Don’t give in to ransomware – prepare your system

Ransomware is an increasingly popular means for malware authors to extort money from people, so a properly prepared system is critical.

By Vicky Sidler - May 5, 2015

Ransomware is an increasingly popular way for malware authors to extort money from people, so a properly prepared system is critical.

Ransomware is malicious software that cyber criminals use to hold a user’s computer for ransom, demanding payment in order for the user to get control back, says Nathan Loftie-Eaton, Security Specialist at ESET South Africa.

Ransomware gets onto a victim’s machine through social engineering tactics or using software vulnerabilities to silently install.

A ransomware threat making headlines is Cryptolocker, which spread quickly via email and affects a user’s files that are on drives which are “mapped” or assigned a drive letter (e.g. D:, E:, F:).

This includes external hard drives, USB drives, or a folder on the network or in the Cloud.

Paying the criminals may get your data back, but there are cases where the decryption key isn’t sent or doesn’t work.

Currently, tens of thousands of machines have been affected – with the criminals sending millions of emails.

What can you do about it?

Ransomware is intimidating, and encrypted files can be considered damaged beyond repair.

But if you have prepared your system, it is nothing more than a nuisance.

Here are a few tips on how to negate the threat of ransomware.

1. Backup

Having a regularly updated backup is step one.

If you are attacked with ransomware you may lose work-in-progress documents, but you can restore your system to an earlier snapshot.

Use an external drive or backup service, one that is not assigned a drive letter or is disconnected when not in use.

2. Show hidden file extensions

Ransomware frequently arrives in a file that is named ".pdf.exe", counting on Window's default behaviour of hiding known file extensions.

Disable the hiding of known file extensions option, making it easier to spot suspicious files.

3. Filter .exe in email

If your gateway mail scanner has the ability to filter files by extension, you may want to to deny mails sent with ".exe" files.

Also deny files that have two file extensions, the last one being executable ("*.*.exe" files, in filter-speak).

If you need to exchange executable files, you can do so with ZIP files or via cloud services.

4. Disable files running from AppData/LocalAppData folders

You can create rules within Windows or with intrusion prevention software to disallow behaviour used by Cryptolocker, which is to run its executable from the App Data or Local App Data folders.

If you have legitimate software that runs from the App Data area, you need to exclude it from this rule.

5. Use the Cryptolocker Prevention Kit

The Cryptolocker Prevention Kit is a tool created by Third Tier that automates the process of making a Group Policy to disable files running from the App Data and Local App Data folders.

It also disables executable files running from the Temp directory of unzipping utilities. Exemptions to these rules can be created.

This tool is updated as new techniques are discovered for Cryptolocker, so make sure you have the latest version.

6. Disable RDP

The Cryptolocker/Filecoder malware often accesses machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access your desktop remotely.

If you do not require the use of RDP, disable it to protect your machine from Filecoder and other RDP exploits.

7. Patch or Update your software

Malware authors rely on people running outdated software with known vulnerabilities, which they can exploit to silently get onto their system.

Updating your software often will help prevent this.

8. Use a reputable security suite

Have both anti-malware software and a software firewall to help you identify threats or suspicious behaviour.

Malware authors regularly send out new variants to try to avoid detection, so it is important to have two layers of protection.

New ransomware variants that get past anti-malware software may be caught by a firewall when it attempts to connect with its Command and Control (C&C) server to receive instructions for encrypting your files.

If you have run a ransomware file without performing the previous precautions, your options are more limited.

There are several things you can do to mitigate the damage, though, particularly if the ransomware in question is Cryptolocker:

9. Disconnect from Wi-Fi or unplug from the network immediately

If you run ransomware, but have not seen the ransomware screen, you can stop communication with the C&C server before it encrypts your files.

Disconnect from the network immediately, and you can mitigate the damage.

The technique is not guaranteed to work, but disconnecting from the network may be better than doing nothing.

10. Use System Restore to get back to a known clean state

Enabling System Restore on your Windows machine allows you to take your system back to a clean state.

New versions of Cryptolocker, though, have the ability to delete "Shadow" files from System Restore, which means those files will not be there when you try to replace your malware-damaged versions.

Cryptolocker will start the deletion process whenever an executable file is run, so you need to move quickly as executables may run without you knowing as part of Windows' operation.

11. Set the BIOS clock back

Cryptolocker has a payment timer that is generally set to 72 hours, after which time the price for your decryption key increases.

At the time of writing the initial price was .5 Bitcoin or $300, which then goes up to 4 Bitcoin.

You can “beat the clock” by setting the BIOS clock back to a time before the 72 hour window is up.

This keeps you from having to pay the higher price, but its is strongly advised that you do not pay the ransom.