A2000ERP ~ IT-RELATED

Ransomware Attacks

In the days of old where computers are locally connected, such risks are rare. However in the advent of Internet connectivity, and aided by crypto-currencies where the recipients (or cyber-criminals) can be paid anonymously, it sparked a fresh wave of cyber extortions or ransomware. Is your computer protected against ransomware attacks? Ransomware is a type of malware (malicious software) which criminals use to encrypt the file contents in your computer to extort money to release them. Companies hit with ransomware have data encrypted and users are locked out of their own devices. With open connectivity to support working anytime, anywhere, many companies become targets because their computers are exposed to the Internet. Even when a company decides to withhold Internet access from their PC/server, it is not fully guaranteed against an attack.

Is your computer protected against ransomware attacks? Ransomware is a type of malware (malicious software) which criminals use to encrypt the file contents in your computer to extort money to release them. Companies hit with ransomware have data encrypted and users are locked out of their own devices.

With open connectivity to support working anytime, anywhere, many companies become targets because their computers are exposed to the Internet. Even when a company decides to withhold Internet access from their PC/server, it is not fully guaranteed against an attack.

Ransomware Prevention

- **Never Click on Unverified Links** Avoid clicking links in spam emails or on unfamiliar websites. Downloads that start when you click on malicious links, is one way that your computer could get infected. Once the ransomware is in your computer, it will encrypt your data or lock your operating system. Once the ransomware has something to hold as ‘hostage,’ it will demand a ransom (usually through crypto-currencies like Bitcoins) so that you can recover your data. Paying these ransoms may seem like the simplest solution. However, this is exactly what the perpetrator wants you to do and paying these ransoms does not guarantee they will give you access to your device or your data back.

- **Do Not Open Untrusted Email Attachments** Another way that ransomware could get onto your computer is through an email attachment. Do not open email attachments from senders you do not trust. Look at who the email is from and confirm that the email address is correct. Be sure to assess whether an attachment looks genuine before opening it. If you’re not sure, contact the person you think has sent it and double check. Never open attachments that ask you to enable macros to view them. If the attachment is infected, opening it will run the malicious macro, giving the malware control over your computer.

- **Only Download From Trusted Sites** To reduce the risk of downloading ransomware, do not download software or media files from unknown websites. Go to verified, trusted sites if you want to download something. Most reputable websites will have markers of trust that you can recognize. Just look in the search bar to see if the site uses ‘https’ instead of ‘http.’ A shield or lock symbol may also show in the address bar to verify that the site is secure. If you’re downloading something on your phone, make sure you download from reputable sources. For example, Android phones should use the Google Play Store to download apps and iPhone users should use the App Store.

- **Avoid Divulging Personal Data** If you receive a call, text, or email from an untrusted source that asks for personal information, do not give it out. Cybercriminals planning a ransomware attack may try to gain personal data in advance of an attack. They can use this information in phishing emails to target you specifically. The aim is to lure you into opening an infected attachment or link. Do not let the perpetrators get hold of data that makes their trap more convincing. If you are contacted by a company asking for information, ignore the request, and contact the company independently to verify it is genuine.

- **Use Mail Server Content Scanning & Filtering** Using content scanning and filtering on your mail servers is a smart way to prevent ransomware. Such software reduces the likelihood of a spam email containing malware-infected attachments or links from reaching your inbox.

- **Never Use Unfamiliar USB Drives** Never insert USBs or other removal storage devices into your computer if you do not know where they came from. Cybercriminals may have infected the device with ransomware and left it in a public space to lure you into using it.

- **Keep Your Software & Operating System Updated** Keeping your software and operating system updated will help protect you from malware. Because when you run an update, you are ensuring that you benefit from the latest security patches, making it harder for cybercriminals to exploit vulnerabilities in your software.

- **Use a VPN When Using Public Wi-Fi** Being cautious with public Wi-Fi is a sensible ransomware protection measure. When you use public Wi-Fi, your

computer system is more vulnerable to attack. To stay protected, avoid using public Wi-Fi for confidential transactions, or use a secure VPN.

- **Use Security Software** As cybercrime becomes more widespread, ransomware protection has never been more crucial. Protect your computer from ransomware with a comprehensive internet security solution like Norton End-point or Kaspersky Internet Security. When you download or stream, our software blocks infected files, preventing ransomware from infecting your computer and keeping cybercriminals at bay.

- **Keep Security Software Updated** To benefit from the highest level of protection that internet security software has to offer, ensure you keep it updated. Each update will include the latest security patches and maximize ransomware prevention.

- **Backup Your Data** Despite all the precautions, you are never 100% safe. Should you experience a ransomware attack, your data will remain safe if it is backed up. Make sure to keep everything copied on an external hard drive, but be sure not to leave it connected to your computer when not in use. If the hard drive is plugged in when you become a victim of a ransomware attack, this data will also be encrypted. The data backed up should allow you to revert to previous versions of your files. Therefore, if they become encrypted by ransomware, you should be able to return to an earlier unencrypted version to restore. Very strongly recommended is to use a cloud storage solution that handles the backup automatically.

How to Respond to Ransomware Attacks? Now you know how to prevent ransomware, but what if you have already become the victim of a ransomware attack? In the event of a ransomware attack, it is important to know what to do. Here are some simple steps to follow to minimize damage.

- **Isolate Your Computer** If you experience a ransomware attack, the first thing to do is to disconnect from any networks and the internet. Disconnecting in this way isolates your computer and minimizes the chance of the ransomware infection spreading to other computers.

- **Never Pay the Ransom** Do not pay any ransom demanded by the cybercriminals carrying out the ransomware attack. It is best to revert to your back-ups to restore on a clean computer. Like a real-life hostage

situation, it is best not to negotiate with cybercriminals. Paying the ransom will not guarantee the return of your data — after all these individuals have already manipulated your trust. Caving in and paying also encourages this sort of crime. The more people that pay the ransoms, the more popular ransomware attacks become.

- **Start Ransomware Removal** To rid your computer of ransomware, follow our simple steps to ransomware removal in the section below.

Step 1: Disconnect from the internet First up, disconnect from the internet to stop the ransomware spreading to other devices.

Step 2: Run a scan using internet security software Use the internet security software you have installed to run a scan. This will help to identify any threats. If it detects any risky files, they can be removed or quarantined.

Step 3: Use ransomware decryption tool If your computer gets infected with encryption ransomware, you may try to recover using a ransomware decryptor to decrypt your files and data so that you can access them again. Not all may be able to do so, but many anti-virus suppliers are releasing the latest forms of decryptors to counter each new threat. Check out your supplier for this.

Step 4: Restore files from backup If you have backed up your data externally or on cloud storage, restore a clean backup of all your files on your computer. This allows you to revert to a version of the software that is malware free. If you don't have a backup, then restoring your data in a clean computer is a lot harder.**To prevent this from happening, we recommend regularly backing up your data**. If you're prone to forgetting, then take advantage of automatic cloud backup services or set up calendar reminders for yourself.

History of Ransomware Attacks

This article has given ransomware prevention tips, discussed how to deal with a ransomware attack, and explained an easy ransomware removal process. Now, let's explore three recent examples of ransomware. Understanding how ransomware spread previously, will help us to appreciate why ransomware protection is so important.

- **Wolverine Breach** A ransomware attack hit the Wolverine Solutions Group (a supplier to the healthcare sector) in September 2018. Malware encrypted many of the company's files, leaving workers unable to access them. Fortunately, forensics experts were able to work to decrypt and restore them on October 3. Less fortunate, however, was the fact lots of patient data was compromised as a result of the attack. Names, addresses, medical data, and other personal information may have fallen into the hands of the

cybercriminals who carried out the attack.

- **Ryuk** Ryuk is a ransomware attack that started in August 2018. It differed from other attacks in the way it was able to encrypt network drives. As a result, hackers were able to lock down the Windows System Restore option, leaving users unable to recover from the attack if they did not have data backed up externally.

- **GandCrab** GandCrab is a destructive ransomware attack that hit in January 2018. It had many versions and became infamous as the infection quickly spread. The police worked closely with internet security providers to produce a ransomware decryptor to counter the effects of this attack.

Unique solution ID: #1026
Author: Roxanne Bernabeu
Last update: 2020-01-14 02:39