Saved With A Click

Anti-Malware

Presented by:

Ottawa Public Library

National Capital FreeNet

National Capital FreeNet | Libertel de la Capitale Nationale

Agenda

- What is Malware
- Types of Malware
- Protecting Yourself
- Recovery Options

What is Malware

- *Malware* is a collective term for a variety of malicious software
- Designed to disrupt computer operation, gather sensitive information, or gain access to private computer systems

What is Malware (Con't)

- First computer virus was found on a Mac in 1982
- In mid 1980s most malware arrived via infected floppy disk
- By mid 1990s business networks were targeted using macro viruses

What is Malware (Con't)

- In late 1990s home users were affected as distribution via email started to appear
- Starting in the 2000s profit became a motivating factor
  - Phishing and credit card scams took off during this period

What is Malware (Con't)

- Targets all types of computers: Windows, Mac, Linux, Unix, Industrial Control
- Distributed via many methods: dodgy software, infected web sites, booby trapped files, web adverts

Types of Malware

- Adware – unwanted software that delivers advertisements. Typically disguised as something else or piggybacked on legitimate software
- Spyware – secretly observes activities without permission and reports back to the attacker

Types of Malware (Con't)

- Virus – replicates itself by modifying other computer programs with its own code
- Worms – similar to a virus but targets other computers on a network
- Trojan – misrepresents itself to gain unauthorized access to the computer. Can be used to steal information or install other malware

Types of Malware (Con't)

- Ransomware – locks your computer or files, usually by encryption, and demands payment to get them back
- Rootkit – provides attacker with elevated privileges. Designed to stay hidden from the user, other software and the operating system

Types of Malware (Con't)

- Keylogger – records keystrokes / screen shots and sends them to the attacker who is seeking usernames, passwords and credit card details
- Cryptojacking – uses your computer resources without permission to create cryptocurrency for the attacker

Types of Malware (Con't)

- Exploits – target bugs and other vulnerabilites in software to perform unwanted actions
- Malvertising – attacks through legitimate websites to unknowingly pull malicious content from a bad site. No clicking required – often referred to as a *drive-by download*

Protecting Yourself

- Several things you can do to minimize your chances of being affected by malware
- Some involve installing software to guard against infection, others are procedural changes that help minimize risk or aid in recovery

Protecting Yourself (Con't)

- First line of defence is Anti-Virus software
  - Some operating systems include own free anti-virus software
  - Commercial and free programs available
  - In most cases free programs are as effective as commercial programs

Protecting Yourself (Con't)

- Programs available for most platforms: Mac, Win, Linux, Android
- Independent assessment of Anti-Virus programs available at:
  - https://www.av-test.org/en/
  - https://www.av-comparatives.org/consumer/
  - https://www.toptenreviews.com/software/security/best-antivirus-software/

Protecting Yourself (Con't)

- Choose a program that includes "real-time" scan
- Don't rely solely on "real-time" scan, do regular full scans too
  - Signature files for new malware programs take time to arrive and could show up after you are already infected

Protecting Yourself (Con't)

- Malware often hard to detect
- Look for: slower performance, frequent crashes, trouble connecting to the Internet, pop up ads, strange ads on legitimate sites, changed browser settings, high network usage

Protecting Yourself (Con't)

- Many Anti-Virus programs also guard against Spyware and Ransomware but stand alone programs for these malware types also available
- Popular, free anti-spyware program is Spybot Search & Destroy https://www.spybot-free-download.com/
  –

Protecting Yourself (Con't)

- Browser extensions can be effective in limiting exposure to malware delivered by compromised sites
- Consider installing ad blocking extensions like:
  - uBlock Origin
  - AdBlock Plus

Protecting Yourself (Con't)

- Use a non-administrator account for day-to-day computing
  - Administrator accounts have near complete access and control
  - Malware run by an administrator account can inflict more damage than if run by a regular user account

Protecting Yourself (Con't)

- Practice safe browsing, be careful what links you click
- Hover over links to see where they lead before clicking
- Be wary of shortened links (e.g. bit.ly, goo.gl, etc.), you don't know where they lead

Protecting Yourself (Con't)

- Use an up-to-date, standards compliant browser and set it to:
  - Block pop-up windows
  - Ask permission to activate plug-ins
  - Show the full URL in the address bar

Protecting Yourself (Con't)

- Question what you see
  - If a site pops up a warning that you need to install something for the site to work, DON'T DO IT – leave the site immediately
- Don't click links in emails, even if it's from someone you recognize
  https://nakedsecurity.sophos.com/2016/10/21/why-you-should-be-cautious-of-emails-from-friends-or-colleagues/

Protecting Yourself (Con't)

- Safeguard your files – back them up regularly
  - Use an external device and disconnect it when not performing back ups
- Your OS often comes with back up software but free options available: https://www.lifewire.com/free-backup-software-tools-2617964

Recovery Options

- If your computer becomes infected despite your best efforts there are steps you can try to remedy the situation
  - Some are simple, others more complex and time consuming

Recovery Options (Con't)

- Good idea to run periodic full system scans using your Anti-Virus program
  - Well crafted Malware can sometimes evade the scan
- Schedule a "boot time" scan by your Anti-Virus software
  - Runs before malware can start and hide itself

Recovery Options (Con't)

- Standalone malware scanners available free from reputable security firms
  - Some run under your OS, others are self contained with their own OS

Recovery Options (Con't)

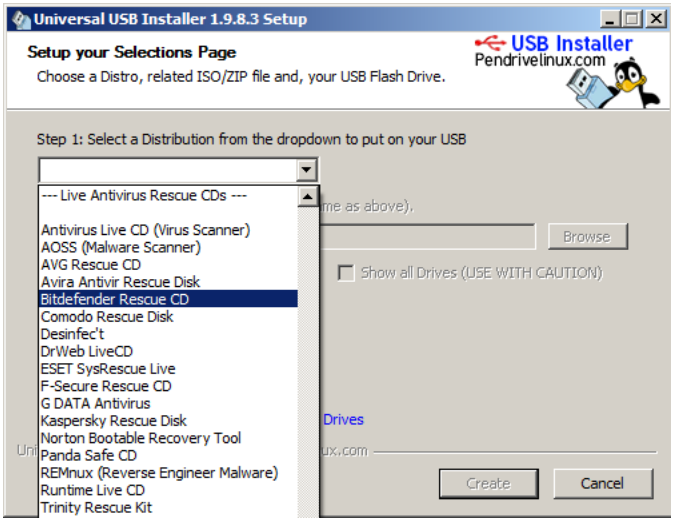
- Standalone options include:
  - Bitdefender *Anti-Ransomware* and *Home Scanner*
  - MalwareBytes *Adware Cleaner* and *Virus Cleaner*
  - ESET *Virus Removal* and *Rootkit Detector*

Recovery Options (Con't)

- Self contained options boot from USB or CD so you need to change your computer start up options
  - Check your documentation on how to change boot settings
  - Sometimes system boot screen has instructions on key to press to access BIOS set up

Recovery Options (Con't)

- Creating bootable USB easy with UUI from Pendrivelinux.com



Recovery Options (Con't)

- If all attempts fail, final option is to reformat the disk, reinstall the OS and other programs, and then restore files from back up
- Reinstall often desirable for Ransomware infection
  - Can't trust crooks to remove infection after payment


QUESTIONS