SECURITY SPOTLIGHT

RANSOMWARE: HOSPITALS ON HOLD

KASPERSKY lab

What is ransomware?

Ransomware is a type of malware that attempts to extort money from a computer user by infecting or taking control of a victim's machine or the files or documents stored on it. Typically, the ransomware will either lock the computer to prevent normal usage or encrypt the documents and files to prevent access to the saved data.

- Prevents you from accessing essential programs and devices
- Encrypts files so you can't use them
- Stops certain apps from running

Ransomware. Just saying the word leads to a lot of questions. What is it? How does it work? Why is it suddenly a big issue for the healthcare industry?

Ransomware is, quite simply, the digital version of extortion, and few industries have such valuable information to extort as the healthcare industry. Freeze up a hospital's computers, and patients can't be checked in, doctors can't access health records and medical procedures can't be performed. As cybercriminals learn that hospitals are an easy target with a lot invested in getting their systems back up and running, this nightmare scenario will continue to hit more and more hospitals.

48.3% The number of users attacked by encryption ransomware increased by 48.3% in 2015.[1]

THE PERFECT DIGITAL CRIME

Ransomware is the perfect crime. It combines two qualities of fear and urgency in a masterful play to get hospital IT staff and administrators to make quick decisions that they don't want to make. What starts out as a simple message on the screen of one employee can quickly spread through a whole organization, leaving panic and confusion in its wake.

This is what happened in the infamous case of the Hollywood Presbyterian Medical Center. When ransomware shut down its systems for more than a week, staff were forced to rely on fax machines and telephones to get work done, while essential systems related to CT systems, lab work and pharmacy were offline. Some patients were transferred to other hospitals, and the hospital declared an internal emergency. The case made headlines after hospital administrators agreed to pay 40 bitcoins—the preferred, untraceable currency of cybercriminals—worth about $17,000 to get their systems back online.

While the Hollywood Presbyterian Medical Center was able to get its systems back up and running by paying the ransom, the payment itself is a gamble, since there is no guarantee that cybercriminals are willing to give up the decryption key or that they actually have access to it. **Most important, the financial and public relations damage that a healthcare organization suffers in cases like these is far greater than any payment they have to make.**

Ransomware is a problem that affects every industry, but healthcare organizations are easy prey for cybercriminals. There are few industries that face life or death consequences when their systems go down, and cybercriminals know it.

1—The Kaspersky Lab Security Bulletin Overall Statistics Report for 2015

4,000 Number of daily ransomware attacks in 2016, up 300% from 2015, according to an interagency U.S. government report.

HOW DOES RANSOMWARE WORK?

Ransomware is a unique kind of cybercrime. Unlike hackers who attempt to steal data, ransomware criminals only attempt to **prevent access to data.** Because of this, hospitals come to a grinding halt when hit by ransomware—and they don't easily forget the experience. They may not have to pay a massive sum of money, but the residual costs, the reputational damage, and the patients left waiting around for appointments and procedures all serve to leave a lasting mark on the collective memories of hospital staff.

When ransomware hits, it usually walks through a number of typical steps.

1. Installs when the user opens a file, usually via email, IM, social network or by visiting a malicious site. Since it is estimated that **93% of all phishing emails contain encryption ransomware**, it is essential that staff be educated about this threat.
2. Generates a pop-up window, web page or email warning from what looks like an official authority.
3. Encrypts the user's files with an AES-256, a randomly generated one-time key.
4. Creates an individual encryption key for each file. Frequently, ransomware, after encrypting the data it was seeking, deletes the original data and leaves only the data in encrypted form.

The first instinct many victims have is to try to unlock the data by decoding the encryption key. This is a losing battle. Looking closely at the math, security experts determined that it would take approximately 7x1040 times longer than the age of the universe to exhaust half of the keyspace of a AES-256 key.[2] In short, don't bother.

2—Time and energy required to brute force an AES-256 decryption key

WHAT DO HIPAA REGULATIONS SAY ABOUT RANSOMWARE?

With IT departments focusing on access over security, many hospitals that are already operating on dated systems are wide open to security incidents. And those incidents—particularly ransomware—are happening with greater frequency than ever.

Because the U.S. government passed a federal mandate in 2015, requiring electronic medical records (EMR) or electronic health records (EHR) to be implemented into personal health information (PHI) systems, the amount of data covered under HIPAA regulations is growing.

According to the HIPAA Security Rule, simply the presence of ransomware—or any malware—on a healthcare provider's or business associate's computer system is classified as a security incident. And hospitals are on the hook to prevent this from happening.

In addition, the HIPAA Security Rule goes beyond simply classifying ransomware as a security incident. It also requires implementation of specific security measures to prevent the introduction of malware, including ransomware.

WHAT ARE THE HIPAA NOTIFICATION REQUIREMENTS WHEN RANSOMWARE HITS?

When a ransomware attack strikes, the HIPAA Privacy Rule states that a breach has occurred because the ePHI encrypted by the ransomware was acquired by unauthorized individuals. This is a disclosure that is not permitted under the HIPAA Privacy Rule.

If the healthcare provider or business associate can demonstrate that there is a "low probability that the PHI has been compromised," then they are not required to treat the incident as a breach under HIPAA requirements. This demonstration includes a risk assessment that considers the following four factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

They must also maintain supporting documentation sufficient to meet the burden of proof that there was a low probability of compromised data.

Under the Breach Notification Rule, the healthcare provider must comply with the applicable provisions, including notification to affected individuals without unreasonable delay. For breaches affecting over 500 individuals, they must also notify the Secretary of Health and Human Services and the media.

THE ROLE OF BACKUPS IN A RANSOMWARE ATTACK

Because ransomware denies access to data, it is essential that hospitals maintain frequent backups to ensure the ability to recover. **In fact, implementing a data backup plan is a Security Rule requirement under HIPAA.**

Backups should be tested periodically to verify their integrity. When ransomware hits, online backups are a frequent target, and many victims have been dismayed to discover that their backups have also been encrypted or wiped out entirely. To avoid this unwelcome scenario, it is recommended that healthcare organizations maintain offline backups as well.

In addition to backups, you should also have a disaster recovery and emergency operations plans in place, and you should periodically test these contingency plans to make sure you're ready to execute on them. This also provides confidence to the rest of your organization and the patients you serve that you are ready to react if ransomware strikes.

Most important, you should understand that backups alone will not protect your organization from ransomware. It is just one layer of defense, and you should have a multi-layered security solution in place to protect all of your systems, such as Kaspersky Lab's full suite of products.

RANSOMWARE PREVENTION REQUIREMENTS FROM HIPAA

Security incident procedures are also required by HIPAA (See 45 C.F.R. 164.308(a)(6).), and they should include processes that:

- Detect and conduct an initial analysis of ransomware
- Contain the impact and propagation of the ransomware
- Eradicate the instances of ransomware and remediate vulnerabilities that permitted the ransomware attack
- Recover from the ransomware attack by restoring data lost during the attack and returning operations to business as usual
- Conduct post-incident activities to determine what obligations the entity has as a result of the incident and what lessons can be learned

In addition, HIPAA recommendations include contacting the FBI or U.S. Secret Service field office, both of which work to assist victims of cybercrime. For more information on HIPAA requirements around ransomware, we recommend downloading "Fact Sheet: Ransomware and HIPAA".

$2.2 million The average amount that healthcare organizations spend to resolve the consequences of a data breach.[3]

WHY IS THE HEALTHCARE INDUSTRY A TARGET?

Easy prey. Cybercriminals look for the path of least resistance, and healthcare organizations have the reputation of putting up little challenge to cyber intruders. Many healthcare organizations don't have streamlined security policies, and the policies they do have are often ignored by medical personnel who are in need of time-saving techniques. Passwords are shared. Files get left open. And security software is not always up to date. Even the most secure healthcare organizations may fall victim to cybercriminals because of the reputation that healthcare organizations have for being an easy target.

Valuable data. The cost of data breaches vary by industry, but the healthcare industry pays most dearly for every record lost. Globally, the average cost of a data breach per lost record is $158, which includes factors such as business continuity costs, mitigation costs and damage to reputation. **In healthcare, the average cost of a lost or stolen record is $355**[4] –by far the most costly of any industry.

Why? Because healthcare records contain the most information in one hit. In addition to your private medical information, cybercriminals can access your social security number, date of birth, and insurance credentials, all of which can be a portal for them to access other areas of your life, including banking and finances.

In addition, there is no expiration date on healthcare records. While credit card numbers may expire or be blocked, healthcare records have no expiration date, making them a valuable commodity on the black market.

With **data breaches causing collective annual losses of $6.2 billion in the healthcare industry**[5], it's an issue that needs to be taken seriously and addressed quickly. And with the arrival of ransomware on the scene, the losses are sure to increase.

3,5—Ponemon Institute's "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data"
4—Ponemon Institute's "2016 Cost of a Data Breach Study: Global Analysis"

170 million

The number of health records that have been exposed in data breaches since 2009, according to the U.S. Department of Health and Human Services.

WHAT DO WE RECOMMEND?

Here are **10 simple tips** every hospital should take to protect your data from ransomware.

1. **Back up your files regularly.** The only way to ensure that you can immediately handle a ransomware attack is to implement a regular backup schedule so that your organization can get access to the files it needs without dealing with the cybercriminals. Your backup should have certain restrictions, such as read/write permissions without an opportunity to modify or delete the files.
2. **Check your backups.** There are times when something can damage your files. Be sure to check regularly that your backups are in good shape.
3. **Protect against phishing attacks.** Cybercriminals often distribute fake email messages that look like an official message from a vendor or bank, luring a user to click on a malicious link and download malware. Teach employees that they must never open attachments from an unknown sender or even suspicious attachments from a friend in case they have been hacked.
4. **Trust no one. Or rather, trust but verify.** Malicious links can be sent by your friends or your colleagues whose accounts have been hacked. Let employees know that if they receive something out of the ordinary from a friend, they should call that person directly to verify that they sent it and find out if their accounts have been compromised.
5. **Enable 'Show file extensions' option in the Windows settings.** This will make it much easier to distinguish potentially malicious files. Because Trojans are programs, employees should be warned to stay away from file extensions like "exe", "vbs" and "scr." Scammers could use several extensions to masquerade a malicious file as a video, photo, or a document.
6. **Regularly update your operating system.** Cybercriminals tend to exploit vulnerabilities in software to compromise systems. With Kaspersky Lab's automated Vulnerability Assessment and Patch Management tools, you can rest assured that your system will be scanned and that patches will be distributed regularly in order to keep your system updated.
7. **Use a robust antivirus program** to protect your system from ransomware. Our Kaspersky Lab products employ a multi-layered system of defense that checks malware from many different angles to ensure that it does not corrupt your system.

But if ransomware hits...

8. **Cut off your internet connection immediately.** If you discover ransomware, shut off your internet connection right away. If the ransomware did not manage to erase the encryption key from the computers in question, then there is still a chance you can restore your files.
9. **Don't pay the ransom.** If your files become encrypted, we do not recommend paying the ransom unless instant access to some of your files is critical. Each payment made helps the criminals to prosper and thrive to go on to build new strains of ransomware.
10. **Try to identify the malware.** If you are hit by ransomware, try to find out the name of the malware. Older version of ransomware used to be less advanced, so if it is an earlier version, you may be able to restore the files. Moreover, cybersecurity experts, including Kaspersky Lab experts, collaborate with law enforcement to provide file restoration tools online and, hopefully, detain the adversaries. Some victims are able to decrypt the files without having to pay the ransom. To check whether that's possible, visit kaspersky.com

HOW DO KASPERSKY LAB'S PRODUCTS PROTECT AGAINST RANSOMWARE?

While there are many things you and your users can do to prevent ransomware from infiltrating your organization, implementing a multi-layered security solution is still the best defense against these sorts of attacks. Kaspersky Lab's products secure your organization through layer after layer of countermeasures that ensure that you are protected.

Our products use a range of sophisticated behavioral technologies to discern suspicious patterns, block malicious activities and roll back any harmful actions, including malicious file encryption.

WORKSTATION PROTECTION

Vulnerability Assessment And Patch Management

Vulnerabilities within any of the applications and operating systems running on your devices can provide entry points for ransomware. Our automated Vulnerability Assessment and Patch Management tools scan your systems, identify known vulnerabilities and help you to prioritize and distribute the necessary patches and updates so that known security vulnerabilities can be eliminated.

Anti-Phishing

Because phishing emails are usually the starting point for many ransomware attacks, Kaspersky Lab's anti-phishing technology uses a multi-layered approach to protect against infiltration. First, it checks sites with the product's local anti-phishing databases on the user's device. Next, it checks URLs of sites against Kaspersky's own vast, continually updated database of phishing sites, which are collected through Kaspersky Security Network. When a new malicious URL is detected on the computer, information about this threat is made available from the cloud database within 15-30 seconds of detection. Finally, our heuristic analysis is an intelligence system that looks at dozens of phishing symptoms and compares it with other indications, classifying them based on known modern phishers' methods and the vast Kaspersky Lab database of already detected phishing sites.

Heuristics

Heuristic analysis provides proactive protection from threats that can't be detected using signature databases. Kaspersky Lab's heuristics enable the detection of new malware or unknown modifications to known malware. Static analysis scans code for signs of suspicious patterns associated with malware, while dynamic analysis examines the machine code the file might try to execute.

Default Deny

Increasingly viewed as the most effective security posture to adopt in the face of ever-evolving, advanced threats, Default Deny simply blocks all applications from running on any workstation unless they have been explicitly allowed by the administrator. Since most malware is delivered as an executable file that cannot be found on any whitelist, organizations that adopt this approach can thus prevent any malicious file from executing without really needing to know what those files actually are. Default Deny means all new, file-based malware varieties are automatically blocked, even for targeted attacks.

System Watcher

System Watcher monitors applications and processes activity to discern behavioral patterns, relying on behavioral stream signatures that look at sequencies of actions, rather than just one isolated action. Malicious actions and destructive behavior patterns suggestive of malware are blocked.

Automatic Exploit Prevention (AEP)

As part of System Watcher, this technology specifically targets malware that exploits software vulnerabilities. AEP acts like a safety net, an extra layer of security that complements Kaspersky Lab's other technologies.

Rollback

Our crypto-malware countermeasure subsystem negates the consequences of crypto-attacks by making local, protected backup copies of user data files as soon as they are affected by a suspicious program, returning user data to its original preserved state.

SERVER PROTECTION

Application Launch Control

Application Launch Control prevents unapproved applications from launching and spreading malware right from startup.

Anti-Malware With Kaspersky Security Network Integration

Our anti-malware protection draws on our global network of sensors to anticipate the latest threats, giving our technology a worldwide perspective on evolving threats. This intelligence is then applied to our technology in order to protect your infrastructure before the attack ever reaches your server.

Anti-Cryptor

Our Anti-Cryptor technology monitors the server for signs of corruption, cuts the infected workstation's access to the server for 30 minutes, and alerts administrator to the infection.

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL TODAY >

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Learn more at usa.kaspersky.com/business-security

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:
usa.kaspersky.com/business-security
(866) 563-3099
corporatesales@kaspersky.com

KASPERSKY lab
THE POWER OF PROTECTION