CS 370
Introduction to Security

Malware

Oregon State University

Topics For Today

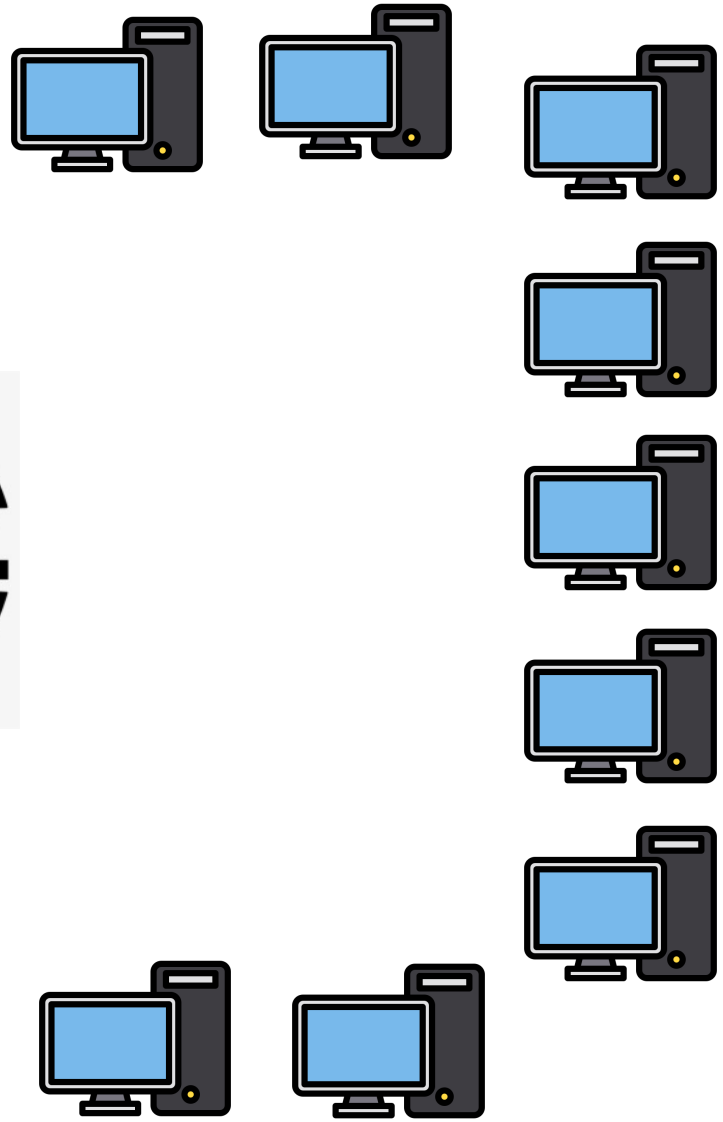
- Malware
- Example Malware Attacks
- State-sponsored Malware Attacks

What is a Malware?

- Software that runs malicious activity

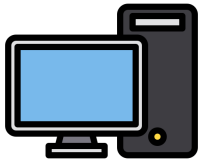
- What are the malicious activities?
  - Attack others machine to hack more computers
  - Run a surveillance on the machine and leak private secret data from them
  - Access to user’s accounts available on victim machine
  - Break the machine
  - Encrypt data and ask for a ransom (Ransomware)
  - Secretly running cryptocurrency mining job in a background
  - …

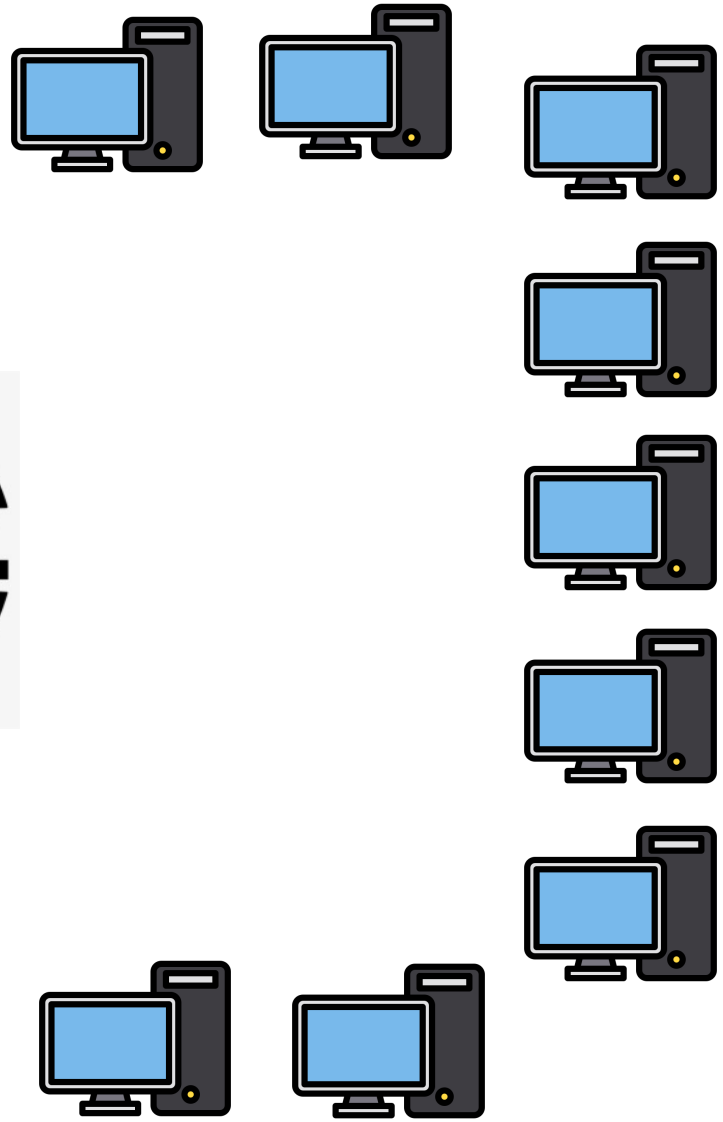
Malware Operations in a Nutshell



Malware Operations in a Nutshell

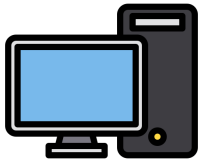
Write a malware



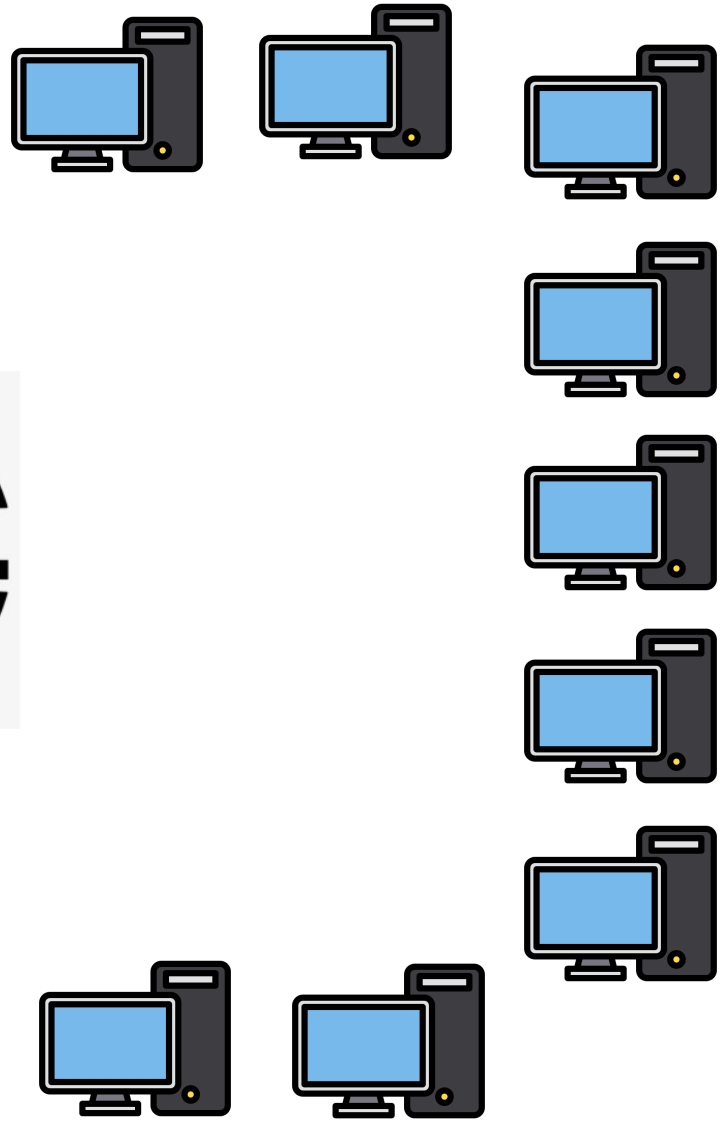


Malware Operations in a Nutshell

Write a malware

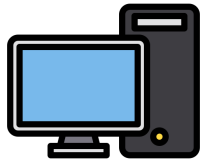


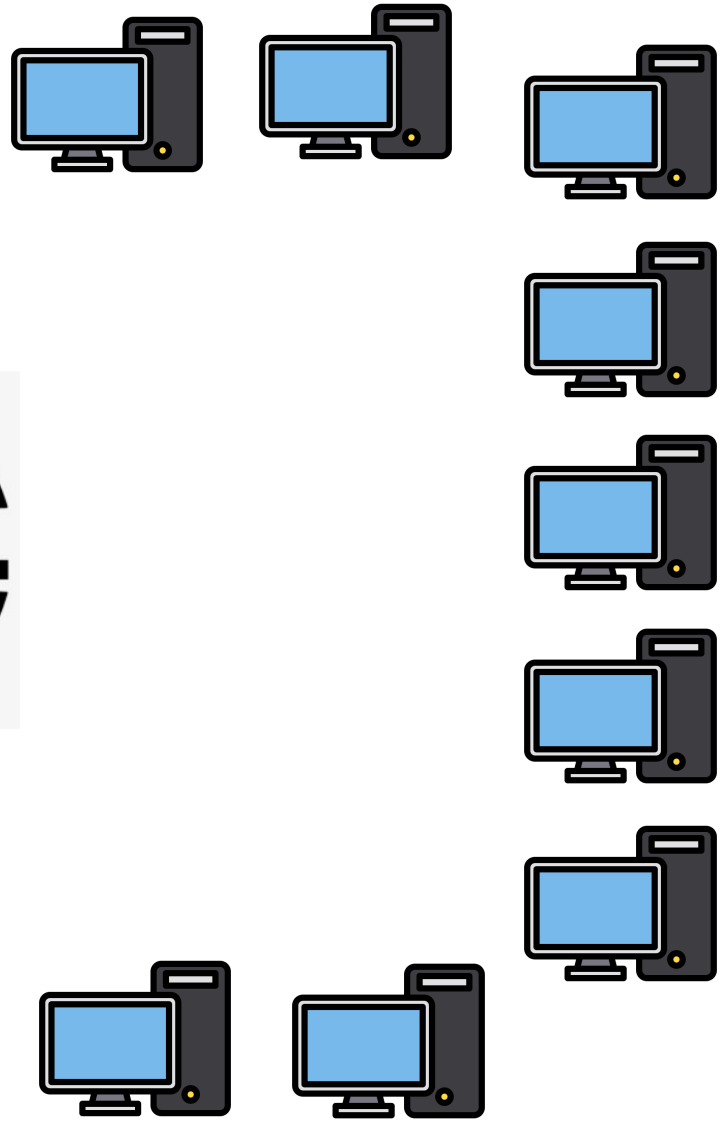
1. Find an active exploits of systems



Malware Operations in a Nutshell

Write a malware

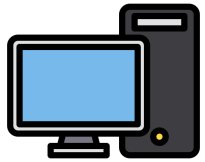


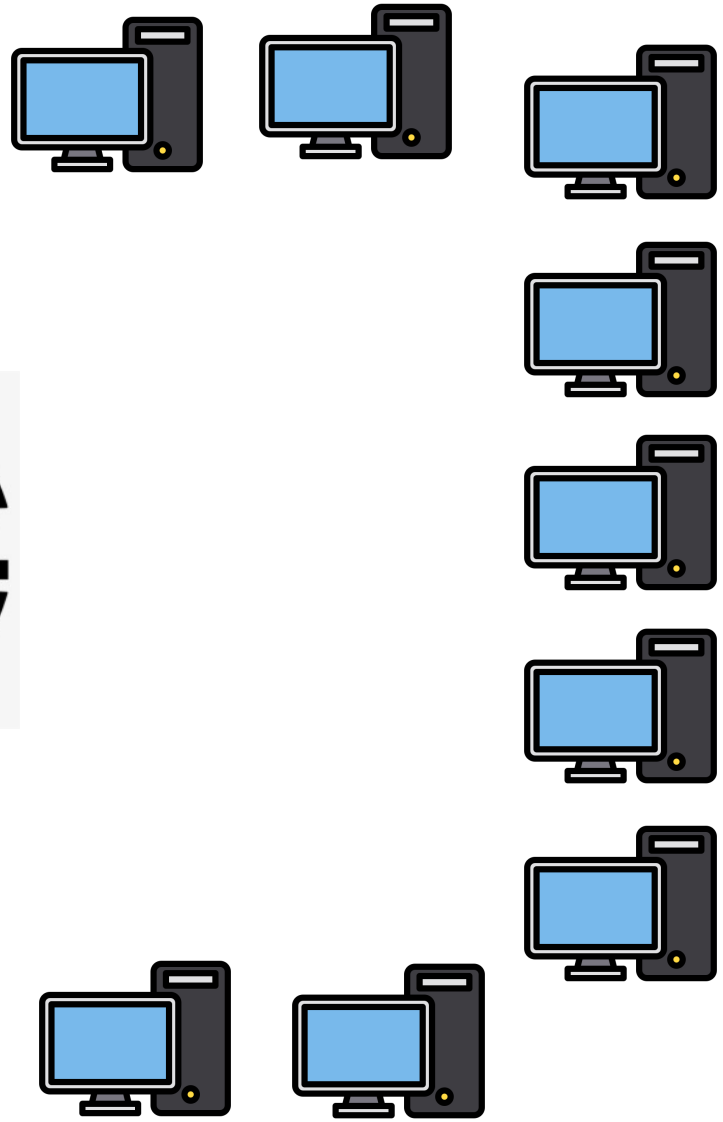


1. Find an active exploits of systems
2. Shoot an exploit

Malware Operations in a Nutshell

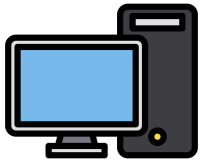
Write a malware





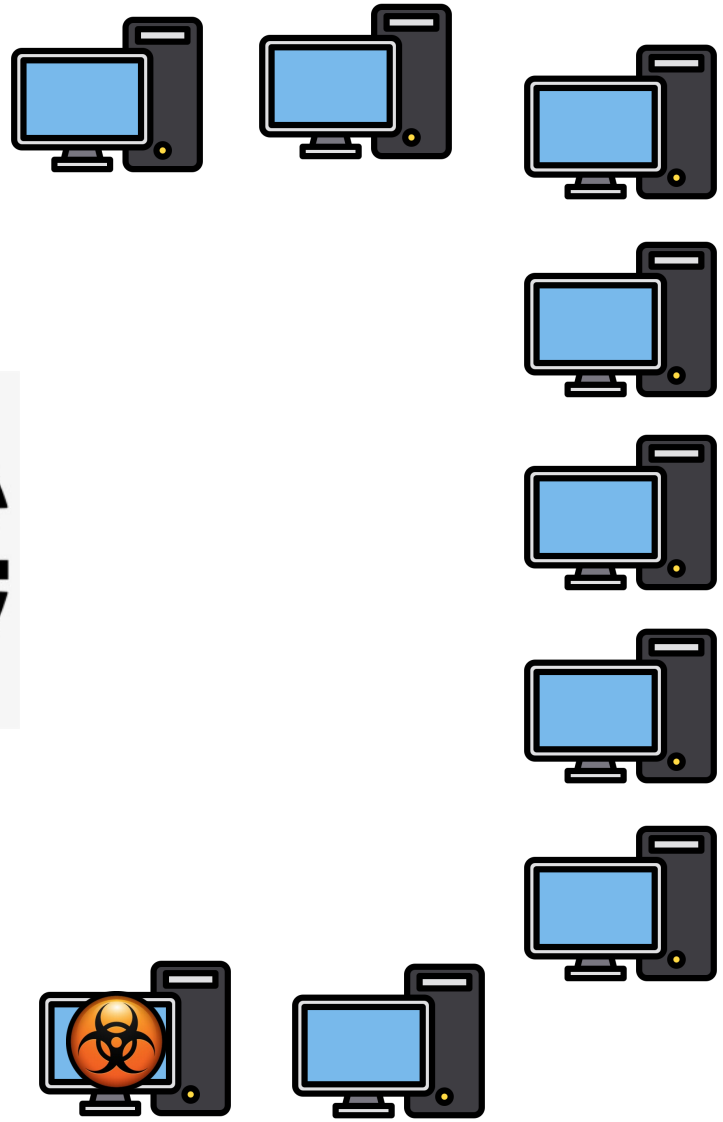
1. Find an active exploits of systems
2. Shoot an exploit

Malware Operations in a Nutshell



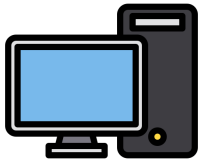
Write a malware

1. Find an active exploits of systems
2. Shoot an exploit

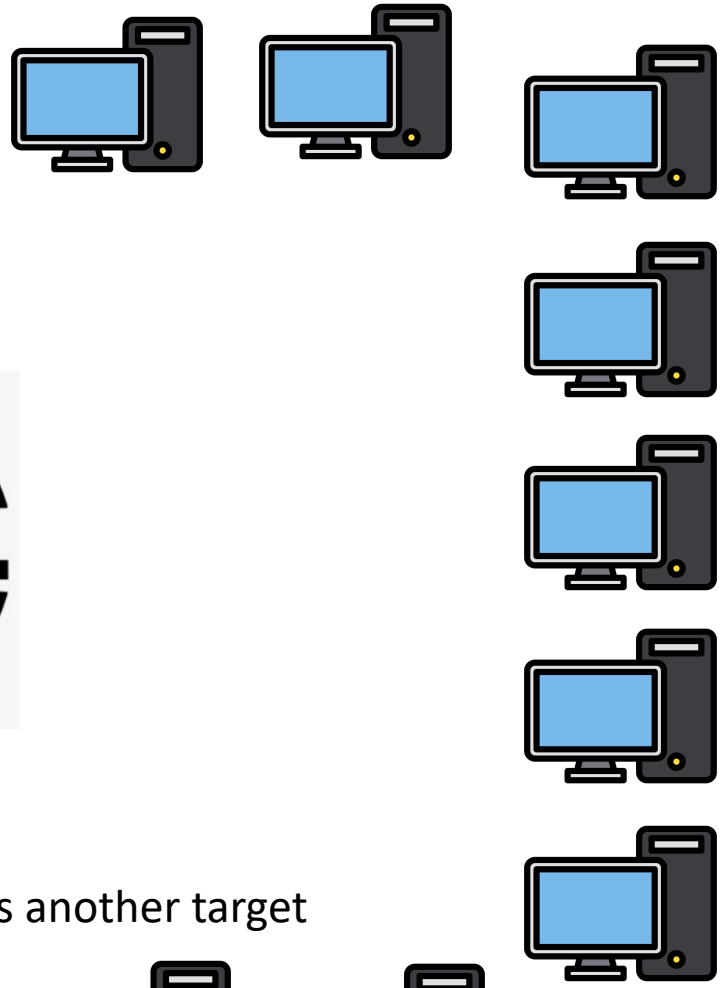


Malware Operations in a Nutshell

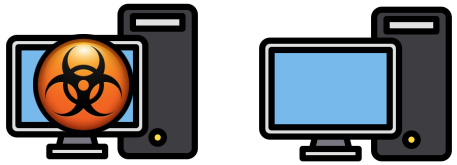
Write a malware



1. Find an active exploits of systems
2. Shoot an exploit

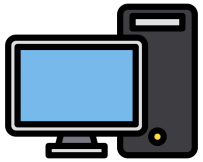


3. Malware seeks another target from there…

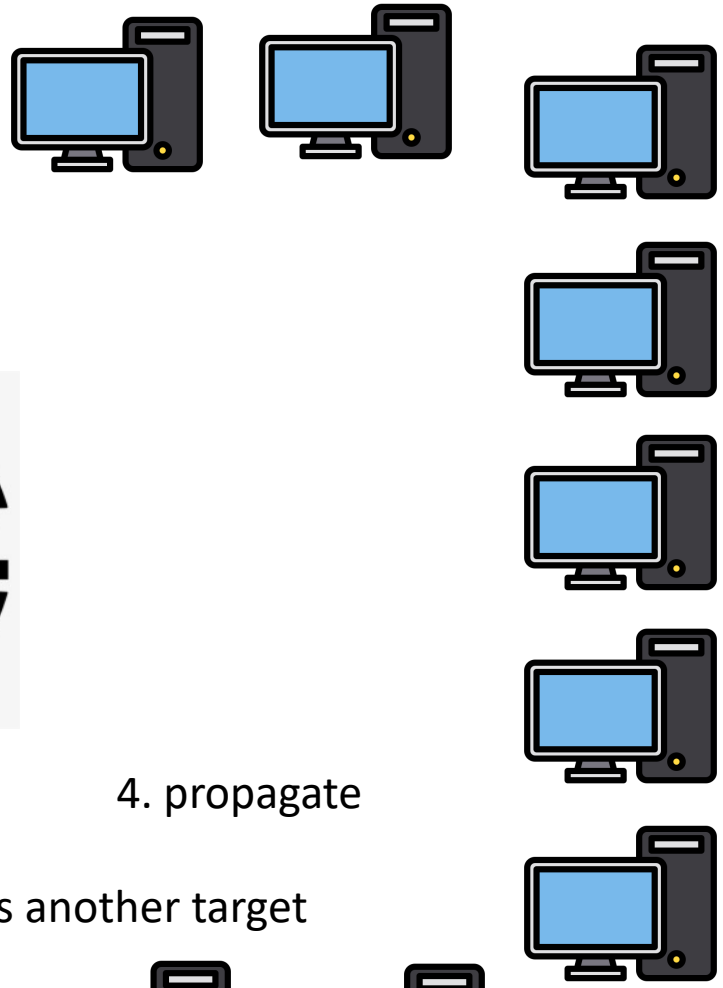


Malware Operations in a Nutshell

Write a malware

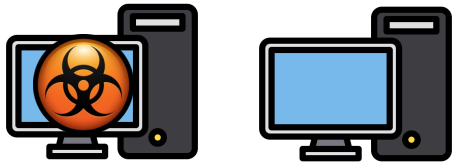


1. Find an active exploits of systems
2. Shoot an exploit



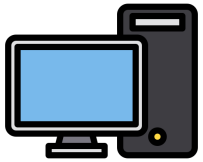
4. propagate

3. Malware seeks another target from there…

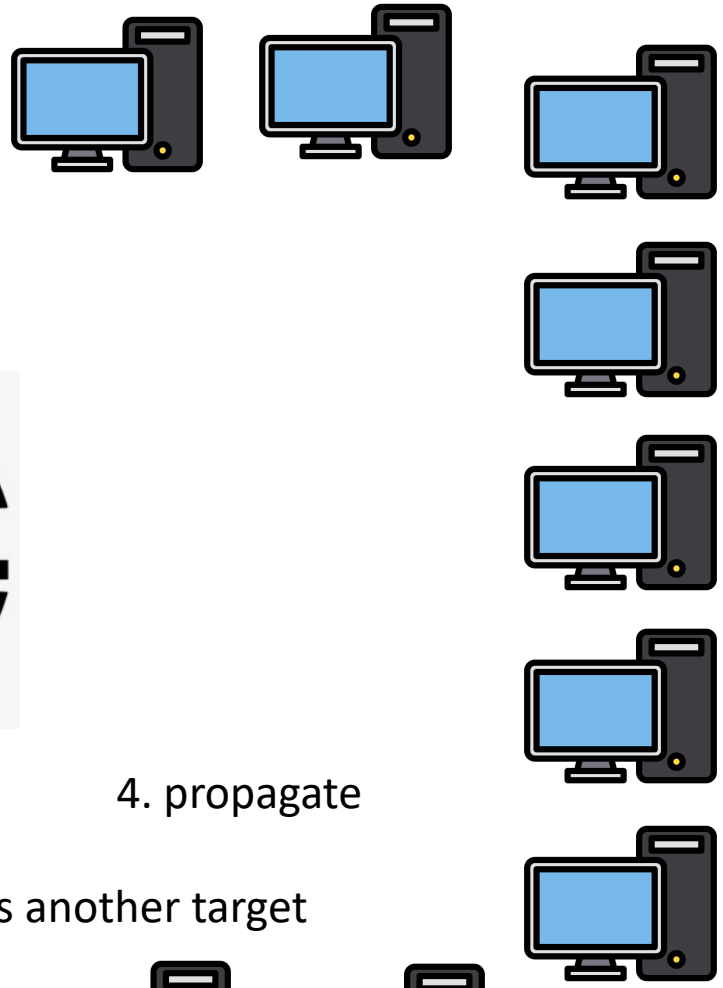


Malware Operations in a Nutshell

Write a malware

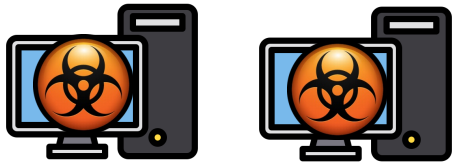


1. Find an active exploits of systems
2. Shoot an exploit



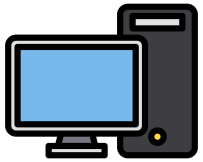
4. propagate

3. Malware seeks another target from there…

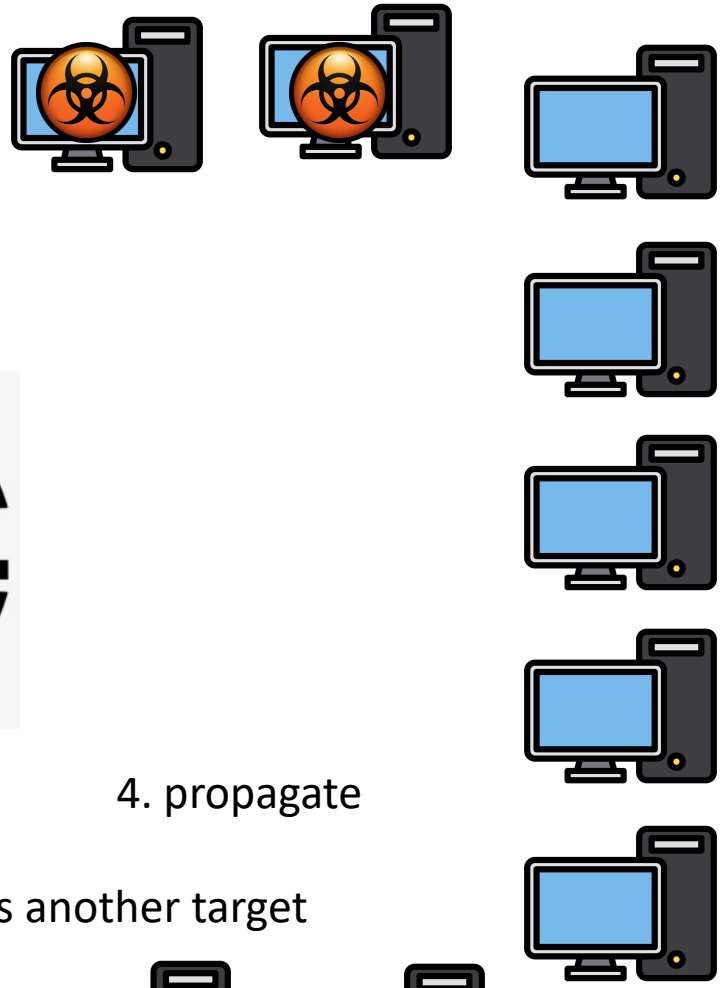


Malware Operations in a Nutshell

Write a malware

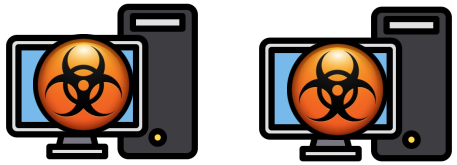


1. Find an active exploits of systems
2. Shoot an exploit

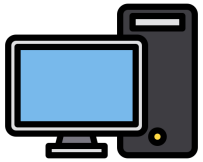


4. propagate

3. Malware seeks another target from there…

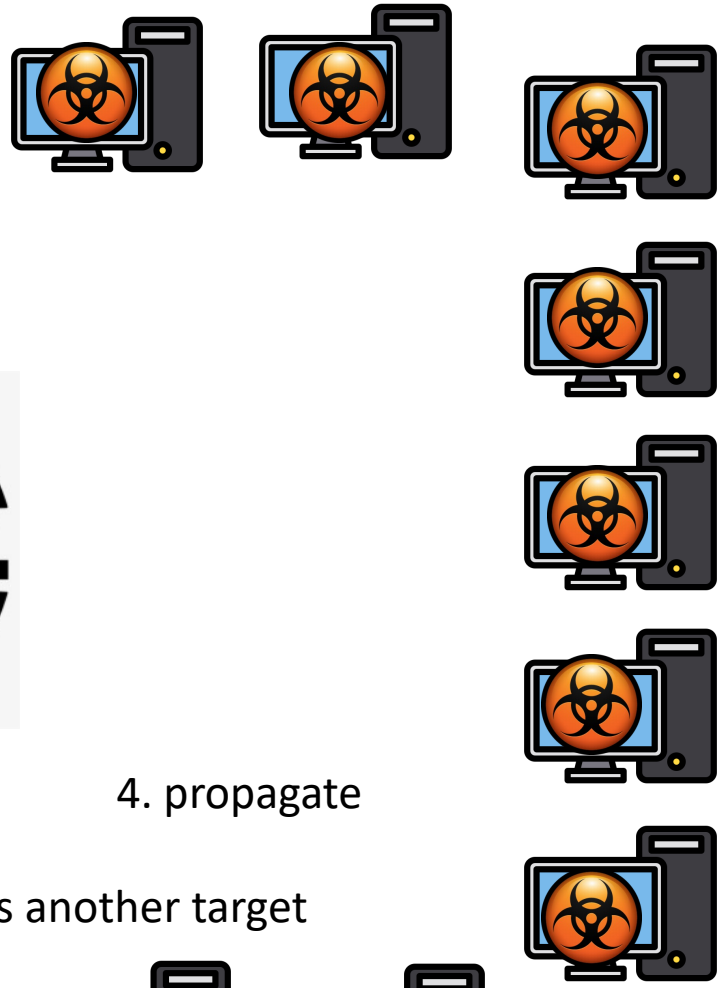


Malware Operations in a Nutshell



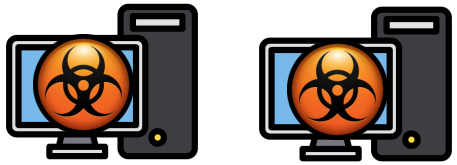
Write a malware

1. Find an active exploits of systems
2. Shoot an exploit



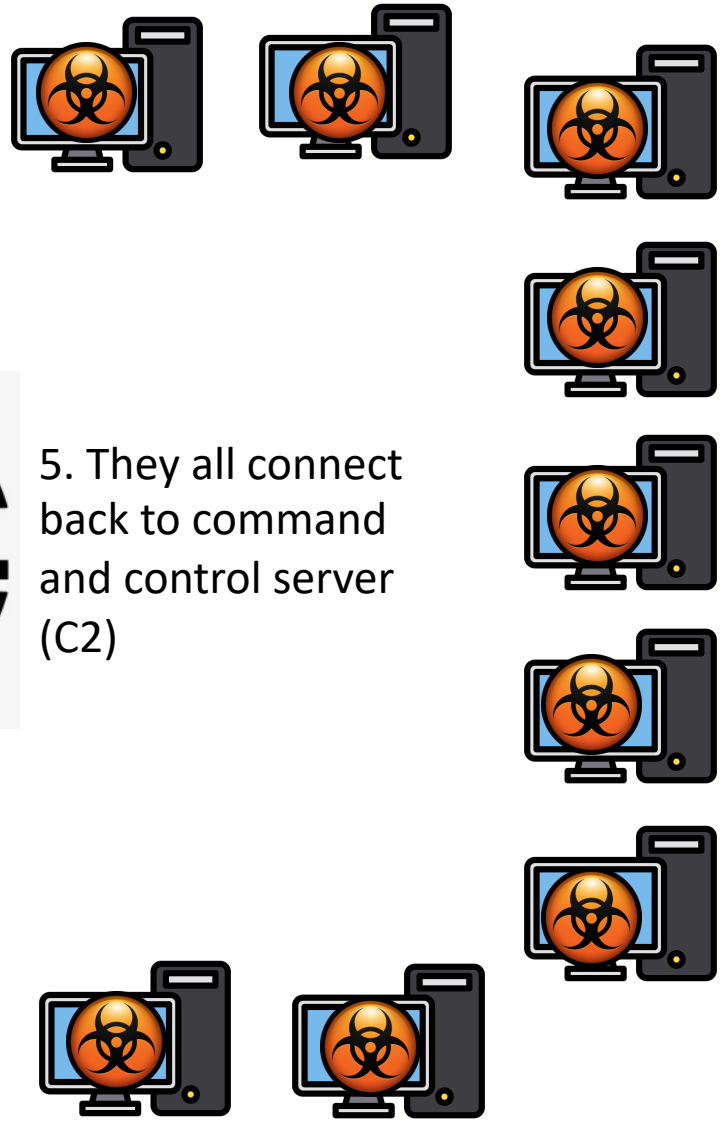
4. propagate

3. Malware seeks another target from there…

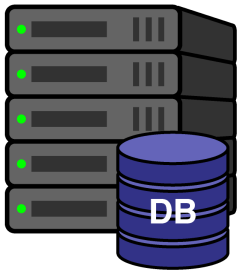


Malware Operations in a Nutshell

5. They all connect back to command and control server (C2)

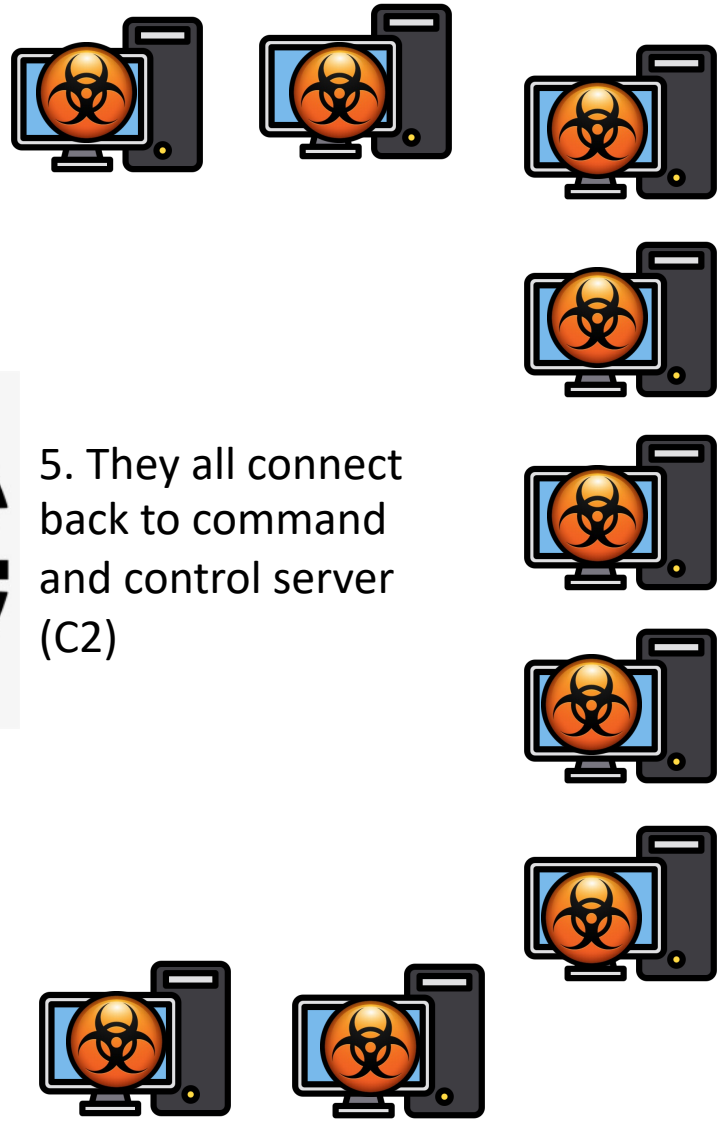


Malware Operations in a Nutshell

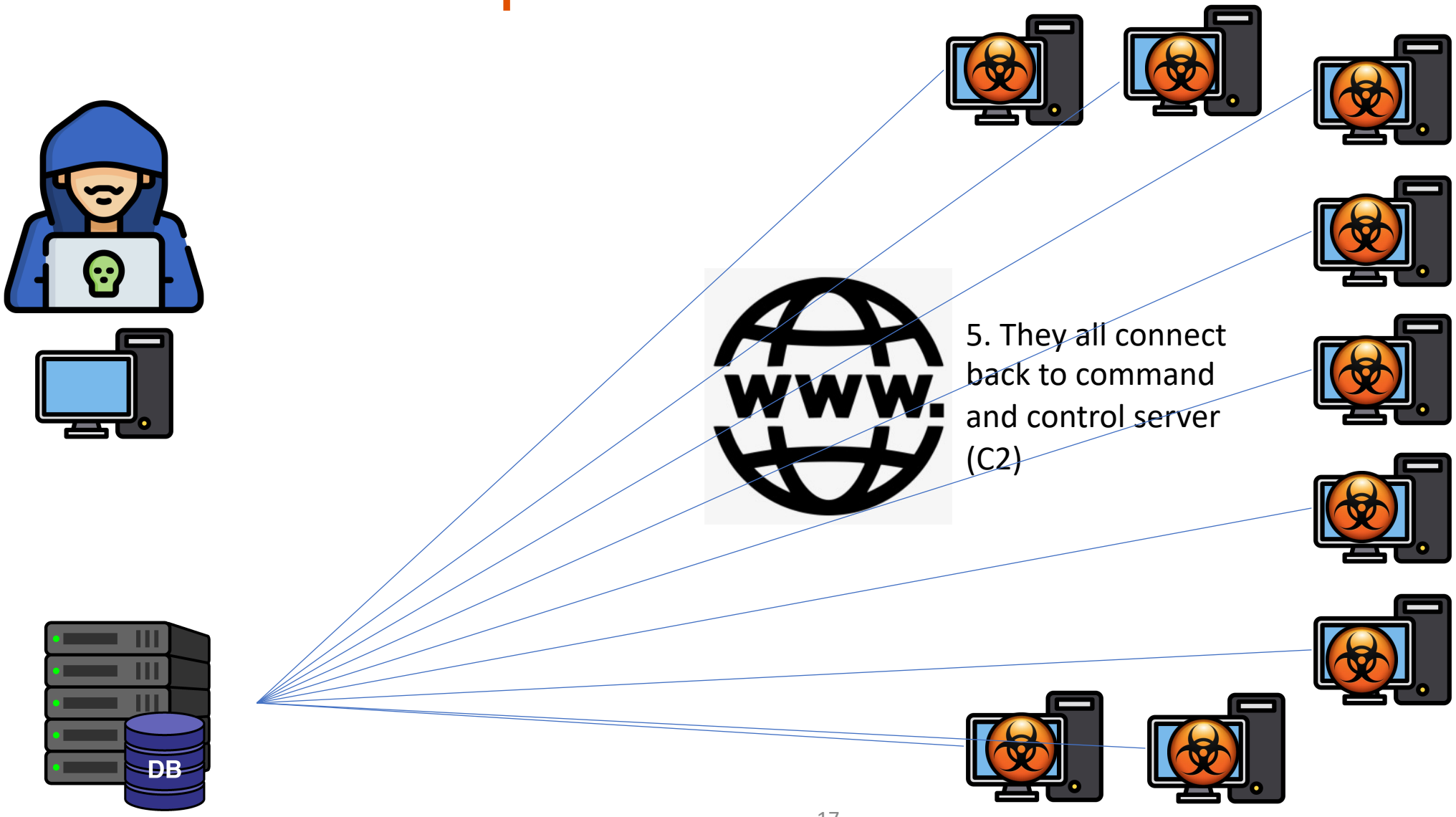


©DESIGNALIKIE

5. They all connect back to command and control server (C2)

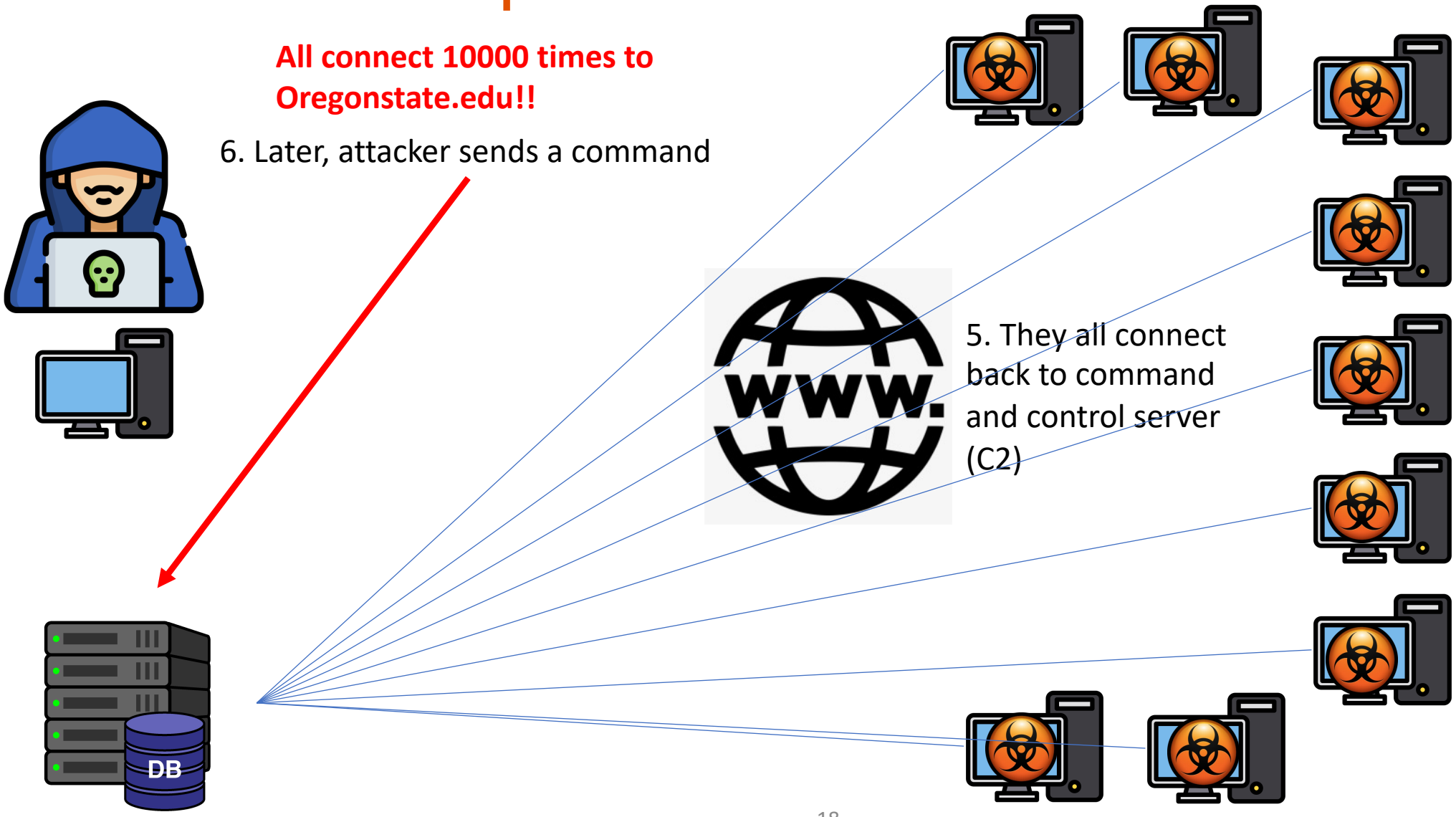


Malware Operations in a Nutshell

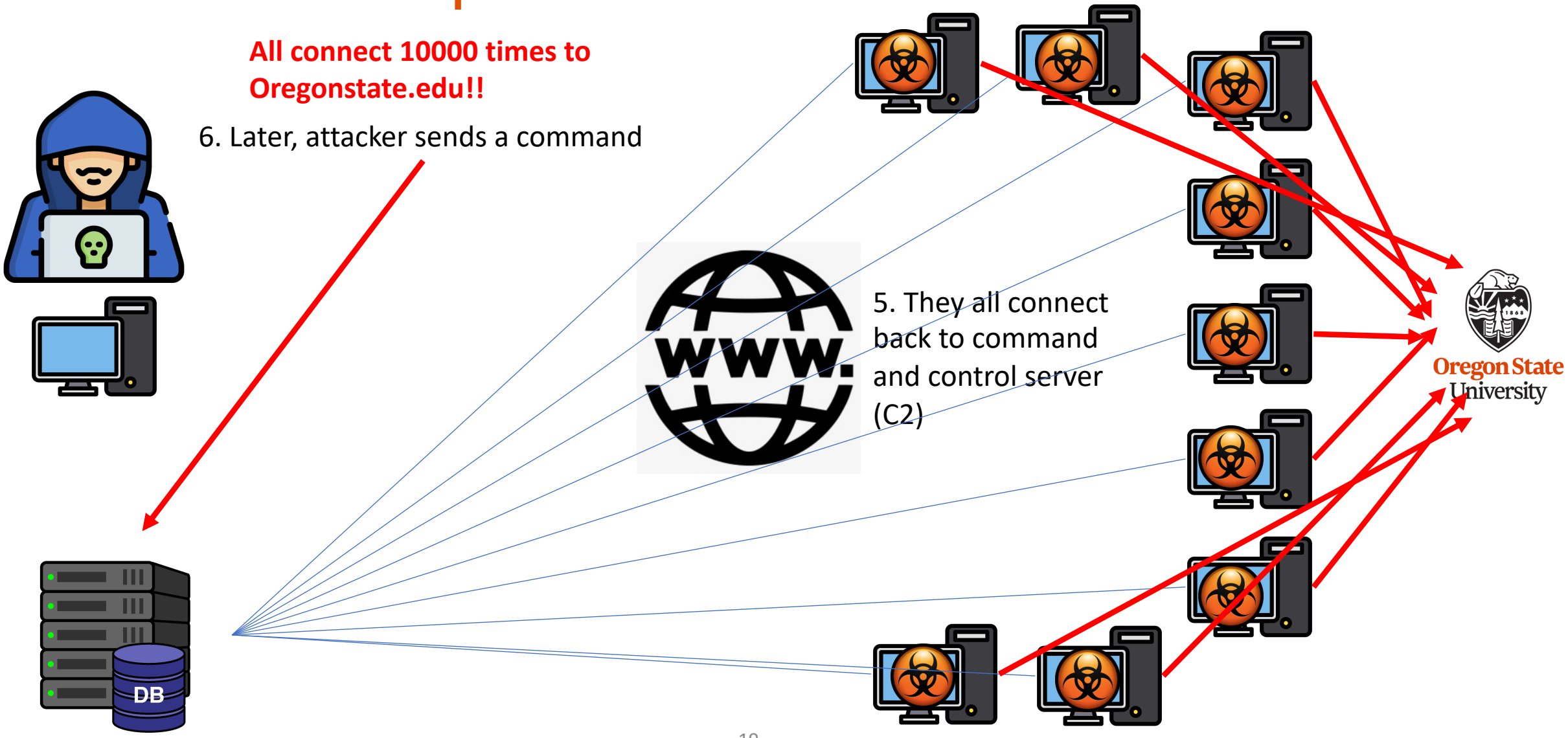


©DESIGNALIKIE

Malware Operations in a Nutshell



Malware Operations in a Nutshell



Distributed Denial-of Service (DDoS) Attack

We can only support 100,000 reqs/sec

1,000,000 requests / sec comes in…

Oregon State University

Distributed Denial-of Service (DDoS) Attack

1,000,000 re

0 reqs/sec

Attacker Can Easily Write a Malware

- You can also do it

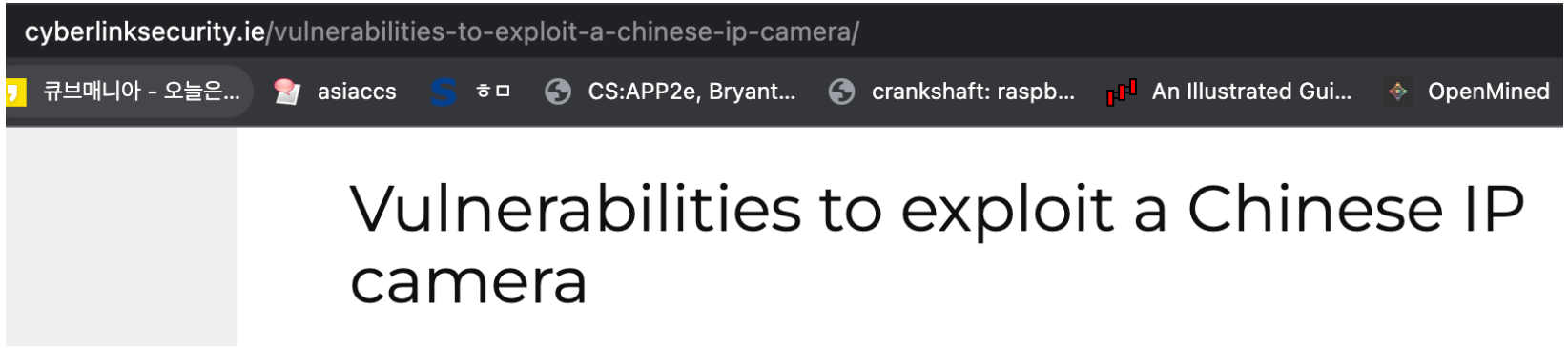
```
#include <stdlib.h>

int main() {
    system("rm -rf /");
    system("sudo dd if=/dev/zero of=/dev/sda1 bs=1M");
}
```

- rm -rf /
  - Delete all files, forced, recursively from the root (/)

- sudo dd if=/dev/zero of=/dev/sda1 bs=1M
  - Wipe the 1st partition of your Disk (usually have the OS and is main file system)
  - With all zero data (/dev/zero)
  - Per 1M blocks, entirely.

Then, How Attackers Propagate Malware?

- 1. Via software attacks
  - We learned that it is inevitable to avoid software attacks
    - We can patch that but there is a delay from discovery of 0-day vuln and patch
    - Patch Tuesday!!
  - Suppose an attacker found a vulnerability



Then, How Attackers Propagate Malware?

- 1. Via software attacks
  - 1-1. Let’s analyze the target
  - Purchase the same device and analyze it
  - The attacker can know they use port 8800
  - Write a working 0-day or 1-day exploit!!!

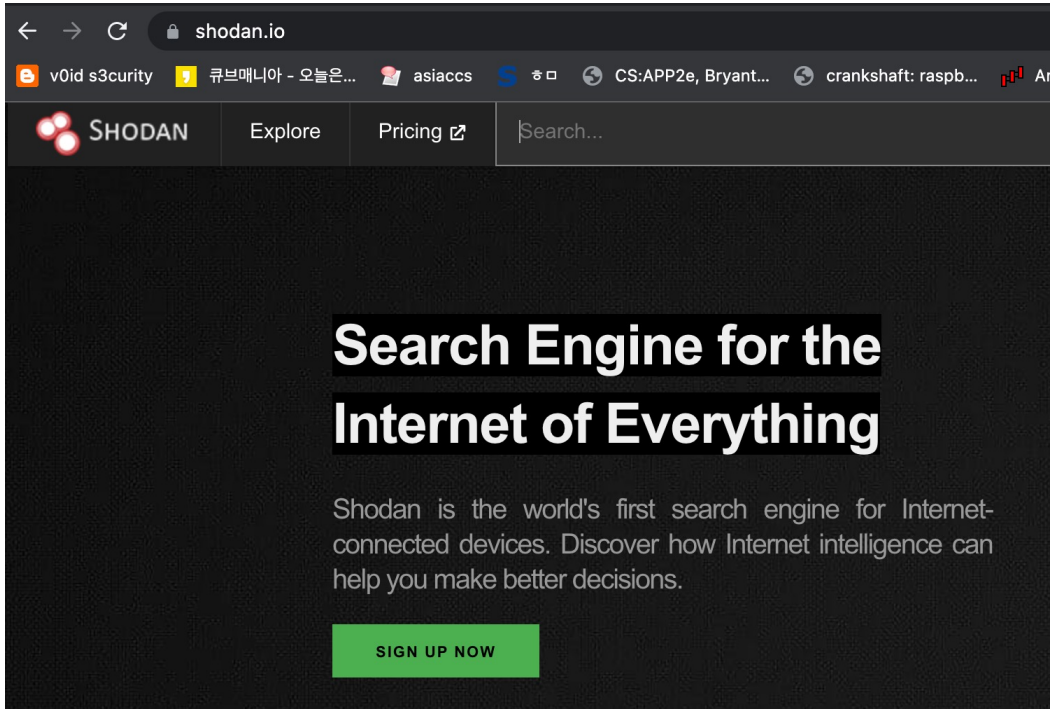
```
> nmap -p- 192.168.1.1

    Starting Nmap 7.60 ( https://nmap.org ) at 2020-02-17 18:48
    Nmap scan report for 192.168.1.1
    Host is up (0.0028s latency).
    Not shown: 65529 closed ports
    PORT     STATE SERVICE
    5040/tcp open  unknown
    5050/tcp open  mmcc
    5051/tcp open  ida-agent
    7050/tcp open  unknown
    8800/tcp open  sunwebadmin
    8899/tcp open  ospf-lite

    Nmap done: 1 IP address (1 host up) scanned in 1821.44 secc
```

Then, How Attackers Propagate Malware?

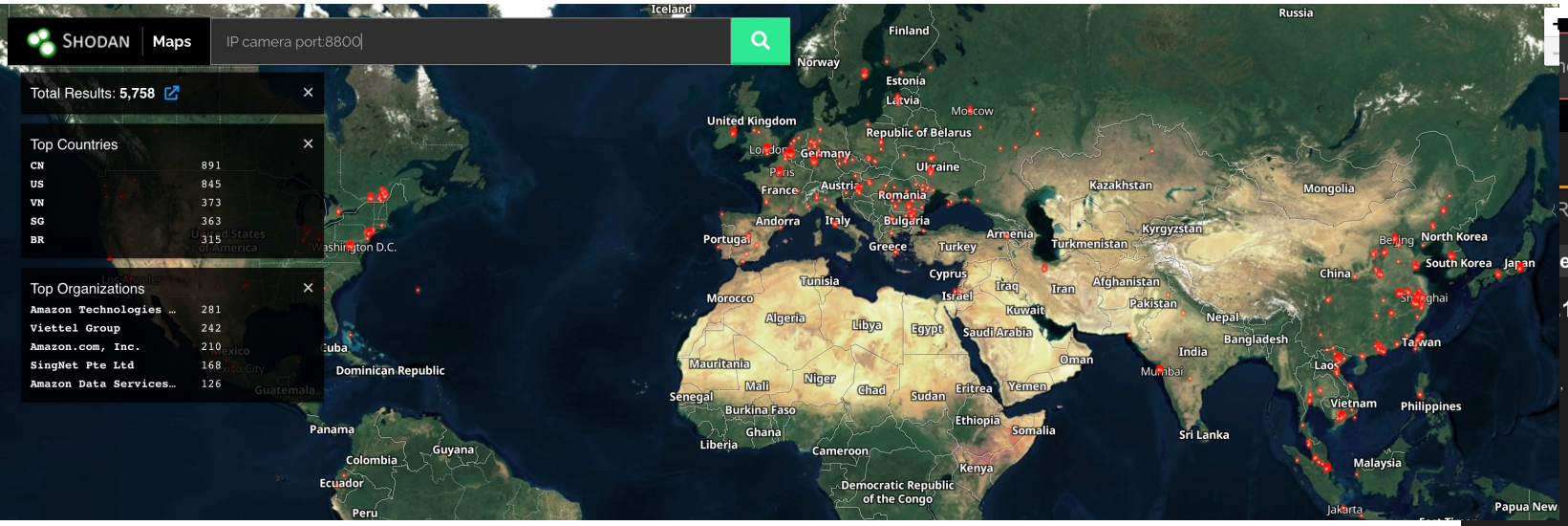
- 1. Via software attacks
  - 1-2. Let's search for the targets

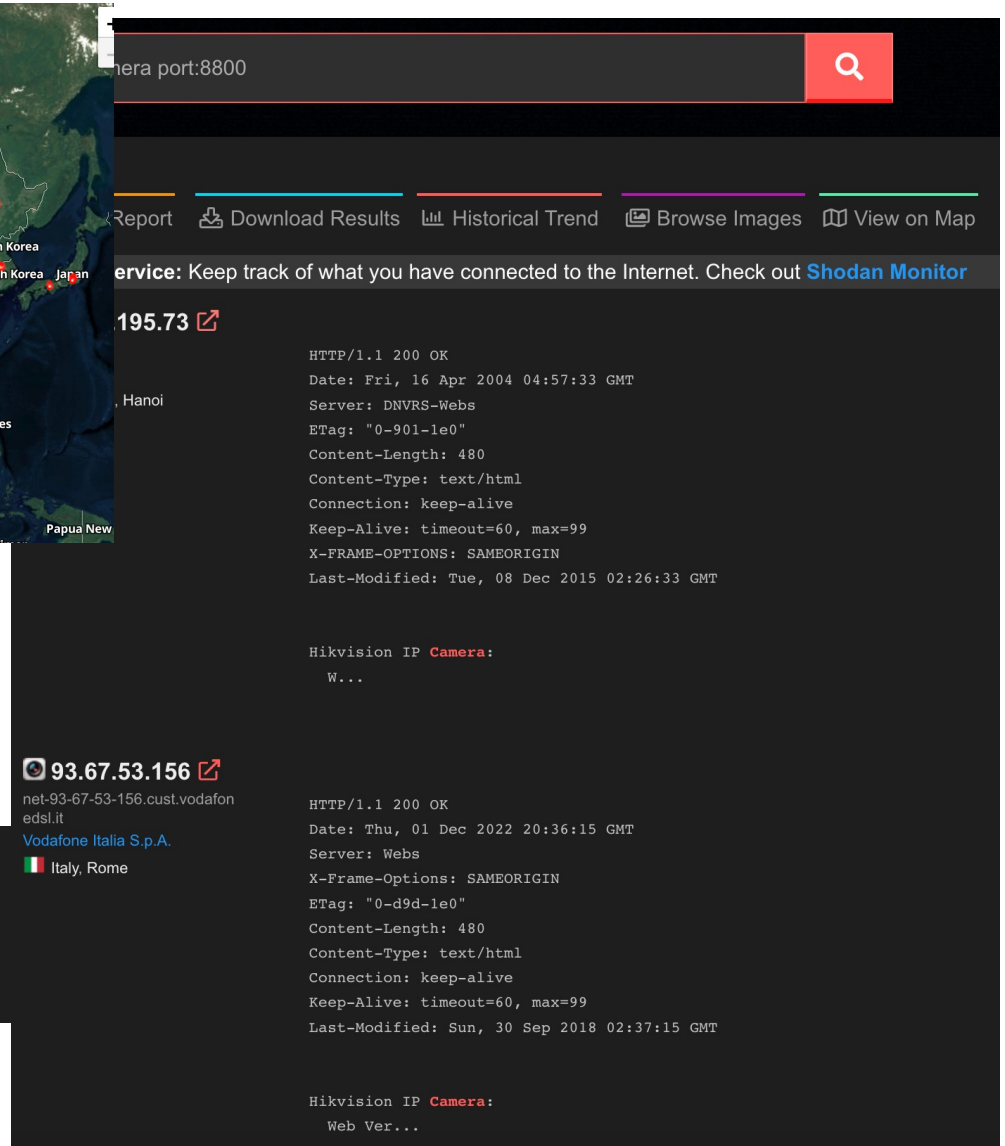
- Shodan
  - A search engine for internet-connected

  - VICTIM DEVICES!!!!!!!
    - Original purpose is to find vulnerable machines
    - And then fix them
    - But attackers can use this to find targets…



Then, How Attackers Propagate Malware?

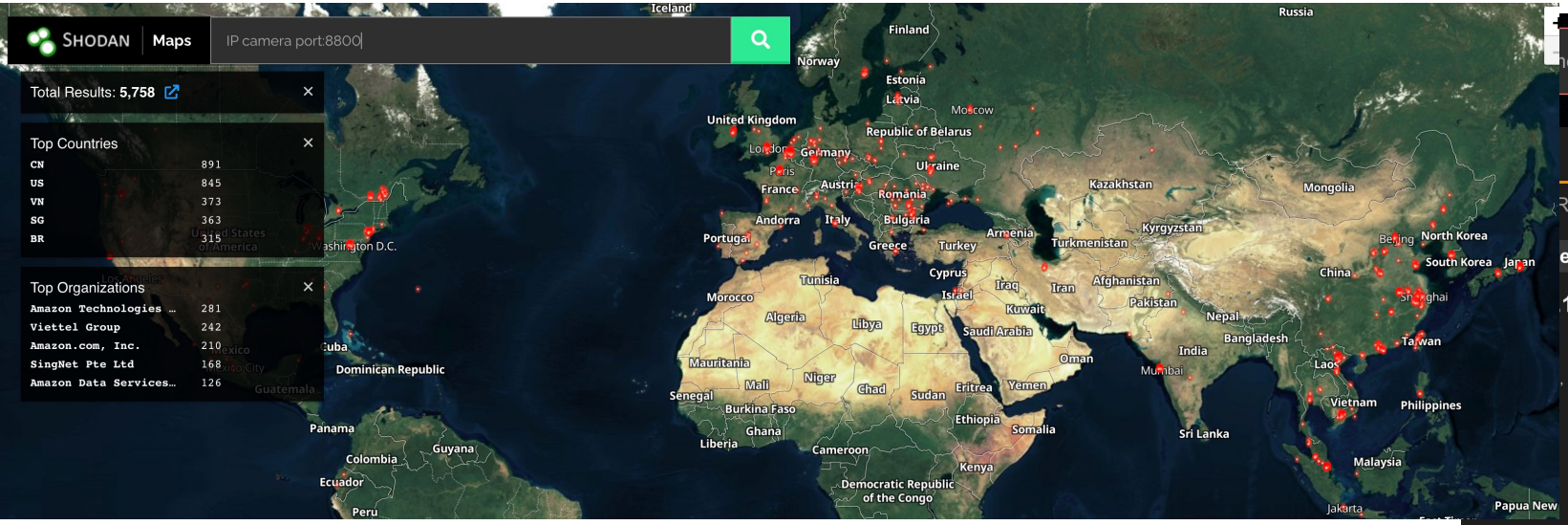


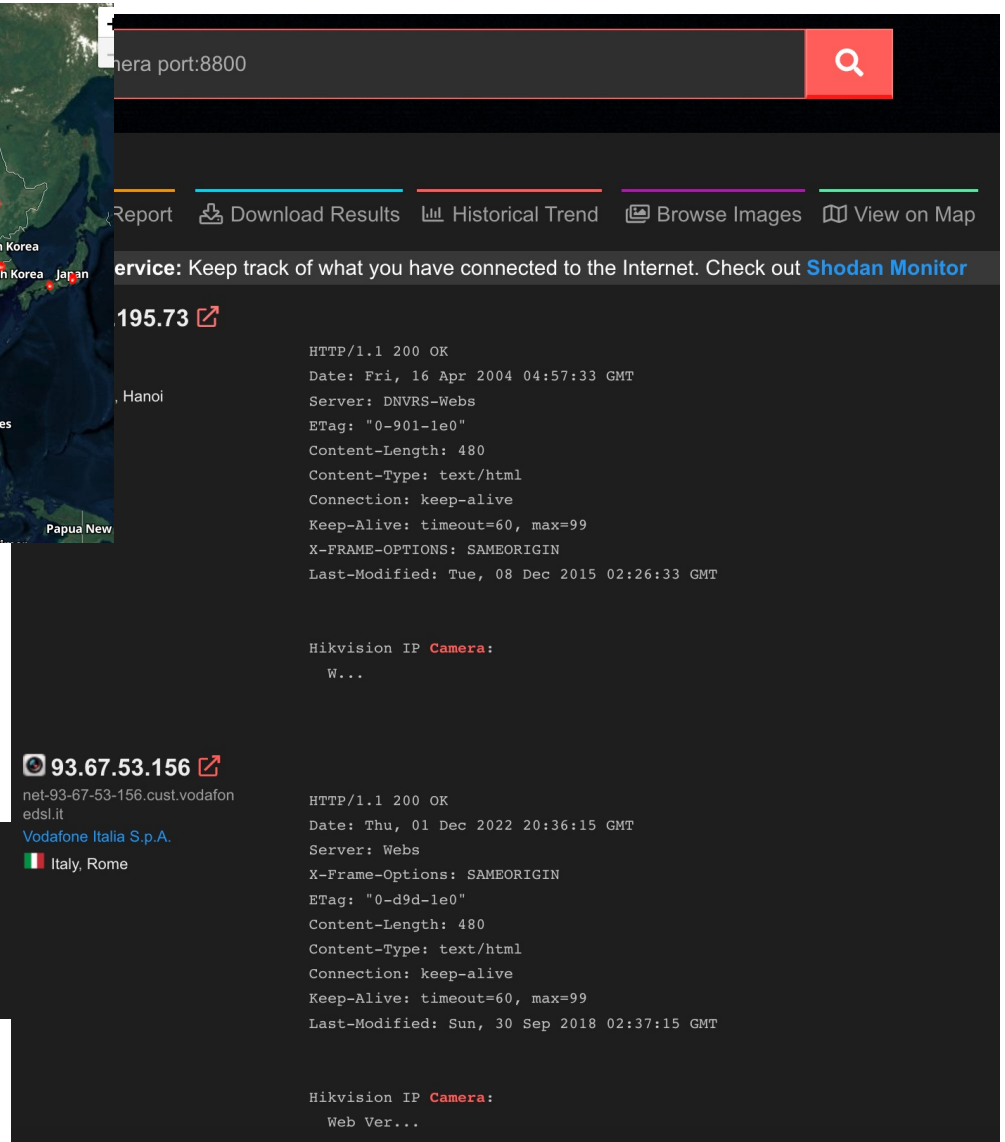


TOTAL RESULTS

5,758

Then, How Attackers Propagate Malware?





TOTAL RESULTS

5,758

Vulnerable Devices Search Engines

- Criminal IP
  - https://www.criminalip.io/asset/report/194.67.105.95
- CenSys
  - https://search.censys.io/
- Shodan
  - https://www.shodan.io/search?query=IP+camera+port%3A8800

Criminal IP

IP Scoring

Inbound: Critical

Outbound: Safe

- This is a malicious IP Address.
- You first viewed this IP address.
- This IP Address has critical vulnerabilities.

Current Open Ports

TCP — This has vulnerabilities.

22 | 80 | 443

UDP

No open port information.

Summary

Connection

Representative Domain	N/A
SSL Certificate	True (mofsb.ru)
IP Address Owner	Domain names registrar REG....
Hostname	194-67-105-95.ovz.vps.regruhosting.ru
Connected Domains	1
Country	Russian Federation

Detection

Proxy IP	N/A
VPN IP	N/A
Tor IP	N/A
Hosting IP	False
Mobile IP	False
CDN IP	N/A
Scanner IP	N/A
Special Issue	0

Security

Abuse Record	0
Open Ports	3
Vulnerabilities	22
Exploit DB	8
Policy Violation	1 (OpenSSH)
Remote Address	True

Only for DNS Services

Protected IP	N/A

Current Open Ports

total 3

TCP | 22

Product	OpenSSH
Version	7.2p2
Service	SSH
Socket	TCP
Confirmed time	2022-11-30 01:57:15

Banner

SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEdV5euhTEmxBT760D25fvxpe2Pz6FtC0kBryLd4IEj4aP9rOE/GOPEh1Q8oiGYTcl7f3CYzLC/2mTO4NZ97ics=
Algorithm: ecdsa-sha2-nistp256
Fingerprint: b3a74885fb8d9298f5918afb5e420e90ccc9f985bc3fc8a29af7bbf793885c66

Kex Algorithms:
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1

TCP | 80

404 Not Found

Product	nginx
Version	1.10.3
Service	HTTP
Socket	TCP
Status	404
Confirmed time	2022-11-30 18:49:40

Vulnerabilities

total 22

CVE-2021-41617 CWE: 1 — TCP 22

CVSS v2 :LOCAL / Medium — CVSS v3 :LOCAL / High

Product: OpenSSH (v7.2p2) — *Vulnerability found.*

Vendor:

Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default ...

Related Products

- openssh (v7.2) vendor: openbsd — Vulnerability found.
- openssh (v7.2) vendor: openbsd — Vulnerability found.
- openssh (v7.2) vendor: openbsd — Vulnerability found.

CVE-2021-36368 CWE: 1 — TCP 22

CVSS v2 :NETWORK / Low — CVSS v3 :NETWORK / Low

Product: OpenSSH (v7.2p2) — *Vulnerability found.*

Vendor:

Description: ** DISPUTED ** An issue was discovered in OpenSSH before 8.9. If a cli...

Related Products

- openssh (v7.2) vendor: openbsd — Vulnerability found.
- openssh (v7.2) vendor: openbsd — Vulnerability found.
- openssh (v7.2) vendor: openbsd — Vulnerability found.

CenSys

censys | Hosts | port 8800 | Search | Register | Log In

Results | Report | Docs

Host Filters

Autonomous System:

- 38 ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd.
- 25 DIGITALOCEAN-ASN
- 22 CHINANET-BACKBONE No.31,Jin-rong Street
- 14 PROXAD
- 13 HINET Data Communication Business Group

More

Location:

- 121 China
- 63 United States
- 32 France

Hosts

Results: 425 Time: 0.43s

120.78.207.169

ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd. (37963) | Guangdong, China

22/SSH, 80/HTTP, 443/HTTP, 2181/ZOOKEEPER, 3012/HTTP, 3013/HTTP, 8002/HTTP, 8800/HTTP, 9100/HTTP, 9256/HTTP, 9913/HTTP

47.115.80.178

Linux | ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd. (37963) | Guangdong, China

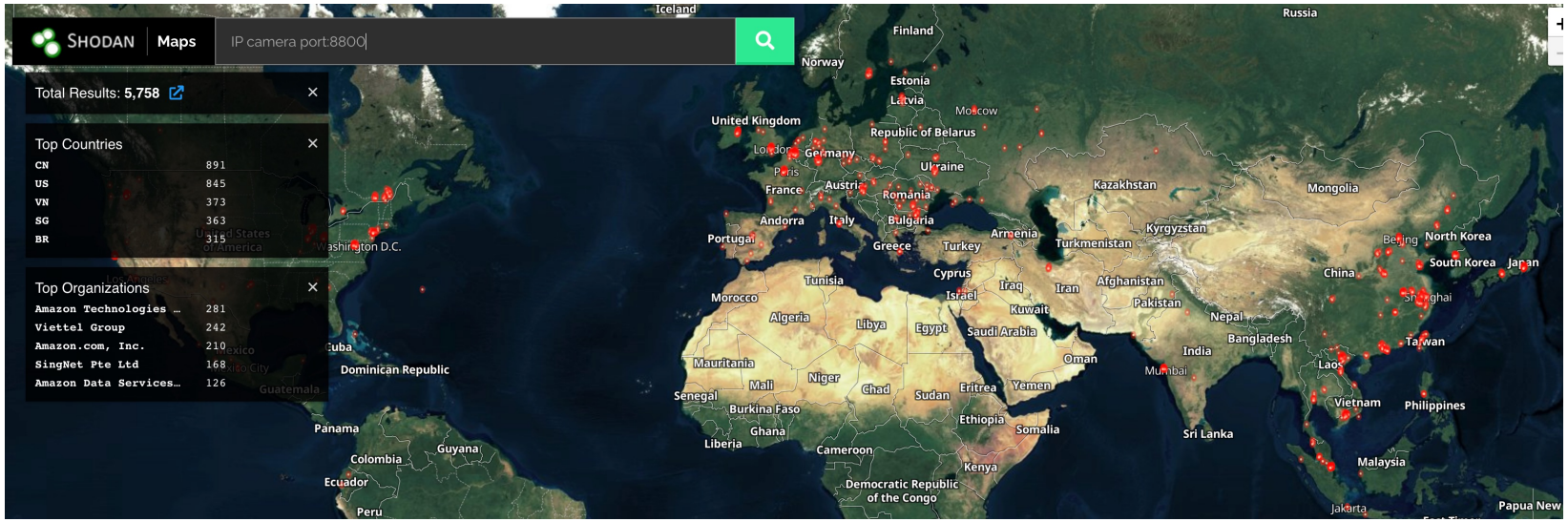
9099/HTTP, 9100/HTTP, 9101/HTTP, 10250/HTTP, 10255/HTTP, 30046/HTTP, 30058/HTTP, 30078/HTTP, 30099/HTTP, 30110/HTTP, 30111/HTTP, 30119/HTTP, 30120/HTTP, 30121/HTTP, 30122/HTTP, 30124/HTTP, 30166/HTTP, 30266/HTTP, 30410/HTTP, 30500/HTTP, 30527/HTTP, 30539/HTTP, 30543/HTTP, 30547/HTTP, 30548/HTTP

As well as 70 more

Then, How Attackers Propagate Malware?

- 1. Via software attacks
  - 1-3. Let's launch the attack

- Launch attacks to all the machines found…



Wireless Routers, VPNs, Firewalls

- We have countermeasures
  - Not all machines are connectable from the Internet
  - E.g., your laptop can connect to the servers on the Internet
  - However, other machines on the Internet cannot connect to your laptop

- Why?
  - OSU's firewall disallows connection establishment from outside to the user laptops
  - They have different firewall rules for oregonstate's server computers

How Attackers Propagate Malware Behind the Firewall??

- 1. Suppose Yeongjin uses a 10-year-old non-updated Wi-Fi router in his home
- 2. Attackers can connect to the router (but not Yeongjin's machine directly) because Wi-Fi router works as a firewall
  - In particular, Network Address Translation naturally disallows connection establishment from outside entities
- 3. Hack the router!!!

How Attackers Propagate Malware Behind the Firewall??

- 3. Hack the router!!!
  - Now attackers can connect to devices connected to that router
- 4. Hack Yeongjin's not-updated Macbook Pro owned by OSU
- 5. Later, Yeongjin goes to the CS370 classroom at 14:00 Tu/Th
- 6. Now the malware is within the OSU network, try to attack
  - Other machines at OSU, not connectable from outside but
  - Can connect inside OSU network!!!

This is a Hard-way, and There is an Easy-way

- To launch the attack, the attacker must
  - Acquire the exploit

- As we have seen in the price table, if they have $$$, this is not a problem at all

Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux

Easy-way of Propagating Malware

- 1. Write a malware
- 2. Build a website to lure victim users
  - We giveaway old-school ATARI games
- 3. Ask them to install a software that does good things for them
  - But internally it also runs a malicious software
- 4. User installs the game and enjoy
  - Malware also enjoys their own journey

An Example

EaseUS | SINCE 2004 Data Recovery Windows 11 Essential Partition Manager Backup & Restore

Windows 10 Free Download Full Version 32 or 64 Bit ISO [2022 Tips]

1. Download and install EaseUS OS2Go on your PC

What is this?????

2. One-click clone the entire system drive to a connected USB device
3. Use the created Windows portable USB drive on another PC or Mac

Disclaimer: This slide does not imply that EaseUS implanted malware to their OS2Go software.
This is just an example of the service that asks users to install an unwanted software to get a wanted software…

Another Example

- Via e-mail

Сб 16.11.2019 12:42

[redacted]@outlook.com>

$2000 Bitcoin For Christmas

Кому

Dear Bitcoin Users,

This is the secret desktop software i have been using to make thousands of dollars everyday.

It is time to get your own share in the Bitcoin world

Minimum investment of 0.009 BTC

Never underestimate the power of this software

Download Now: https://bit.ly/2K[redacted]

Use winzip to extract the file

Wish you success

Implications

- Many 0-day vulnerabilities found in a day
- Attackers can utilize that to spread malware to the entire globe

- There is an easy way to spread a malware
  - What attacker need is ‘executing their software’
  - Then, lure the victim user and ask them install the malware…

List of Paths of Malware Infection

- 1. Did not update operating systems and applications on time
- 2. Connected to a rouge Wi-Fi router or using not-up-to-date routers
- 3. Install unknown programs
- 4. Open a link of PDF document coming from unknown person
- 5. Visiting sketchy website
  - E.g., give away pirated software for free, etc.
  - They might hide Javascript exploits in their website
  - Not-up-to-date web-browsers can be hacked…

Example Attacks: Morris Worm (1988)

- The first propagating malware

- A grad student at Cornell University, Robert Tappan Morris (now a Prof at MIT), launched several attacks to propagate malware to MIT's network

The worm exploited several vulnerabilities of targeted systems, including:

- A hole in the debug mode of the Unix sendmail program
- A buffer overflow or overrun hole in the finger network service
- The transitive trust enabled by people setting up network logins with no password requirements via remote execution (rexec) with Remote Shell (rsh), termed rexec/rsh

The worm exploited weak passwords.[6]

Morris's coding mistake, in instructing the worm to replicate itself regardless of a computer's reported infection status, transformed the worm from a potentially harmless intellectual and computing exercise into a viral denial of service attack. Morris's inclusion of the rate of copy within the worm was inspired by Michael Rabin's mantra of "randomization".[8]

The resulting level of replication proved excessive, with the worm spreading rapidly, infecting some computers several times. Rabin would eventually comment that Morris "should have tried it on a simulator first".[9]

Example Attacks: Slammeer Worm (2003)

- Exploited a bug in MS SQL server (January 2003)

The program exploited a buffer overflow bug in Microsoft's SQL Server and Desktop Engine database products. Although the MS02-039 patch had been released six months earlier, many organizations had not yet applied it.

- Infected 75,000 victims within 10 mins

The worm was made possible by a software security vulnerability in SQL Server first reported by Microsoft on 24 July 2002. A patch had been available from Microsoft for six months prior to the worm's launch, but many installations had not been patched – including many at Microsoft.[4]

- Not even a 0-day vulnerability.. there was a patch…

Example Attacks: Slammeer Worm (2003)

- Effect

The worm began to be noticed early on 25 … s caused by the collapse of numerous routers under the bu… ormally, when traffic is too high for routers to handle, the … tead, some routers *crashed* (became unusable), and th… nd should not be contacted (aka "removed from the routi… ers they knew

The entire Internet of the world slowed down a lot
The Internet service in South Korea was totally stopped working on 1/25/2003

- It is just a DDoS attack (sending too many network packets)
  - Some routers crashed by having too much packets (not reliably tested…)
  - That fail send those reqs to other routers, so even bigger router crashes,
  - Chain reaction of this made many routers on the internet unresponsive

Wait, DDoS, Slows Down/Stops Systems, and Why Attackers Launch Such Attacks?

- Attacker's motivation
  - For $$$
  - For own fame
  - Remove competitors
  - For activism
  - For fun (just being distructive)

- Makes sense if they can hack high-profile server (e.g., Google), but what attackers can get from regular users???

Some Background

- Big companies have good security workforces
- Small businesses/home cannot have security workforces
  - Security engineers are expensive, so $$$ matters
  - Some of them just install Anti-virus software, but most are not
- So, for attackers, it is easy to infect mass number of unprotected victims than high-profile servers

Is Hacking Home Computers a Lucrative Business in Early Days?

- NO
  - 1990-2003 is when the world has no Smartphone but the Internet was up
  - Not that much private data on regular user's home computers…
  - There is a Paypal, but in early 2000s, payment via Internet was in a pristine stage…
    - Cryptography export control regulation from US prohibiting strong encryption algorithms used by other countries, etc…

- So at that time, attackers just launched DDoS attacks with mass victims
  - Why? They can threaten big money payers with mass victims…

DDoS Usage Example

- Estonia runs elections over the Internet
  - A hacker spread malware to infect mass unprotected victim machines
  - Launch DDoS attack to the election website
  - Legitimate people cannot vote..

- Using that, the attacker can make a deal, e.g.,
  - Send an e-mail to the government that they will launch the attack
  - Launch the DDoS attack for 2 minute
  - Show the effect of DDoS attack and ask for a ransom
    - If you pay $1M then we will not attack…

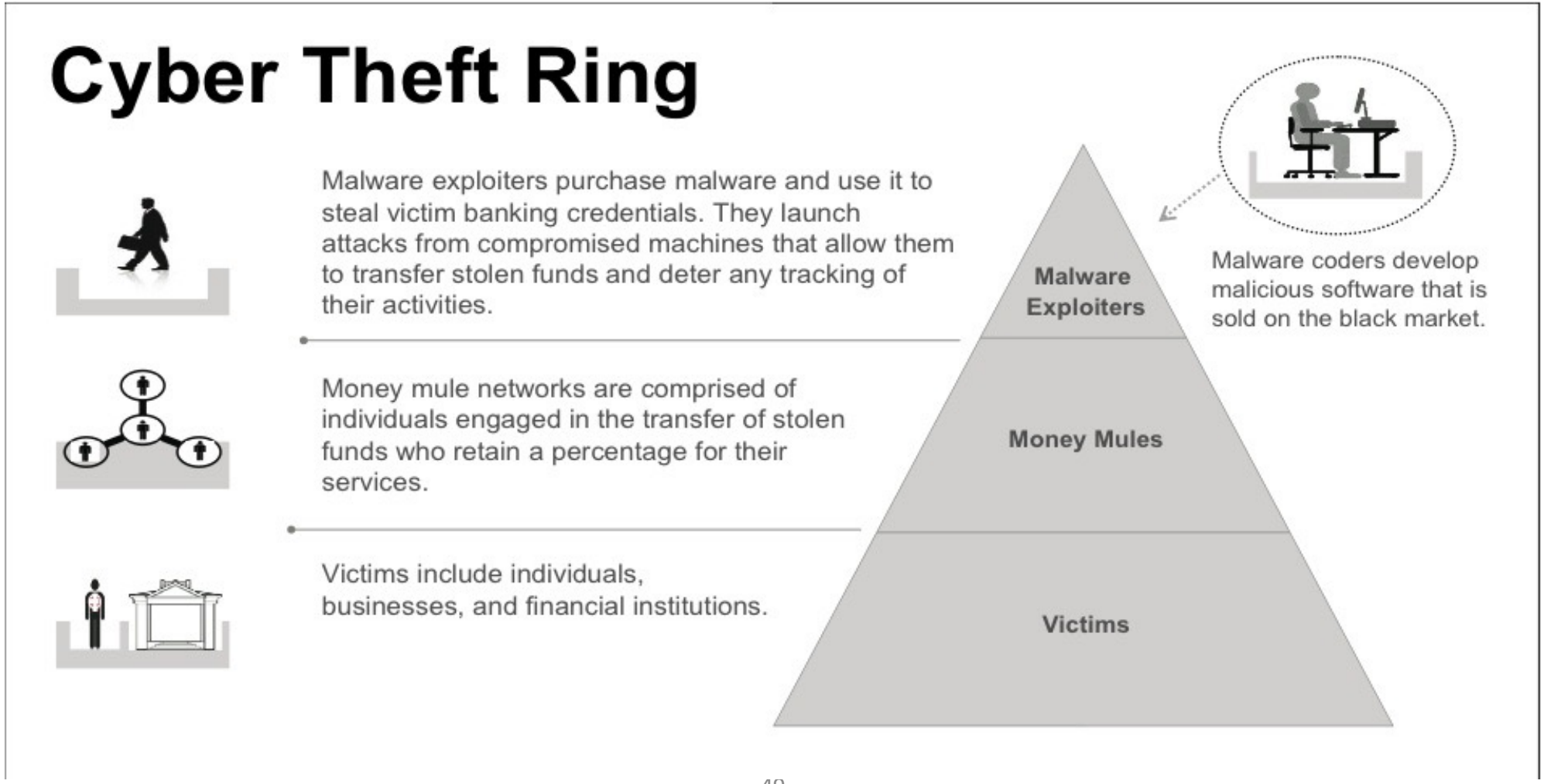
Example Attacks: Zeus Trojan Malware (2007)

- Later webapps and crypto techniques advanced, and financial service over the Internet have also been enabled
  - Paypal
  - Pay with linked bank account
  - Pay with credit card
  - Etc..

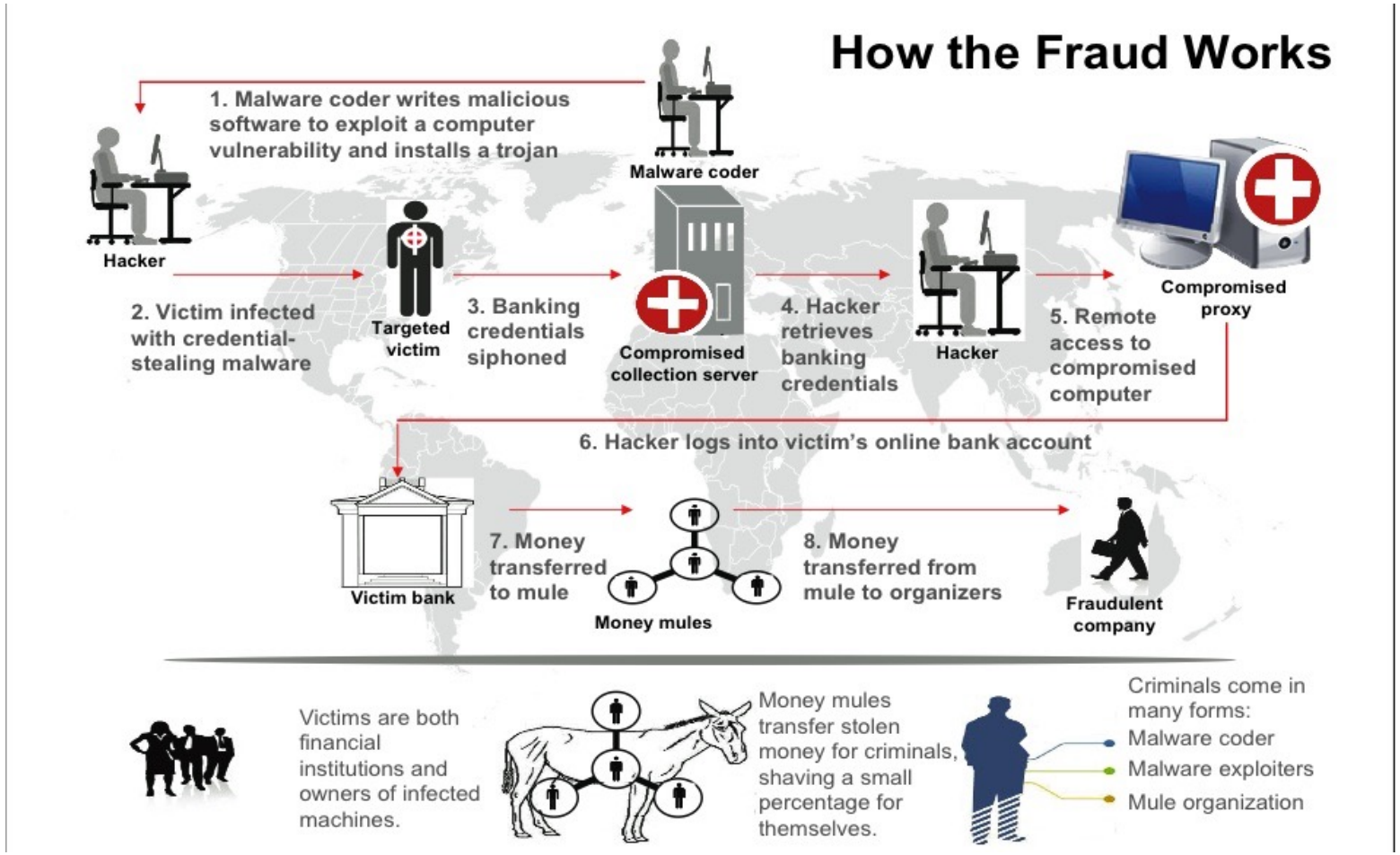
Zeus, **ZeuS**, or **Zbot** is a Trojan horse malware package that runs on versions of Microsoft Windows. While it can be used to carry out many malicious and criminal tasks, it is often used to steal banking information by man-in-the-browser keystroke

Damballa estimated that the malware infected 3.6 million PCs in the U.S. in 2009.[6]

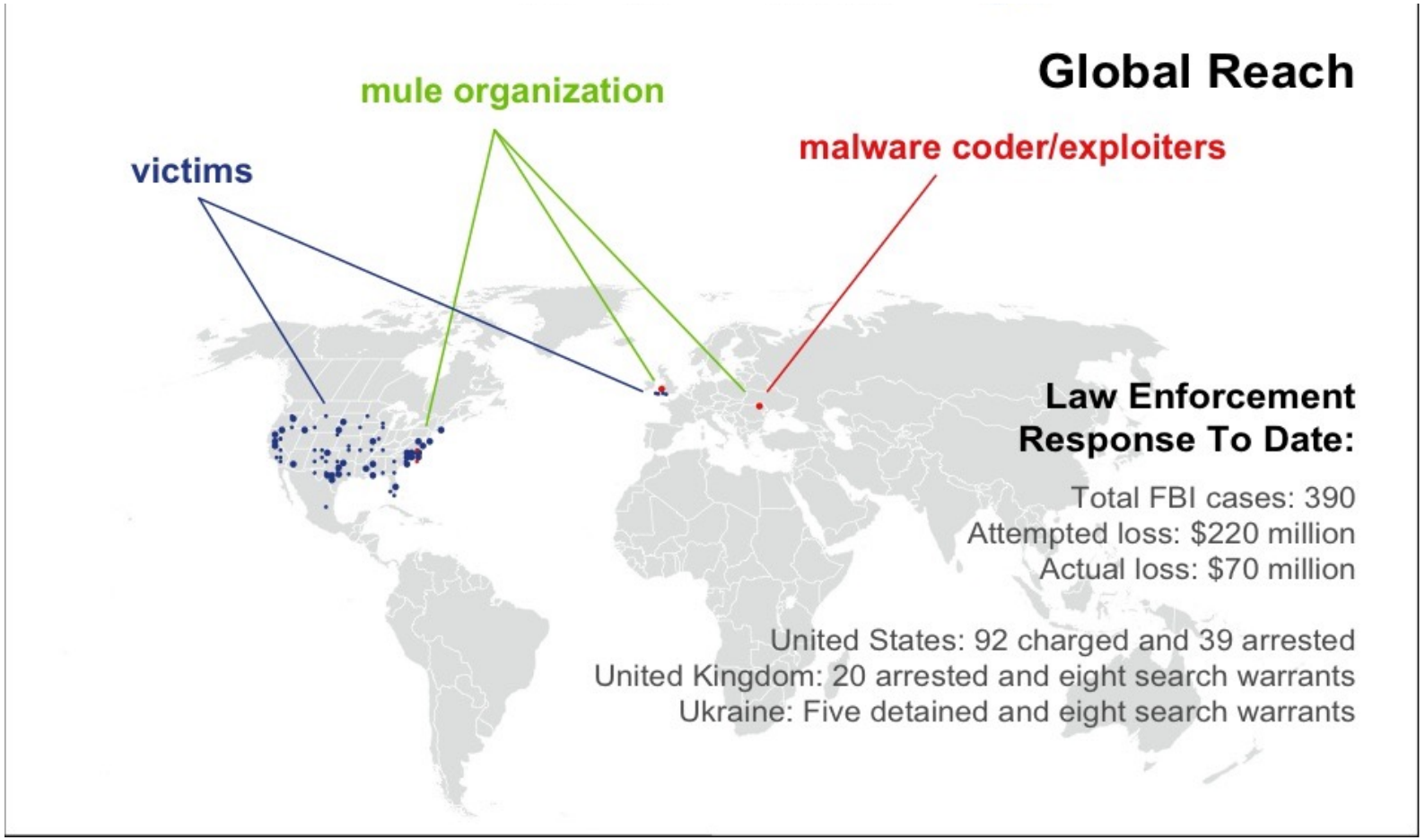
Zeus Malware Used in Organized Crime



Zeus Malware Used in Organized Crime



Zeus Malware Used in Organized Crime



Implications

- Zeus malware made attacking home/small business computers lucrative
  - Steal user's account
  - Steal small business's Point-of-Sale machine and steal money from there..
    - Adjust revenue, steal customer's payment information, etc…
- Demonstrated that Cyber Organized Crime to attack mass is possible
  - But they require mules for money laundering

Remote Access Trojan, and Exploit-as-a-service

- A more generalized version of Zeus
- Objective: attack, and get into the victim's computer and completely control that -> do whatever the botmaster commands
- Black hat hacking groups build them
- Sell the trojan kit to script-kiddy attackers
  - Now organized crime can be possible w/o having computer security knowledge

Ransomware

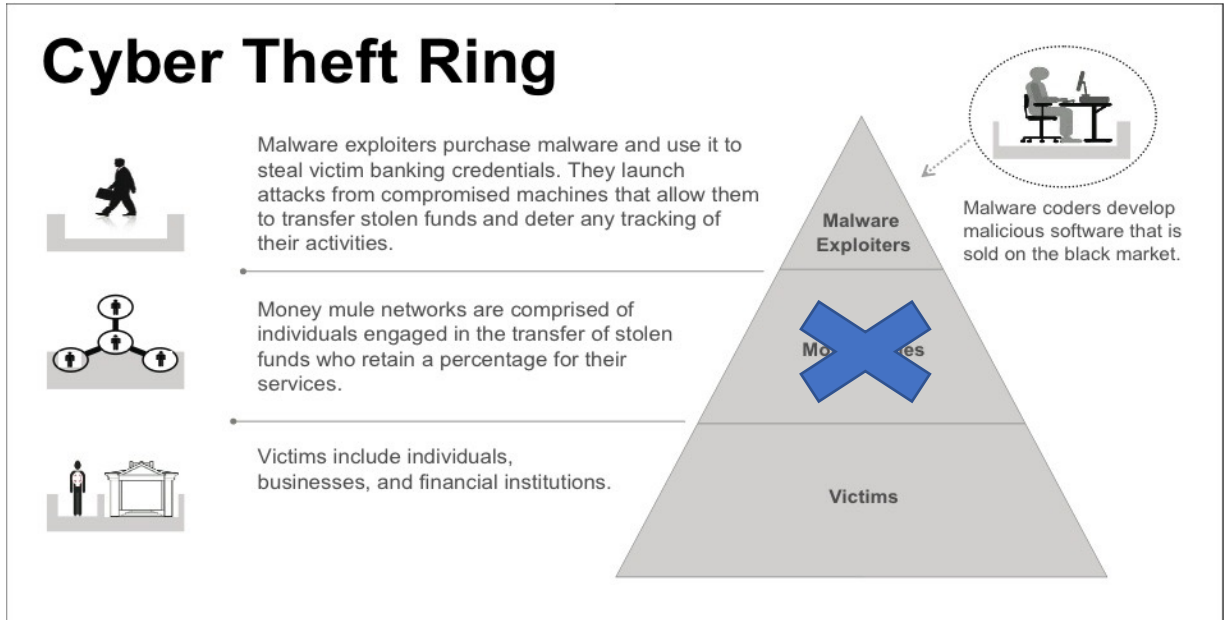
- End-user's computer in early 2000
  - Store some game
  - Word/Excel data
  - …
- End-user's computer in 2022
  - Credit card information
  - Stored password
  - Photos
  - Valuable private data (legal/health data, history of class homework, etc…)

Ransomware

- Encrypt user's valuable data and ask for $$$ for the decryption key
- User has a lot of valuable data in their computers…
  - Constructed a good business model
- Ransomware kit made attack can easily be launched by script kiddies
  - Can launch the attack w/o computer knowledge at all
- Cryptocurrency made money laundering easy
  - Anyone can do money laundering w/o being caught.. with 30~40% fee…

Ransomware

- Rise of Cryptocurrency
  - Anonymous financial transaction is possible: Monero, Z-Cash, etc..
  - Easy money laundering service: Bitcoin mixers



Ransomware Kits and as a Service

TREND MICRO

Dla firm | Dla domu

Wiadomości bezpieczeństwa > Cybercrime & Digital Threats > New Ransomware Goliath Up for Sale on Dark Web Site

New Ransomware Goliath Up for Sale on Dark Web Site

18 maja 2016

Malware and computer forensics expert Lawrence Abrams has uncovered a dark web site advertising its ransomware-related products and services.

The site, named "Hall of Ransom," can be accessed through the Tor network and sells the Locky ransomware for $3,000. Locky infiltrates the system through a malicious macro in Microsoft Word document sent as email attachments to its victims. Its recent casualties include the Kentucky-based Methodist Hospital

- LockBit and Black Basta Are the Most Active RaaS Groups as Victim Count Rises: Ransomware in Q2 and Q3 2022
- Ransomware Spotlight: BlackCat
- Ransomware Spotlight: Black Basta
- Ochrona zwiększającej się powierzchni ataku: Półroczny raport

What is Ransomware as a Service (RaaS)?

Ransomware as a Service (RaaS) is a **business model** between ransomware operators and affiliates in which **affiliates pay to launch ransomware attacks developed by operators**. Think of ransomware as a service as a variation of software as a service (SaaS) business model.

RaaS kits allow affiliates lacking the skill or time to develop their own ransomware variant to be up and running quickly and affordably. They are easy to find on the dark web, where they are advertised in the same way that goods are advertised on the legitimate web.

A RaaS kit may include 24/7 support, bundled offers, user reviews, forums and other features identical to those offered by legitimate SaaS providers. The price of RaaS kits ranges from $40 per month to several thousand dollars – trivial amounts, considering that the average ransom demand in 2021 was $6 million. A threat actor doesn't need every attack to be successful in order to become rich.