“Malaware” - A Malware Education and Awareness Exercise

Overview of malware, including common types and variants.

Understand how malware is distributed.

Discuss strategies and techniques to prevent against threats caused by malware.

Participate in a malware threat prevention incident response tabletop exercises and game.

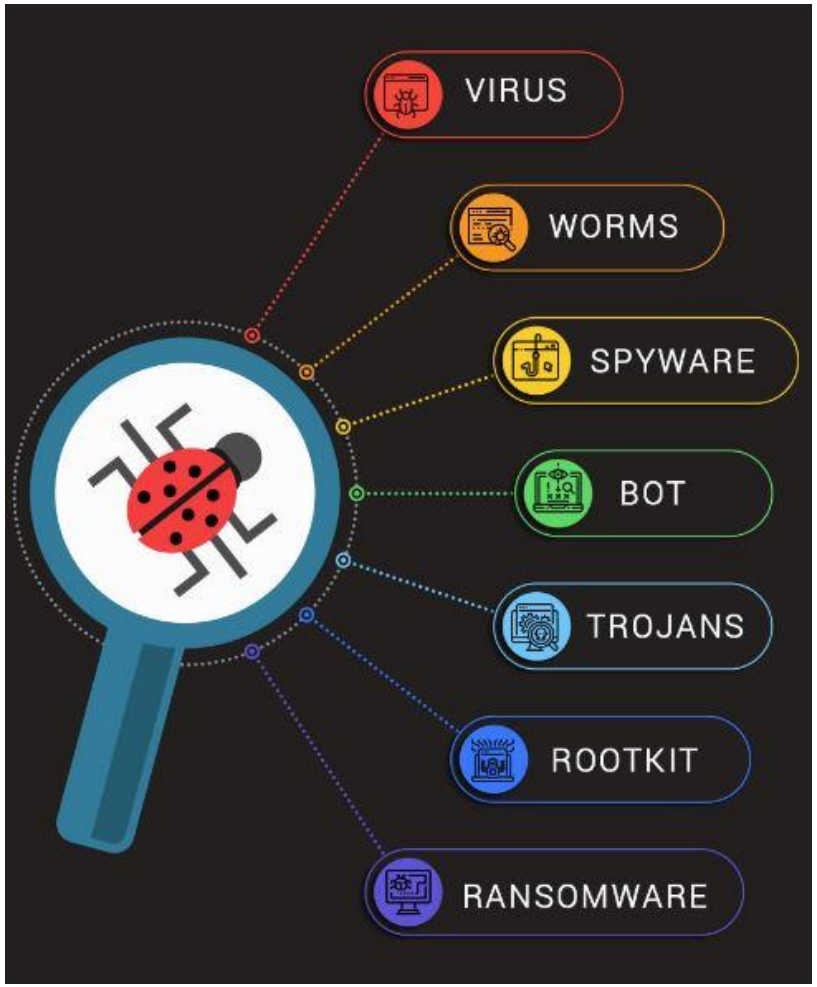
What is Malware?

- Malware is malicious software that can cause harm to users' devices or business systems. Such as locking and making them unusable, stealing, deleting, encrypting data, or even taking over full control of them.

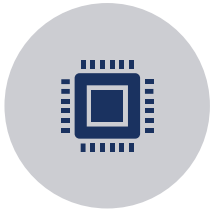
- It can also mine cryptocurrency and make premium rate calls that could cost the end-user huge sums of money.

Types of Malware

- Malware comes in many forms or variants, and anyone can become a victim of a malware attack.
- This figure on the right shows some of the most common types of malware in the wild.



Common Types or Variants of Malware



Viruses:

These are the most common types of malware. They are malicious software that, once deployed, can disrupt the ability of a system to operate, leading to operational issues and even data loss

Trojan:

A trojan poses as a legitimate application. Named after the Trojan horse, it attaches to emails and websites and tricks users to execute it so that it can infect their devices.

Spyware:

Malware is used to monitor users' activity without their express permission. It is often used to harvest sensitive information such as financial or personal details.

Ransomware:

This malware variant locks users out of their devices, encrypts their files and demands a ransom payment, usually in cryptocurrency.

Worms:

Computer worms are malware that replicate itself on a device. They can destroy operating system files, corrupt data on drives or even wipe them, rendering the drive empty and unusable.

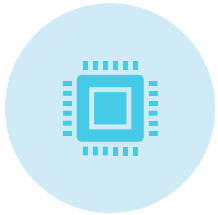
Adware:

Also known as advertising malware can display annoying, unwanted adverts, often directing users to sites with malicious content and others that promote adult content.

Common Types or Variants of Malware

Fake Virus:

Bogus software that pretends to scan users' devices. It charges them for services and can also steal data or sensitive information.

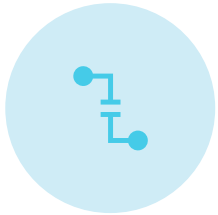


Bot:

A bot is a software program that performs an automated task without interaction. Bots can execute attacks much faster than humans ever could. They are used to launch DDoS attacks or brute force attacks

Fileless Malware:

Malware, which doesn't directly impact files or the file system. Instead, it uses non-file objects like Microsoft Office macros, PowerShell, WMI, and other system tools.

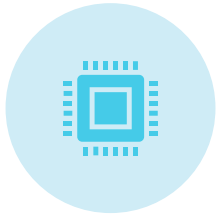


Backdoor or Rat:

This is malware that allows unauthorised remote access to a system enabling an attacker to monitor, interfere of modify transactions in a targeted system.

Rootkit:

Rootkits were not originally designed as malware but have become a common attack vector for threat actors. A rootkit allows a user to maintain privileged access within a system without detection.



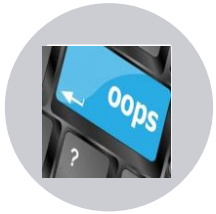
Mobile Malware:

Designed specifically to target mobile devices. Mobile malware has become more common with the proliferation of smartphones and the increased use of mobile and tablet by businesses and their employees.

Malware Distribution Channels

Accidental or planned insider attacks

Unpatched systems and applications



Human error and carelessness.

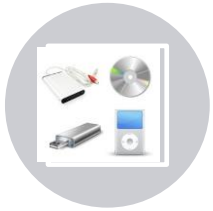
Spam/Phishing and emails and texts.

Emails files, attachments and links

Malware Distribution Channels

Pirated or unsolicited software

Malicious web adverts, (malvesting).



Removable media, e.g., USB drives.

Unsecure Wi-Fi connections.

Social network spam

Symptoms of Malware Infection

Systems that have been infected by malware display common behaviours such as.

1. **Slow or faulty system operation**

   Malware often uses extra system resources, so if a system is running slower than normal, constantly rebooting, crashing or frequently freezing, it can be an indication of malware infection.

2. **Ransom demands**

   Devices infected by ransomware have their data or files encrypted, with no access. Victims get a pop-up message instructing them to pay a ransom, usually in Bitcoin, to access their files.

3. **Unwanted pop-up ads or false security alerts**

   Most computers with an up-to-date browser and antivirus automatically block pop-up adverts. If a system has many pop-ups and security alerts, it could be an indication of a malware infection.

Malware Prevention Strategies

Security Education & Awareness

Regular Patching & Updates

Use Secure, Encrypted Connections

Apply a Zero Trust Security Policy

Install an Antivirus Program

Take Regular Backups

Malware Prevention Strategies

Use Official/ Licensed Software

Implement an Incident Response (IR) Plan that is Regularly Tested

Use a Security Incident & Event Management, SIEM/SAOR Tool

Draft and Implement an InfoSec Policy and Procedure.

Change Review/Approval Boards

Use Log Analytics and Auditing

Questions/ Observations

Thank You!

From the MalAware TTX and Card Game Team