Topic 4

Malware Detection and Prevention

Slides developed by

What you will learn in these slides...

- Common types of malwares
- Detecting malware
- Malware prevention tips

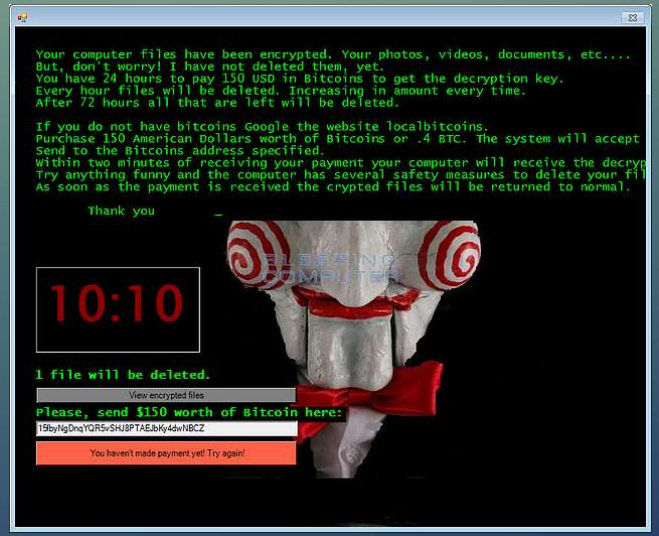
Recap on Topic 2

- We briefly discussed about malware as a type of cyber attack
  - Malware is an intrusive software with intent to disrupt, damage, steal or gain unauthorized data to a computer system
  - In this topic, we will dive deeper into malware and learn different ways on how it can affect your system

- Common types of malware
  - Ransomware, Virus, Worm, Trojan, Adware, Spyware, Rootkit

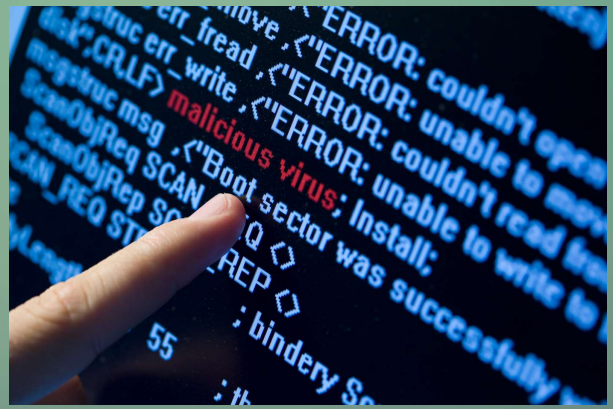
Ransomware

- Malware that encrypts files or locks access to a computer until a ransom is paid
- Often delivered through phishing emails or trojans
- Aims to extort money from victims by demanding payment in exchange for decryption keys



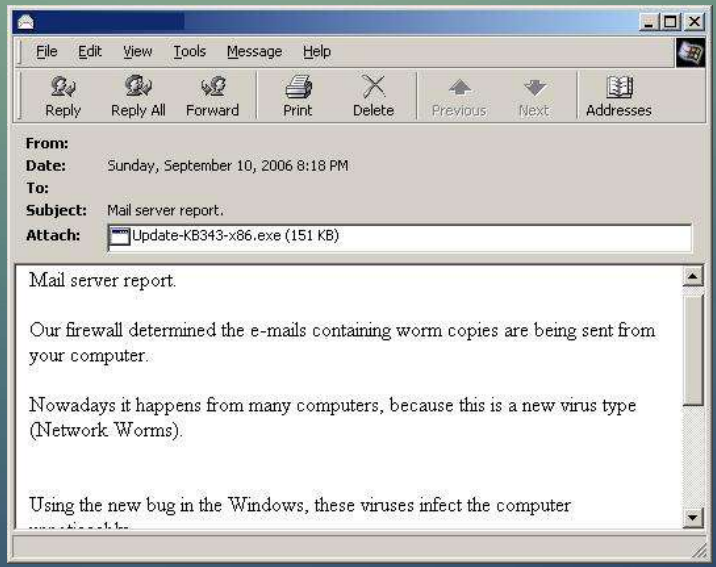
Virus

- Malware that attaches itself to legitimate programs
- Can spread to other files upon running the infected file



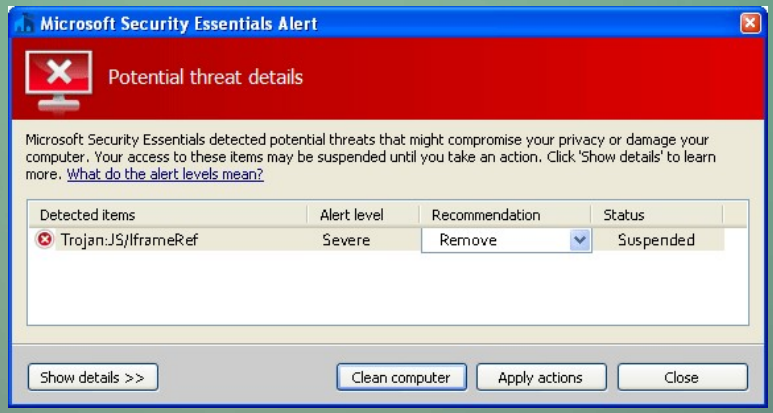
Worm

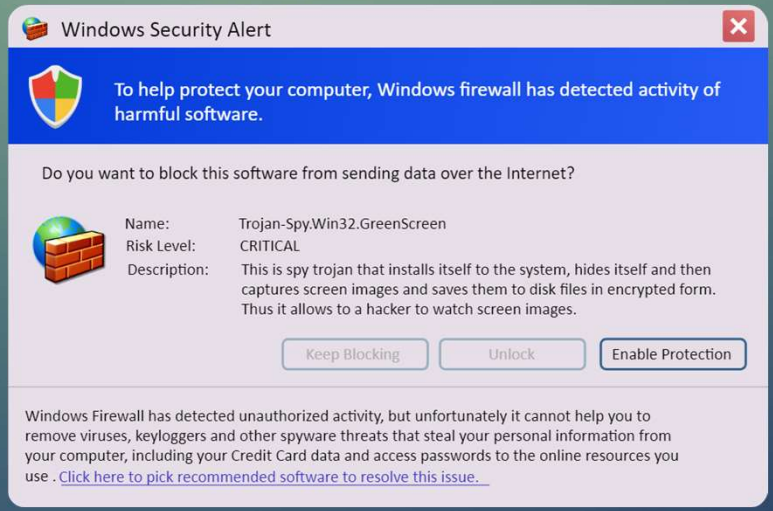
- Self-replicating malware that spreads across networks and systems by exploiting vulnerabilities
- Need NOT require user interaction to execute



Trojan

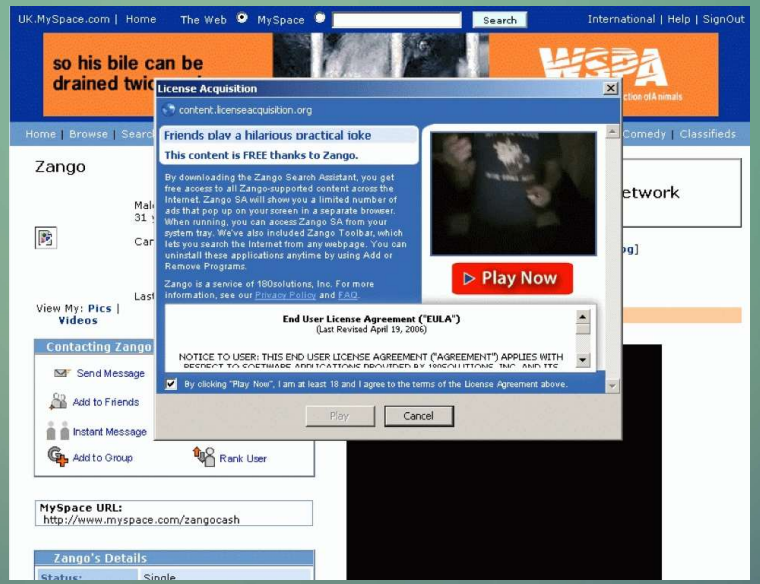
- Malware disguised as legitimate software to deceive users into downloading them, thus revealing sensitive data to attackers
- Derived from ‘Trojan Horse’, a term used to describe hiding one’s true intentions
- Ransomwares and/or spywares may result from Trojan execution





Adware

- Displays unwanted advertisements or pop-ups on a user's device
- Often includes legitimate software downloads or browser extensions.

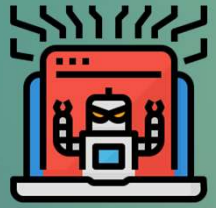


Spyware

- Installed on a device without the user's knowledge or consent
- Can monitor user activities and gather sensitive data
- Is not always malicious but often misused

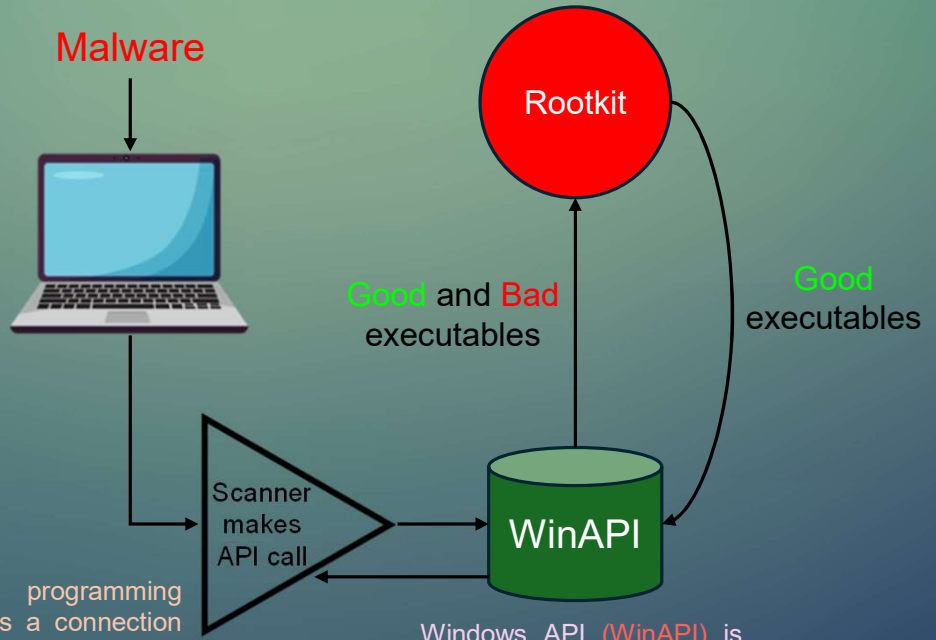
- Types of spywares include:
  - Keyloggers
  - Trojans
  - Tracking cookies (be very careful when accepting cookies on websites!)

Rootkit



- This malware hides deep within a computer system and is difficult to detect
- Allows attackers to gain privileged access and control over the system while evading detection

How a rootkit executes



An application programming interface (API) is a connection between two different computer programs, allowing users to use features of other software in their program

Windows API (WinAPI) is the API that allows users to access features of the Windows operating system

Reference: https://www.wallarm.com/what/rootkit-definition-how-to-remove-it

Detecting malware

- Indicators of Compromise / Attack (IOC/IOA)
- Malware analysis techniques
  - Static analysis
  - Dynamic analysis
- Malware Honeypot

Indicators of Compromise (IOC)

- Clues or evidence that suggest a system or network has been breached
- Uses known indicators (aka signatures)
- Detected after the attack has happened
- Some examples of IOCs
  - Large number of requests from an IP address in a short time
  - Random and changes in system logs
  - Presence of suspicious software that indicate presence of malware

Reference: https://www.aquasec.com/cloud-native-academy/vulnerability-management/indicators-of-compromise/

Types of IOCs

- Common types of IOCs include host-based and network-based IOCs
- Host-based IOCs involve detecting breaches on individual devices or systems
  - Examples include unexpected file changes, registry alterations or unknown running processes (especially those that use excessive CPU or memory resources)
- Network-based IOCs involve detecting breaches by monitoring network traffic, typically using security devices such as firewalls
  - Examples include sudden spikes in network traffic, unfamiliar IP addresses, malicious/phishing URLs or presence of command-and-control (C2) servers
- Other types of IOCs include file-based, email-based and behavioural to name a few

Indicators of Attack (IOA)

- Unlike IOCs, IOAs are detected while the attack is happening
- Some examples of IOAs
  - Unusual network traffic
  - Unauthorized access attempts
  - Abnormal user behaviour

Reference: https://www.infosectrain.com/blog/ioa-indicators-of-attack-vs-ioc-indicators-of-compromise/

Malware detection techniques

Static Analysis	Dynamic Analysis
• Analyzing a malware without executing the code • Is signature-based (compares the code's digital footprint against known signatures) • Not as effective as dynamic analysis as some information may only be seen while the code is executing • Only the malware properties are identified such as ASCII/Unicode strings and metadata	• Analyzing a malware while the code is running • Is behaviour-based (indicators are observed in real-time) • For safety concerns, a sandbox/virtual machine is required for dynamic analysis • Often more accurate than static analysis as the analysis is more in-depth • More things are identified such as network traffic and how the malware communicates with various functions

Reference: https://www.bitdefender.com/blog/businessinsights/the-differences-between-static-malware-analysis-and-dynamic-malware-analysis/

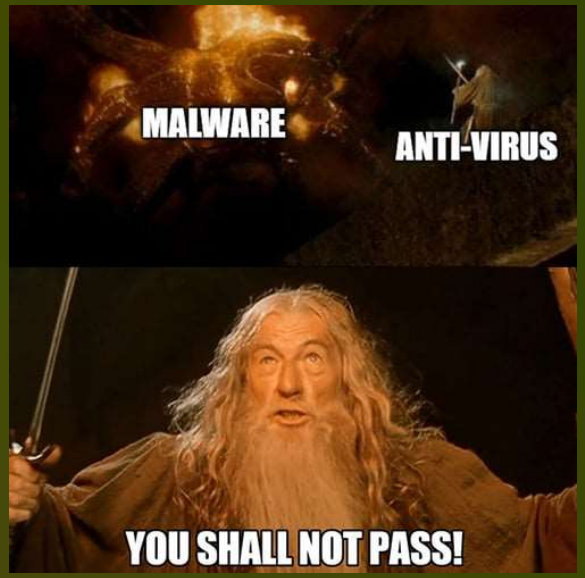
Malware Honeypot

Have you ever wanted to bait attackers by purposely making your system ‘vulnerable’ to lure them into attacking it?

- A honeypot is like a normal computer system but is specially used for detecting attacks (just like a bait)
- Is used to detect attacks early so that preventive measures can be taken quicker for actual systems
- Often consists of two components
  - A vulnerable feature (can be a website or server) that lures attackers into ‘compromising’ the honeypot
  - A detection/monitoring tool that updates the user when the honeypot has been ‘compromised’

Reference: https://www.apriorit.com/dev-blog/568-honeypots-for-malware-detection

Good ways to prevent malware



- Install and enable antivirus software
  - Helps to remove most malware from a system before it spreads further
- Update your software regularly
  - Apply security patches to certain software when necessary
- Enable firewalls (will be covered in Topic 7)
- Use email filtering to block spam/malicious emails
- Practice safe browsing
  - Do not click on suspicious links or download suspicious files
- Disconnect from the internet if you suspect malware on your system
  - Seek assistance from IT/cybersecurity experts

Topic 4 Summary

- Common types of malware
- Various ways to detect malware
- Good ways to prevent malware

In the next topic...

Secure Web Browsing

- Safe web browsing practices
- HTTP status codes