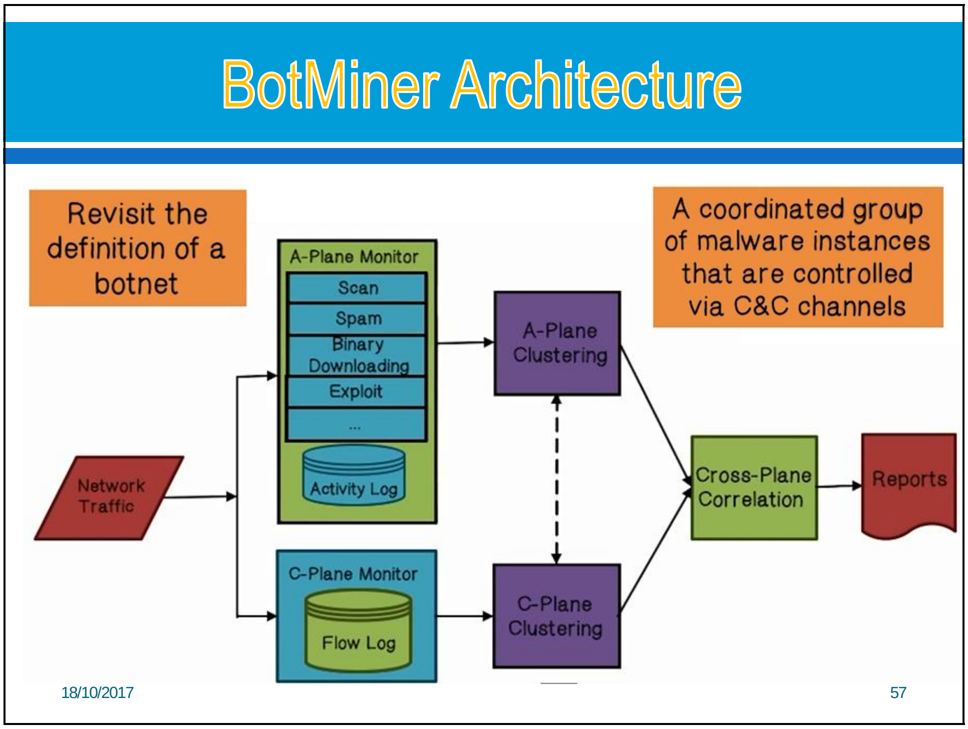
- Replaces all standard snort rules with five custom rulesets: e[1-5].rules"

Scope: Dialog content

- Known worm/bot exploit signatures, shell/code/script exploits, malware update/download, C&C command exchanges, outbound scans"

Rule sources

- Bleeding Edge malware rule sets
- Snort community rules
- Cyber-TA custom bot-specific rules

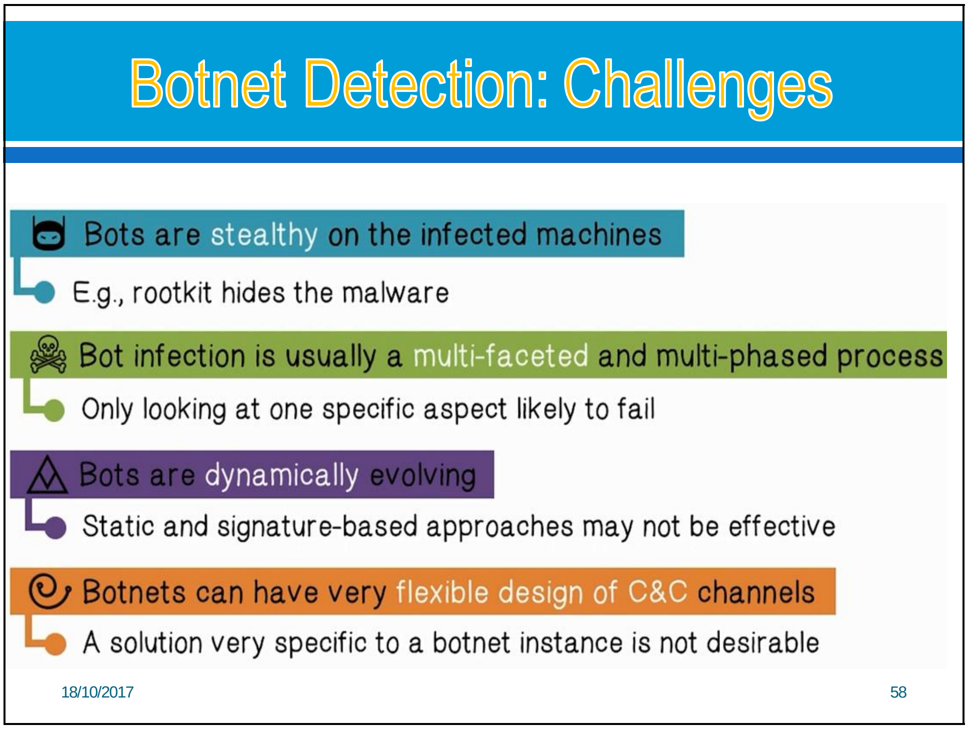


BotMiner Architecture

Revisit the definition of a botnet

A coordinated group of malware instances that are controlled via C&C channels

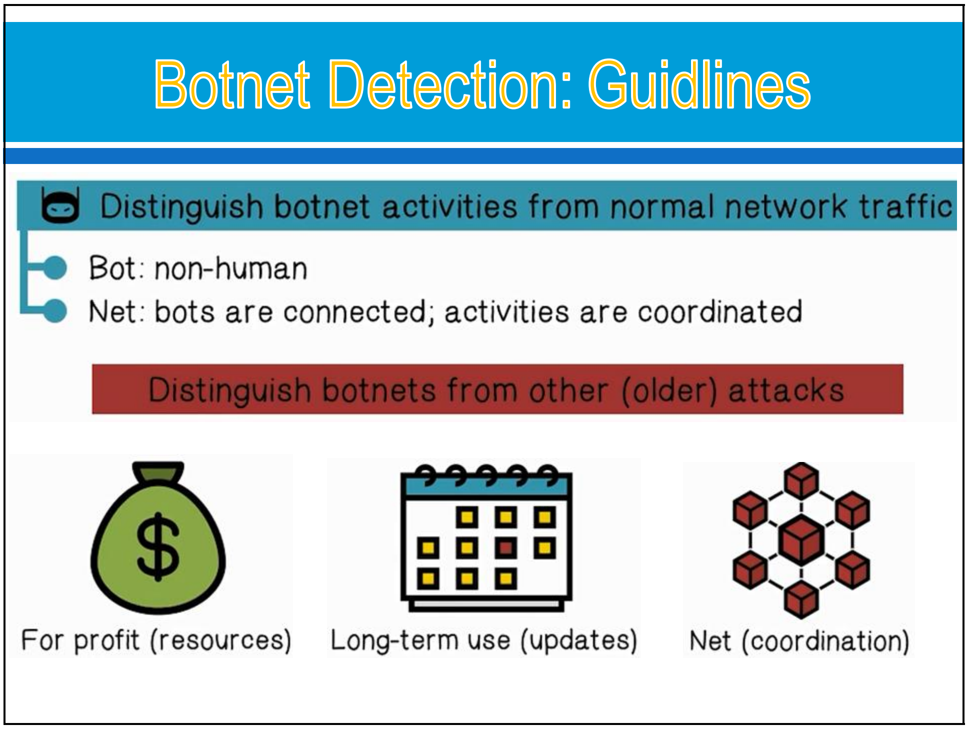
18/10/2017 57



Botnet Detection: Challenges

- Bots are stealthy on the infected machines
  - E.g., rootkit hides the malware
- Bot infection is usually a multi-faceted and multi-phased process
  - Only looking at one specific aspect likely to fail
- Bots are dynamically evolving
  - Static and signature-based approaches may not be effective
- Botnets can have very flexible design of C&C channels
  - A solution very specific to a botnet instance is not desirable

18/10/2017 58



Botnet Detection: Guidlines

Distinguish botnet activities from normal network traffic

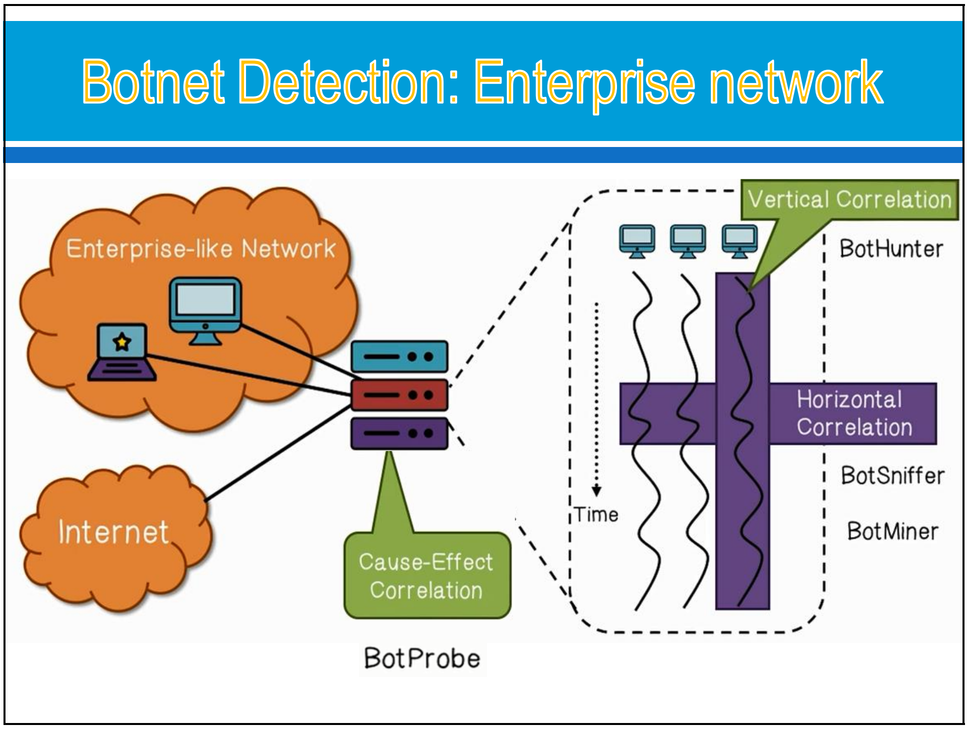
- Bot: non-human
- Net: bots are connected; activities are coordinated

Distinguish botnets from other (older) attacks

For profit (resources)

Long-term use (updates)

Net (coordination)

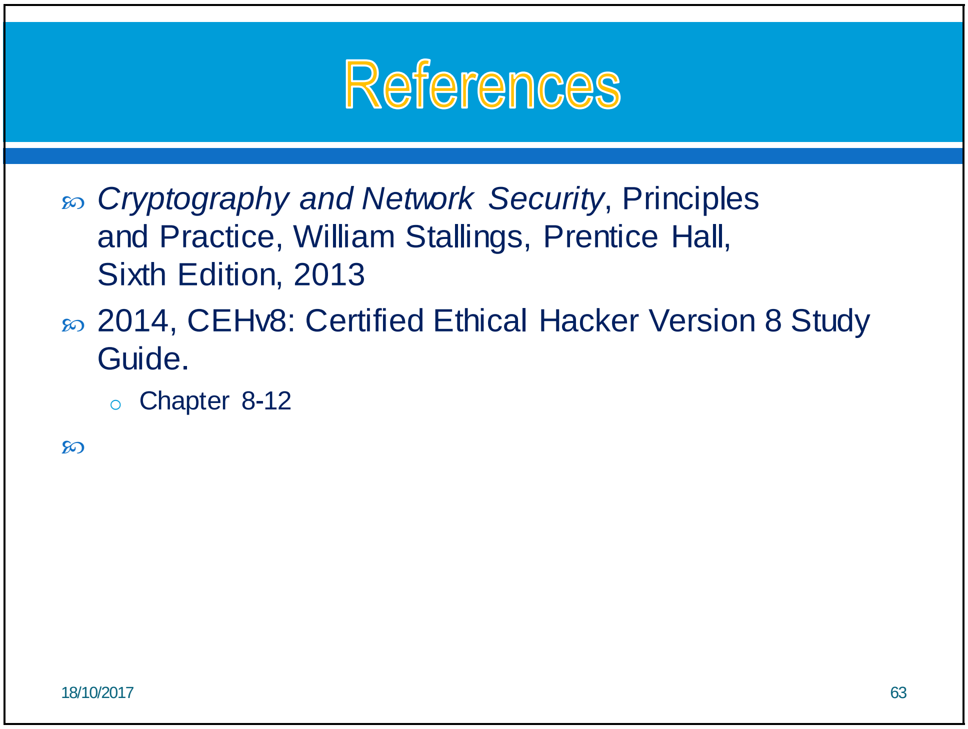


Botnet Detection: Enterprise network

Adware

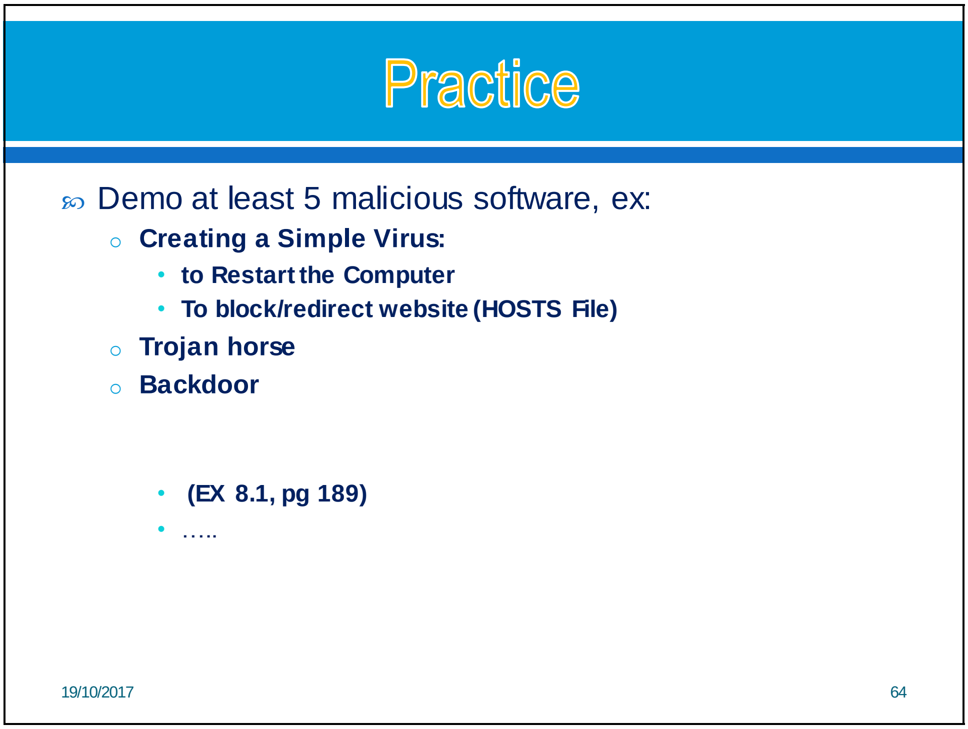
Summary

- Intruder
- Hacker: 4 phases
- Attack: many types
- Malicious Software: many types



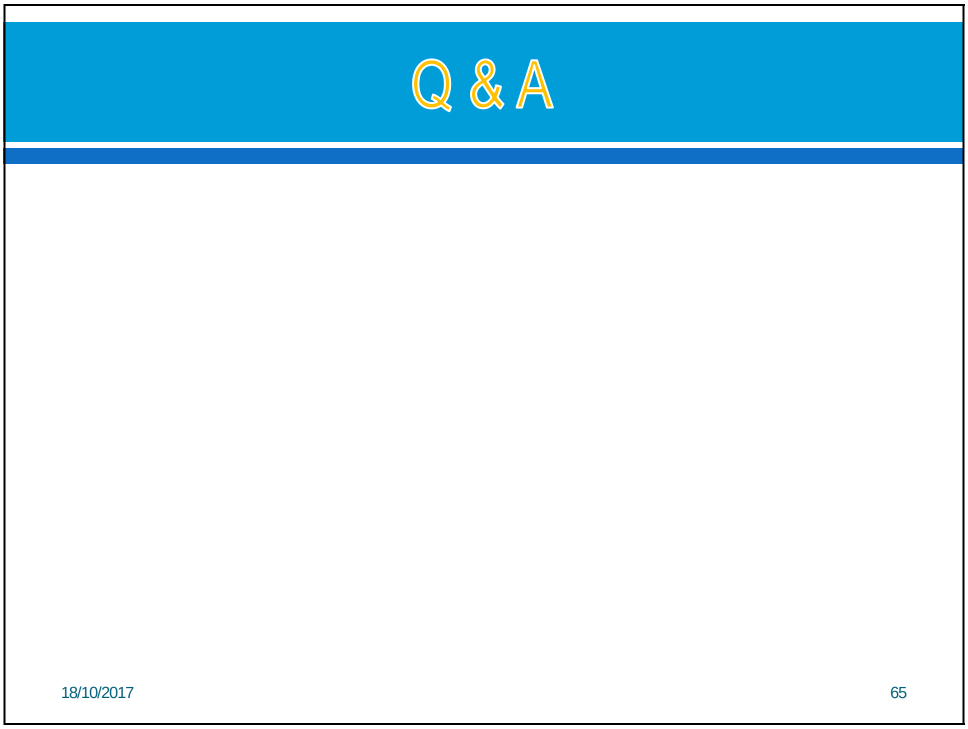
References

- *Cryptography and Network Security*, Principles and Practice, William Stallings, Prentice Hall, Sixth Edition, 2013
- 2014, CEHv8: Certified Ethical Hacker Version 8 Study Guide.
  - Chapter 8-12



Practice

- Demo at least 5 malicious software, ex:
  - **Creating a Simple Virus:**
    - **to Restart the Computer**
    - **To block/redirect website (HOSTS File)**
  - **Trojan horse**
  - **Backdoor**
    - **(EX 8.1, pg 189)**
    - …..



Q & A

18/10/2017

65