School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko
Cybersecurity Fundamentals

Malware

Learning goals

- Malware and goodware
- Trojans, viruses and worms
- Delivery methods
- Infection targets
- Malware payloads

PART I:

What is malware? And the different types of malware

Malware

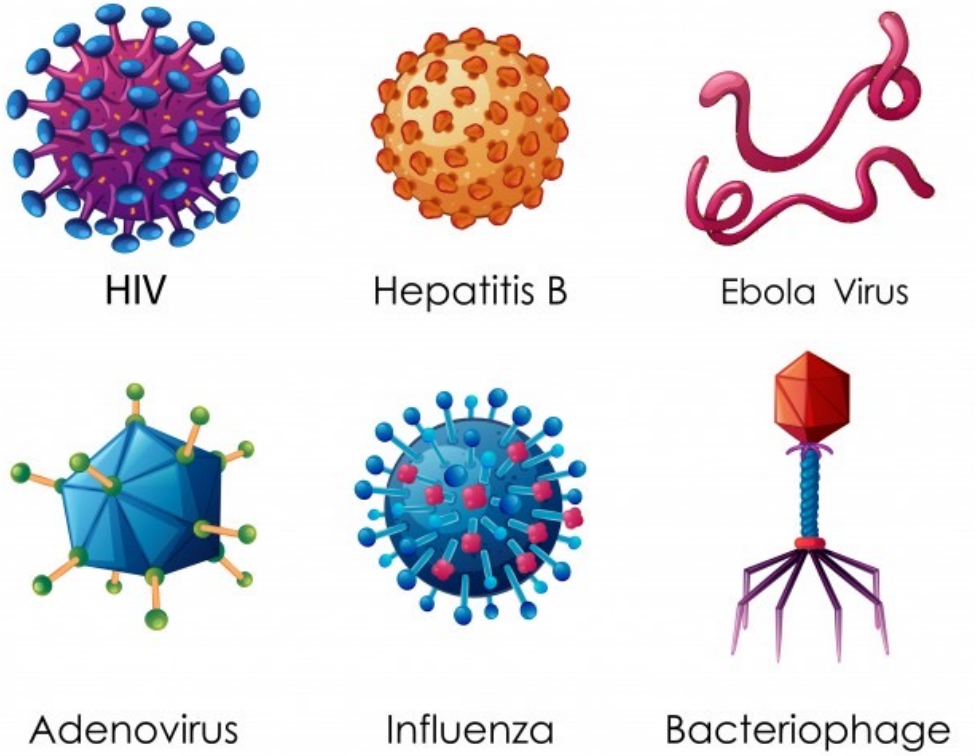
- Computer malware is the **broad category** of **software** that is **specifically** designed to disrupt, damage, or gain unauthorised access to a computer system.
- Includes viruses, trojans, ransomware etc.
- Can be **distinguished** from each other in terms of how they **propagate** between computers and how they **operate**.
- Multiple malware types might be **packaged together** – blended attacks.

Trojan Horse

- Program with an ***overt*** purpose (known to the user) and a ***covert*** purpose (unknown to the user)
- It looks **legitimate** but can take **control** of your computer.

- The user must choose to **execute** the Trojan.
- Examples:
  - fake AV trojan, infostealer trojan, remote access trojan ...

Viruses



- Infective agent.
- **Multiplies** within the living cells of a host.
- Doesn't have any purpose beyond **replicating** itself.

Definition of a Virus

- A program that **inserts** itself into one or more files and performs some **action**
  - The **insertion phase** is inserting itself into file
  - The **execution phase** is performing some (possibly null) action

  The insertion phase must be present

- Need not always be executed

Pseudocode

```
beginvirus:
    if spread-condition then begin
        for some set of target files do begin
            if target is not infected then begin
                determine where to place virus instructions
                copy instructions from beginvirus to endvirus
                    into target
                alter target to execute added instructions
            end;
        end;
    end;
    perform some action(s)
    goto beginning of infected program
endvirus:
```

BRAIN (Pakistani) virus

- The first PC virus (1986)
- Written for IBM PCs
- Alters boot sectors of floppies, spreads to other floppies

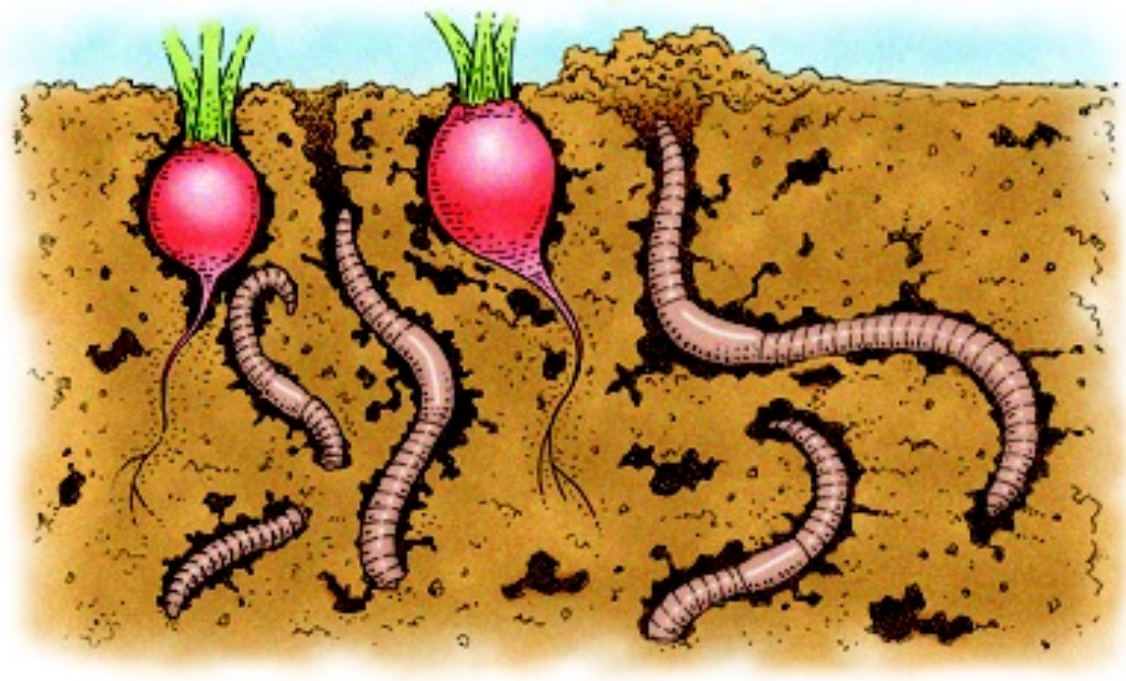
https://www.youtube.com/watch?v=lnedOWfPKT0&t=4s

Victoria University history

Stoned (New Zealand) virus (1987)

- Written for IBM PCs
- Boot sector virus
- One in eight times “Your PC is now Stoned!”

Worms



- Worms follow tunnels
- Find vulnerable vegetables

Worms

A program that **copies** itself from one computer to another

1. **Probes** other machines looking for a **vulnerability** that can be exploited to copy itself to.
2. **Penetrate** the vulnerable machine by performing the operations for **exploiting** the vulnerability.
3. **Download** itself to the remote machine, and store itself there. This is often called the **'persist' stage**.
4. **Propagate** itself by picking new machines to attempt to probe.

First ever worm (1988)

https://www.youtube.com/watch?v=fj8S6Hd-5bk

The Dark Genius

- 23-year old Cornell graduate student
- *Robert Tappan Morris*
- More a **prank** than an attack
- Prosecuted in 1989 under Computer Fraud and Abuse Act
- Fined, probation and 400 hours of community service
- Lead to first ***Computer Emergency Response Team*** (CERT) in the world

Morris Worm — FBI

Morris Worm of 1988

- Targeted Berkeley, Sun UNIX systems
  - Used virus-like attack to inject instructions into running program and run them
  - To recover, they had to **disconnect** the system from the Internet and reboot
  - To prevent **re-infection**, several critical programs had to be patched, recompiled, and reinstalled

- Disabled several thousand systems in 6 or so hours

PART II:
Delivery methods

How does malware spread?

- *How does malware hop from machine to machine (**propagate**)?*
- Combination of **human** and **technical factors**.
  - Links in email.
  - Malware attached to email.
  - Illegal copies of software.
  - Network shared.
  - Messaging services.
  - USB sticks.
  - Web sites via drive-by-downloads.

Malware often arrives in stages

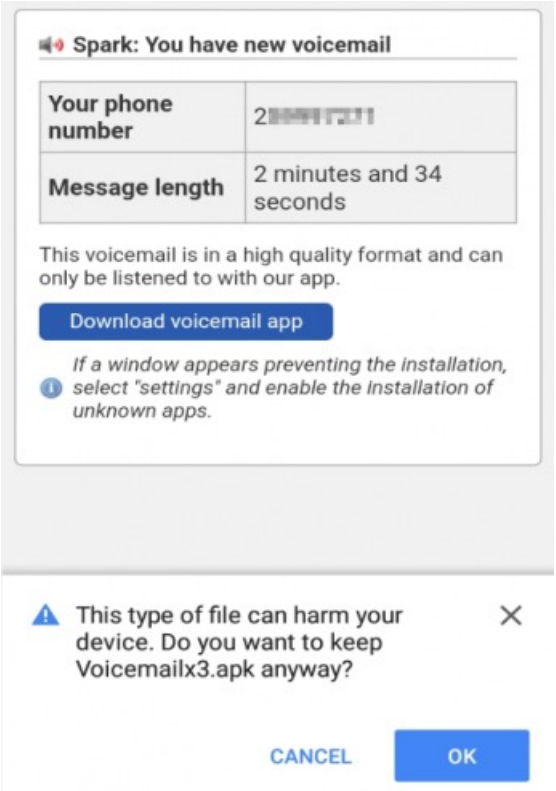
- Dropper malware
  - **Downloads** other malware
  - Designed to **evade anti-virus**
  - Delivery system for criminals

- Multi-stage malware exploits
  - More than one dropper involved
  - Use encryption to obfuscate activity

https://unit42.paloaltonetworks.com/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/

Example: Flubot (2021)

- Flubot trojan (FluBot malware infecting Android phones | CERT NZ)
  - Receive a mesage "***you have a new voicemail***" etc.
  - Click on link to trojan to download
  - Downloading and running trojan leads to infection
  - Steal financial login and password data

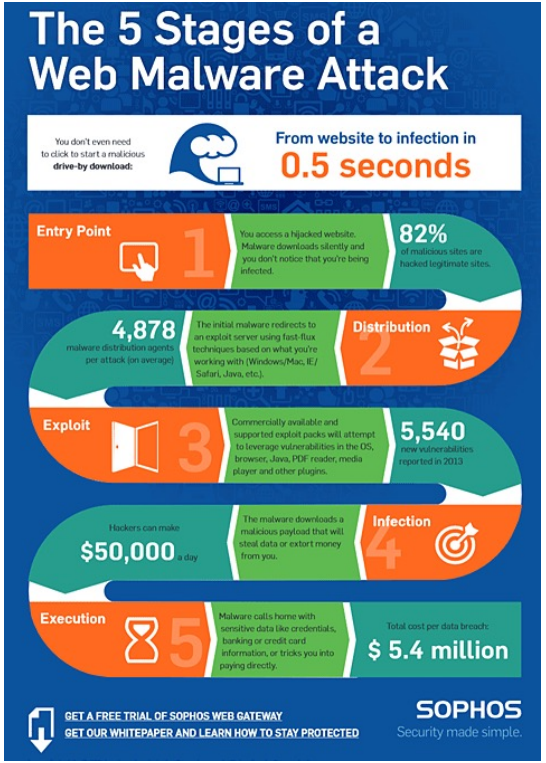


Example: APT 34 (June 2019)

- APT34 – **Advanced Persistent Threat**
  - Nation-state hackers
  - Attributed to **Iranian government**
  - **Espionage** against decision-makers and key organisations
  - Financial, energy and government entities
- Methods
  - Impersonate members of Cambridge University to gain access via **emailed** malicious documents
  - **LinkedIn** used to deliver malicious documents
  - Malicious documents allow **persistent backdoor** access to systems
- **Stealthy** infiltration over a long time period

Example: Drive-by-download

- Web malware attack.
- Visit a website.
- Code on site **exploits vulnerability** in web browser.
- **Drops** malware onto your machine.
- Waterhole attack is where delivered via legitimate site (e.g. **Metservice**)



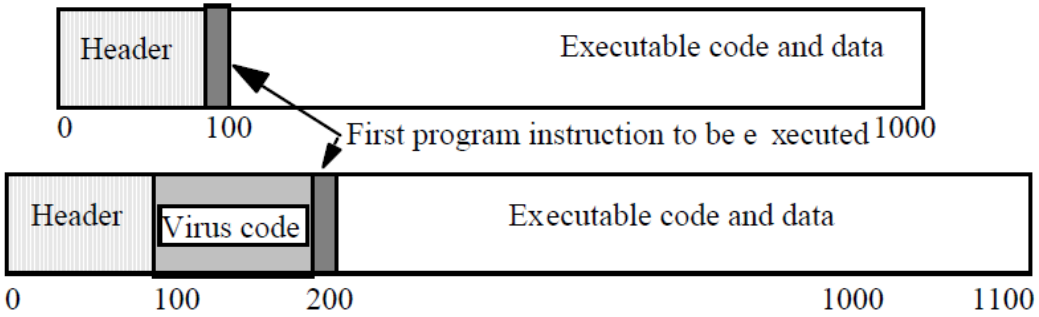
https://www.webopedia.com/definitions/drive-by-download/

PART III:
Infection targets

Infect media

- **Boot sector** virus targets the boot sector used to start operating system
- Propagates by infecting connected **media**
- **Stoned** was an example of this with **floppy disks**.
- **Autorun virus**, triggered when insert USB drive into Windows machine.
  - Disable autorun

Infect executable files



A virus that infects executable programs

- Can infect .EXE, .DLL or .COM on PCs
- May prepend itself (as shown) or put itself anywhere, fixing up binary, **so it is executed at some point**

Infect memory (RAM)

- A virus that **stays active in memory** (RAM) after the initial infection
- May **delete itself** from the hard drive to **avoid detection** by anti virus
  - Example: TSR viruses
  - TSR is "Terminate and Stay Resident"
- It may never even end up on the hard drive
  - Cryptojacker malware
  - Javascript executing in victim's webpage
    https://blog.sucuri.net/2018/10/obfuscated-javascript-cryptominer.html

Infect documents

- Many programs support an **interpreted macro-language**
  - E.g. Visual Basic for Applications (VBA)
- A macro virus infects a document and executes when opened
- Trick people into **enabling** macros

Author:
Elizabeth Montalbano
April 17, 2020 / 10:33 am

Hackers Update Age-Old Excel 4.0 Macro Attack

XLS files sent via emails appear password protected but aren't, opening automatically to install malware from compromised macros, according to researchers.

https://threatpost.com/hackers-update-age-old-excel-4-0-macro-attack/154898/

Infect ALL the things

- **Multipartite virus** - originally a virus that can infect either boot sectors or executables
  - If one infection path is blocked, choose the other

- Today it is more general
  - Any virus that has multiple ways to infect a computer

PART IV:
Malware payload types

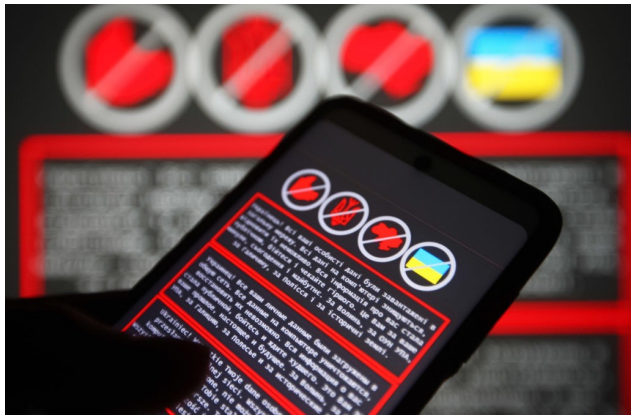
Financial gain

- Ransomware
  - Steal your data
  - Prevent access via encryption
  - Sell your data
- REvil (Ransomware Evil)
  - Waikato DHB May 2021
  - Hundreds of servers, network sites, thousands of workstations, mobile devices and medical equipment
  - Surgeries, chemo services cancelled and release of data
  - Took months to recover from the attack

https://www.the420.in/revil-ransomware-gang-hacked-and-taken-down-in-multi-country-operation/

Destruction

- Wiper malware
  - May pretends to be ransomware
  - Destroys data to disrupt target activities
- WhisperGate (2022)
  - Targetting at least 70 Ukranian government websites
  - First stage wipes the boot sector
  - Downloads second stage DLL from discord server
  - Second stage executes DLL dropper
  - DLL dropper downloads third stage to do wipe
  - Seeks out all attached drives



https://gridinsoft.com/blogs/microsoft-discovered-the-whispergate-wiper-attacking-ukrainian-users/

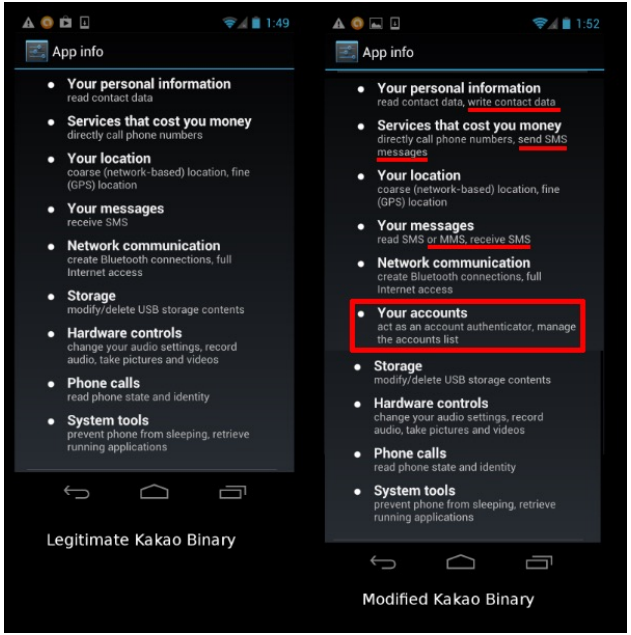
Defacement

- Target websites
  - Political message
  - Bragging rights
- UK National Health Services website (2018)
  - Hosting data from patient surveys
  - AnoaGhost are a hacking crew
  - It was up for **five days** before being noticed

https://www.bbc.com/news/technology-43812539

Information gathering

- **Spyware** tracking user activity
- **Keyloggers** capturing passwords
- Malware targeting Tibetans (2013)
  - Android malware
  - Trojan messaging software
  - Delivered via email
  - Reports base station ID, tower ID, mobile network code and mobile area code
  - Part of ongoing campaign

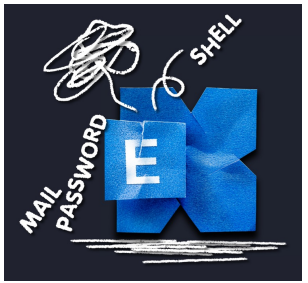


https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/

Maintain access

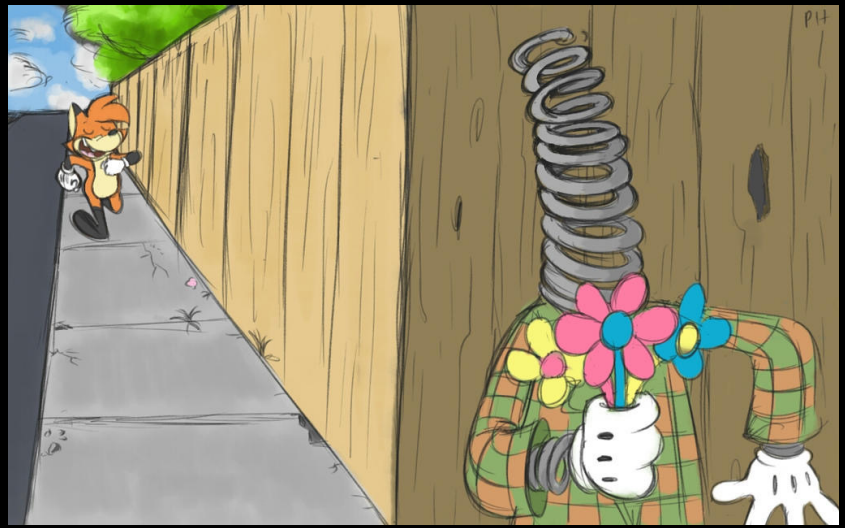
- Backdoor
  - Method to get around normal security
  - Cheat codes built into the system
- Remote access trojan
  - Network access
  - Installed by the attacker
  - Example: **Hodur** (2022) RAT from China
- Web shells
  - Installed on web server
  - Written in Javascript, PHP etc.
  - Navigate to magic URL for access
  - Example: **ProxyLogon** (2019) affects Microsoft exchange

https://thehackernews.com/2022/03/chinese-mustang-panda-hackers-spotted.html



https://proxylogon.com/

PART V:
What’s next



What's up next

- Next lecture we look at anti-malware approaches.

- How do we protect ourselves against malware?