What Healthcare Providers Must Know about Ransomware

In late 2015, security experts predicted that 2016 would be the year of online extortion. They were right. There has been a 300% increase in online extortion this year. It is anticipated that over one million US businesses will be infected with ransomware by the end of this year.

Ransomware prohibits computer users from accessing their digital files by encrypting, or password protecting, the files with a key known only to the hacker. The hacker prevents the files from being recovered until a ransom is paid for the encryption key. Downtime associated to infection and cost of recovery are the consequences of a ransomware infection, but the consequences are far greater for those working directly in the healthcare industry and the business associates who support them.

In late June 2016 the Health and Human Services Department's Office for Civil Rights released its long awaited guidance on HIPAA and ransomware. Their guidance was clear: "*When ePHI is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted was acquired (i.e. unauthorized individuals have taken possession or control of the information, and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.*"

Ransomware is unlike any virus you are accustomed to. It is not an attack on computer systems – it is an attack on human vulnerabilities. These sophisticated viruses prey on human mistakes in order to take control of your organization. These threats require *just one* user to make *just one* ill-fated mouse click. That *one* click could be devastating to your entire organization.

This white paper provides information to healthcare providers about the ransomware threat including steps to reduce the likelihood of a ransomware infection and most importantly, how to secure ePHI in a manner that eliminates the need to report a HIPAA breach in the event of an infection cannot be prevented.

Content provided by:

KALLEO
TECHNOLOGIES

The Ransomware Threat

There are 390,000 (Paganini, 2015) new variations of malicious software (malware) released by hackers into cyberspace every single day. This equates to roughly twelve million new variations per month. A malware variant is a modified version of an existing piece of malicious software. That software is altered enough to prevent its detection from anti-virus and anti-malware security solutions. It now takes thirty to sixty days for anti-virus software providers to respond with updated signatures to recognize and stop new variants due to the large volume of threats developed daily. As a result, in any given week, computer users find themselves unprotected from millions of new variants that cannot be detected by their security software.

Ransomware is dangerous because it is untargeted. Attacks are broad in nature and threatens to infect any individual who uses the internet. This is an attack is on human beings and their vulnerabilities. It is relatively easy to protect computer systems from attacks. Protecting humans from themselves is much, much more difficult. (As healthcare providers, you are probably very familiar with that.)

What is Ransomware?

Ransomware is a form of malicious software developed to restrict user's access to their data until a ransom is paid to the hacker in exchange for a decryption key to unlock the files. Ransomware infects all files it is able to gain access to such as image files (jpeg, tif, etc), Adobe PDF documents, Microsoft Office generated files (such as Word, Excel and PowerPoint files) and other files that computer users have direct access to.

Ransoms are usually demanded in bitcoin, a form of cryptocurrency or digital money that is very difficult to track. In addition, a time limit is imposed upon the victim – generally a period of 24 hours from the time the malware encrypts the file. If the victim fails to pay the ransom (or successfully restore their data from their own backup solutions), the key is destroyed and access to the files is lost forever.

Unlike traditional viruses, the hacker is completely uninterested in the contents of the files they attack. These individuals are not trying to obtain ePHI data. They are not trying to steal corporate credit cards or bank information. A ransomware infection is a quick and dirty extortion attempt that aims to take advantage of a corporation's reliance upon their digital files in hopes that the organization lacks sufficient recovery tools thus forcing them to pay a funds to regain access to their data.

The Threat to Healthcare Providers:

The consequence of malware is much greater to healthcare providers and their business associates than the consequences to other industries because of the regulations surrounding the healthcare industry. Healthcare providers who are infected with ransomware are not are not just inconvenienced with losing access to their files: they are now faced with notifying the Secretary of Health and Human Services about a potential breach. This is the result of new guidelines release in late June 2016, by the Health and Human Services Department's Office for Civil Rights (Department of Health and Human Services, 2016).

OCR's long awaited guidance on HIPAA as it relates to ransomware infected PCs was clear:

"When ePHI is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted was acquired (i.e. unauthorized individuals have taken possession or control of the information, and thus is a "disclosure" not permitted under the HIPAA Privacy Rule."

If an organization's computers and/or network is infected with ransomware and there are any files containing ePHI encrypted as a result of the infection, the following steps must be taken by the victim to satisfy the requirements of the OCR HIPAA Ransomware Guidelines:

Action Steps Required:

1. The victim must report the ransomware infection as a HIPAA breach to the Secretary of the Department of Health and Human Services. (Department of Health and Human Services, 2016)

2. The Department of Health and Human services may assess a fine.

3. The infected entity must notify the affected patients of the HIPAA breach. (Department of Health And Human Services, 2014)

4. The infected entity may have to provide the affected patients with up to 2 years of identity theft protection. It is best practice to provide guidance to patients for how to effectively manage their risk of identity theft following a breach of information (HIPAA Journal, 2016) however the law requiring the provision of credit monitoring to affected patients varies by state (Simon, 2010).

5. As a result of the report, the infected entity may be subject to a full HIPAA audit.

6. If the encrypted files contain ePHI for 500 or more patients (and that is very easy to do) the infected entity must notify the local media in the form of a press release that it has suffered a HIPAA breach. (Department of Health And Human Services, 2014)

7. Last, if the infected entity lacks good backups, they will be forced to pay the ransom to the hacker that put them in this unfortunate position.

All of this devastation because one individual made one devastating mouse click.

How Does Ransomware Get On My PC?

If an organization is to reduce its risk of becoming infected with ransomware, its users must have an understanding of how ransomware exploits human error to gain access to the user's computer files.

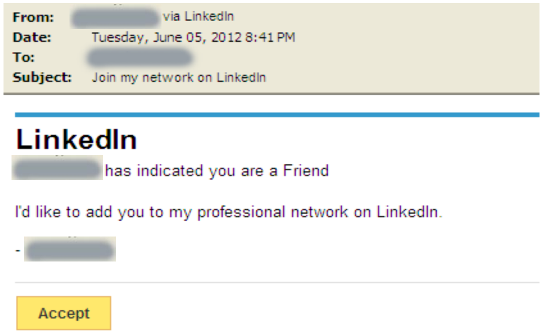
Email

Most commonly, ransomware is distributed by email to unsuspecting emails users. These emails are sent in bulk to user databases that have been mined or purchased with one goal: to defraud the recipient. This practice is known as phishing. To the untrained eye, the emails often appear to be legitimate. Below is an introduction to common phishing schemes used today to distribute ransomware and other forms of malicious software:

EXHIBIT
A

Social Media Malware Campaign

The security team at IBM recently witnessed a malware campaign that targets LinkedIn users. The process begins with a simple connection request sent to the victim's inbox. The email looks very similar to a legitimate LinkedIn connection invitation. Below are two examples:



From: [redacted] via LinkedIn
Date: Tuesday, June 05, 2012 8:41 PM
To: [redacted]
Subject: Join my network on LinkedIn

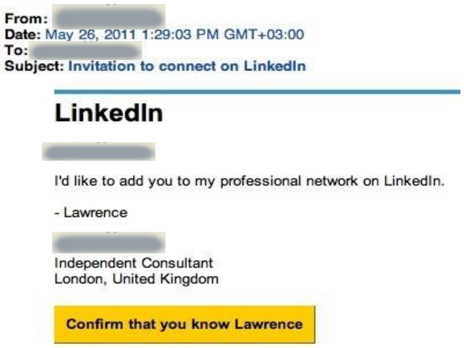
LinkedIn

[redacted] has indicated you are a Friend

I'd like to add you to my professional network on LinkedIn.

- [redacted]

Accept



From: [redacted]
Date: May 26, 2011 1:29:03 PM GMT+03:00
To: [redacted]
Subject: Invitation to connect on LinkedIn

LinkedIn

[redacted]

I'd like to add you to my professional network on LinkedIn.

- Lawrence

[redacted]
Independent Consultant
London, United Kingdom

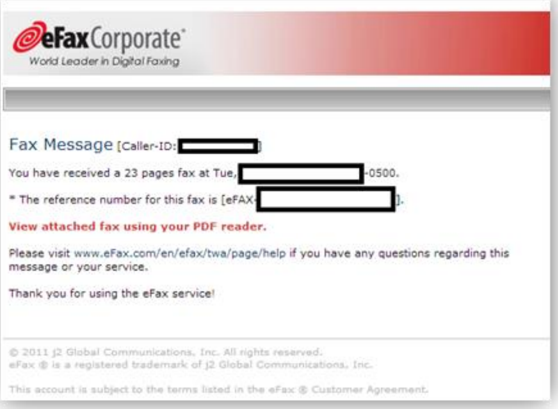
Confirm that you know Lawrence

The email on the left is the fake. The email on the right is a legitimate connection request. It is not possible to determine the real request from the fake request by visual inspection of these images, alone. Inspection of the URLs associated to the call to action buttons in the email provide additional intelligence regarding the validity of the email messages, but that, too, is not a fool proof method of protection. Best practice for responding to social media requests is to accept connection requests from within your social media accounts, not from emails that may (or may not) be generated from those accounts.

EXHIBIT
B

Fax/Scan Malware Campaign

The use of faxing and scanning is prevalent in healthcare practices. Cyber criminals have created phishing emails that look like the eFax and Scan notifications that are commonly seen in the work place. Below are two examples. Both of these notices contained links or attachments that contained malicious software.



eFax Corporate®
World Leader in Digital Faxing

Fax Message [Caller-ID: [redacted]]

You have received a 23 pages fax at Tue, [redacted] -0500.

* The reference number for this fax is [eFAX- [redacted]].

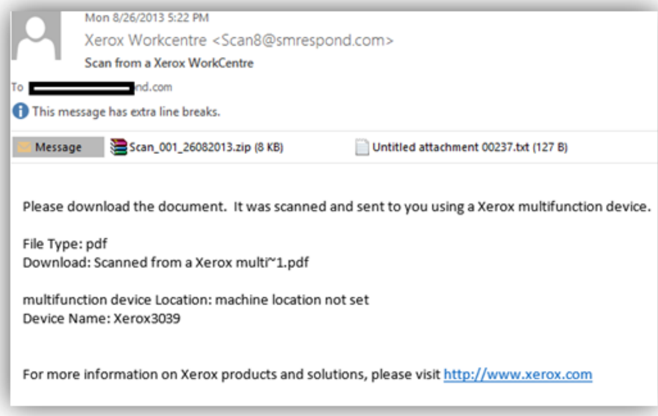
View attached fax using your PDF reader.

Please visit www.eFax.com/en/efax/twa/page/help if you have any questions regarding this message or your service.

Thank you for using the eFax service!

© 2011 j2 Global Communications, Inc. All rights reserved.
eFax ® is a registered trademark of j2 Global Communications, Inc.

This account is subject to the terms listed in the eFax ® Customer Agreement.



Mon 8/26/2013 5:22 PM
Xerox Workcentre <Scan8@smrespond.com>
Scan from a Xerox WorkCentre
To [redacted]nd.com
This message has extra line breaks.

Message | Scan_001_26082013.zip (8 KB) | Untitled attachment 00237.txt (127 B)

Please download the document. It was scanned and sent to you using a Xerox multifunction device.

File Type: pdf
Download: Scanned from a Xerox multi~1.pdf

multifunction device Location: machine location not set
Device Name: Xerox3039

For more information on Xerox products and solutions, please visit http://www.xerox.com

Be mindful of the generic emails you receive regarding fax and scan files. If your organization does not receive faxes or scans by email, delete them. If you are a practice that commonly received eFax and Scan notices by email, be diligent in verifying the sender prior to clicking on a link or attachment.

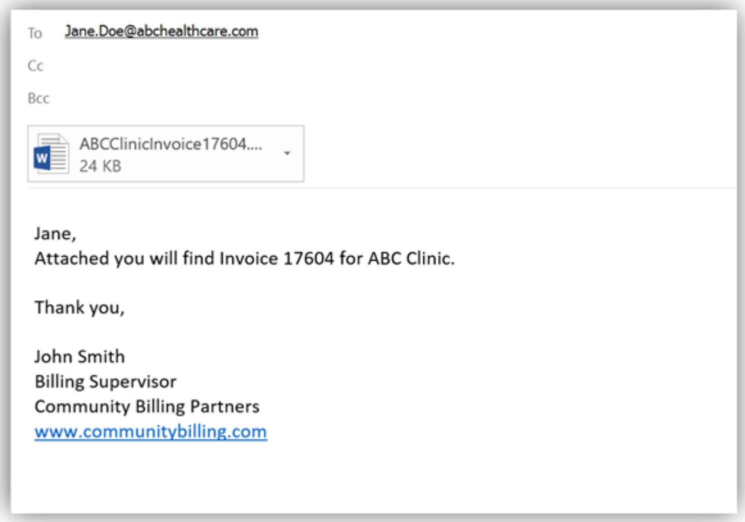
Ransomware is dangerous because it is untargeted. Attacks are broad in nature and threatens to infect any individual who uses the internet. This is an attack is on human beings and their vulnerabilities. It is relatively easy to protect computer systems from attacks. Protecting humans from themselves is much, much more difficult.

EXHIBIT
C

exhibitsticker.com

Healthcare Focused Malware Campaign

This is a phishing attempt that was engineered specifically for the healthcare industry:



To Jane.Doe@abchealthcare.com

Cc

Bcc

Jane,
Attached you will find Invoice 17604 for ABC Clinic.

Thank you,

John Smith
Billing Supervisor
Community Billing Partners
www.communitybilling.com

The email is addressed to a specific individual and the attachment is personalized to the organization to whom it was sent. This sort of campaign is very easy for a hacker to generate with software that automates the creation of these personalized spam messages. Do not be fooled into thinking your practice is too small to fall victim to such an attack. Do not open attachments or click on links from individuals you do not know.

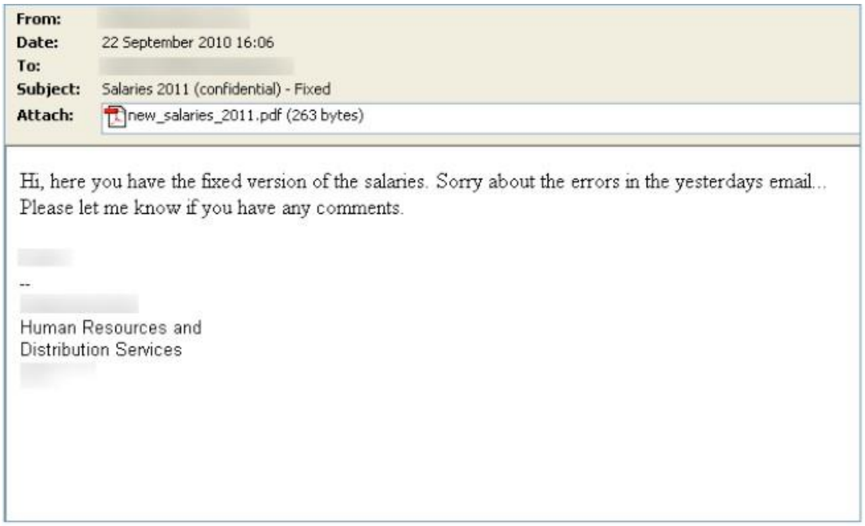
EXHIBIT
D

exhibitsticker.com

Spear Phishing Malware Campaign

A spear phishing attack is a targeted attempt to defraud an individual by posing as someone that he or she knows. You may be thinking "my practice is too small to be a victim of an attack like this." We have seen companies with as few as three employees receive spear phishing emails. In reality, these emails are incredibly easy to fake. Today's sophisticated data and contact mining tools available on the internet (many of them at no charge) provide hackers with everything they need to automate the creation these with relative ease and minimal time.

This is an example of a spear phishing email attempt:



From: [redacted]
Date: 22 September 2010 16:06
To: [redacted]
Subject: Salaries 2011 (confidential) - Fixed
Attach: new_salaries_2011.pdf (263 bytes)

Hi, here you have the fixed version of the salaries. Sorry about the errors in the yesterdays email...
Please let me know if you have any comments.

[redacted]
--
[redacted]
Human Resources and
Distribution Services
[redacted]

In this example the email was sent from an HR Manager to his Payroll Clerk claiming to have attached a PDF of a salaries document. The document contains malware and was not, in fact, generated by the HR Manager.

The lesson here is a difficult one to enforce, but is critical to the protection of your computer users. Do not open an attachment you are not expecting, even if you think you know the sender.

Malicious Websites

Another common way that ransomware makes its way to your PC is through “drive by downloads” from shady websites. A drive-by-download attack does not require a user to click on an attachment as with email delivery techniques. These attacks are the result of a sophisticated hacker who is able to embed hidden code into a malicious website. The code executes the download of ransomware to the user’s PC when the user merely visits the website containing the virus.

To avoid this type of attack, inspect website addresses thoroughly. Never click on a web link sent to you by email from an unknown sender (or, for that matter, from a known sender if the website address looks suspicious or the email is in any way unusual).

Do not be fooled by thinking that malware can only be found on "shady" websites. Affiliate links on popular website have been known to contain malicious code.

Pirated Software

It should go without saying that you should never, ever install software that you do not obtain through legitimate means. When you use pirated software you are not only breaking the law and infringing on the copyright of the software manufacturer, but you are also putting yourself at serious risk of downloading ransomware.

How Do I Defend Against a Ransomware Infection (and Subsequent HIPAA Breach Reporting)?

There is not a product or service available today that can 100% protect you from a ransomware infection. The number of new malware variants engineered each day makes it impossible today for software developers to create a solution that can guarantee protection. Fortunately, there are steps you can take proactively to significantly reduce your risk of a ransomware infection and subsequent HIPAA breach reporting.

Backup and Disaster Recovery

First and foremost, you must be certain that you have adequate backups of your computer systems and data. In fact, the HIPAA Security Rule requires covered entities and business associates to implement policies and procedures that can assist an entity in responding to and recovering from a ransomware attack.

Not all backup solutions are created equal. You must consider *what* you are backing up, *how often* you are backing up that data, and most importantly, **you must test your backups**. A backup report that shows no faults is not a guarantee that your data is adequately protected from disaster. You must know with certainty that your backup system will prevent you from having to pay the ransom associated to a ransomware attack. The only way to be certain of this, is to test your system. Do not wait until you have to restore a backup to learn whether or not you were adequately protected.

Finally, you must have a clear understanding of where your backups are stored and who can access them. Ransomware infects all files accessible to the user who initiates the infection. Are your backups at risk of infection?

Isolate Your ePHI from Your Local Network

Remember that ransomware infects all files accessible by the user who contracts the virus. We recommend that practices identify and remove all ePHI from their network. You can mitigate your risk of malware infection by isolating all ePHI in a manner that allows your users to access it but prevents access by malicious software.

You should start by evaluating your EHR. You must determine if your EHR vulnerable. Some EHR platforms are lightly vulnerable while others are highly vulnerable to a ransomware attack. (Note: Kalleo supports over a dozen EHR platforms and can provide guidance as to the level of vulnerability of a particular system upon request.)

Do not assume if you are using a cloud-based EHR that you do not have local access to ePHI. Have you migrated to a new EHR in recent years? Where's the data from the old EHR?

Second, ensure your staff do not store information containing eEHI outside EHR. If this is unavoidable, determine your staff's requirements for having widely accessible ePHI outside of the EHR. Restrict access to include only the staff members who require the information. Enforce policies related to how long the information should be accessible and a process for destruction.

Regardless of which EHR is in use by your practice, you almost certainly have ePHI outside the platform they are unaware of. Consider folders on your network with names like *scan folder, old correspondence stuff we may need someday*. Kalleo supports over 500 physicians nationwide. We have never seen a medical office that does not have some ePHI outside the EHR. It is likely we can easily find ePHI for over 500 patients on your network – in fact, odds are we can find this amount of ePHI in a single file.

Train Your Staff

Your employees are your computer network's most significant liability. A recent Verizon wireless survey showed that 30% of email users will open a phishing message they receive and 12% of targets will open a malicious attachment or click on a malicious link (Verizon, 2016). Think about that. How many employees do you have in your organization? One out of twelve of those individuals will unwittingly expose your workplace to ransomware (even with training).

You must train and retrain your staff often. Make cyber security part of your workplace culture. Your goal with training is to help people who are ignorant become better informed about the *consequences* of their actions.

Create policies and procedures regarding the use of IT resources, especially email. Ensure you provide adequate training to your staff about those policies. Make sure that your policies include instruction on how ePHI is to be moved and stored throughout your systems. Give your employees real life examples the ways they can be fooled by cyber criminals. Teach them how to verify the emails they receive are valid and best practices for handling emails related to social media requests.

Train, train and retrain often.

How Can I Obtain Assistance in My Defense Against Ransomware?

Founded in 2004, Kalleo Technologies is a managed IT service provider specializing in highly efficient, remote managed systems. Kalleo's professionals have extensive knowledge of the challenges facing healthcare industry and currently provides support to over 500 physicians in 28 states.

Kalleo is uniquely positioned to assist healthcare providers in creating a plan of defense against ransomware. Kalleo has direct experience supporting over a dozen EHR solutions. We can provide assistance to practices who wish to inquire about potential vulnerabilities posed by their EHR. We provide audits of existing backup and disaster recovery systems to ensure adequate recovery in the face of disaster. We also can provide assistance in policy creation, HIPAA / HITECH Security Risk Analysis, and educational content to aid in user training.

Ransomware poses a significant threat to your healthcare practice. The financial impact of an infection, even if you recovery quickly and are not forced to pay the ransom, can cripple if not devastate your organization.

About Kalleo Technologies

Founded in 2004, Kalleo Technologies is a managed IT service provider specializing in highly efficient, remote managed systems. Kalleo's professionals have extensive knowledge of the challenges facing the healthcare industry. Kalleo uses this knowledge to help its clients leverage technology in a way to further their advancement towards their strategic business goals. Learn more at www.kalleo.net or contact us at (270) 908-4136.

Connect with Kalleo

www.facebook.com/kalleotechnologies

www.twitter.com/kalleotech

www.linkedin.com/company/kalleo-technologies

References

Department for Health and Human Services. (n.d.). *Department for Health and Human Services*. Retrieved from Submitting Notice of A Breach to the Secretary: http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

Department of Health And Human Services. (2014, November 1). *Breach Notification Rule*. Retrieved from HIPAA For Professionals - Breach Notification Rule: http://www.hhs.gov/hipaa/for-professionals/breach-notification

Department of Health and Human Services. (2016, June). *FACT SHEET: Ransomware and HIPAA*. Retrieved from Department of Health and Human Services: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

HIPAA Journal. (2016, February 2). *How to Retain Patients After a Data Breach*. Retrieved from HIPAA Journal: http://www.hipaajournal.com/how-to-retain-patients-after-a-data-breach-8292/

Paganini, P. (2015, January 17). *AV-TEST Estimates 12 Million New Malware Variants Per Month*. Retrieved from secuJanuaryrityaffairs.co: http://securityaffairs.co/wordpress/32352/malware/av-test-statistics-2014.html

Simon, J. (2010, June 1). *States with Laws Requiring Consumer Notification of ID Theft*. Retrieved from CreditCards.com: http://www.creditcards.com/credit-card-news/data-security-breach-notification-laws-1282.php

Verizon. (2016). *2016 Data Breach Investigations Report*. Retrieved from Verizon Enterprise: http://news.verizonenterprise.com/wp-content/uploads/2016/04/B808-Verizon-DBIR_2016_Exec_summary-160425-28-US-FastWeb.pdf