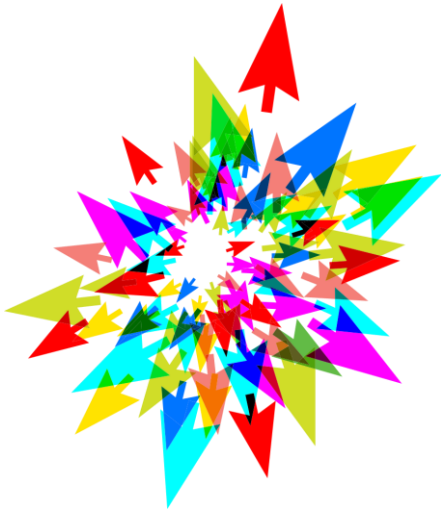
# Securing your Research on Compute Canada Clusters and Clouds

## Day 1




Prepared by:
Raphaelle Gauriau
Information Systems Security Manager, SciNet

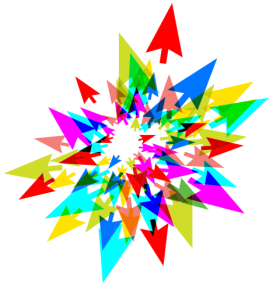
# A few words

- Cybersecurity Operations since 2011
- Worked in different sectors (legal, energy, security consultation)
- Compliance: NERC, ISO-27001

# Audience

- To **researchers** who…
  - are using Compute Canada clusters and Cloud
  - want to learn more about cybersecurity
  - want to know **practical best practices** from an end user perspective
  - want to **better protect** their research

# Agenda



## Day 1

Cybersecurity Concepts

Cybersecurity Attacks

Best practices

Assignment 1

## Day 2

Best practices (suite)

Cryptography Concepts

SSH keys usage

Assignment 2

## Day 3

*Speaker*: Rachel Zand
Director, Human Research Ethics at the University of Toronto

Human Research Data

Security and Research Ethics Board

Assignment 3

# SCMP183 Securing Your Research on Compute Clusters and Clouds (Nov/Dec 2021)

Dashboard / My courses / SCMP183 - Nov/Dec 2021

Your progress

## SCMP183 Securing Your Research on Compute Clusters and Clouds (Nov/Dec 2021)

Learn how to protect your research using cybersecurity techniques. During the three days of this workshop, we will cover various aspects of cybersecurity to help you protect your research! Cybersecurity concepts, cyberattack models, as well as best practices to protect your research will be reviewed. We will talk about cryptography and you will get to apply the concepts to a real life scenario using SSH keys. Finally, we will discuss cybersecurity in the context of human research data and the Research Ethics Board. The workshop will be a mix of theory and practical exercises. We hope you will learn something new and, more importantly, enjoy the sessions!

Sessions will be delivered in English, but we will have the ability to respond to questions in French. The lesson material will be available in English. A French version of this workshop will take place at a later date.

This workshop is part of the National Training series of the Compute Canada Federation. Registration is handled at

https://www.eventbrite.ca/e/ccf-national-training-securing-your-research-on-compute-clusters-and-cloud-tickets-173830691277

Teachers: Raphaelle Gauriau, Paul Preney, Ramses van Zon, Rachel Zand
Start date: 29 Nov 2021
End date: 3 Dec 2021
Scientific Computing Credits: 4

Announcements

### Day 1: Mon., Nov. 29, 12:30PM to 2:00 PM EST

Zoom Link Day 1 (Monday, 29 November, 12:30 PM - 2:00 PM)

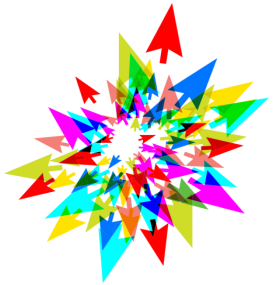
Assignment - Day 1

Day 1 Feedback

Restricted Available from **29 November 2021, 2:00 PM**

Please provide us feedback concerning Day 1 of this course. (Any feedback left is anonymous unless you identify yourself in the feedback.)

# Agenda



## Day 1

Cybersecurity Concepts

Cybersecurity Attacks

Best practices

Assignment 1

## Day 2

Best practices (suite)

Cryptography Concepts

SSH keys usage

Assignment 2

## Day 3

*Speaker*: Rachel Zand,
Director, Human Research Ethics

Human Research Data

Security and Research Ethics Board

Assignment 3

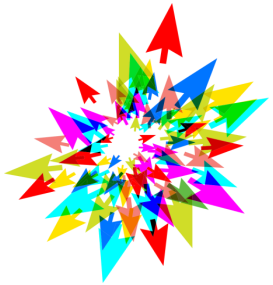
# Agenda – Day 1

- Cybersecurity Concepts
- Cybersecurity Attacks
- Best practices

Assignment 1

# Cybersecurity Concepts

# What is Cybersecurity? (1/3)



Answers from non cybersecurity practitioners:

“It aims at protecting **digital assets**”

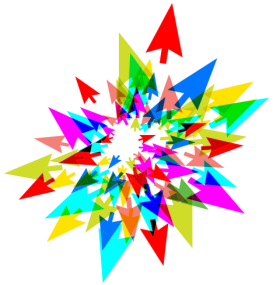
“It prevents **hackers** from breaking into systems and **stealing data and money**’’

“It refers to **protocols** established to **defend** information data”

“The protection against the **risks** of attacks to computers by limiting **vulnerabilities**”

# What is Cybersecurity? (2/3)

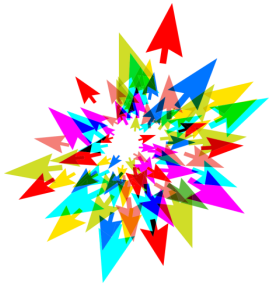
# What is Cybersecurity? (3/3)



- **Cybersecurity:** An approach or series of steps to **prevent or manage the risk** of damage to, unauthorized use of, exploitation of, and—if needed—to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems.
- **Vulnerability:** A **weakness** in a system, application, or network that is subject to exploitation or misuse.

Source: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary

# What do we do about risks?

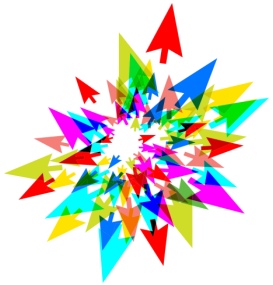


## Scenario 1:

Arbutus Cloud Team contacts you to let you know that two virtual machines (VMs) in your Cloud lab are exposed on the Internet while they should not be.

Those VMs were configured by a researcher from your group who has retired.

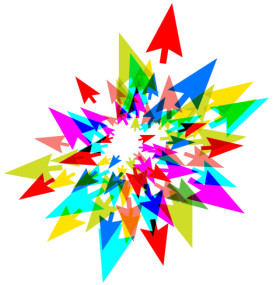
# What do we do about risks?



## Scenario 2:

You have a Windows 2003 server in your lab environment that contains a legacy application used for some important project. It cannot be upgraded at this time.

# What do we do about risks?



## Scenario 1:

Arbutus Cloud Team contacts you to let you know that two virtual machines (VMs) in your Cloud lab are exposed on the Internet while they should not be.

Those VMs were configured by a researcher from your group who has retired.

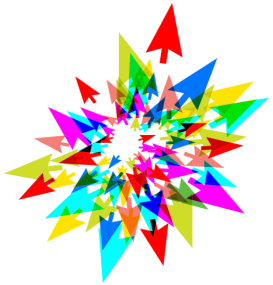
## Scenario 2:

You have a Windows 2003 server in your lab environment that contains a legacy application used for some important project. It cannot be upgraded at this time.

**Our Options:**

- **Avoid/Resolve**
- **Mitigate**
- **Transfer**
- **Accept (when none of the other options are feasible; often based on a ratio cost/benefit)**

# Cybersecurity



| | List of domains |
|---|---|
| 1 | Security and Risk Management |
| 2 | Asset Security |
| 3 | Security Architecture and Engineering |
| 4 | Communications and Network Security |
| 5 | Identity and Access Management |
| 6 | Security Assessment and Testing |
| 7 | Security Operations |
| 8 | Software Development Security |

Source: https://resources.infosecinstitute.com/certification/the-cissp-domains-an-overview/

# Defense in-depth

# Types of defense

- **Physical Controls**

  Examples: security guards; locked doors.

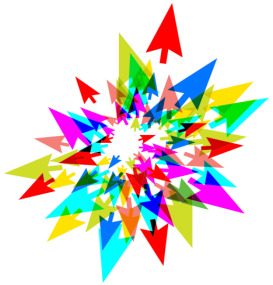
- **Technical Controls**

  Examples: firewalls; anti-virus.

- **Administrative Controls**

  Examples: training employees against phishing attacks.

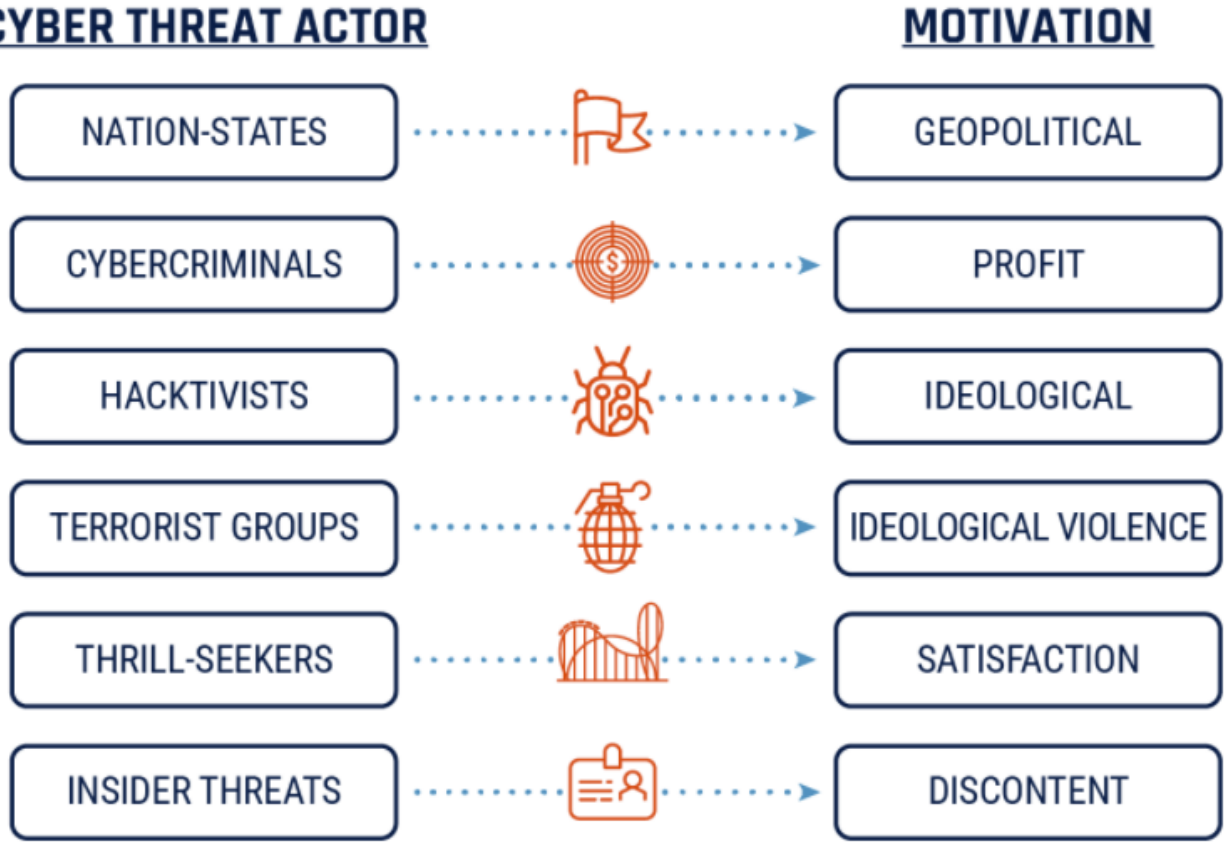
# Cybersecurity Attacks



‘’If you **know the enemy and know yourself**, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.’’

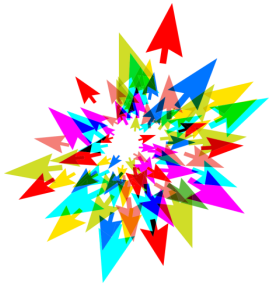
Sun Tzu, *The Art of War*

# Who are the attackers?




Source: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

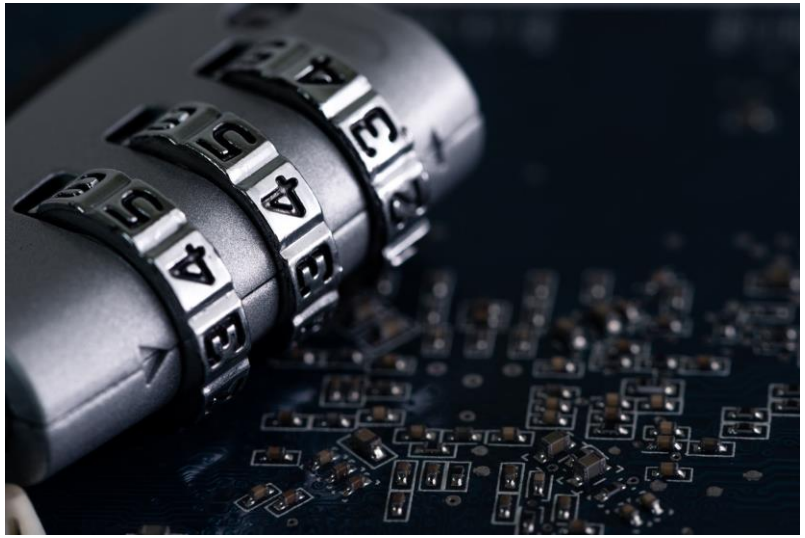
# Scenario – let’s be creative!



You are a white hat and have been tasked to steal the list of personal information at company X as part of a security mandate.

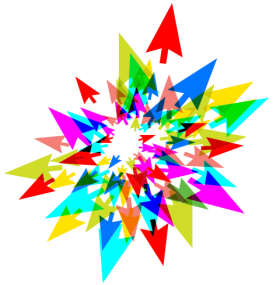
How do you achieve this goal?

What are the steps?



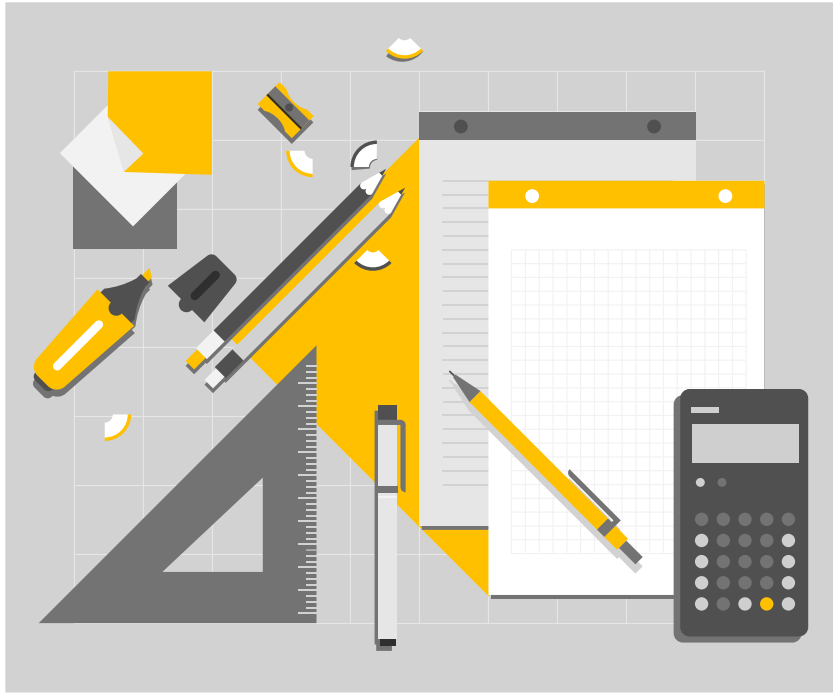
Source: PowePoint stock images

# Scenario – step 1



## Gather information

- Collect information on the employees
- Go to company X office, monitor trends
- Collect technical details



Source: PowerPoint stock images

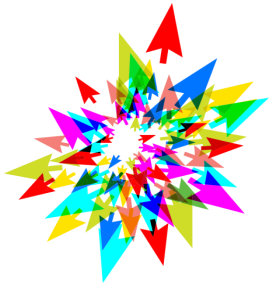
# Scenario – step 2

## Craft the attack

- Define initial access (phishing, external remote access, trusted relationship…)
- Payload

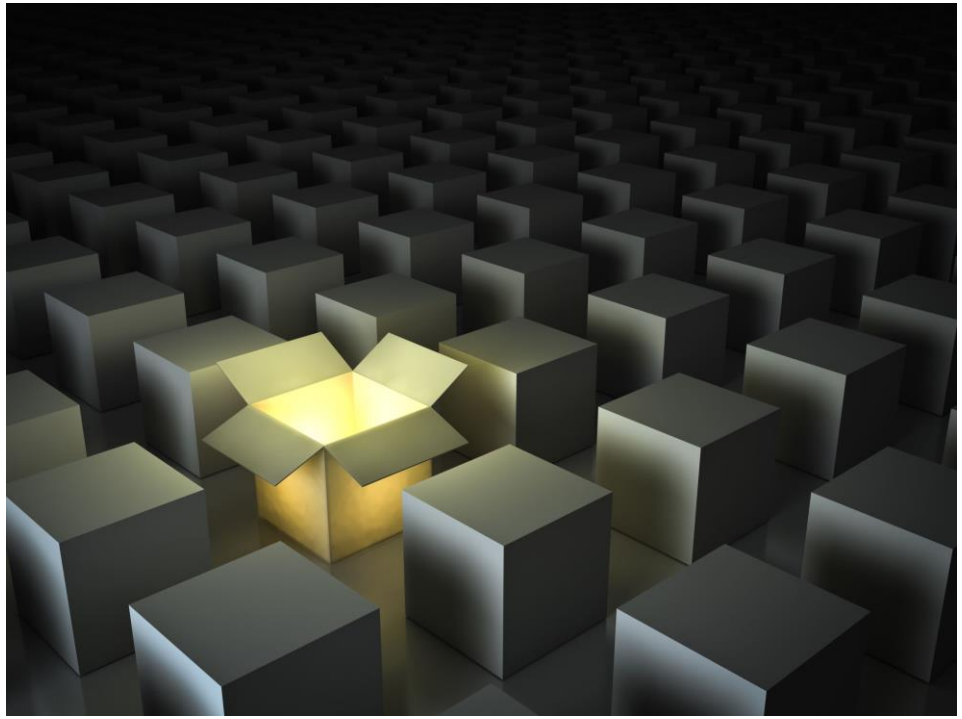
Source: PowerPoint stock images

# Scenario – step 3



## Deliver, exploit, install

- Execute the attack previously crafted
- Compromise system



Source: PowerPoint stock images

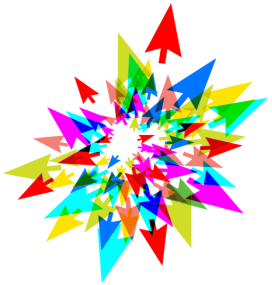
# Scenario – step 4

## Command&Control, Achieve objective

- Escalate privileges
- Move laterally
- Steal personal information

Source: PowerPoint stock images

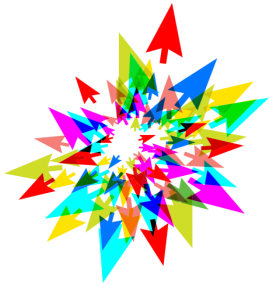
# Cyber Kill Chain



# Anonymous Survey –

## What is your workstation's operating system?

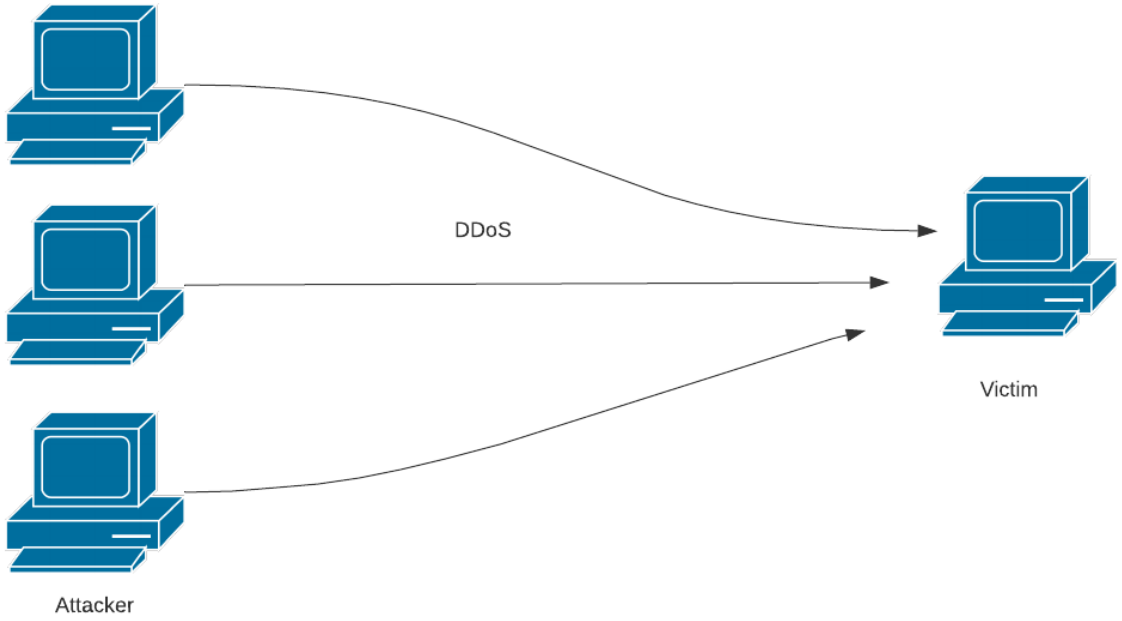
# Types of Cyberattacks – Malware (1/4)



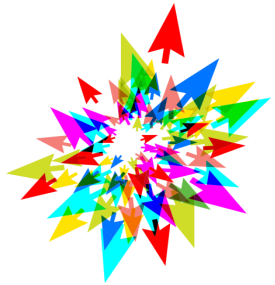
- Malicious computer program
- Many types: viruses, worms, ransomware, Trojan horses, rootkits…
- Popular: Ransomware
- How to prevent them: anti-malware; keep your systems updated

# Types of Cyberattacks – DoS (2/4)

- DoS = Denial of Service
- DDoS = Distributed Denial of Service
- Makes a machine or network resource unavailable
- How to prevent them: Intrusion Prevention System (IPS)



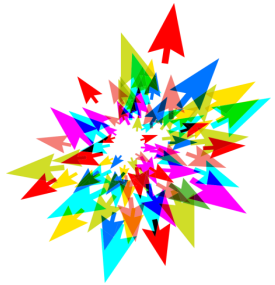
# Types of Cyberattacks – Man-in-the-Middle (3/4)



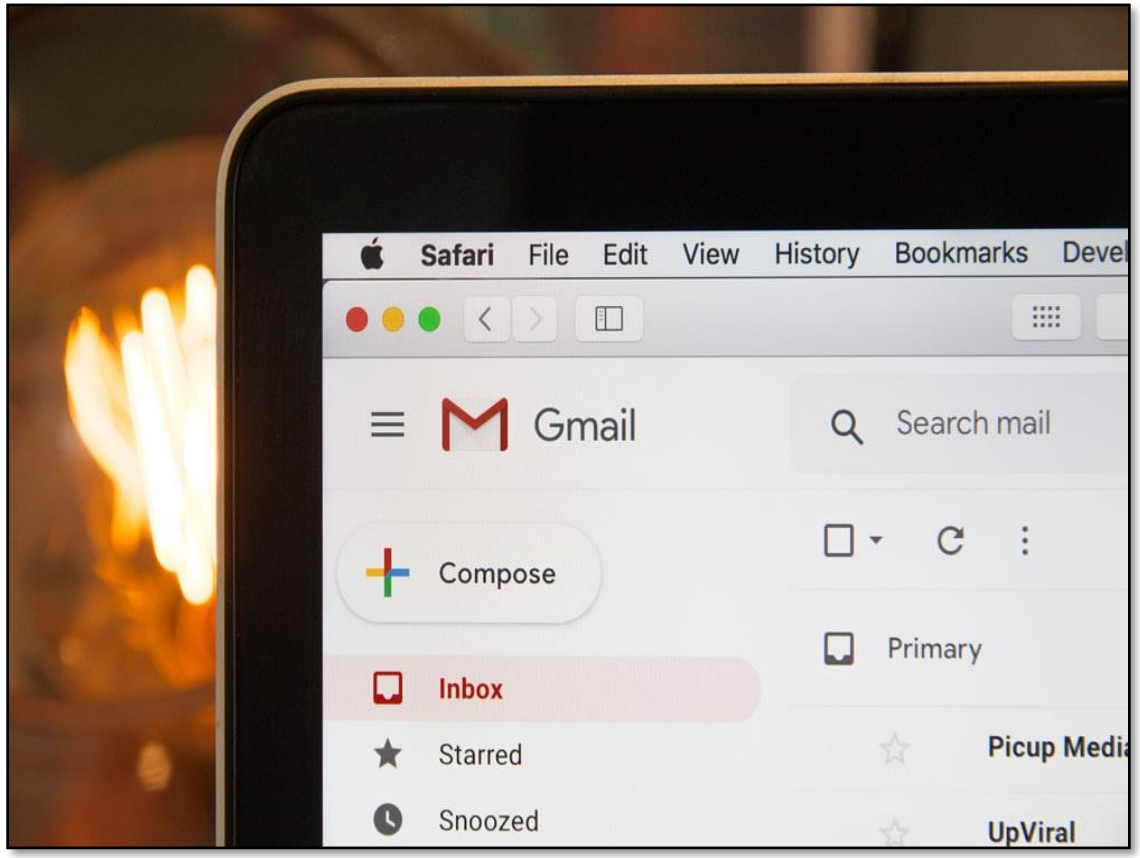
- Proxies the data between the sender and recipient


- How to prevent it: encryption

# Types of Cyberattacks - Phishing (4/4)



- Attempts to acquire sensitive data
- Emotions
- Increase during the pandemic
- How to prevent them: users training awareness



**From:** Dr. Jane Doe <Jane.Doe.utoronto.ca@gmail.com>
**Sent on:** Friday, April 10, 2020 5:58:02 PM
**To:** [redacted]@mail.utoronto.ca
**Subject:** Got a moment

Available?
--

Dr. Jane Doe
University Professor
B.Eng., M.Eng (McGill), Ph.D. (Stanford), P.Eng.
Canada Research Chair in in Transnational Molecular Geometry

Source: https://securitymatters.utoronto.ca/phish-got-a-moment/

**From:** Parking Ticket <billing@christiancinque.com>
**Sent:** Wednesday, August 1, 2018 16:44
**To:** [redacted]
**Subject:** Parking Ticket Reminder 39345008


# Parking violation notice

The City of Toronto records indicate that a parking tickets issued to the vehicle described below has not been paid. this fines and applicable penalty charges area past due and must be paid within the next 14 calendar days. Driving Records show that you are/were the registered proprietor at the time this vehicle was cited. Consequently you are legally responsible for responding to this notification.

| Ticket Number | Violation Type | Reduced Amount | Total Amount |
|---|---|---|---|
| 39345008 | No Stopping Zone | $22.00 | $25.00 |
| 39345783 | Wrong Colour Zone | $22.00 | $25.00 |
| | | **TOTAL:** | **$50.00** |

View photos taken by the bylaw officer who issued your ticket here.
Canada Parking Global Service

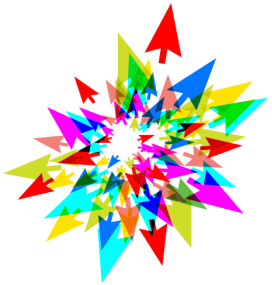


impark

Source: https://securitymatters.utoronto.ca/phish-got-a-moment/

# Best Practices

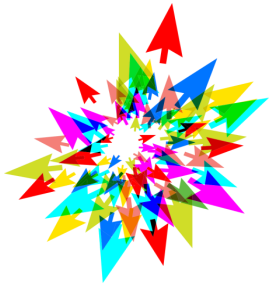
## End-Users



# Anonymous Survey –

## How often do you patch (update) your workstation?

# Do I really need to patch (update)?

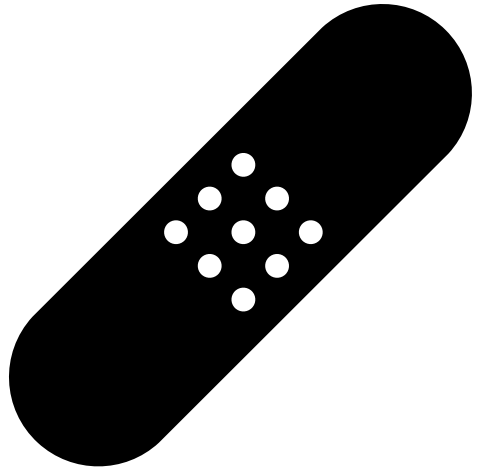


But… I am using multi-factor authentication!

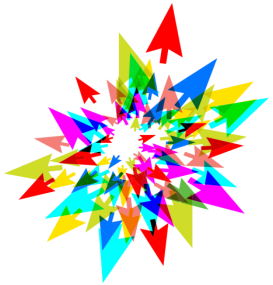
But… I am using a VPN!

But… I am only browsing on websites I know!

YES – YOU STILL NEED TO PATCH.



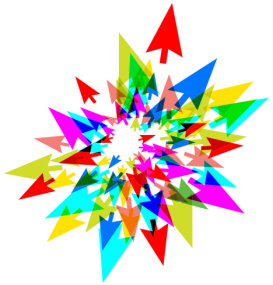
# WannaCry



- Happened in **May 2017**
- **Ransomware** infected over **230,000 machines** in over **150 countries**
- Estimated: **$4 billion in losses** across the globe.
- Organizations impacted: Telefónica (Spain); thousands of NHS hospitals and surgeries (UK); Fedex (US); Universities (China) etc….
- **Spreads itself** within corporate networks **without user interaction**

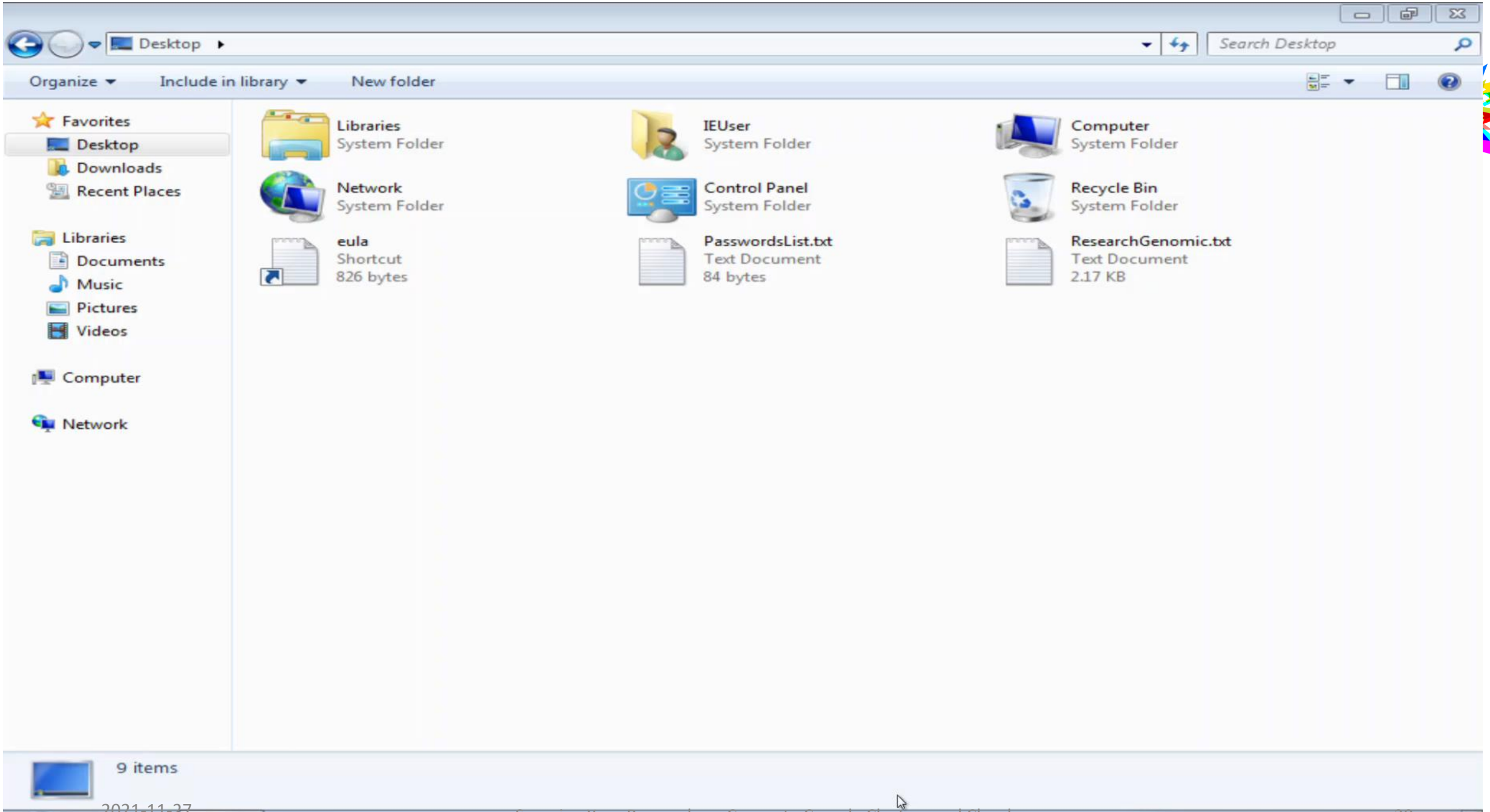
Source: https://www.sentinelone.com/blog/are-we-done-with-wannacry/
https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

# WannaCry



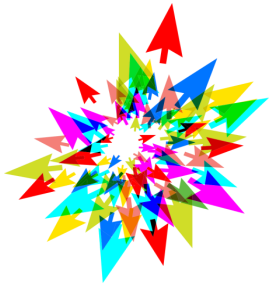
- **U.S. National Security Agency** discovered the vulnerability and **developed a code** to exploit it, called EternalBlue
- **Shadow Brokers** hacking group **stole the code** and made it public before WannaCry hit
- EternalBlue vulnerability in a Windows protocol called SMBv1
- Patch released in **March 2017**: MS17-010

Source: https://www.sentinelone.com/blog/are-we-done-with-wannacry/
https://www.kaspersky.com/resource-center/threats/ransomware-wannacry


Desktop
Search Desktop
Organize
Include in library
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Libraries
System Folder
IEUser
System Folder
Computer
System Folder
Network
System Folder
Control Panel
System Folder
Recycle Bin
System Folder
eula
Shortcut
826 bytes
PasswordsList.txt
Text Document
84 bytes
ResearchGenomic.txt
Text Document
2.17 KB
9 items
2:46 PM
5/16/2021

# Cyber Kill Chain

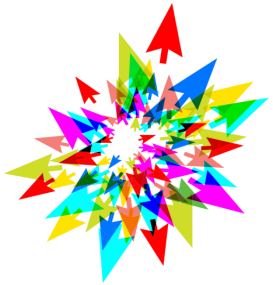
# Best practice #1 - Patch (update)



- Most breaches could be avoided by patching
- Operating systems
  - Windows, MacOS, Linux…
    - Windows 11
    - MacOS Monterey
    - Ubuntu 21.10
- Applications
  - Update to the latest version…
  - ….or uninstall them!

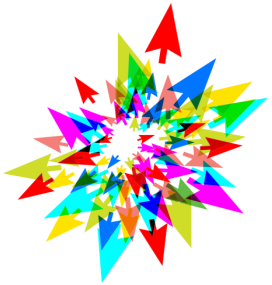
| macOS | Latest version |
|---|---|
| macOS Monterey | 12.0 |
| macOS Big Sur | 11.4 |
| macOS Catalina | 10.15.7 |
| macOS Mojave | 10.14.6 |
| macOS High Sierra | 10.13.6 |
| macOS Sierra | 10.12.6 |
| OS X El Capitan | 10.11.6 |
| OS X Yosemite | 10.10.5 |

# Exercise 1



Take a moment to collect the following information:

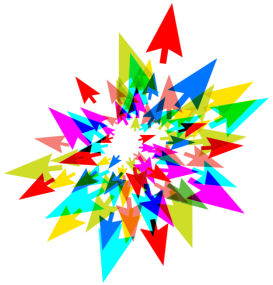
- Check your operating system version
- Find some application that needs to be updated or that is not needed anymore



# Anonymous Survey –

## Do you use an anti-malware on your workstation?

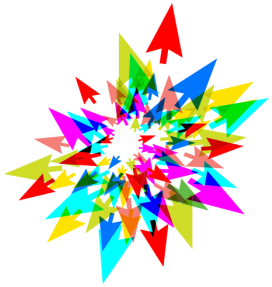
# Types of Anti-Malware



| Traditional methods | Modern methods |
|---|---|
| **Malware signature**<br><br>Signature: a continuous sequence of bytes that is common for a certain malware sample.<br><br>It tracks known threats | **Behavior analysis** (includes Machine learning)<br><br>It detects more sophisticated attacks: unknown threats; ‘’fileless attacks’’ |
| **Heuristic analysis**: detect viruses by examining code for suspicious properties<br>- Static<br>- Dynamic | |

Source: https://www.forcepoint.com/cyber-edu/heuristic-analysis

# Best practice #2 - Anti-Malware (1/3)



- Is it efficient?

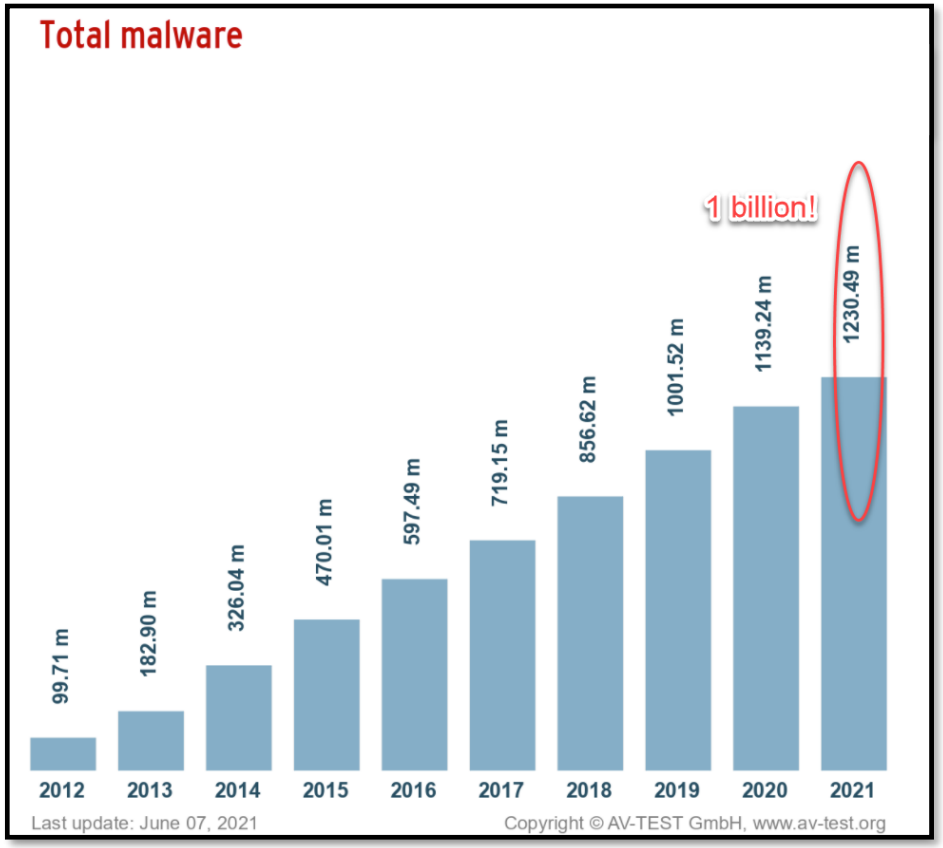
- Do I need it for MacOS?

Trojan Flashback - Malware Top 10 for macOS

- Do I need it for Linux?

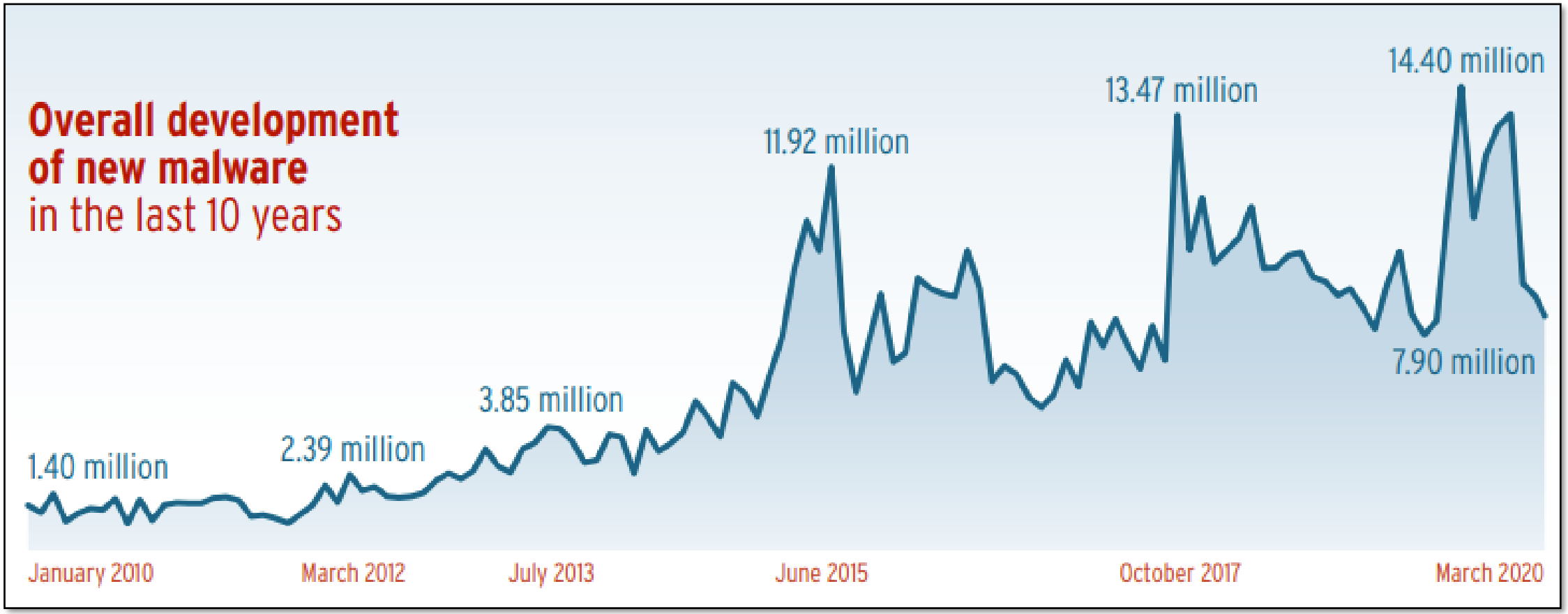
Mirai (IoT top 1)
EvilGnome spyware (2019)

- Do I need it on my mobile phone?



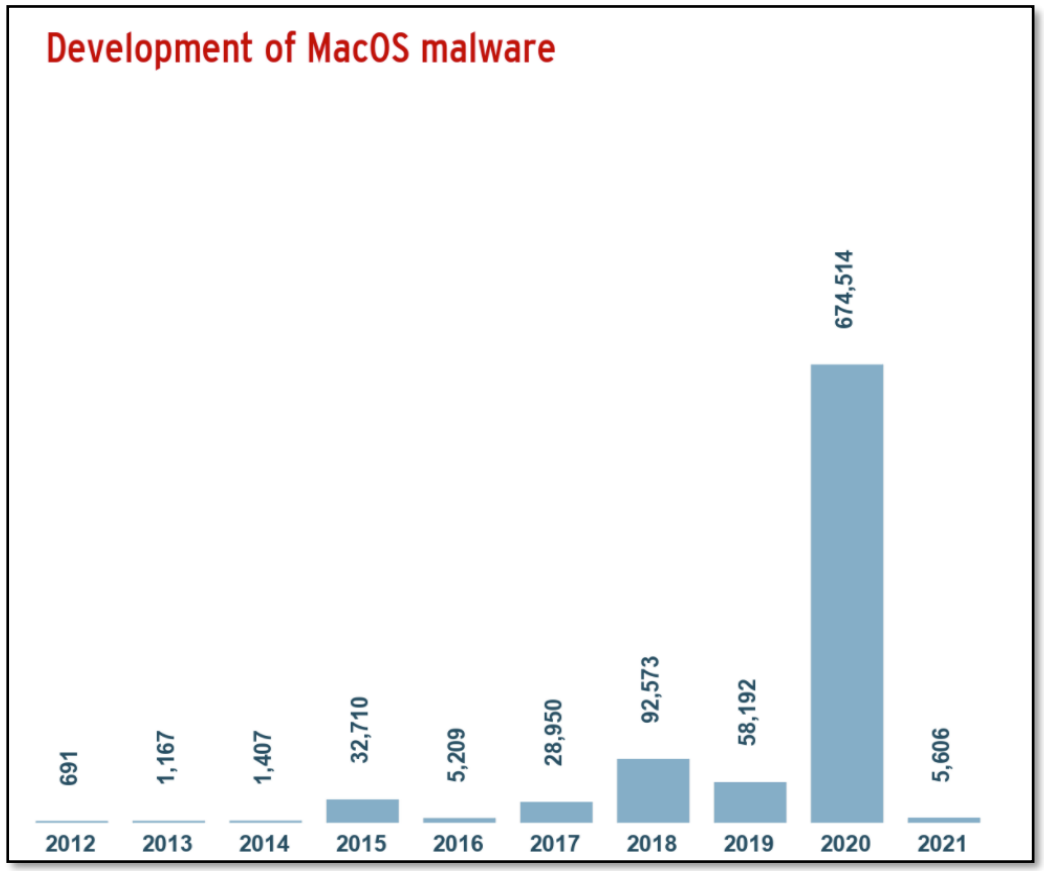

Source: AVTest Security Report 2021

# Best practice #2 - Anti-Malware (2/3)

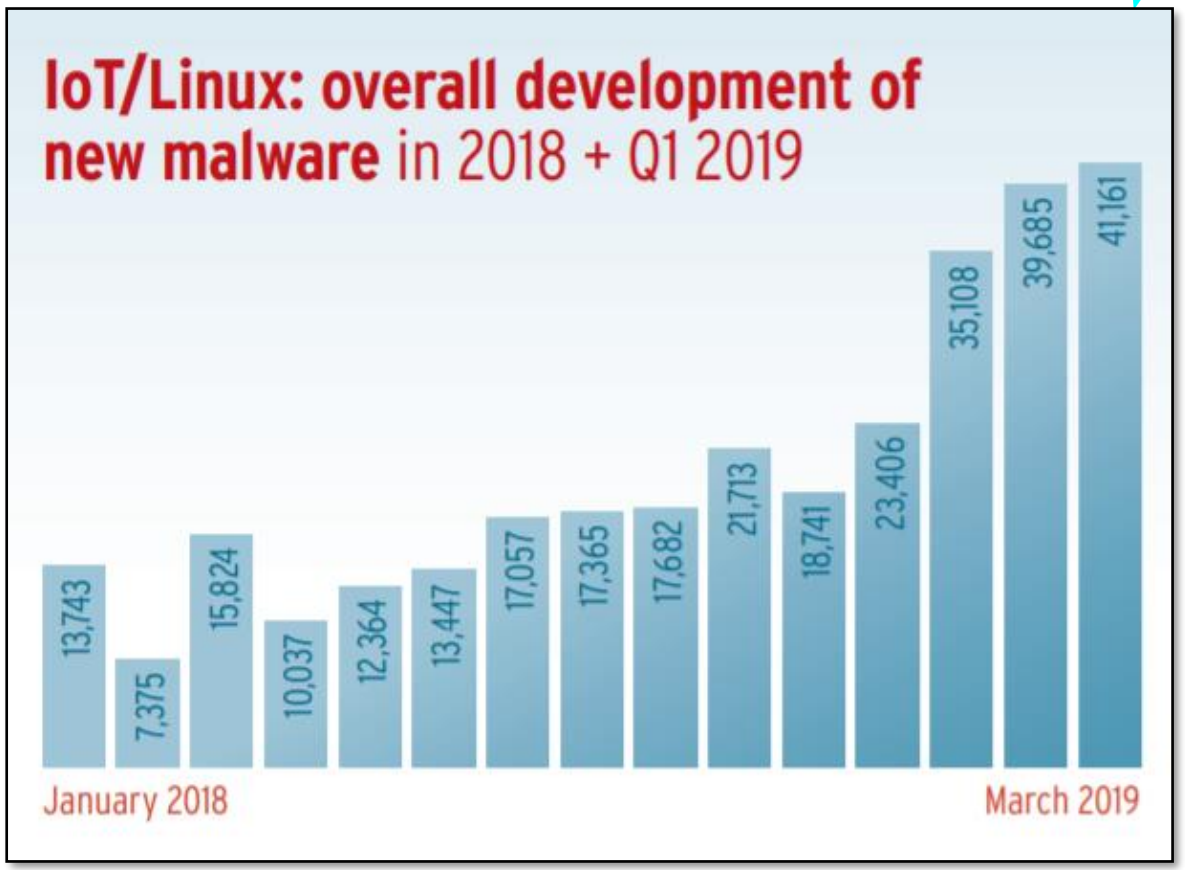



Source: AVTest Security Report 2019/2020

# Best practice #2 - Anti-Malware (3/3)




Source: AVTest Security Report June 2021




Source: AVTest Security Report 2018/2019

# Key Take-Aways – Day 1

- CIA triad
- Defense in-depth
- Cyber Kill Chain
- Keep your systems up to date!

# SCMP183 Securing Your Research on Compute Clusters and Clouds (Nov/Dec 2021)

Dashboard / My courses / SCMP183 - Nov/Dec 2021

Your progress

## SCMP183 Securing Your Research on Compute Clusters and Clouds (Nov/Dec 2021)

Learn how to protect your research using cybersecurity techniques. During the three days of this workshop, we will cover various aspects of cybersecurity to help you protect your research! Cybersecurity concepts, cyberattack models, as well as best practices to protect your research will be reviewed. We will talk about cryptography and you will get to apply the concepts to a real life scenario using SSH keys. Finally, we will discuss cybersecurity in the context of human research data and the Research Ethics Board. The workshop will be a mix of theory and practical exercises. We hope you will learn something new and, more importantly, enjoy the sessions!

Sessions will be delivered in English, but we will have the ability to respond to questions in French. The lesson material will be available in English. A French version of this workshop will take place at a later date.

This workshop is part of the National Training series of the Compute Canada Federation. Registration is handled at

https://www.eventbrite.ca/e/ccf-national-training-securing-your-research-on-compute-clusters-and-cloud-tickets-173830691277

Teachers: Raphaelle Gauriau, Paul Preney, Ramses van Zon, Rachel Zand
Start date: 29 Nov 2021
End date: 3 Dec 2021
Scientific Computing Credits: 4

Announcements

### Day 1: Mon., Nov. 29, 12:30PM to 2:00 PM EST

Zoom Link Day 1 (Monday, 29 November, 12:30 PM - 2:00 PM)

Assignment - Day 1

Day 1 Feedback

Restricted Available from **29 November 2021, 2:00 PM**

Please provide us feedback concerning Day 1 of this course. (Any feedback left is anonymous unless you identify yourself in the feedback.)

# Assignment – Day 1

1. What did you learn in today's session (1-2 items)?
2. Find one vulnerability in your workstation and remediate it (either at the operating system level or the application level).
   Note: if you are upgrading to a major version of the OS, make sure you backup your important data before proceeding.
3. Install a shell terminal with an SSH client in your computer:

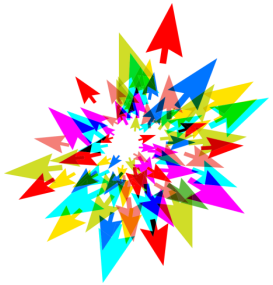
   If you have a Windows workstation: install MobaXterm

   https://mobaxterm.mobatek.net/download.html

   If you have a Linux or MacOS workstation, make sure you can find the terminal.

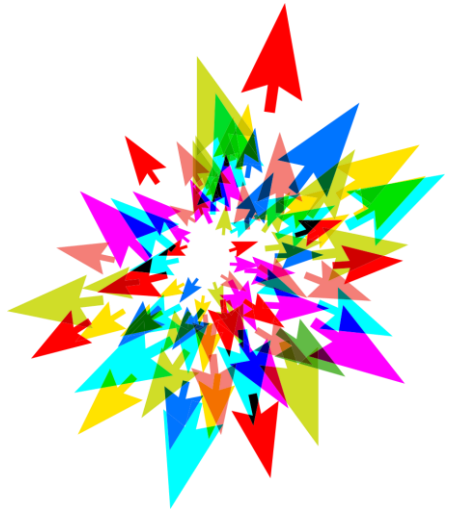
Notes: Please write a brief report including your answers and submit them in the Education website via the online text box (press add submission).https://education.scinet.utoronto.ca/course/view.php?id=1195
For question #2, please include a few sentences describing how you found the vulnerability and how you fixed it.
For question #3, please explain what OS you are using and which application you will be using as an SSH client.

# Sources and Images (day 1 and day 2)




- https://resources.infosecinstitute.com/certification/the-cissp-domains-an-overview/
- https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors
- https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary
- https://www.avast.com/en-ca/business/resources/defence-in-depth
- https://securitymatters.utoronto.ca/resources/it-professionals/ - (image)
- https://securitymatters.utoronto.ca/phish-got-a-moment/
- https://unsplash.com/s/photos/email - (image)
- https://unsplash.com/s/photos/castle - (image)
- https://www.sentinelone.com/blog/are-we-done-with-wannacry/
- https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
- https://www.av-test.org/en/
- https://www.forcepoint.com/cyber-edu/heuristic-analysis
- https://www.zdnet.com/article/flashback-trojan-wake-up-call-for-mac-users/
- https://cofense.com/knowledge-center/signs-of-a-phishing-email/
- https://www.pexels.com/photo/man-in-red-shirt-wearing-black-framed-eyeglasses-3965246 – (image)
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
- CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition by Darril Gibson; James M. Stewart; Mike Chapple ; Backups Chapter
- https://www.ssh.com/academy/ssh/protocol

# Thank You!
# Questions?



SciNet