Lec 19: Malware

CSED415: Computer Security

Spring 2025

Seulbae Kim

POSTECH

POHANG UNIVERSITY OF SCIENCE AND TECHNOLOGY

Recap

- Authentication and access control = “gatekeepers” that protect resources
- What happens if an attacker installs software that bypasses those gatekeepers?
- Today’s topic: Malware

Malware

Malware is malicious software

- NIST SP 800-83 definition:
  - Malware is a program that is covertly inserted into a system 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

Representative species

- Virus
- Worm
- Trojan horse
- Rootkit
- Backdoor
- Spyware
- Bots
- Ransomware

Computer Virus

Virus

- Definition: A program that can “infect” other programs
- First appeared in 1980s
- Term coined by Fred Cohen
  - “Computer Viruses: Theories and Experiments,” Computers and Security, Vol. 6, 1984

Virus

- Biological viruses
  - Tiny scraps of genetic code (DNA/RNA) that can take over the machinery of a living cell
  - Tricks the cell into making replicas of the original virus
  - Key properties: Replication and propagation

Virus

- Computer viruses
  - Key properties: Copy (replication) & embedding (propagation)
  - Carries the code for making copies of itself
  - Gets embedded in a host program
  - Searches for uninfected programs and copies itself into them
  - Conduct malicious activities after infecting host programs

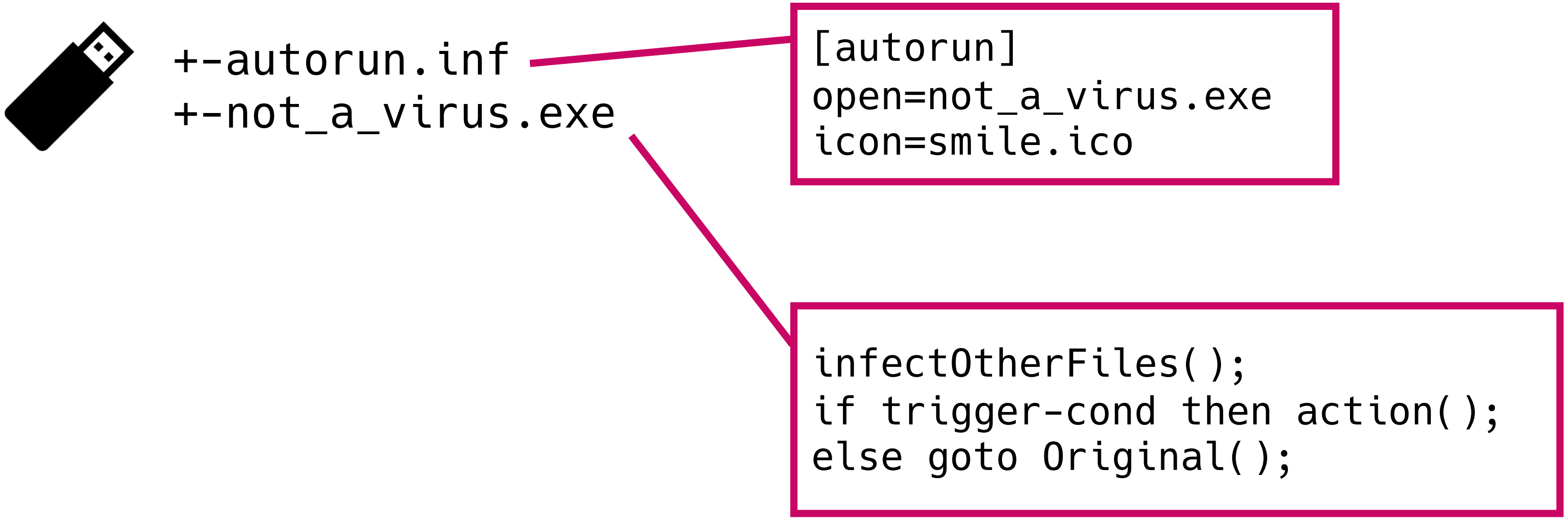
History of virus

- Pre-1990s
  - Operating systems had no inter-process isolation
  - A virus could easily infect all executables on a system
  - These executables were copied to other computers via floppy disks
    - exe: Statically linked all-in-one package

image: Wikipedia

History of virus

- Autorun era
  - Pre-modern operating systems had flawed access control
  - e.g., “Autorun” feature for USB drives (before Windows 7)



```
+-autorun.inf
+-not_a_virus.exe
```

```
[autorun]
open=not_a_virus.exe
icon=smile.ico
```

```
infectOtherFiles();
if trigger-cond then action();
else goto Original();
```

History of virus

- Modern computers have access control
  - It does not make sense to copy-paste powerpoint.exe to other computers anymore
  - New trend: Macro viruses
    - Attackers insert macro viruses into document files (e.g., *.xls, *.doc)
    - Macro viruses are platform independent
      - Works on any OS with MS Office installed
    - These files are not protected by the same access controls as programs

Macro virus example

- Microsoft Visual Basic for Application (VBA) macro example
  - Intended usage: Automation within a document
  - Malicious usage:

```
Private Sub Workbook_Open()
    txt = "You are doomed :)"

    Dim i As Integer

    For i = 1 To 10000
        MsgBox txt
    Next i

End Sub
```

  - Viral usage:

```
Sub bad_behavior()
    ...
End Sub

Private Sub Workbook_Open()
    overwrite_global_macro_template()
    bad_behavior()
End Sub
```

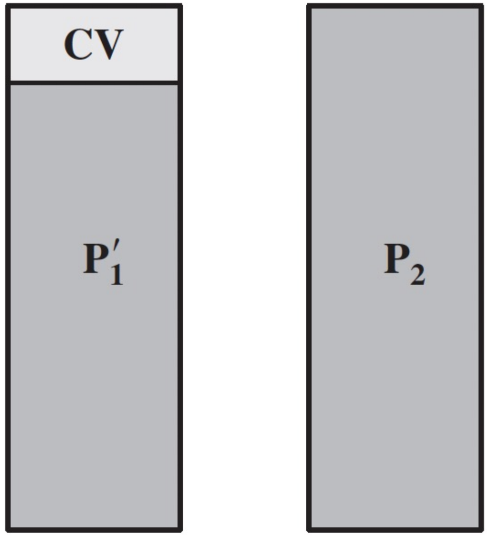
→ Propagation: Send an email with a macro-activated file attached

Example: Compression virus (CV)

```
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 (t0)
      attach-to-program;
      uncompress rest of this file into tmpfile; // t3
      execute tmpfile; // t4
end;
```



t0:

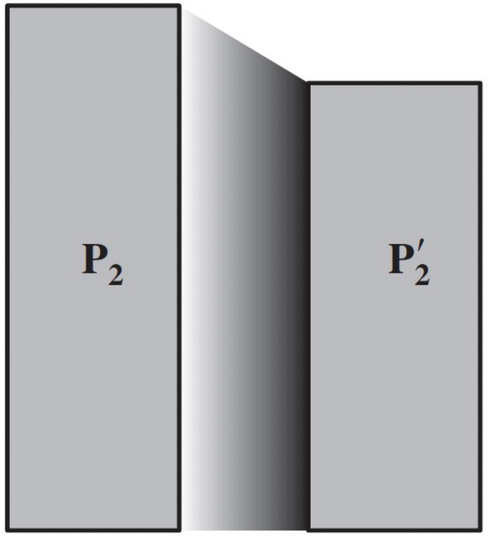
P_1' is an infected version of P_1.
P_2 is uninfected.
When P_1 is invoked, the main action block is executed first.

Example: Compression virus (CV)

```
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 (t0)
       attach-to-program;
       uncompress rest of this file into tmpfile; // t3
       execute tmpfile; // t4
end;
```



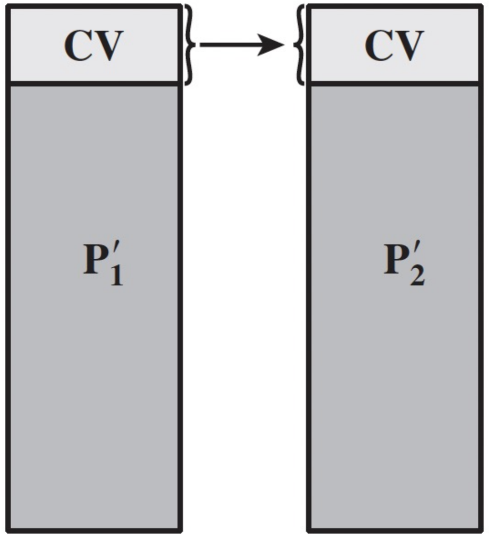
t1:
The virus searches for and compresses uninfected programs (e.g., P_2 into P_2')

Example: Compression virus (CV)

```
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 (t0)
    attach-to-program;
    uncompress rest of this file into tmpfile; // t3
    execute tmpfile; // t4
end;
```



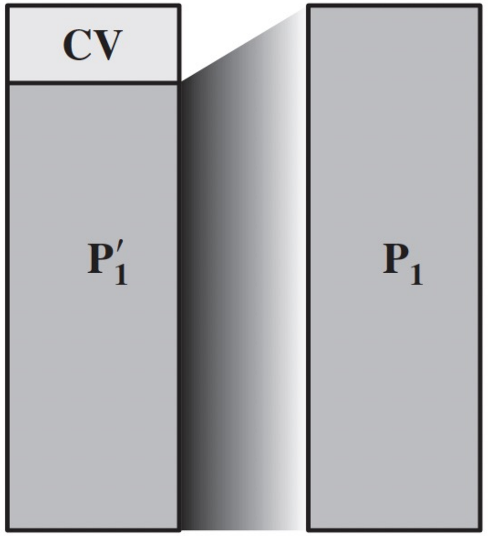
t2:
A copy of CV is prepended to the compressed program

Example: Compression virus (CV)

```
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 (t0)
      attach-to-program;
      uncompress rest of this file into tmpfile; // t3
      execute tmpfile; // t4
end;
```



t3:

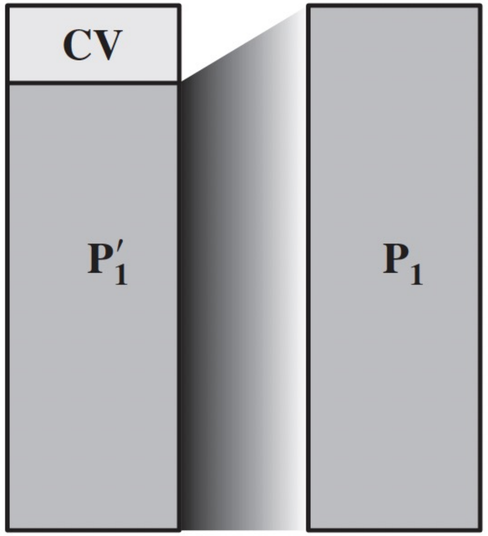
The compressed progrm (P_1') is uncompressed so it can be executed

Example: Compression virus (CV)

```
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 (t0)
    attach-to-program;
    uncompress rest of this file into tmpfile; // t3
    execute tmpfile; // t4
end;
```



t4:

The uncompressed original program (P_1) is executed

The virus does not alter the original functionality while propagating

Worm

Worm

- Definition
  - A program that actively seeks out more machines to infect
  - Worm exploits software vulnerabilities in client or server programs
  - Use network connections to spread to remote systems
- vs Virus
  - Virus needs a host program to infect
  - Worm is a self-contained program that does not need hosts

Recall: Morris Worm

- The very first internet worm (1988)
  - Infected over 6,000 computers online
    - Out of 60,000 online hosts

Robert Morris

Creator of *Morris Worm*
Graduate student at Cornell
(Now a tenured professor at MIT)

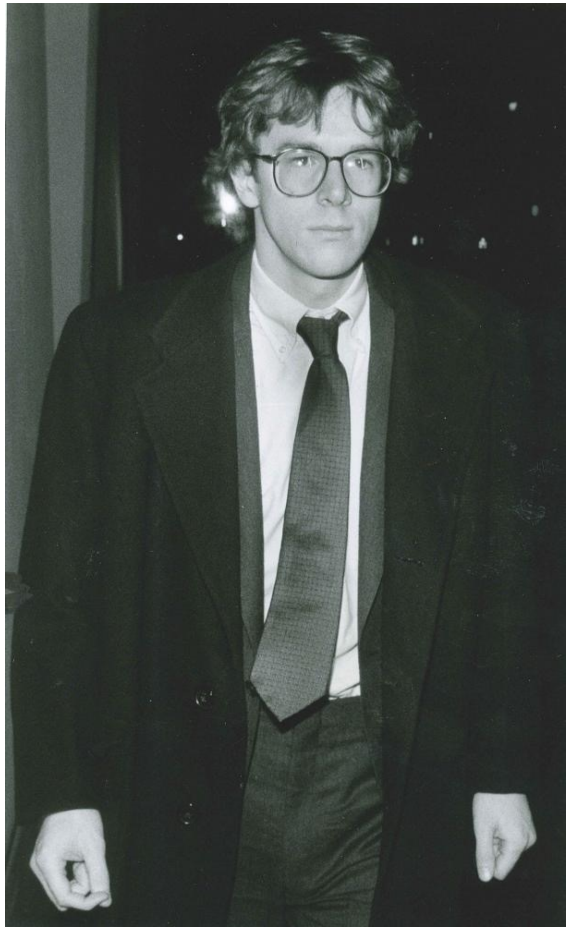


Photo by Stephen D. Cannerelli

Morris Worm

- Exploited a buffer overflow vulnerability in `fingerd`
  - `fingerd` is a root-privileged daemon that provides user and system information upon remote request
  - Implementation (simplified):

```c
/* morris.c */
int main(int argc, char* argv[]) {
  char buffer[512]; // to store remote requests
  gets(buffer); // oops!
  return 0;
}
```

  - Compilation:

```
$ gcc -O0 -fno-stack-protector -fno-pic -no-pie -z execstack morris.c -o morris
```

Worm propagation model

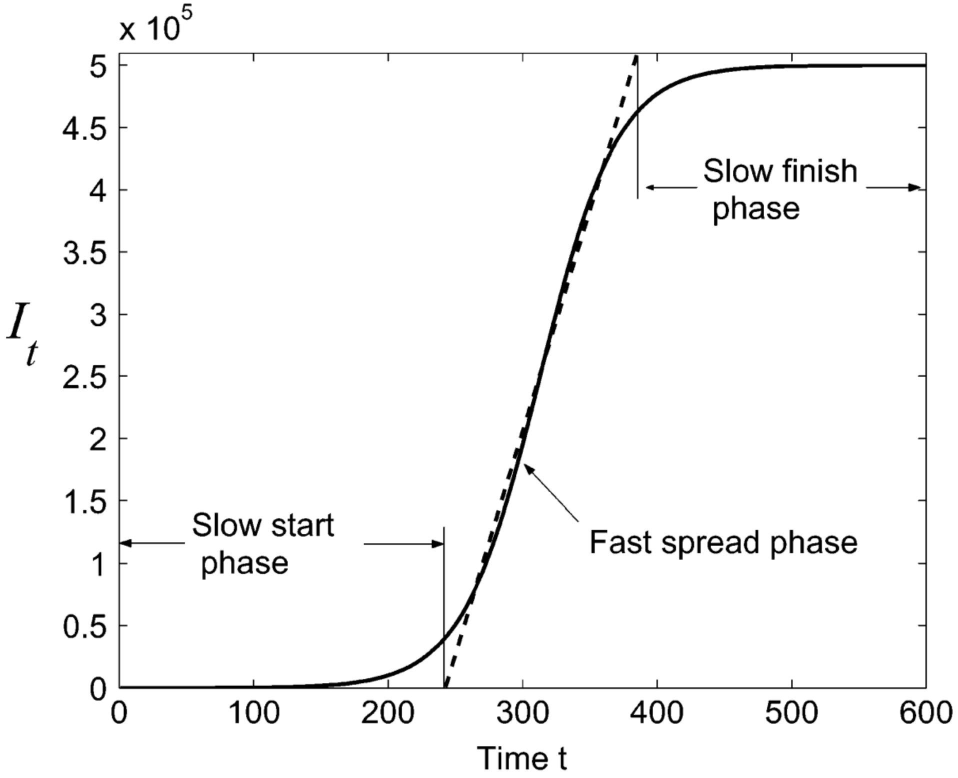
$$\frac{dI(t)}{dt} = \beta * I(t) * \left(N - I(t)\right)$$

where

- $I(t)$ = Number of individuals infected as of time t
- β = Pairwise rate of infection
- N = Size of the entire population

Worm propagation model

$$\frac{dI(t)}{dt} = \beta * I(t) * \left(N - I(t)\right)$$



- Slow start phase
  - $N - I(t) \approx N$
  - Not many infected hosts to spread virus
- Fast spread phase
  - $N - I(t) \approx I(t)$
  - Rapid infection
- Slow finish phase
  - $N - I(t) \approx 0$
  - Not many remaining uninfected hosts

Trojan Horse

Trojan horse

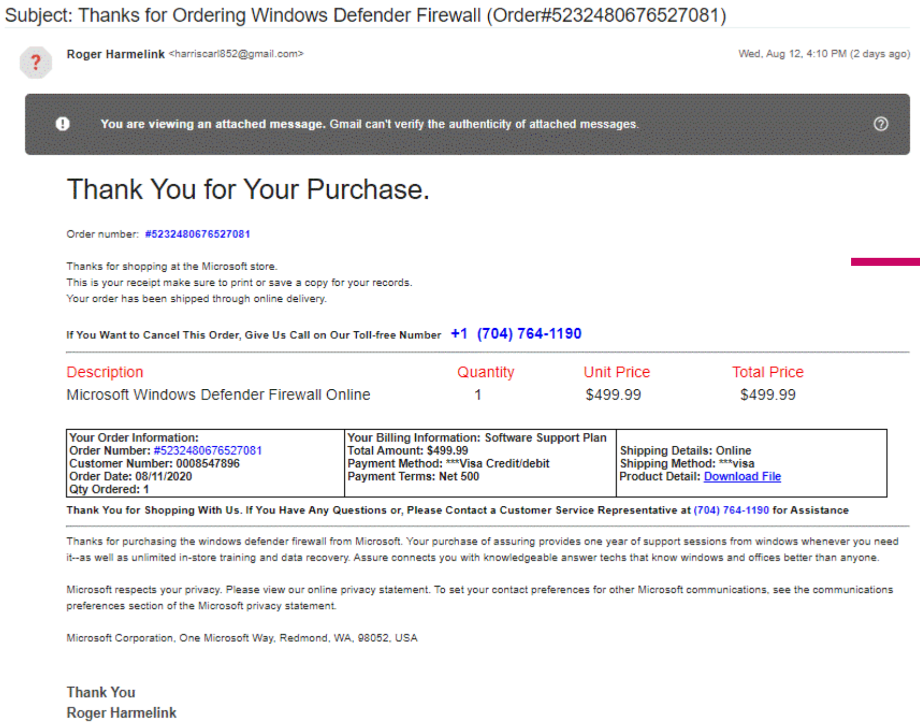
- Trojan horse in Greek mythology
  - Used by the Greeks to infiltrate the city of Troy
  - They sent a large wooden horse as a gift to the Trojans
  - Trojans accepted the gift, taking it into the city
  - Greek soldiers were hiding inside the horse
  - That night, the Greeks emerged from the horse and initiated an attack from inside the city

Trojan horse

- Definition
  - An apparently useful computer program or utility that contains hidden code that, when invoked, performs some unwanted or harmful function
  - A type of malware disguised as legitimate software

Trojan horse

- Propagation vectors
  1. Social engineering: Tricks users into downloading and installing it
     - Email, social media, phishing, …



Subject: Thanks for Ordering Windows Defender Firewall (Order#5232480676527081)

Roger Harmelink <harriscarl852@gmail.com> Wed, Aug 12, 4:10 PM (2 days ago)

You are viewing an attached message. Gmail can't verify the authenticity of attached messages.

Thank You for Your Purchase.

Order number: **#5232480676527081**

Thanks for shopping at the Microsoft store.
This is your receipt make sure to print or save a copy for your records.
Your order has been shipped through online delivery.

If You Want to Cancel This Order, Give Us Call on Our Toll-free Number +1 (704) 764-1190

Description	Quantity	Unit Price	Total Price
Microsoft Windows Defender Firewall Online	1	$499.99	$499.99

Your Order Information: Order Number: #5232480676527081 Customer Number: 0008547896 Order Date: 08/11/2020 Qty Ordered: 1	Your Billing Information: Software Support Plan Total Amount: $499.99 Payment Method: ***Visa Credit/debit Payment Terms: Net 500	Shipping Details: Online Shipping Method: ***visa Product Detail: Download File

Thank You for Shopping With Us. If You Have Any Questions or, Please Contact a Customer Service Representative at (704) 764-1190 for Assistance

Thanks for purchasing the windows defender firewall from Microsoft. Your purchase of assuring provides one year of support sessions from windows whenever you need it--as well as unlimited in-store training and data recovery. Assure connects you with knowledgeable answer techs that know windows and offices better than anyone.

Microsoft respects your privacy. Please view our online privacy statement. To set your contact preferences for other Microsoft communications, see the communications preferences section of the Microsoft privacy statement.

Microsoft Corporation, One Microsoft Way, Redmond, WA, 98052, USA

Thank You
Roger Harmelink

→ Thanks for shopping at the Microsoft store. This is your receipt. Your order has been shipped through online delivery. Total price: $499.99

Product Detail: Download File

Trojan horse

- Propagation vectors
  2. Drive-by-download: Download and install malware without the user’s knowledge or consent
     - Exploit browser and plugin vulnerabilities
     - When the user views an attacker-controlled webpage, malware is downloaded and executed

Adobe Flash (1993-2020)

Started as a “rich internet application”
→ i.e., for creating moving web, animations, … (multimedia)

Became bloated with functions and privileges
→ Give websites privileges to run system functions through browsers (e.g., execute a program from a web page!)

Caused too many security issues, including drive-by-download attacks
→ Officially discontinued in 2020. HTML5 became the web standard.

Trojan horse

- Propagation vectors
  3. Supply-chain trojan
     - Malicious code inserted before the software reaches customers
       - e.g., Inside the vendor’s build, update or distribute pipeline
     - Bypasses perimeter & endpoint defenses because the code arrives digitally signed and delivered by a trusted source
     - Example: SolarWinds Orion (2020) attack (recall: Lecture 04)
       - Flagship IT-monitoring and network management suite
       - Attacker gains access to SolarWinds build environment and inserts malicious code
       - Trojanized update posted to Orion download portal
       - Customer installs update → The trojan horse is installed

Targeted Trojan horse

- Watering-hole attacks
  - Attacker profiles victims and the websites they frequently visit
  - Attacker tests these websites for vulnerabilities
  - Attacker compromises a vulnerable website and injects an exploit leading to drive-by-download attacks
  - User, visiting the compromised website, gets infected

image: Threatpost

Summary

- Virus/worm/trojan differ in propagation mechanism
  - Virus: Propagate through infecting existing executables or contents
  - Worm: Propagate through exploiting software vulnerabilities
  - Trojan: Propagate through social engineering / supply chain attacks

Spyware

Spyware

- Definition
  - Software that collects information from a computer and covertly transmits it to another system

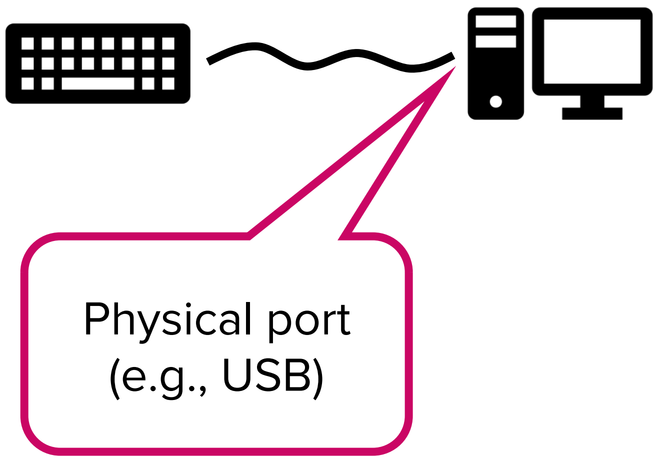
- Typical payloads
  - Keystrokes
  - Screen or webcam feed
  - Network traffic
  - Application logs

Spyware

- Keylogger
  - Captures keystrokes on the infected machine to allow an attacker to monitor sensitive information

Spyware

- How does a keylogger work?

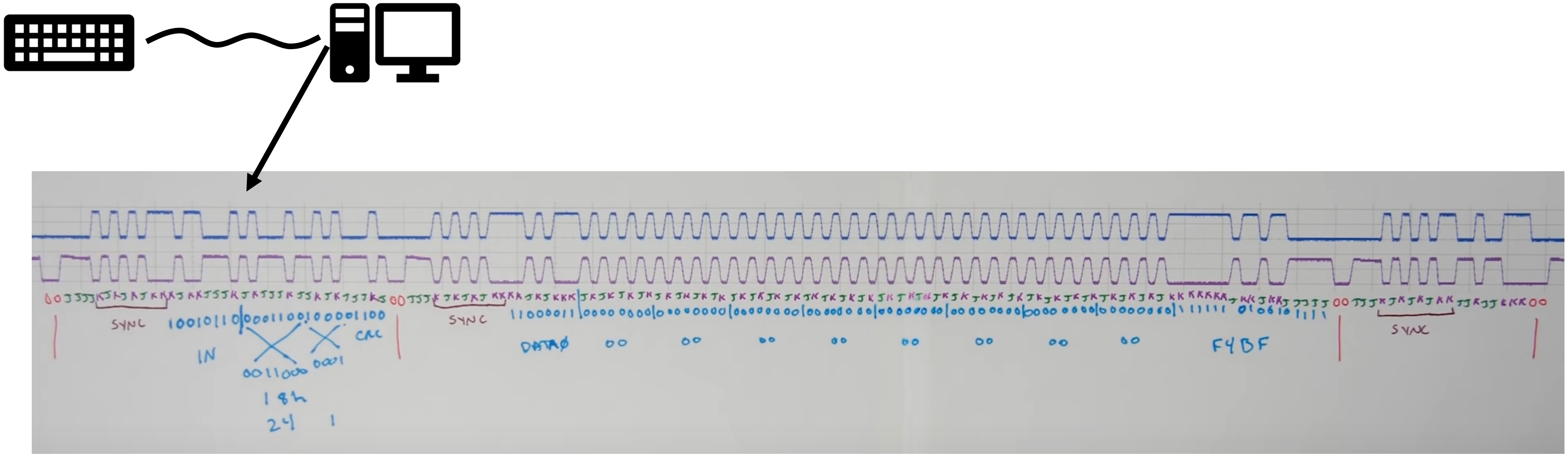


Physical port (e.g., USB)

Keystrokes are electronic signals

Spyware

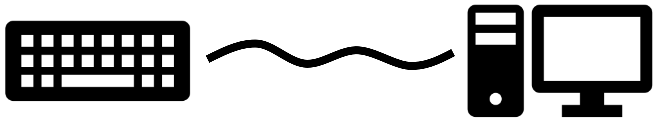
- How does a keylogger work?



Kernel’s keyboard device driver decodes the signal and maps it to keycodes and triggers an interrupt request to the CPU

Spyware

- How does a keylogger work?



The kernel has a buffer to store these keycodes until they are read by processes

A keylogger reads the kernel buffer
and exfiltrates data

Spyware

- Mitigations
  - On-screen keyboard / PIN pads for banking
    - Not a fundamental solution. Why?
  - OS-level input filtering (e.g., macOS TCC – Transparency, Consent, and Control)
    - Give least privilege to applications – default deny
      - e.g., Zoom application requests webcam access
      - A keylogger must request keystroke monitor permissions, and users can quickly notice its malicious intent

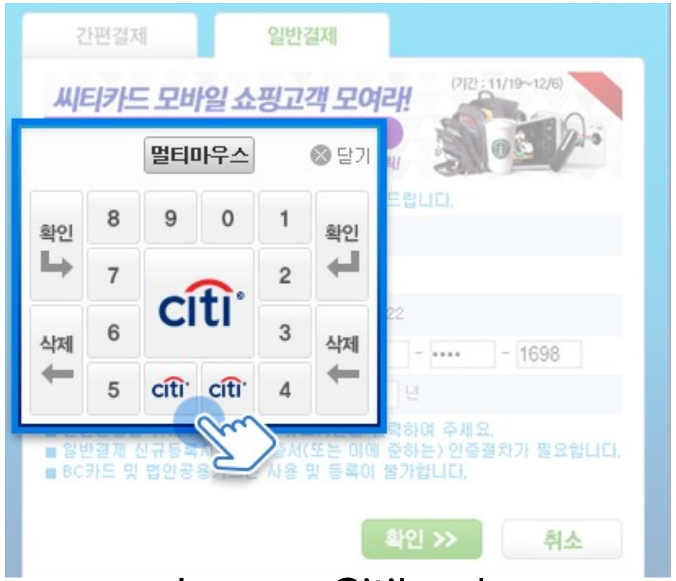

간편결제
일반결제
씨티카드 모바일 쇼핑고객 모여라!
(기간 : 11/19~12/6)
멀티마우스
닫기
확인
8
9
0
1
확인
7
citi
2
삭제
6
3
삭제
5
citi
citi
4
드립니다.
22
••••
1698
년
력하여 주세요.
■ 일반결제 신규등록 증서(또는 이에 준하는) 인증절차가 필요합니다.
■ BC카드 및 법인공용 사용 및 등록이 불가합니다.
확인 >>
취소

Image: Citibank

Rootkits and Backdoor

Rootkits

- Definition
  - A set of programs that grant administrator access to unauthorized entities
  - Makes malicious and stealthy changes to the host OS
  - May hide its existence, e.g.,
    - Override the `ps` command to not show the rootkit process
    - Override the `ls` command to not show malicious files

Rootkits

- Syscall table maps syscall # with actual implementations
  - Kernel-mode rootkits can modify syscall table entries to invoke malicious syscalls instead of the legitimate routine

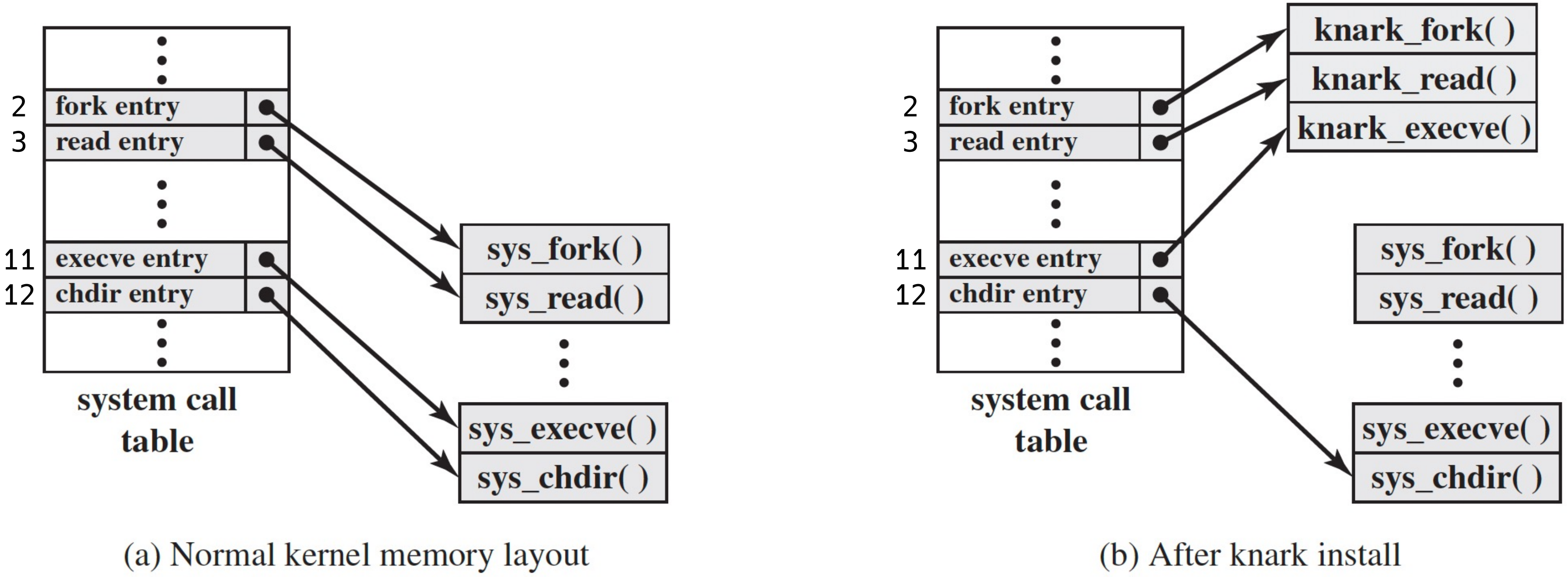


Figure 6.3 System Call Table Modification by Rootkit

Backdoor

- Definition
  - Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system
  - Often inserted by developers
    - vs Rootkits are often inserted by hackers

Backdoor examples

- Some routers are shipped with backdoors inserted

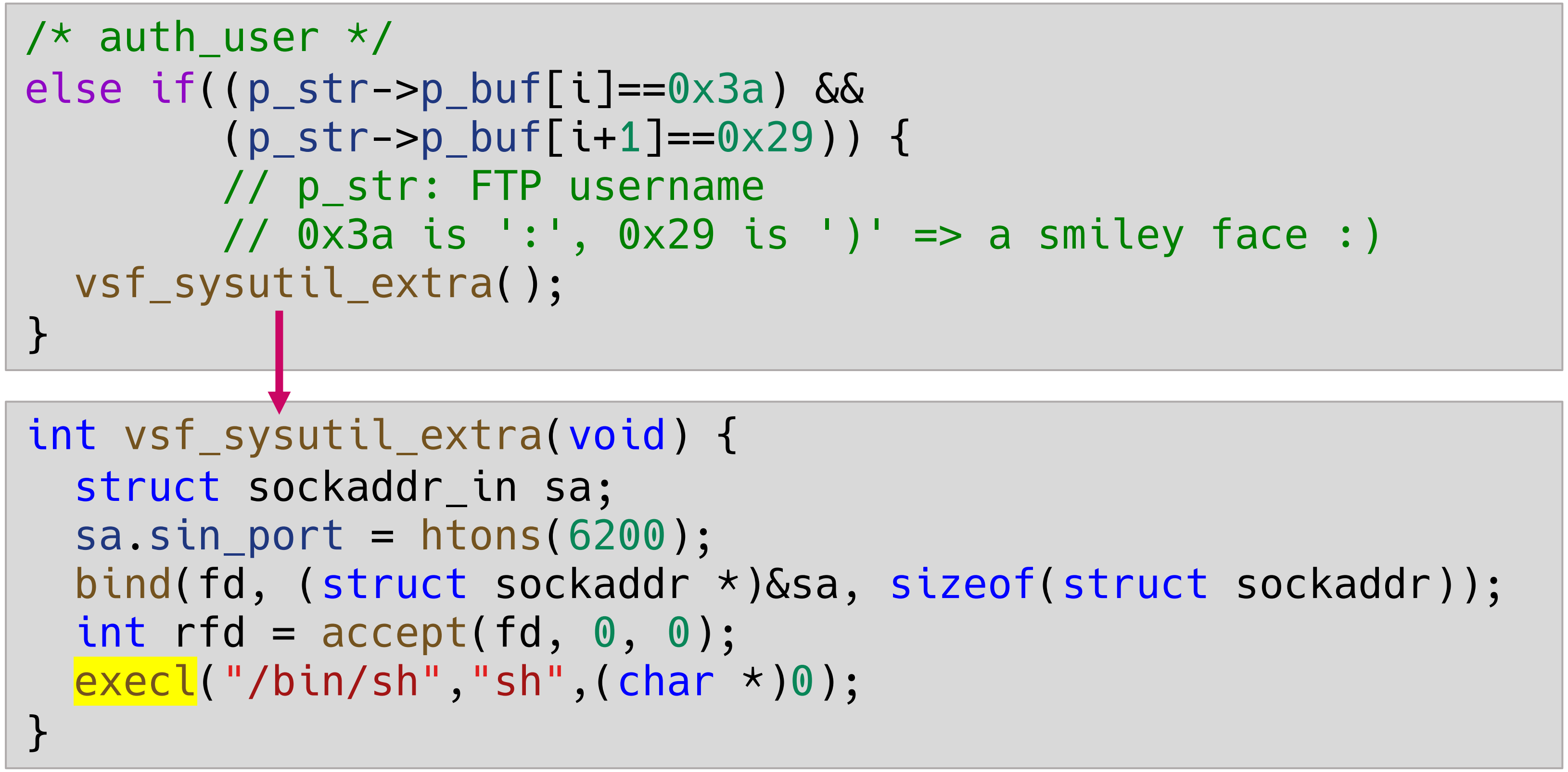
D-Link DIS-100
- Hard-coded string in User-Agent bypasses HTTP authentication

```
int alpha_auth_check(struct http_request_t *req) {
  if(strstr(req->url, "graphic/") ||
     strstr(req->url, "public/") ||
     strcmp(req->user_agent, "xmlset_roodkcableoj28840ybtide") == 0) { return AUTH_OK; }
  else {
     if(check_login(request->0xC, request->0xE0) != 0) { return AUTH_OK; }
  }
  /* ... */
```

edit by 04882 joel backdoor

Backdoor examples

- vsftpd 2.3.4: A backdoored file transfer protocol (FTP) server



```c
/* auth_user */
else if((p_str->p_buf[i]==0x3a) &&
        (p_str->p_buf[i+1]==0x29)) {
        // p_str: FTP username
        // 0x3a is ':', 0x29 is ')' => a smiley face :)
  vsf_sysutil_extra();
}
```

```c
int vsf_sysutil_extra(void) {
  struct sockaddr_in sa;
  sa.sin_port = htons(6200);
  bind(fd, (struct sockaddr *)&sa, sizeof(struct sockaddr));
  int rfd = accept(fd, 0, 0);
  execl("/bin/sh","sh",(char *)0);
}
```

FTP login attempt with username staring with :) opens a shell on TCP port 6200

SK Telecom user info leak (April 2025)

- Malware used: BPFDoor
  - BPF (Berkeley Packet Filter): OS-level network packet filter
  - BPFDoor: Backdoor that hides in BPF filter
    - A single “magic” packet opens a reverse shell
      - Magic packet received → BPFDoor filter rule triggered → Open a reverse shell to the source IP of the packet
    - The attacker connects to the server via the reverse shell
  - SK Telecom’s user information, mobile identifiers, and keys have been exfiltrated → Can be used for SIM swapping attacks (recall: Lecture 16)

Bot (Zombie)

Bot

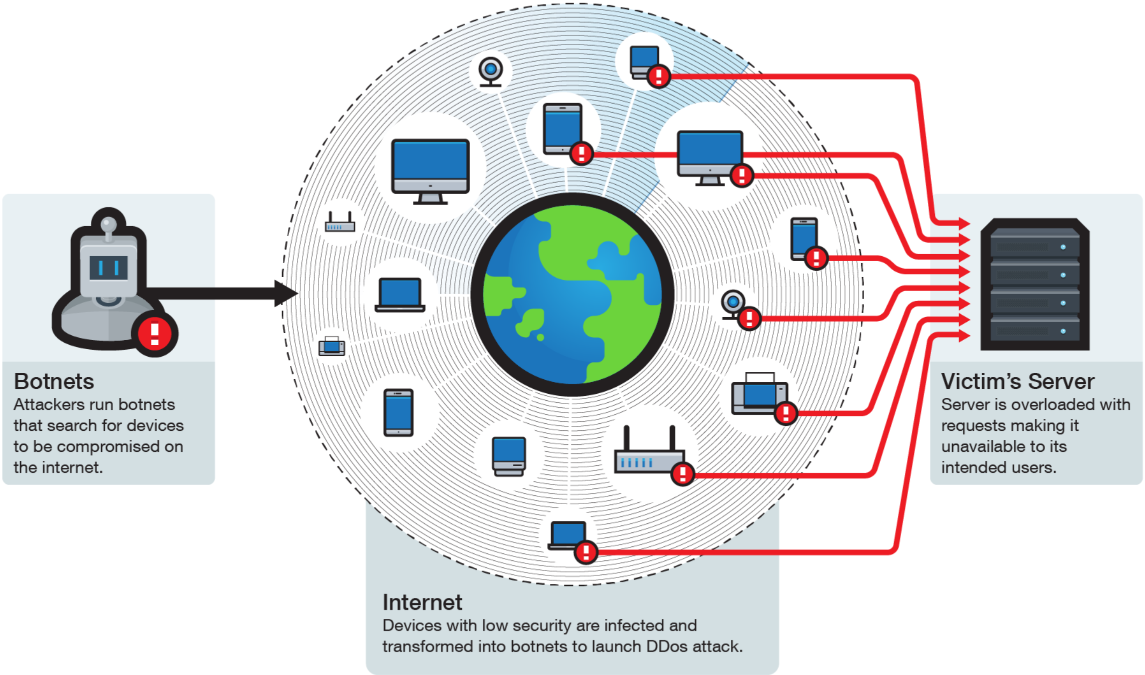
- Definition
    - A malware agent that can be remotely controlled to launch attacks on other machines
- Botnet
    - Collection of bots

Bot

- Bots utilize frequently used internet protocols
  - IRC (internet relay chat), HTTPS, Blockchain, Discord webhooks, …
- Command and Control (C&C) server
  - For controlling botnet
  - Workflow:
    - All bots in a botnet connect to a server (e.g., Discord) and joins a specific channel
    - The C&C server commands the connected bots in the channel

Uses of bots

- DDoS
  - Stream of requests from multiple bots to a server results in DoS
    - HTTP (GET, POST, HEAD), TCP (SYN, RST, FIN, ACK, PSH), UDP (DNS, ICMP) flooding attacks



Botnets
Attackers run botnets that search for devices to be compromised on the internet.

Internet
Devices with low security are infected and transformed into botnets to launch DDos attack.

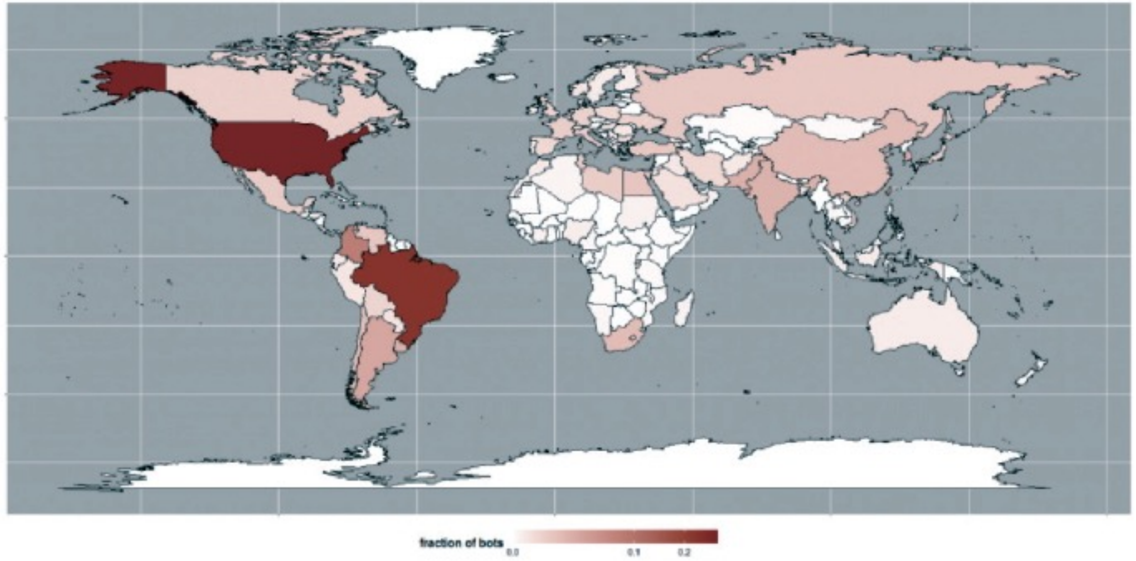
Victim's Server
Server is overloaded with requests making it unavailable to its intended users.

Uses of bots

- Cryptojackers
  - Cryptocurrency miners are embedded in bots
  - When commanded, they start mining
    - Steals electricity and CPU instead of data

Mirai Botnet

- One of the biggest botnet incidents
  - Primarily targeted IoT devices with weak security
    - Embedded systems typically lack security mitigations due to their resource-constrained nature and slow updates
  - Infected over 100,000 devices at all over the world



Mirai Botnet

- One of the biggest botnet incidents
  - Launched a DDoS attack
    - Throughput peaked at 1.5 Tbps (unprecedented!)
  - The developer released Mirai botnet’s source code online
    - Led to copycat crimes

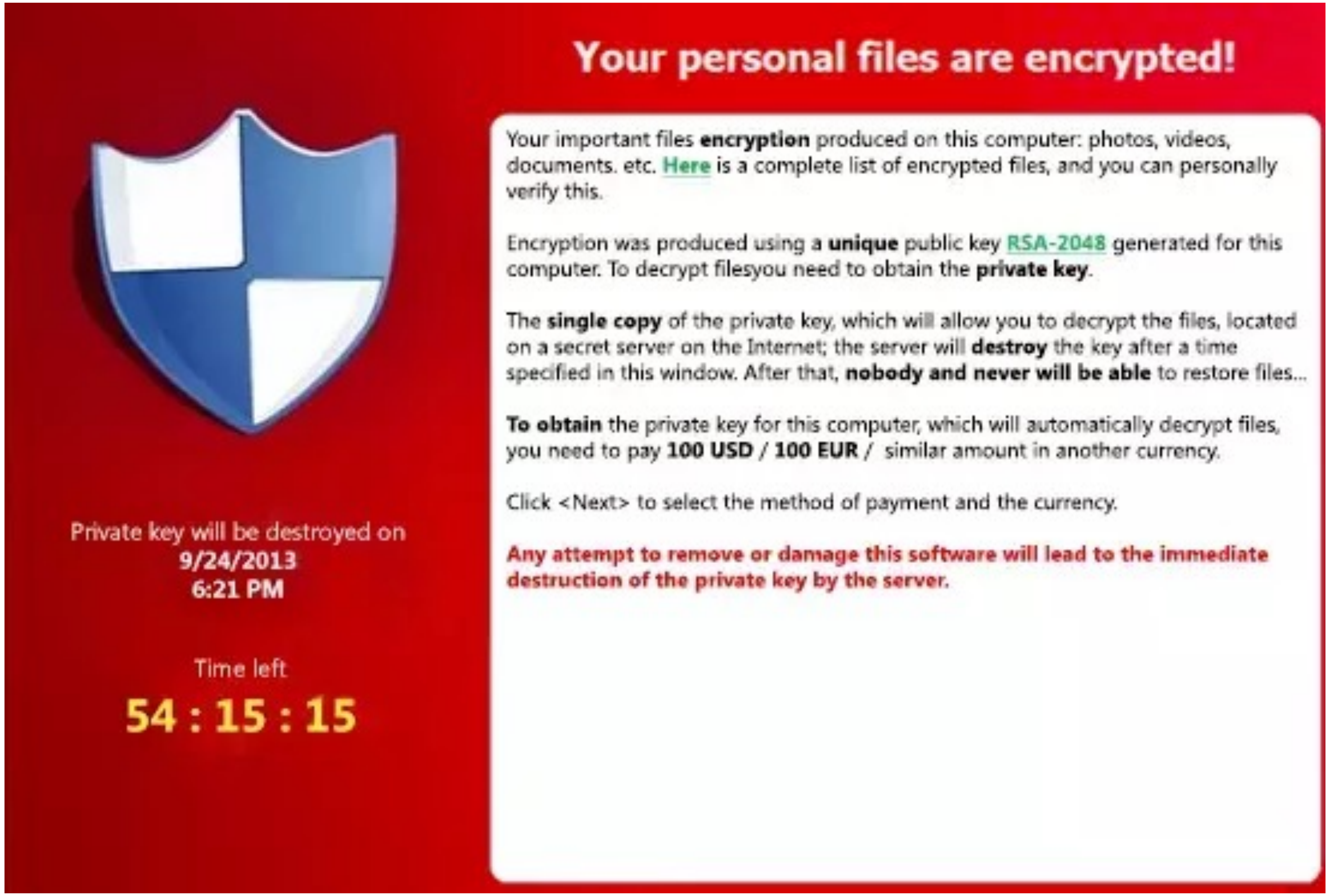
Ransomware

Ransomware

- Negative usage of cryptography
  - Attacker generates a key pair <k_s, k_p> and embeds the public key k_p in the malware
  - Malware generates a symmetric encryption key k_E and encrypts the victim’s data with the key (e.g., using AES)
  - Malware encrypts k_E using k_p and deletes k_E
  - Victim sees ransom note containing encrypted k_E and payment instructions
  - When the payment is received, the attacker decrypts k_E with his/her secret key k_s and (sometimes) sends k_E to the victim

Ransomware examples

- CryptoLocker (2013)
  - Encrpyts all files with RSA-2048 key
  - *.encrypted



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

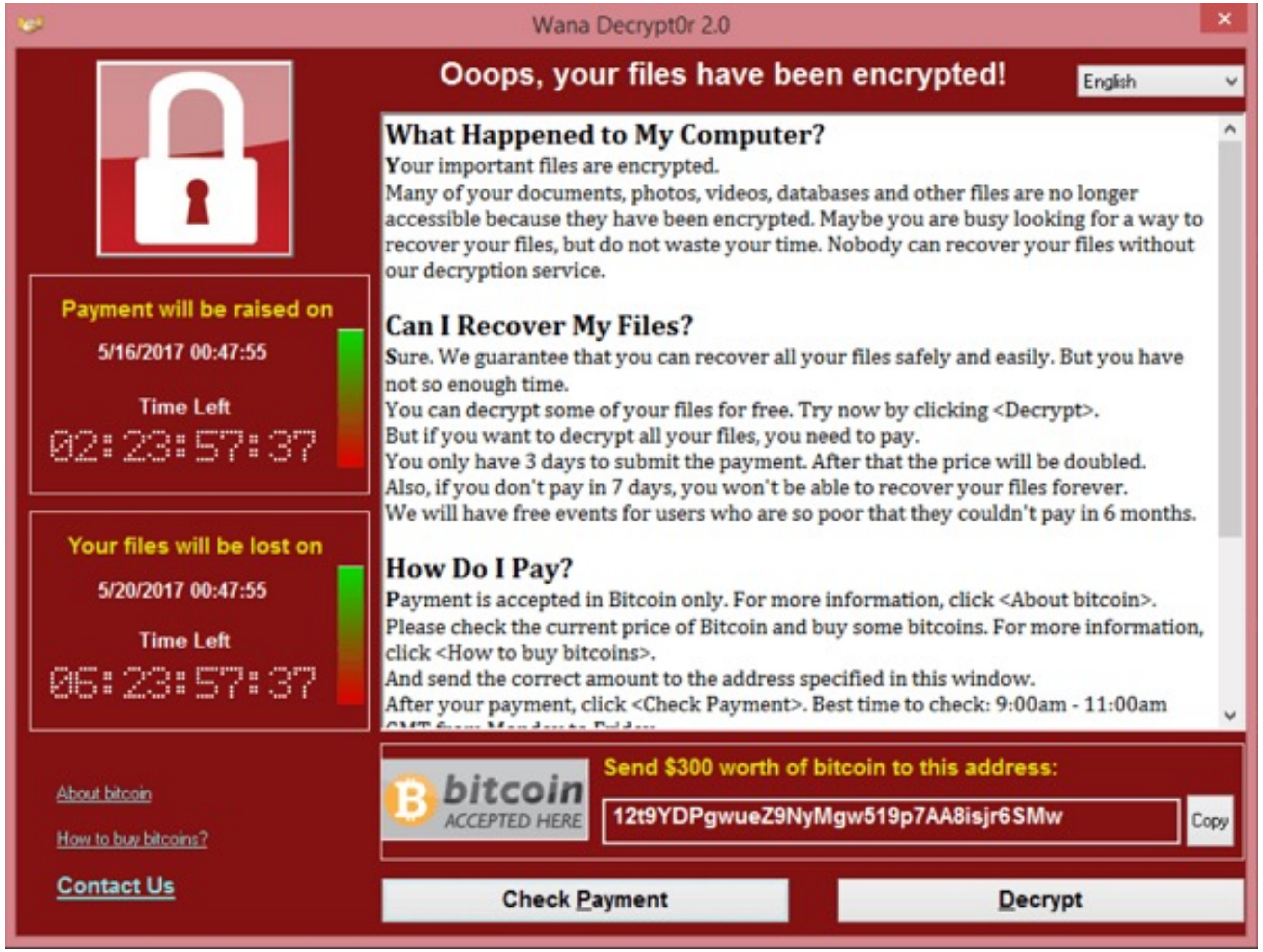
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Ransomware examples

- WannaCry (2017)
  - Exploits Windows SMB (server message block) protocol to get privilege escalation
    - comm. protocol exposed to the network
  - Encrypts all files and asks for ransom



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Summary

- Spyware/rootkits & backdoor/bots/ransomware differ in malicious activity
  - Spyware: Data theft (exfiltration)
  - Rootkits and Backdoor: Infiltration
  - Bot: Denial of service
  - Ransomware: Data destruction

Coming up next

- How can we fight back?
  - Anti-malware techniques

Questions?