Protect your Organization from Malware

JULY 2022

ITSAP.00.057

Threat actors can use **malware**, or malicious software, to infiltrate or damage networks, systems, and devices. Once malware is installed on your organization's systems and devices, threat actors can gain access to sensitive information. This document introduces duces some common types of malware, tips for detecting whether your devices have been infected, and steps to protect your organization from being compromised by malware.

Common Types of Malware

Some of the most common types include the following examples:

- **Ransomware**: A type of malware that denies your access to data or systems until a sum of money is paid to the threat actor. For more information on ransomware and how to protect your organization, please see the *Ransomware Playbook (ITSM.00.099)* on the Cyber Center website.
- **Spyware**: Infected software that threat actors use to access your devices and steal sensitive information.
  - **Trojan Horse**: A type of **spyware** disguised as harmless software to fool you into downloading the program.
  - **Adware**: A type of **spyware** that tracks your Internet history and downloads to display pop-up advertisements related to products and services that might interest you.
- **Wiper:** The hard drive, data, and programs of the computer infected are wiped, overwritten, or deleted. Wiper malware may disguise itself as ransomware but will continue to destroy all data and files in the background. However, if there are solid backup processes in place, data may be partially or fully restored.
- **Virus**: A computer program that spreads, usually without you knowing, by making copies of itself.
- **Keystroke logger (Keylogger)**: Software or hardware designed to capture your keystrokes. The keystrokes are stored or transmitted so that threat actors can use them to collect valued information.
- **Rootkit**: Programs that provide threat actors with access to your networks, systems, and devices. A rootkit disguises itself as an operating system component on your device.
- **VPNFilter Malware**: Malware designed to infect routers so that threat actors can collect information, exploit devices, and block network traffic.
- **Worm**: A malicious program that executes independently and self-replicates, usually through network connections, to cause damage (e.g. deleting files, sending documents via email, or taking up bandwidth).

Ways that Malware can Infect

Some ways in which you could infect your networks, systems, and devices with malware include the following examples:

- Accepting pop-up advertisements
- Downloading unreliable software (e.g. disguised as a Flash Player update)
- Opening malicious email attachments
- Downloading media and software through untrusted vendors or means
- Sharing files (e.g. peer-to-peer file sharing services)
- Using removable media (e.g. USB, hard drives, CD, DVD) before scanning and verifying it

Signs of an Infected Device

It can be difficult to detect whether your devices have been infected with malware. Some symptoms to look out for include the following examples:

- Pop-up windows appearing on your device
- Homepage changes
- Spam emails sent from your account
- Page or system crashes
- Slow computer performance
- Unknown programs running on your device
- Unauthorized password changes

AWARENESS SERIES

Cat. No. D97-1/00-057-2022E-PDF
ISBN 978-0-660-43195-6

Tips to Protect Against Malware

Some ways that you can protect your device from malware include the following:

- Back up your devices and information
- Install software updates and patches regularly and as soon as they are made available
- Use anti-virus and anti-malware software and keep it updated
- Use anti-phishing software
  - Align software with the Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy (e.g. email authentication and reporting protocol [domain-name visibility, notification of intrusion])
- Use a host intrusion detection system (HIDS)
- Use a firewall
- Install and execute only authorized applications via application allowlisting
- Verify that files and attachments are legitimate before downloading them
- Use an ad blocker
- Use a data consumption application (e.g. track data usage on apps when not in use for suspicious activity)
- Avoid using public Wi-Fi
- Turn off Wi-Fi, GPS, and Bluetooth when not in use
- Refrain from sharing personal information on social media that could help threat actors hack into your other accounts (e.g. home address used as a security question to access banking information)
- Avoid jailbreaking (e.g. disable security measures imposed by device manufacturer) your device

Steps to Address Infected Devices

If your device has been infected with malware, take the following steps to address the issue:

1. Contact your IT security service desk immediately
2. Disconnect the infected device from the network
3. Turn off Wi-Fi and unplug network-carrying cables (e.g. Ethernet)
4. Connect the device to a clean network and reinstall the operating system
5. Run anti-virus software and scan all back-ups before restoring the device
6. Reconnect the device to your network
7. Monitor traffic and run anti-virus scans to ensure no malware remains

Computers:

- Ensure that your device and programs are updated
- If you have run anti-virus scans and your computer is still showing signs of infection, you may need to wipe your computer and re-install all programs
- Data can be retrieved if the computer was backed up before showing signs of malware infection

Other Devices

- Phones or tablets that cannot run antivirus scans may require a factory reset. If this does not resolve the issue, expert help may be required.

Anti-virus Software

Anti-virus software defends devices against viruses, Trojans, worms, and spyware. Anti-virus software can identify known malware by scanning start-up files, boot records, and all files that go through the system. It can also monitor common applications.

HIDS

Host intrusion detection systems monitor your system to detect intrusions and unauthorized access. HIDS allows you to see who is accessing and changing files in your system and what they are trying to do.

Firewalls

A firewall is a security barrier that protects the local system's resources from being accessed from the outside. A network firewall restricts traffic from passing from one network to another. A host-based firewall restricts incoming and outgoing network activity for a single host or end points.

Anti-malware

Anti-malware software works by scanning files to determine if they meet the appropriate predetermined characteristics, known as their signature. If not, the files are detected as malware and removed. Observing the behaviour of files for irregularities or isolating suspicious files are also methods used by anti-malware.

Protective DNS (PDNS)

Protective Domain Name Systems (DNS) refer to security solutions that offer protection online by analyzing IP addresses and domain names and blocking unwanted content before there is a chance of exposure to the malware.

For more information on preventive security tools, please see *Preventative Security Tools (ITSAP.00.058)* on the cyber centre website. You can also find more information on PDNS in the following publication Protective DNS (ITSAP.40.019).

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at the Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**