Protect Your Hospital From Ransomware

"Ransomware" attacks on healthcare organizations are on the rise.

Read this document for steps you can take to protect your organization from this serious threat.

Ransomware, heard of it?

Hackers spreading the ransomware computer viruses are increasingly targeting hospitals; holding their data hostage and demanding payment for its safe return. There are many different types of ransomware; however, all of them will prevent you from using your PC normally, and will ask you to do something before you can use your PC again.

Ransomware is a class of malware that holds a computer "hostage" until the user pays a particular amount or abides by specific instructions. The ransomware then restricts access to the computer system when executed, or in some cases, repeatedly show messages or graphic images that forces users into paying the "ransom" or performing the desired action. Cybercriminals behind this threat made use of online payment methods such as Ukash, PaySafeCard, MoneyPAK or Bitcoin as a way for users to pay the ransom. There are ransomware variants that encrypt files found on the system's hard drive, holding the encrypted data for ransom. Again, users are then forced to pay up in order to decrypt the important or critical files that were altered by the ransomware due to file encryption.

Recent Ransomware Attacks on Hospitals

These are just a few of recent report cases in the national news.

- February 5, 2016, Hollywood Presbyterian Medical Center in Los Angeles, CA, had medical systems infected with the Locky crypto-ransomware affecting computers essential to laboratory work, CT scans, emergency room systems, and pharmacy operations were all infected. After almost two weeks, the hospital paid a ransom of 40 Bitcoins ($17,000) to unlock their machines because paying the ransom was the quickest and most efficient way to restore their systems.
- March 16, 2016, Ottawa Hospital in Canada is hit with Locky crypto-ransomware attack affecting four computers, but is fortunate enough to fend off the attack, by completely wiping the affected computers and restoring data through backups.
- March 18, 2016, Methodist Hospital in Henderson, KY is hit with the Locky crypto-ransomware, which came in as an attachment on a spam e-mail, and attempted to spread across the network after it had infected the computer it was triggered on. Hackers demand a ransom of four bitcoins ($1,600), to unlock their machines.
- March 23, 2016, Chino Valley Medical Center and Desert Valley Hospital part of the Prime Healthcare, were both hit with ransomware. Fortunately, both facilities had a good defense strategy and were able to defend off the attack. Neither facility paid the ransom.

Ransomware Prevention Tips

Window OS

We recommend that you take the following immediate and ongoing steps to reduce your exposure to a ransomware attack.

- ☐ Backup import files regularly to an encrypted portable HHD, network share, or cloud storage. Check the integrity of the data backups, by periodically validating the data backups are good.
- ☐ Make sure your Windows Operating System is up to date with patches and security updates on all Windows Operating Systems. Security updates supporting the operating systems should be applied as quickly as possible after release.
- ☐ Earlier Windows versions such as, Windows XP, Windows Server 2003, and earlier versions are no longer supported or patched by Microsoft and should be avoided due to security risks they pose to the organization. At the very least, deny or limit public internet exposure for the earlier versions of the Windows Operating System, until the can be upgraded.
- ☐ Ensure antivirus/adware/malware security software solution with current up to date subscriptions. Apply virus definition updates from your software provider as quickly as possible following release. Automate the process to prevent human error.
- ☐ Keep Adobe Reader, Abode Flash Player, Java and other software applications patched and up-to-date.
- ☐ Enhance security of Microsoft Office components (Word, Excel, PowerPoint, Access, etc) by disabling ActiveX, Macros, and blocking external content from been automatically executed on your device.
- ☐ Avoid or refrain from clicking on links or opening attachments in emails from people you do not know. Train all staff continually on these issues so they do not fall prey to Social Engineering attacks exploiting the human factor.
- ☐ Make sure the pop-up blocker is enabled and running within the web browser.
- ☐ Ensure "SmartScreen Filter" is enabled on "Internet Explorer" browser. Microsoft's SmartScreen Filter is a feature within Internet Explorer that helps detect phishing and malware websites, and can protect you from downloading or installing malware. SmartScreen Filter checks websites you visit against a dynamic list of reported phishing and malware websites. If it finds a match, the SmartScreen Filter will warn you the website has been block for your safety.
- ☐ Disable auto play or loading of external media devices such as USB memory sticks or portable HDD's.
- ☐ Disable files running from ProgramData, AppData, LocalAppData, and Temp folders. These directories are commonly used for hosting malicious processes. Define software restriction policies to prevent executable file from running when they are in these specific folder locations.
- ☐ Disable file sharing. If you do fall victim to a ransomware infection, this will help to keep it isolate to your machine. Quickly remove your machine from the network and report it immediately to your IT Help Desk.
- ☐ Turn on Windows Firewall (This can help prevent malware infections by stopping suspicious programs from getting onto your PC, or access the internet once installed).
- ☐ Disable wireless connections, Bluetooth, and Infrared communication ports when they are not in use.
- ☐ Report suspicious emails and websites to your IT Department

Active Directory / File Server

- ☐ Be certain that backups are current, completing, and validated regularly. In event of a ransomware or virus infection, this may be your only defense for recovery.
- ☐ Limit user privileges (Many malware programs need full access to your pc to run properly). Only use Local Admin privileges when absolutely required by an application, tightly protect the system admin accounts to access by trained IT professionals on your staff.
- ☐ Implement Group Policies (GPO's) to control access to end device firewalls, RDP service, end device USB port, or CD/DVD rom drives and other security aspect that can be controlled by Active Directory Group Policies.
- ☐ Disable RDP (Remote Desktop Services) or use a non-standard port for RDP and severely restrict usage to appropriate IT staff.
- ☐ Be certain all user access is individually identifiable
- ☐ Review all network shares are only available to those who absolutely need the network share. Limit or restrict individual user access to appropriate network folders and files, and only grant the level of access require for the user job description (read only access, read/write access, full access).

Email Server Security

- ☐ Ensure antivirus/adware/malware security software solution with current up-to-date subscriptions. Apply virus definition updates from your software provider as quickly as possible following release. Automate the process to prevent human error.
- ☐ Configure policies on email server to block from sending email attachments with the file extensions exe, .scr, and .zip.

Network Security

- ☐ Ensure Internet Content Filter is up-to-date and cannot be disabled by end users.
- ☐ Be certain security appliances or firewalls are current and up to date.
  - Implement Foreign IP block list on network edge routers, security appliances and firewalls.
  - Ensure network routers, switch, and firewalls are patches to highest vendor supplied security release.
  - Regularly run and monitor the Fail2Ban list on Thrive EHR System.
  - Regularly run and monitor system access audit report on Thrive EHR System.
- ☐ Monitor network perimeter activity for abnormalities and respond quickly.
- ☐ Run intrusion detection software on your network perimeter.
- ☐ Conduct regular external vulnerability and/or penetration tests.
  - Fix all vulnerabilities found or fully understand why you do not.
- ☐ Be certain your wireless infrastructure is at current security levels. Segregate public wireless access from the hospital network with a separate public SSID.
- ☐ Re-evaluate your risk assessments, especially any risks not mitigated and determine if those widen your exposure, if so, develop a plan to address.

What To Do If You Become a Victim of Ransomware

$26 Million received by hackers in first two months: not going away anytime soon

1. Analyze the file structures to determine extent of attack.
   - If you do not have the resources to do this, contact a professional immediately.
2. Review sys log server and block port utilized.
3. Immediately pull impacted devices from the network to avoid propagation.
   - Wipe the device and reinstall from bare metal if necessary.
4. Restore from backup files.
5. Once recovered either from paying ransom or restoring backup - Focus on prevention going forward.