MNP Clients: Protection from Latest Ransomware Attack

A series of cyber attacks across the globe have seized control of public and private sector computer systems, freezing data until a ransom is paid. While most of these attacks have happened overseas, there is evidence the malware (virus) has surfaced in Canada.

MNP is aware of this threat and is providing the following information to help protect organizations' computer networks.

Who's at Risk?

Organizations or individuals who are running an older Microsoft Windows system or who have not applied a March 2017 patch are vulnerable. The ransomware spreads with the help of a file-sharing vulnerability in Windows that opens whenever it loads itself onto a new machine. It can infect an entire network.

The Threat

The ransomware, known as WannaCrypt, WanaDecrypt and WannaCry, encrypts a victim's data until the victim pays for a key to unlock them. Without a good backup system, there currently is no solution other than to pay the ransom.

Microsoft issued a patch to fix this flaw in March 2017, but it was unavailable to older versions of Windows, such as Windows XP, leaving many organizations and individuals open to hacking.

Today Microsoft announced it has made the patch available to older, unsupported systems. **It is imperative to run the patch as soon as possible.** See link below.

How Do You Know if You've Been Infected?

One sign is not being able to access your systems, files and data base. However, in most cases a red pop-up appears on your computer screen. The red screen is the "ransom note" that demands payment to get back access to your data.

This is what the pop-up could look like:

How Do You Limit Your Exposure?

1. Patch your systems with the latest information from Microsoft for this “Wanna” Ransomware: **https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/**
2. Patch your systems for any other security vulnerabilities (hardware / software) as quickly as possible.
3. Backup your systems. Make sure you have offline backups. Test those backups to make sure they can be restored.
4. Avoid clicking on links or opening attachments or emails from people you don't know or companies you don't do business with.
5. Have an antivirus / antimalware solution installed and up-to-date.
6. Communicate to your organization to let them know if anything suspicious is seen to shut down their systems, remove from the network and report immediately.

How to Respond if You’ve Been Infected

1. Remove any devices you suspect of having ransomware from the network immediately and shut that system down - be aware other systems may have also been infected.
2. Run tools as soon as possible to discover the extent of the problem.

3. If you have an emergency and need help, **call MNP's Cyber Security hotline at 1.866.370-8575 and select option 2**.
4. If you are concerned, or not sure what to do, **email MNP's Security Operating Centre at soc@mnp.ca**

For more information on boosting your cyber security, **click here**.

How Can MNP Help?

MNP is one of the leading cyber security firms in Canada. Please use the numbers above to call in case of an emergency. If you are looking for future advice on cyber security contact Danny Timmins, National Cyber Security Leader, at **danny.timmins@mnp.ca**