bizcommunity

Tips on how to fight and avoid ransomware, from ESET South Africa

Ransomware is malicious software that cyber criminals use to hold a user's computer or computer files for ransom, demanding payment in order for the user to get the files back. Sadly, ransomware is becoming an increasingly popular way for malware authors to extort money from companies and consumers alike, said Nathan Loftie-Eaton, Security Specialist of ESET South Africa...

There is a variety of ways that ransomware can get onto a person's machine, but, as always, those techniques either boil down to social engineering tactics or using software vulnerabilities to install on a victim's machine silently.

One specific ransomware threat that has been in the news a lot lately is Cryptolocker, which has spread quickly by its perpetrators via email.

You may wonder why the big fuss over this one particular ransomware family - in essence, it is because Cryptolocker's authors have been both nimble and persistent. There has been a concerted effort to pump out new variants, keeping up with changes in protection technology and targeting different groups over tim Initially, emails were targeting home users, then small-to-medium businesses, and now they are aiming at enterprises.

The malware also spreads via Remote Desktop Protocal (RDP) ports that have been left open to the internet, as well as by email. Cryptolocker can also affect a user's files that are on drives that are 'mapped' which is to say, they have been given a drive letter (e.g. D:, E:, F:). This could be an external hard drive including USB thumb drives, or it could be a folder on the network or in the cloud. If you have, for example your Dropbox folder mapped locally, it can encrypt those files as well.

Paying the criminals may get your data back; however there have been plenty of cases where the decrypti key has never arrived or where it has failed to properly decrypt the files. Plus, it encourages criminal behaviour! Ransoming anything is not a legitimate business practice, and the malware authors are under n obligation to do as promised - they can take your money and provide nothing in return, because there is nc backlash if the criminals fail to deliver.

At this point, tens of thousands of machines have been affected, though it is estimated that the criminals have sent millions of emails. Hopefully the remainder of the recipients have simply deleted the malicious emails without opening them, rather than having the emails unopened in their in-box, waiting to unleash mo pain.

What can you do about it?

On the one hand, ransomware can be very scary - the encrypted files can essentially be considered damaged beyond repair. But if you have properly prepared your system, it is really nothing more than a nuisance. Here are a few tips that will help you keep ransomware from wrecking your day:

- Back up, back up, back up: The single biggest thing that will defeat ransomware is having a regularly updated back up. If you are attacked with ransomware you may lose the document that you started earlier in the morning, but if you can restore your system to an earlier snapshot or clean up your machine and restore your other lost documents from back up, you can rest easy. What you need is a regular back-up routine, to an external drive or back up service, one that is not assigned a drive letter is disconnected when it is not doing back up.
- Show hidden file extensions: One way that ransomware frequently arrives is in a file that is named witl the extension '.PDF.EXE', counting on Window's default behaviour of hiding known file extensions. If you re-enable the ability to see the full file-extension, it can be easier to spot suspicious files.
- Filter EXEs in email: If your gateway mail scanner has the ability to filter files by extension, you may w to deny mails sent with '.EXE' files, or to deny mails sent with files that have two file extensions, the la one being executable ('*.*.EXE' files, in filter-speak). If you do legitimately need to exchange executable files within your environment and are denying emails with '.EXE' files, you can do so with Z files (password protected, of course) or via cloud services.
- Disable files running from AppData/LocalAppData folders: You can create rules within Windows or wi Intrusion Prevention Software, to disallow a particular, notable behaviour used by Cryptolocker, which to run its executable from the App Data or Local App Data folders. If (for some reason) you have legitimate software that you know is set to run not from the usual Program Files area, but the App Dat area, you will need to exclude it from this rule.
- Use the Cryptolocker Prevention Kit: The Cryptolocker Prevention Kit is a tool created by Third Tier th automates the process of making a group policy to disable files running from the App Data and Local App Data folders, as well as disabling executable files from running from the Temp directory of variou unzipping utilities. This tool is updated as new techniques are discovered for Cryptolocker, so you wil want to check in periodically to make sure you have the latest version. If you need to create exemptio to these rules, they provide this document that explains that process.
- Disable RDP: The Cryptolocker/Filecoder malware often accesses target 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, you can disable RDP to protect your machine from Filecoder and othe RDP exploits. For instructions to do so, visit the appropriate Microsoft Knowledge Base article: Windows XP RDP disable; Windows 7 RDP disable; Windows 8 RDP disable.
- Patch or update your software: These next two tips are more general malware-related advice, which applies equally to Cryptolocker as to any malware threat. Malware authors frequently rely on people running outdated software with known vulnerabilities, which they can exploit to silently get onto your system. It can significantly decrease the potential for ransomware-pain if you make a practice of updating your software often.
- Use a reputable security suite: It is always a good idea to have both anti-malware software and a software firewall to help you identify threats or suspicious behaviour. Malware authors frequently send out new variants to try to avoid detection, so this is why it is important to have both layers of protection If you run across a ransomware variant that is so new that it gets past anti-malware software, it may sti 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 find yourself in a position where you have already run a ransomware file without having perform any of the previous precautions, your options are quite a bit more limited. But all may not be lost. Ther are a few things you can do that might help mitigate the damage, particularly if the ransomware in question is Cryptolocker:

- Disconnect from WiFi or unplug from the network immediately: If you run a file that you suspect may b ransomware, but you have not yet seen the characteristic ransomware screen, if you act very quickly you might be able to stop communication with the C&C server before it has finished encrypting your files. If you disconnect yourself from the network immediately, you might mitigate the damage. It take some time to encrypt all your files, so you may be able to stop it before it succeeds in distorting them all. This technique is definitely not foolproof, and you might not be sufficiently lucky or be able to mov more quickly than the malware, but disconnecting from the network may be better than doing nothing.
- Use System Restore to get back to a known clean state: If you have System Restore enabled on you Windows machine, you might be able to take your system back to a known clean state. But, again, yo have to outsmart the malware. Newer versions of Cryptolocker can 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 run, so you will need to move very quickly as executables may be started as part of an automated process. That is to say, executable files may be run without you knowing, as a normal part of your Windows system's operation.
- Set the BIOS clock back: Cryptolocker has a payment timer that is generally set to 72 hours, after whi time the price for your decryption key goes up significantly. (The price may vary as Bitcoin has a fairly volatile value. 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' somewhat, by setting the BIOS clock back to a time before the 72-ho window is up. However, all this does is it keeps you from having to pay the higher price, and it strongly advised that you do not pay the ransom.

If you are an ESET customer and you are concerned about ransomware protection or think you have beer targeted by ransomware, call our customer care. They will have the latest details on how to prevent and remediate ransomware attacks.