RCMP
ROYAL CANADIAN MOUNTED POLICE

MAJOR MALWARE THREATS BULLETIN

Recognize, Reject and Report it!

Is your computer or phone acting strange lately? If so it may be infected with malware. Malware can prevent your device from operating, steal your data, and even control its operation.

Bulletin 4. Version 1.0
May 2019

RECOGNIZE IT!

What is malware and what can it do? Malware is malicious software that can infiltrate an electronic device. The effect it has depends on the type of malware that has infected your device. Three major types of malware which are on the rise are: spyware, ransomware and zombie malware.

SPYWARE

Data-stealing malware used to collect your passwords, personal information or credit card data. Often installs "key logging" software which lets the attacker know what buttons you press on your keyboard.

RANSOMWARE

Infects a computer and then locks your data/files through 'encryption'. Victims receive an alert and a demand for payment to restore the data. Payment often demanded in the form of cryptocurrency such as Bitcoin.

ZOMBIE MALWARE

Takes control of a device causing it to send spam or force it to create cryptocurrency through a process known as 'mining', making the device run slowly. Infected devices may also be used to attack websites by overloading their networks, causing them to crash.

How do I know if my device has been infected?

- If it is running slowly
- If it is crashing often
- If it is overheating
- If applications are refusing to open
- If you are receiving a higher volume than usual of pop-up ads and/or spam

All of the above are indicators that your electronic device could be infected with malware.

REJECT IT!

How can I protect myself or loved one? There are easy preventative steps to take to help make sure you don't become a victim of malware.

DO:

1. Create complex passwords using numbers, symbols and text.
2. Avoid using same password for multiple accounts.
3. Ensure your wifi is secure.
4. Frequently backup all important files to a separate device that is not connected to the same network.
5. Keep software up to date; regularly run updated anti-virus software.
6. Talk to others about online risks. Know what your children are downloading.

DO NOT:

1. Download files from unknown websites.
2. Open, reply to, or download attachments from e-mails from unknown sources.
3. Install apps from unknown sources.

REPORT IT!

How should I respond? If you suspect your electronic device is infected with malware immediately turn it off and/or unplug it from the main power source. Contact a trusted IT professional who can determine how best to address the problem.

For suspected attacks or data compromise communicate with:

Spyware	Ransomware	Zombie Malware
• Your bank for stolen credentials • Service Canada: 1 800 O-Canada for federally-issued ID • Responsible provincial / territorial ministry for driver's license or health card • Privacy Commissioner at 1-800-282-1376 or www.priv.gc.ca for potential identity theft	• Local police for money demands/payments • Canadian Anti-Fraud Centre to report incident: www.antifraudcentre.ca or 1-888-495-8501	• A trusted IT professional if device is performing unwanted actions. • Police and financial institutions if money is demanded.

Reporting helps authorities warn people about current threats, monitor trends and disrupt cybercrime activities where possible.

Don't be afraid or embarrassed to report an incident. Perpetrators are using more sophisticated techniques that can infect the devices of even the most tech savvy user.

Additional information can be found at:

Canadian Anti-Fraud Centre www.antifraudcentre.ca
Get Cyber Safe www.getcybersafe.gc.ca
Canadian Centre for Cyber Security www.cyber.gc.ca

In consultation with: