Cybersecurity

2.4.4 - Lesson 2.4.4 - Viruses, Worms, Spyware & Adware

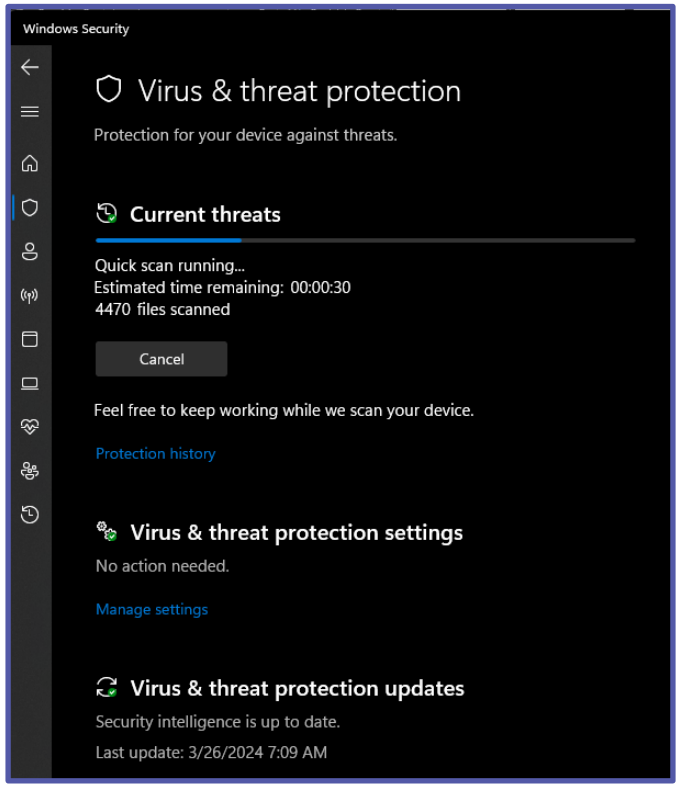
CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Viruses and Worms

- These types of malware are categorized by how they replicate.
- Viruses attach themselves to files, programs, and system processes and use them as carriers to enact on their intended effects – non-self-replicating
- Worms do not need to rely on other programs or files to spread – self-replicating
- Both can affect programs, boot sectors, databases, and networks

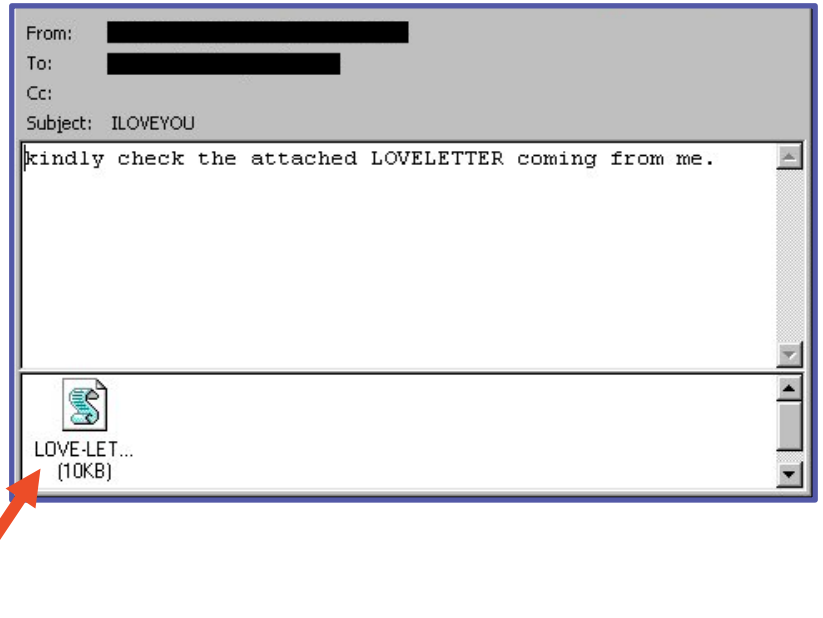
Preventing Viruses from Spreading

- Because viruses are usually attached to a file or process, restricting the level of privilege users and processes run in as well as monitoring for irregularities can assist in mitigating their effects
  - Anti-virus monitors for irregularities such as this
  - Data protection measures such as the least privilege principle and monitoring file modifications can also assist



Preventing Worms from Spreading

- Since worms are self replicating, moving across networks with less interaction, more preventative measures are needed
- Network monitoring and intrusion detection should be used as well as implementing a full defense in depth strategy is best



The ILOVEYOU or Love Bug worm infected millions of Windows users across the world, overwriting files, crashing computers, and automatically sending itself to user contacts.

Adware

- Software that installs additional advertising components, often leading to an influx of pop-up ads or toolbars in web browsers.
- Can increase network traffic, slowing down computer performance and disrupting system functions.
- Can be bundled with free software downloads.
- But if its removed, the software may cease to function as intended, leading to potential inconvenience for users.

Spyware

- A type of malware that monitors computer and internet usage
- Typically tracks
  - Internet traffic
  - Website visits
  - Clicked advertisements
  - Other browsing habits
- This data can be exploited by advertisers or companies for targeted marketing campaigns.

Bloatware

- Refers to pre-installed software applications on devices or computer systems often deemed unnecessary or undesirable by users due to:
  - Consuming system resources
  - Taking up storage space
  - Providing minimal value

Pre-Installed Bloatware

- Manufacturers pre-install bloatware to generate additional revenue through partnerships with software developers or to promote their own products and services.
- Some users may find these applications useful, but others may see them as unwanted and choose to uninstall or disable them.

Defense Measures

- Keep anti-virus and security software up-to-date to detect the latest adware and spyware.
- Regular system backups are also crucial for defense against all types of malware.
- Tools like Malwarebytes and Adaware can be used to monitor and defend against adware and spyware specifically.