Ransomware

The Biggest Threat to Your Data in 2016

Malware is far from a new problem but the inexorable rise of Ransomware has taken many by surprise. The Health IT industry made headlines when MedStar Health was hit and its data was breached by Ransomware. The threat of Ransomware has now become so great, that the US and Canada issued joint security alerts.

What is Ransomware?

Ransomware is malicious software designed to block access to your computer until a sum of money is paid. Hackers can demand hundreds or thousands of dollars, just so you can retrieve your own data.

Types of Ransomware

SMS Ransomware:
This type of Ransomware locks your computer and displays a ransom message with a code. To unlock your computer, you are instructed to send the code via text message to a premium-rate SMS number to receive the corresponding code to unlock it.

Winlocker:
This variant of Ransomware also locks your computer, but it displays a more intimidating ransom message which appears to be from your local law enforcement agency. Unlike SMS Ransomware, this particular kind instructs you to pay through an online payment.

File Encryptors:
This kind of Ransomware can encrypt your personal files and folders using complex encryption algorithms to make your computer's data unusable. The malware author then demands that you pay for the decryption key using one of the online payment systems mentioned above.

How does the Malware Attack?

You can be infected when you unknowingly download Ransomware from:

Unsafe Websites
Your system can be infected by surfing compromised websites

Spammed Emails
Clicking on spam emails and its content

Other Malware
Lack of security protocols in your system

How to Avoid Infection?

Always Have a Backup

Create a backup and store it offline. Remember that Ransomware may search for documents on any connected drives or shares, so backing up to a system that is directly connected or uses a shared volume could result in the backed up files being encrypted as well.

Gateway Anti-Malware Filtering

Make sure the Anti-virus software and firewall security are functional and up-to-date in your system in order to filter out currently-known variants of Ransomware.

Desktop Anti-Malware Filtering

Always use high quality anti-malware on end point computers to avoid infection via network shares, USB sticks, etc.

User Education

Never click on unknown links in unsolicited e-mails, or install any software without knowing it's safe.

Separate System Admin Accounts

System Administrators should never give normal user accounts extended privileges, and they should use a separate administrator account when performing tasks requiring their privileges.

Sandboxing

Run your e-mail client inside a sandbox to further protect and scan against a Ransomware infection.

System Lockdown

Consider locking down your computer with a security policy by using the best security software to lock down Windows to prevent infection by the malware or Ransomware.

Execution Restriction

Limit the areas in which executables (.exe files) are allowed to be run and limit the damage caused by malware.

What to Do if Infected?

- Alert law enforcement so they are aware of the criminal activity.
- Turn off your infected computer and disconnect it from the network
- Decide if you want to pay the ransom. However, there is no guarantee criminals will unlock your data
- If you have a back-up, remove the malware and restore your system