NEWS & VIEWS

A Complimentary Newsletter from Med-Net Concepts, LLC
and its Network of Independent Affiliated Companies

Volume 5 Issue 11
November 2019

In This Issue:

Med-Net Concepts, LLC

Dangers from Ransomware Could Pose Serious Concerns for Healthcare Providers

By:
Louise Lindsey, Editor

BIG BROTHER IS WATCHING YOU... a phrase that George Orwell coined in his famous novel "1984"-a book written in 1949 as a political satire where "Big Brother" represented a totalitarian state, and people were under constant surveillance via listening devices and cameras.

It is not a secret that local, state, and federal governments today have access to great deal of information about organizations and individuals living and operating in this country. This information can be accessed through a myriad of places where data is entered into databanks like the IRS, Social Security Administration, Veterans' Affairs, colleges and universities, county records, healthcare providers, and personal computerized devices like cell phones, desktop computers, and laptops, to name just a few. Fortunately, there are state and federal laws in place to protect this information and to control who can access it.

However, the "Big Brother" causing concern today involves criminals using vicious computer malware called "ransomware" to conduct cybersecurity attacks, access computerized systems, and force payment of a ransom to have the system restored. Cybersecurity attacks against healthcare providers are increasing at a phenomenal rate and not only do they disrupt clinical care operations, they can put patients at risk.

How Ransomware Has Evolved

With cyberattacks, a.k.a. ransomware, on the rise, understanding how it has evolved is the first step in planning how to defend against it.

Ransomware has been around since 1989 when Joseph L. Popp, a Harvard educated biologist, created what was called the AIDS Trojan (PC Cyborg) and sent 20,000 infected diskettes with the label "AIDS Information -

Introductory Diskettes" to the attendees of the World Health Organization's International AIDS conference. That virus was easily overcome but nonetheless opened the "Pandora's Box" for what was to come 17 years later.

In 2006, the Archiveus Trojan encrypted everything in the "My Documents" directory on a computer and required the victims to purchase items from an online pharmacy in order to get a password that released the encrypted files. Later that year, an encryption Trojan that spread via an email attachment disguised as a job application entered the picture, giving birth to a rising criminal enterprise.

Year by year ransomware has continued its advancement into more sophisticated and invasive viruses that use a myriad of methods to sneak their way into the computerized systems of all kinds of enterprises, not the least of these is ransomware's cyberattacks upon healthcare facilities with potentially life-endangering results.

Throughout this span of ransomware development, there are two distinct varieties that have remained consistent: crypto and locker-based. Crypto-based ransomware and its variants encrypt files, folders, hard drives, etc., while locker-based ransomware only locks a user out of their devices. This is usually seen in Android-based ransomware.

The availability of anonymous payment options, i.e., gift cards, prepaid credit cards, bitcoin, etc., has further enabled the spread of cybersecurity attacks.

Here are some examples of the risk and impact faced by the targets of ransomware attacks:

- Temporary or permanent loss of sensitive or proprietary information and equipment,
- Disruption of regular operations
- Financial losses incurred to restore systems and files
- Potential harm to an organization's reputation and clientele

FBI-Issued Warning Regarding Healthcare Vulnerability to Ransomware

In April 2016, the Federal Bureau of Investigation (FBI) in a blog post warned about the dangers and implications ransomware holds for healthcare cybersecurity. According to the FBI warning, "hospitals, state and local governments, law enforcement agencies, and businesses of all sizes could find themselves victims of a ransomware attack." The FBI further warned that "Ransomware attacks are not only proliferating; they're becoming more sophisticated."

These recently reported ransomware attacks in 2019 bear witness to the FBI's concerns and warnings:

- 5 More Healthcare Providers Fall Victim to Ransomware Attacks:
    - Colorado-based NEO Urology paid $75,000 ransom to unlock its systems
    - Baltimore Ransomware Attack Keeps Health Department Locked
    - Ransomware Attack on Connect Provider Impacts 25,148 Patients
    - Cyberattacks on New York Olean Medical Group and Seneca Nation Health System
    - California Shingle Springs Health and Wellness Center Experiences Cyberattack
- Michigan Doctor's Office Closes after Ransomware Attack Erases Patients' Files
- Wyoming County Health Ransomware Attack Disrupts Patient Care-Surgeries, Laboratory, Respiratory Therapy, and Radiology Exams/Procedures Cancelled
- Four Minnesota Healthcare Providers Report Breaches of Patients' Personal Health Information-a reproductive medicine clinic, a behavioral health clinic, a Catholic-operated hospital, and a community hospital district.

Emisoft, a cybersecurity firm, predicts that ransomware's mounting costs could reach $186 million in 2019.

How Ransomware Affects Healthcare Providers

Ransomware typically prevents an organization from accessing certain parts of its system. This is particularly problematic for healthcare providers like hospitals and nursing homes that are closely tied to their patient/resident data source. An example would be the attack cited above on the Wyoming County Health Organization that disrupted patient care and the Michigan physicians whose patient files were totally erased, requiring them to close their office.

It should be noted that more and more organizations are expanding and beginning to use "bots" which are Internet robots-also called spiders, crawlers, and web bots. An Internet bot is a software application that does repetitive and automated tasks in the Internet that would otherwise take humans a long time to do. The most common Internet bots are the spider bots which are used for web server analyses and file data gathering [*www.tech-faq.com/internet-bots.html]*.

Healthcare providers are starting to use "bots" to perform automated tasks such as indexing a search engine. Another type of bot is called a "chatbot" that conducts a conversation via auditory or textual methods and whose use is being broadly expanded for patients to use. Bots are also vulnerable to cybersecurity attacks and

criminals use them to gain access to an organization's computerized environment.

According to a vice president of a cybersecurity company specializing in the detection and mitigation of situations where "bots" are used maliciously, hackers can use bots to "find test results, financial information, debit and credit card numbers, patients' Social Security numbers" and much more than just "basic health information." The vice president describes it as the perfect tool for "identity theft."

Also, considering the media coverage of the opioid epidemic, it is not surprising that a "bot's" identity theft capabilities are being maliciously used to obtain medication information in order to obtain prescriptions for controlled substances. All a cyber thief has to do is "grab the prescription, go to the patient's pharmacy, state the patient's name and address, and walk out with the opioids." What this means is that anyone with personal health information online who is prescribed opioids is a potential target.

It should be noted that the criminals involved in cybersecurity attacks are expanding and being creative regarding new ways to launch a ransomware attack. They now have the capability to launch a cybersecurity attack through an infected website that someone may access on a computer at work. Even more concerning, some of those little "free" USB drives that are found in places like conventions and other marketing arenas may not be so "free." Some have been found to have embedded ransomware in them

[https://blog.knowbe4.com/alert-usb-sticks-could-infect-your-network-with-new-spora-ransomware-worm].

Critical Tools for Preventing and Responding to Ransomware Attacks: Employee Training, Strong Technology, and Comprehensive Disaster Recovery Planning

For all the benefits and the good derived by the computer age, there is an evil counterpart that seeks to derive benefits from illegal methods. For healthcare providers and other organizations with a growing dependence on computerized systems, the burden for preventing and responding to ransomware attacks rests with them.

Here are steps that healthcare providers can take to significantly reduce the effects of a cybersecurity/ransomware attack

[https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time]:

- **Frequent, Tested Backups:** Backing up every vital file and system is one of the strongest defenses against ransomware. All data can be restored to a previous save point. Backup files should be tested to ensure data is complete and not corrupted. (Note: Healthcare providers may want to consider using cloud resources for cost-effective recovery in the event of an attack. Creation of a separate data center isn't always necessary since organizations can now take advantage of low-cost blob storage provided by several public cloud providers.)
- **Structured, Regular Updates:** Most software used by healthcare providers is regularly updated by the software creator. These updates can include patches to make the software more secure against known threats. Every healthcare provider should designate an employee to update software. (Having fewer people involved with updating the system means fewer potential attack vectors for criminals.)
- **Sensible Restrictions:** Certain limitations should be placed on employees and contractors who:
    - Work with devices that contain company files, records and/or programs
    - Use devices attached to company networks that could be made vulnerable
    - Are third-party or temporary workers
- **Develop Ongoing Employee Education/Training Program:**The first step is to get an employee to be suspicious about opening or clicking an executable file like-
    - An email
    - An attachment, or
    - On a website

Ensure that training is appropriate for all users including those who may have limited familiarity with technology.

One of the ways a healthcare organization can avoid being hacked by malicious "bot" malware, is to "routinely monitor web traffic into the facility." If malware is suspected, contact an expert who knows how to deal with the problem. A non-expert may not be able to "keep up with an automated application that disappears and then reappears somewhere else in a system."

The following are some additional, specific suggestions from the FBI's Cyber Division for preventing and responding to ransomware:

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
- Manage the use of privileged accounts-no users should be assigned administrative access unless

absolutely needed, and only use administrator accounts when necessary.
- Configure access controls, including file, directory, and network share permissions, appropriately. If users only need read-specific information, they don't need write-access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).

The FBI's former Cyber Division Assistant Director, James Trainor, made this statement regarding prevention of ransomware attacks: "There's no one method or tool that will completely protect you or your organization from a ransomware attack, but contingency and remediation planning is crucial to business recovery and continuity-and these plans should be tested regularly."

If an organization or an individual believes a ransomware attack has occurred, the local FBI field office should be contacted, and the incident reported to the Bureau's Internet Crime Complaint Center.

"Fraud Avoidance Courses from Med-Net Compliance, LLC Provide Valuable Lessons for Long-Term Care Administrators"

Jo Ann Halberstadter, Esq

ADMINISTRATORS TAKE NOTE

Med-Net Compliance, LLC now offers two series of fraud modules with NAB/NCERS CEs on our website. Modules 1-8 offers 3 NAB CEs and modules 9-16 offer 3.75 CEs. All modules provide education on fraud, waste and abuse prevention and offer a combined total of 6.75 CEs for successful completion.

To review the NAB Approved courses visit our website:
https://www.mednetcompliance.com/med-net-academy/nab-approved-courses/

All 16 courses on fraud, waste and abuse were developed by Betty Frandsen, our Vice President of Professional Development and her staff.

Med-Net Concepts, LLC Affiliates

Med-Net Compliance, LLC

Med-Net Healthcare Consulting, LLC

Med-Net Risk Management, LLC

Med-Net IPA, LLC

STAY CONNECTED