Ransomware: What It Is and What Can Be Done About It

This edition of the NeHII Cyber Security Newsletter covers the topic **Ransomware: What It Is and What Can Be Done About It**.

Ransomware has made the headlines recently, especially as related to healthcare organizations. Holding clinical systems for ransom can have serious patient care consequences.

Definitions

Executable — An executable file is a type of computer file that runs a program when it is opened. This means it executes code or a series of instructions contained in the file.
Source: http://techterms.com/definition/executable_file

Encrypt — convert data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. An encrypted file will appear scrambled to anyone who tries to view it. It must be decrypted in order to be recognized. Some encrypted files require a password to open, while others require a private key, which can be used to unlock files associated with the key.
Source: http://techterms.com/definition/encryption

Macro — small program, or script, that automates common tasks
Source: http://techterms.com/definition/macro

Malware — Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system
Source: http://techterms.com/definition/malware

Ransom — a consideration paid or demanded for the release of someone or something from captivity
Source: http://www.merriam-webster.com/dictionary/ransom

Ransomware — a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.
Source: http://www.trendmicro.com/vinfo/us/security/definition/ransomware/

Background

In 2011-2012, locker style ransomware was prevalent. This type of ransomware would lock a user out of his/her system, usually with a bogus warning from 'law enforcement' claiming that the system was being used for illegal activities.

Starting in late 2013, cryptolocker malware made the scene, distributing itself primarily via executable attachments in email.

Today, ransomware primarily gets in through:

- Compromised websites – User visits a compromised website which redirects the user to a malicious web page that delivers the ransomware to the user's system
- Malicious email attachments – User opens infected document containing malicious macros that download ransomware from URLs within the document
- Malicious links in emails – User clicks on link to a malicious web page that delivers the ransomware to the user's system

Reference: ISACA sponsored webinar "Ransomware: Breaking the Criminal Business Model", June 9, 2016

Preparation Recommendations

The FBI published the story "Incidents of Ransomware on the Rise: Protect Yourself and Your Organization" on April 29, 2016, warning that "…the number of ransomware incidents—and the ensuing damage they cause—will grow even more in 2016 if individuals and organizations don't prepare for these attacks in advance." The FBI does not recommend paying the ransom since it incentivizes criminals to continue this activity and does not guarantee that the data will be given back.

Recommendations focus on two main areas:

- Prevention efforts including user education, strong access controls, software patching, security software
- Business Continuity efforts – backing up data regularly and securing the data backups offline

Go to the link provided below to see the full listing of tips provided by the FBI to deal with ransomware attacks. As FBI Cyber Division Assistant Director James Trainor states, "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."

Source: *https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise*

To learn more about cybersecurity threat remediation as well as cyber liability and cyber insurance considerations, register for the **Cybersecurity Forum being held on June 21, 2016**.

2016 Cybersecurity Forum

June 21, 2016

JOIN US AT:

Tiburon Golf Club
10302 South 168th Street
Omaha, NE 68136

RESERVE YOUR SPOT TODAY

Register Now

Learn about cybersecurity challenges and solutions that could affect your organization. Speakers will look at cybersecurity from a variety of perspectives to help you deal with the challenges you face every day. We will include a panel discussion that includes Q and A.

Who Should Attend?

- Information Security Officers
- Network Administrators
- System Administrators
- IT Auditors
- Compliance Officers
- Risk Management Officers
- Anyone Involved in Security and Compliance

Schedule and Presentations:

9:30am - Registration

10:00am - Introduction

10:05 - "The Current State of Cybersecurity"

11:05 - "Take Your Information Security Program to the Next Level"

Noon - Lunch & Networking (Lunch included with registration)

12:30pm - "Cyber Insurance - Does Your Coverage Match Your Exposures?"

1:30pm - Cybersecurity Panel Discussion

2:30pm - Wrap-Up

Sponsors:

********** **HIPAA SECURITY REMINDER** **********

Per NeHII HIPAA policy

- **IF YOU ARE A PROVIDER -** DO NOT ACCESS PATIENT INFORMATION USING NEHII UNLESS YOU HAVE A TREATMENT RELATIONSHIP WITH THE PATIENT.
- **IF YOU ARE A PAYOR -** DO NOT ACCESS PATIENT INFORMATION USING NEHII UNLESS YOU ARE DOING SO FOR PAYMENT OR APPROVED HEALTHCARE OPERATIONS PURPOSES.

Please review the attached NeHII HIPAA Training document with your staff members as a refresher.

Helix Security

Helix Security, a NeHII preferred partner for HIPAA Security Compliance services, can assist you with your risk assessment activities. If you have already conducted your own risk assessment, Helix can provide services to help you in the development and implementation of your Risk Management Plan. Services include:

- Risk management planning and mitigation services
- Contact information: Buzz Hillestad at buzz.hillestad@helixsec.com

Please send in topics and/or questions that you would like to see addressed in future Cyber Security Newsletters to:

Lianne Stevens at 402.290.7029 or lstevens@nehii.org