CAN304
Computer Systems Security

Lecture 8. Malware

Week 9: 2022-04-22, 14:00-16:00, Friday

Jie Zhang
Department of Communications and Networking
Email: jie.zhang01@xjtlu.edu.cn
Office: EE522

Group project

- Orinal deadline
  - Submission of presentation slides + report + code: Sunday, 8 May 2022, 23:59
- New deadline
  - Submission of presentation slides + video: Sunday, 8 May 2022, 23:59
  - Submission of report and code: Sunday, 15 May 2022, 23:59

Arrangement of presentation

- 7 minutes presentation (recorded video) + 3 minutes Q&A (live)
  - Running over time will negatively affect your grade

- CSIS2022
  - Computer Systems & Information Security
  - A virtual conference invovling 2 branches and 6 sessions for CAN304

1st workshop on Computer Systems & Information Security

CSIS2022

Location: BBB
UG Sessions

Agenda

Attendees: CAN304 Students and Module Leader

Session	Date	Start Time – End Time	Attendees
1	May 12	18:00 – 19:00	Group 1 – 5
2	May 13	13:00 – 14:00	Group 6 – 10
3	May 19	18:00 – 19:00	Group 11 – 15
4	May 20	13:00 – 16:00	Group 16 – 31
5	May 26	18:00 – 19:00	Group 32 – 36
6	May 27	13:00 – 16:00	Group 37 – 52

Final exam

- Online open-book exam
- Time allowed: 2 hours

- Answers should be written in blank papers
- 15 minutes for submitting your answer to learning mall (in a single PDF file)

Review of last time

- ✓ Overview of concepts
- ✓ Access control policies and implementations

Learning objetives

1

Describe three broad mechanisms malware uses to propagate.

2

Learn about the basic operation of viruses, worms, and Trojans.

3

Learn about some malware countermeasure elements.

Outline


Overview of malware
Common types of malware
Countermeasures

1. Introduction

Malware

- **Mal**icious soft**ware**

- Any software intentionally designed to cause damage to a computer, server, client, or computer network.

Compromise CIA

Annoy or disrupt the victim

Malware types

One popular approach to classify malware:

- First on how it **spreads** or **propagates** to reach the desired targets
- Then on the **actions** or **payloads** it performs once reaching target

Also classified by:

- Malware that needs a host program (parasitic code)
- Malware that are independent and self-contained

- Malware that does not replicate
- Malware that does replicate

Propagation mechanisms

Infection of existing content by **viruses** that is subsequently spread to other systems.

Exploit of software vulnerabilities by **worms** or **drive-by-downloads** to allow the malware to replicate

Social engineering attacks that convince users to bypass security mechanisms to install **Trojans** or to respond to **phishing attacks**.

Payload actions

Corruption of system or data files

Theft of service or make the system a **zombie agent** of attack as part of a botnet

Theft of information from the system/keylogging

Hiding its presence on the system to make it **stealthy**

Attack kits

- Attack toolkits are often known as “crimeware”
  - Include a variety of **propagation** mechanisms and **payload** modules that even novices can deploy

- Widely used toolkits include:

Zeus | Blackhole | Sakura | Phoenix

Attacker source

- Early attacker:
  - individuals often motivated to demonstrate their technical competence to their peers
- Now
  - more organized and dangerous attack sources

2. Common types of malware

Common types of malware

Propagation

- Infected Content: Viruses
- Vulnerability Exploit: Worms
- Social Engineering: Spam E-Mail, Trojans

Payload

- System Corruption
- Attack Agent: Zombie, Bots
- Information Theft: Keyloggers, Phishing, Spyware
- Stealthing: Backdoors, Rootkits

2.1 Propagation: Infected Content — Viruses

Viruses

- Piece of software that infects programs
  - Modifies them to include a copy of the virus
  - Replicates and goes on to infect other content

- When attached to an executable program, a virus can do anything that the program is permitted to do.

Virus components

Infection mechanism

- Means by which a virus spreads or propagates
- Also referred to as the *infection vector*

Trigger

- Event or condition that determines when the payload is activated or delivered
- Sometimes known as a *logic bomb*

Payload

- What the virus does (besides spreading)
- May involve damage or benign but noticeable activity

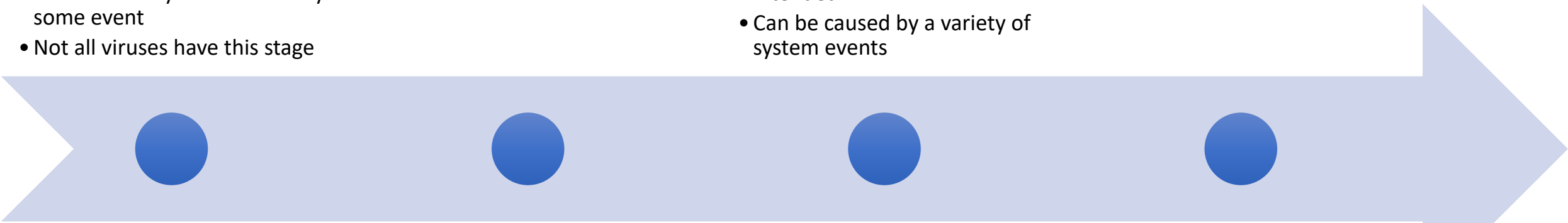
Virus phases

Dormant phase

- Virus is idle
- Will eventually be activated by some event
- Not all viruses have this stage

Triggering phase

- Virus is activated to perform the function for which it was intended
- Can be caused by a variety of system events



Propagation phase

- Virus places a copy of itself into other programs or into certain system areas on the disk
- May not be identical to the propagating version
- Each infected program will now contain a clone of the virus which will itself enter a propagation phase

Execution phase

- Function is performed
- May be harmless or damaging

Virus structure

- Example virus logic

```
program V
1234567;

procedure attach-to-program;
begin
   repeat
       file := get-random-program;
   until first-program-line ≠ 1234567;
   prepend V to file;
end;

procedure execute-payload;
begin
   (* perform payload actions *)
end;

procedure trigger-condition;
begin
   (* return true if trigger condition is true *)
end;

begin (* main action block *)
   attach-to-program;
   if trigger-condition then execute-payload;
   goto main;
end;
```

Find non-infected program and infect it

If trigger, then action

(a) A simple virus

How to detect such a virus?

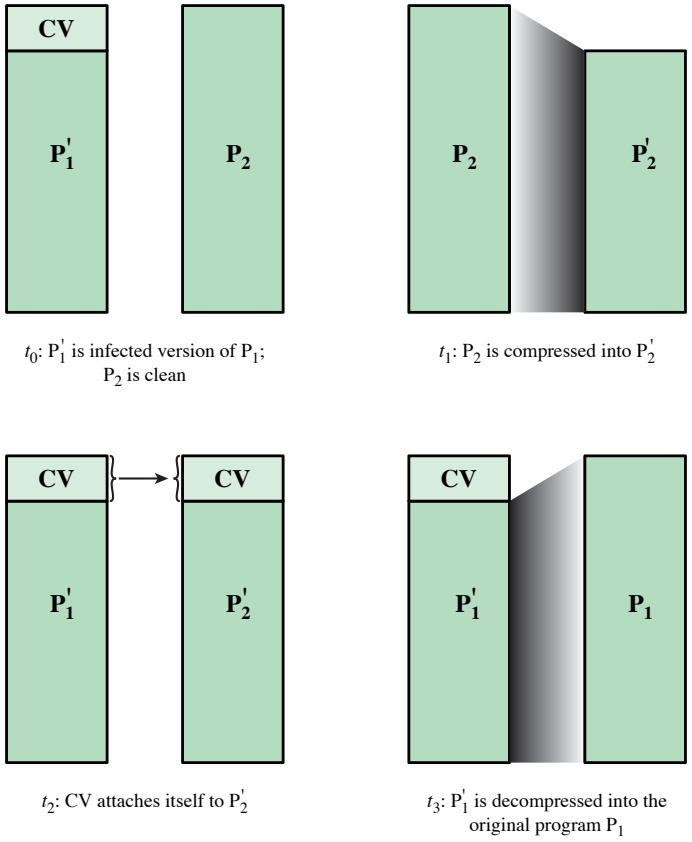
File-size based detection

Virus structure

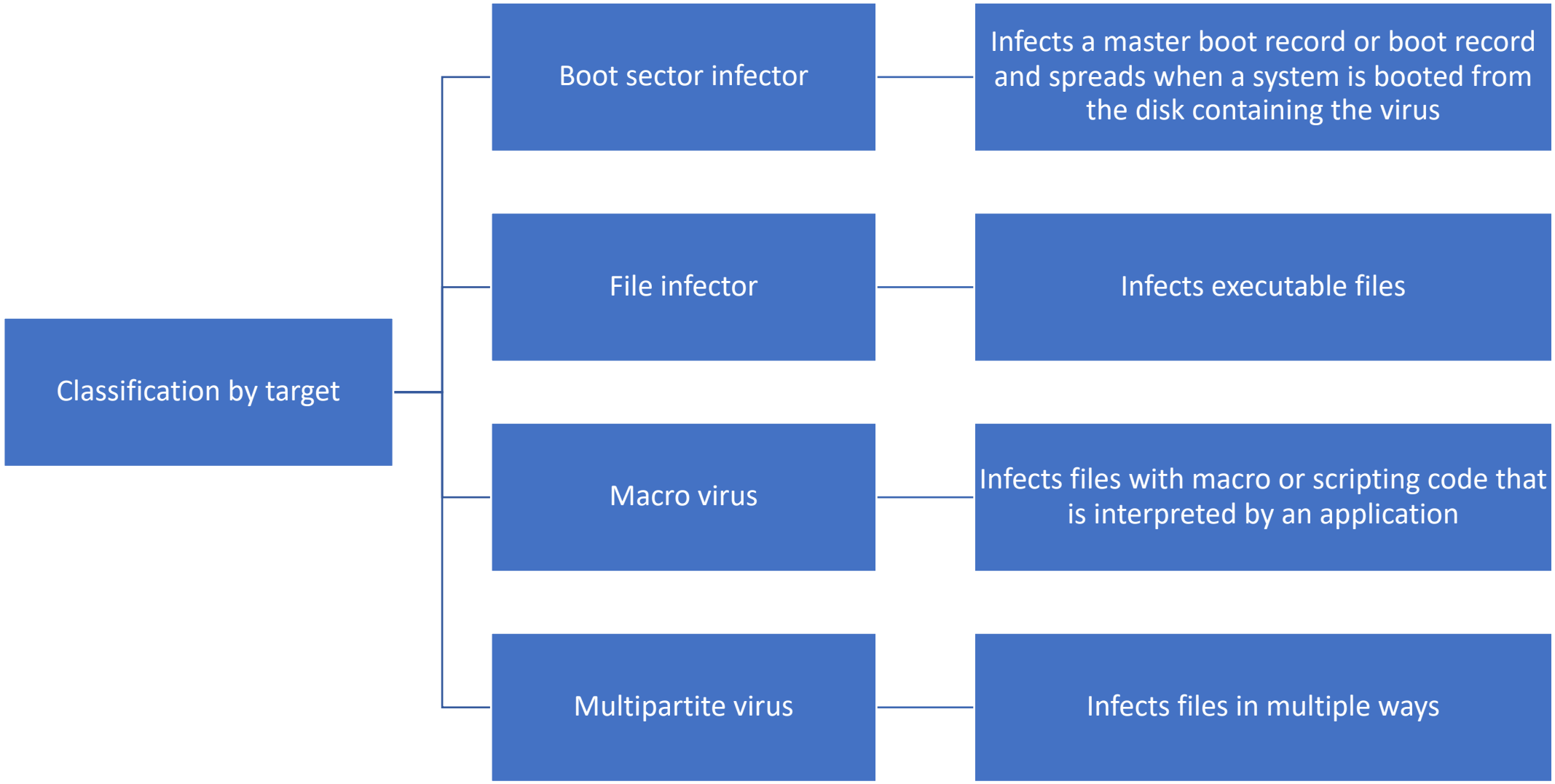
- Compression virus to avoid file-size-based detection

```
program CV
1234567;

procedure attach-to-program;
begin
   repeat
       file := get-random-program;
   until first-program-line ≠ 1234567;
   compress file;    (* t1 *)
   prepend CV to file;   (* t2 *)
end;

begin (* main action block *)
   attach-to-program;
   uncompress rest of this file into tempfile;   (* t3 *)
   execute tempfile;   (* t4 *)
end;
```

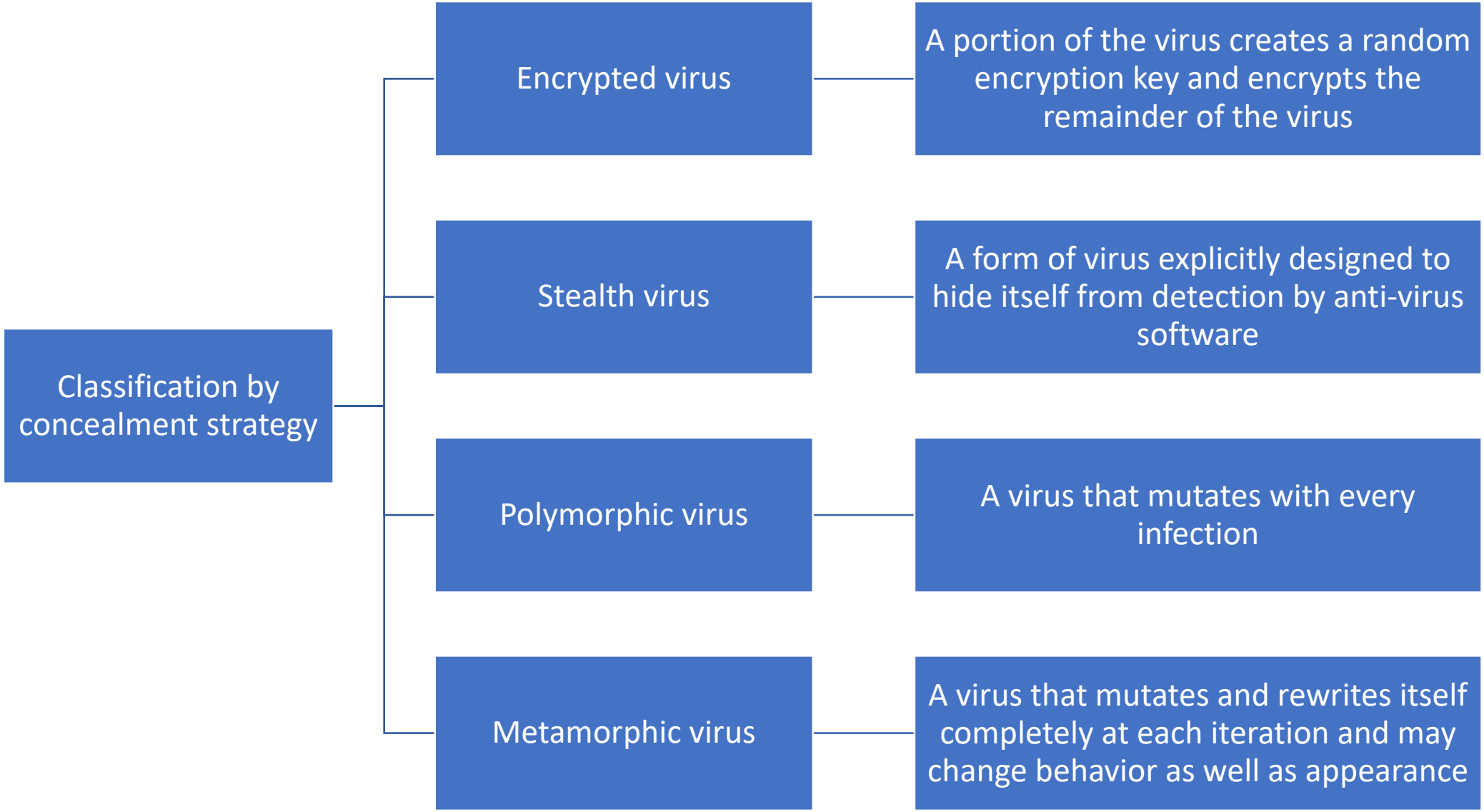
(b) A compression virus



Virus classification

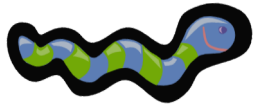


Virus classification



2.2 Propagation: Vulnerability Exploit — Worms

Worms



- A standalone malware computer program that replicates itself in order to spread to other computers.
- Making use of software vulnerabilities

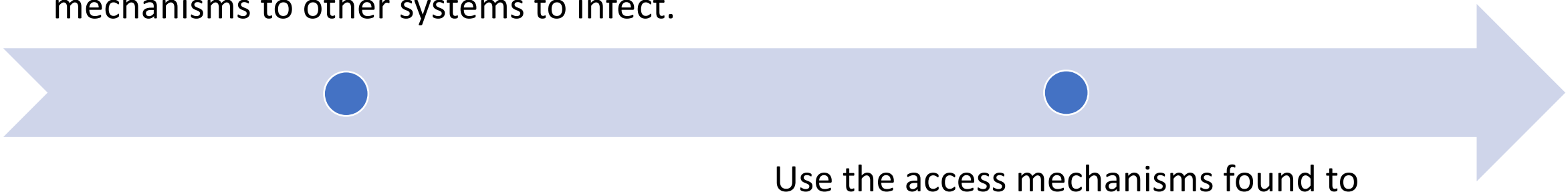
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments

- Upon activation the worm may replicate and propagate again

Warm propagation

- The propagation phase generally performs the following functions:

Search for appropriate access mechanisms to other systems to infect.



Use the access mechanisms found to transfer a copy of itself to the remote system, and cause the copy to be run.

Worm or Virus?

- Terms often used interchangeably
- Viruses seek to infect other programs
- Worms seek to move from machine to machine
- Don’t obsess about classifications

Drive-by-downloads

- Exploits browser vulnerabilities to download and install malware on the system when the user views a Web page controlled by the attacker
- In most cases does not actively propagate
- Spreads when users visit the malicious Web page

2.3 Propagation: Social Engineering
—Spam E-Mail, Trojans

Social engineering

- “Tricking” users to assist in the compromise of their own systems

Spam / phishing e-mails	Trojan horse	Mobile phone Trojans
• Unsolicited bulk e-mail • Significant carrier of malware • Used for phishing attacks	• Seemingly useful program that contains code that does harmful things	• First appeared in 2004 (Skuller) • Target is the smartphone

Phishing example

From: "XJTLU.EDU.CN" <gillianadrianbayfordb@gmail.com>
Date: Friday, June 11, 2021 at 8:39 AM
Subject: Staff, Employees XJTLU.EDU.CN.

3rd Party Domain is the first clue this is a malicious email.

Staff, Employees XJTLU.EDU.CN.

Today, June 11th, 2021, We're migrating the entire email account of employees and Staff into the XJTLU.EDU.CN Outlook 2021 Office Webmail. As a result, all active employees and Staff must review and sign up for an urgent update and migration to improve the security and efficiency of current spam email.

Please all employees and Staff should CLICK HERE to switch to Outlook Webmail 2021 for employees and staff.

Note that this migration to Outlook 2020 applies to all emails in this service. We disable all unchecked and inactive email accounts that have not been migrated within the next 24 hours without further notice.

Best regards,

External email administrator
XJTLU.EDU.CN Outlook service for employees and internet service
Copyright 2021.
Xi'an Jiaotong-Liverpool University
111 Ren'ai Road
Suzhou Industrial Park
Suzhou
Jiangsu Province
P. R. China
215123

Phishing example

From: Professor Xi Youmin <jessicagraphis240898@gmail.com>
Sent: 2021 年 4 月 10 日 10:05
To: Youmin Xi <Youmin.Xi@xjtlu.edu.cn>
Subject: Urgent Request

Can i have a quick moment,Please drop me an email when you are available. Thanks

Regard
Professor Xi Youmin
Director, Executive Principal

2.4 Payload

- **Corruption** of system or data files
- **Theft of service** or make the system a **zombie agent** of attack as part of a botnet
- **Theft of information** from the system/keylogging
- Hiding its presence on the system to make it **stealthy**

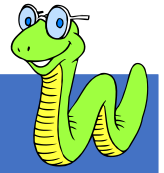
System corruption

- Data destruction

Chernobyl virus

- First seen in 1998
- Windows 95 and 98 virus
- Infects executable files and corrupts the entire file system when a trigger date is reached

Klez



- Computer worm that propagates via e-mail
- First appeared in 2001
- On trigger date causes files on the hard drive to become empty

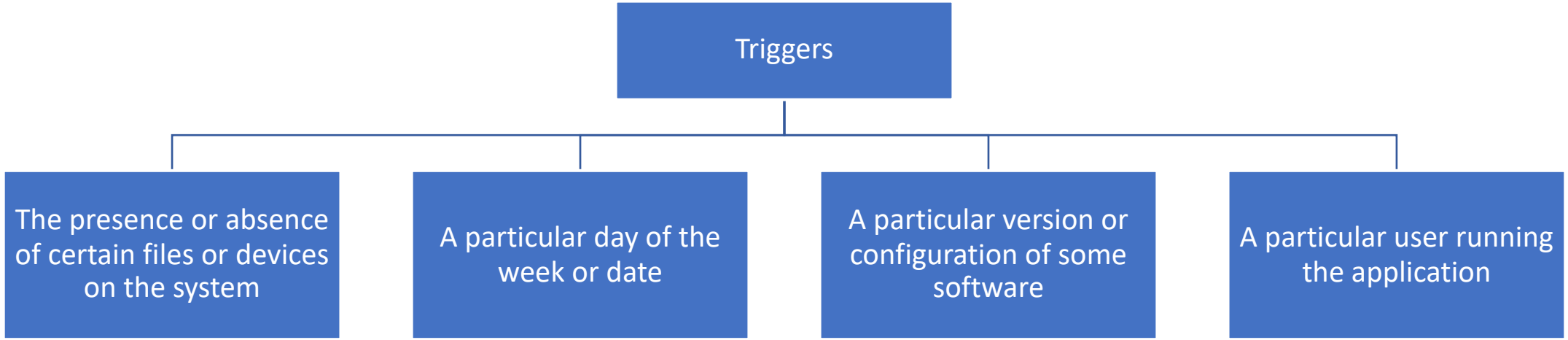
Ransomware

- Encrypts the user's data and demands payment in order to access the key needed to recover the information
- Recent ransomware demands the victim pay in Bitcoin.

System corruption

- Real-world damage
  - Chernobyl virus rewrites BIOS code

- Logic bomb
  - Code embedded in the malware that is set to “explode” when certain conditions are met



Attack agent

- Takes over another Internet attached computer and uses that computer to launch or manage attacks
- Botnet - collection of **bots** capable of acting in a coordinated manner

Uses

- Distributed denial-of-service (DDoS) attacks
- Spamming
- Sniffing traffic
- Keylogging
- Spreading new malware
- ...

Information theft

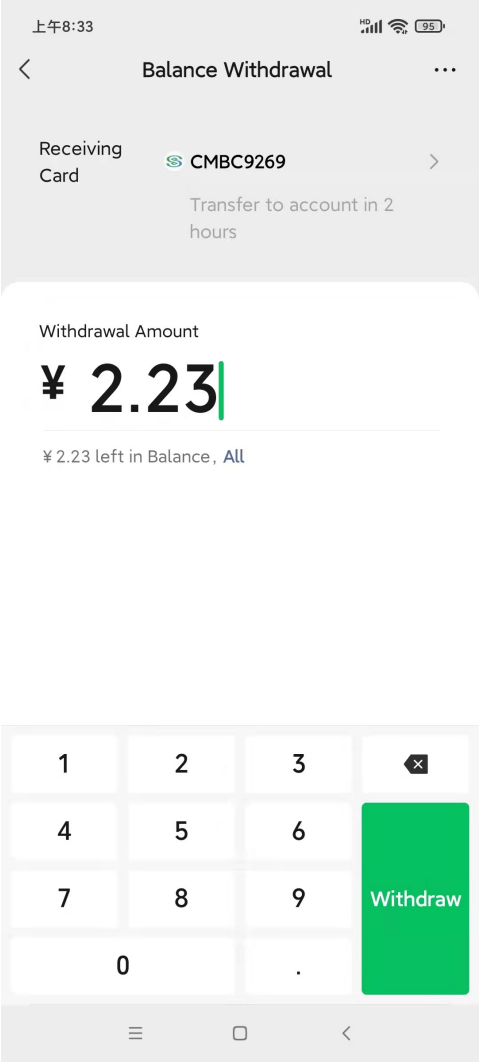
- Keyloggers, and Spyware

Keylogger

- Captures keystrokes to allow attacker to monitor sensitive information
- Typically uses some form of filtering mechanism that only returns information close to keywords (“login”, “password”)

Spyware

- Subverts the compromised machine to allow monitoring of a wide range of activity on the system
  - Monitoring history and content of browsing activity
  - Redirecting certain Web page requests to fake sites
  - Dynamically modifying data exchanged between the browser and certain Web sites of interest



Information theft

- Phishing: Exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source

From: "XJTLU.EDU.CN" <gillianadrianbayfordb@gmail.com>
Date: Friday, June 11, 2021 at 8:39 AM
Subject: Staff, Employees XJTLU.EDU.CN.

3rd Party Domain is the first clue this is a malicious email.

Staff, Employees XJTLU.EDU.CN.

Today, June 11th, 2021, We're migrating the entire email account of employees and Staff into the XJTLU.EDU.CN Outlook 2021 Office Webmail. As a result, all active employees and Staff must review and sign up for an urgent update and migration to improve the security and efficiency of current spam email.

Please all employees and Staff should CLICK HERE to switch to Outlook Webmail 2021 for employees and staff.

Note that this migration to Outlook 2020 applies to all emails in this service. We disable all unchecked and inactive email accounts that have not been migrated within the next 24 hours without further notice.

Best regards,

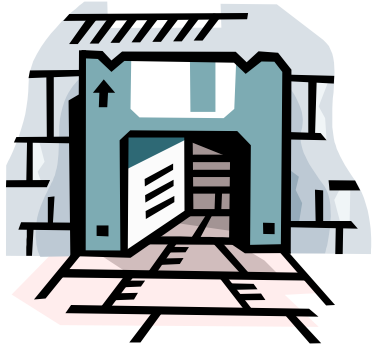
External email administrator
XJTLU.EDU.CN Outlook service for employees and internet service
Copyright 2021.
Xi'an Jiaotong-Liverpool University
111 Ren'ai Road
Suzhou Industrial Park
Suzhou
Jiangsu Province
P. R. China
215123

Include a URL in a spam e-mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site

Suggests that urgent action is required by the user to authenticate their account

Attacker exploits the account using the captured credentials

Stealthing



- Backdoor
  - Also known as a trapdoor
  - Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
  - Maintenance hook is a backdoor used by Programmers to debug and test programs

- Malware that has taken over a machine often inserts a trapdoor
  - To allow the attacker to get back in
  - Infected machine should be handled carefully to remove such trapdoors

Stealthing

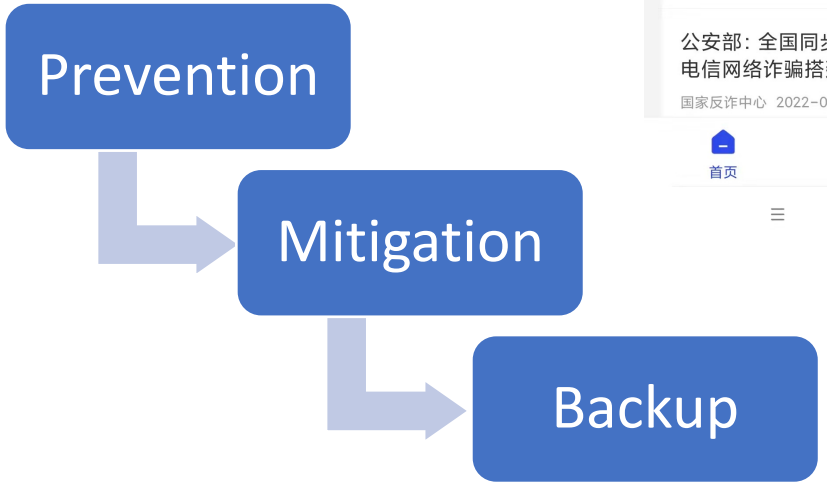
- Rootkit
  - Software designed to maintain illicit access to a computer
  - Installed after attacker has gained very privileged access on the system
  - Goal is to ensure continued privileged access
    - By hiding presence of malware
    - By defending against removal

3. Countermeasures

Malware countermeasure approaches

- Prevention
  - Policy
  - Ensure all systems are as current as possible
    - Reduce vulnerabilities
  - Set appropriate access controls on the applications and data
  - Provide appropriate user awareness and training

- Threat mitigation options:
  - Detection
  - Identification
  - Removal



General requirements for countermeasures

- Generality
- Timeliness
- Resiliency
- Minimal denial-of-service costs
- Transparency
- Global and local coverage

Generations of anti-virus

First generation: simple scanners

- Requires a malware signature to identify the malware
- Another approach is length checking

Second generation: heuristic scanners

- Uses heuristic rules to search for probable malware instances
- Another approach is integrity checking

Third generation: activity traps

- Identify malware by its actions rather than its structure in an infected program

Fourth generation: full-featured protection

- Packages consisting of a variety of anti-virus techniques used in conjunction

Generic decryption

- Enables the anti-virus program to easily detect complex polymorphic viruses and other malware while maintaining fast scanning speeds

- Executable files are run through a GD scanner which contains the following elements:
  - CPU emulator
  - Virus signature scanner
  - Emulation control module

Host-based behavior-blocking software

- Integrates with the operating system of a host computer and monitors program behavior in real time for malicious action
  - Blocks potentially malicious actions before they have a chance to affect the system
  - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics

- Limitations
  - Because malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked

Summary

- Overview of malware
- Common types of malware
  - Propagation
    - Infected Content: Viruses
    - Vulnerability Exploit: Worms
    - Social Engineering: Spam E-Mail, Trojans
  - Payload
    - System Corruption
    - Attack Agent: Zombie, Bots
    - Information Theft: Keyloggers, Phishing, Spyware
    - Stealthing: Backdoors, Rootkits
- Countermeasures