IDC

INDUSTRY SPOTLIGHT

Sponsored by: Proofpoint

Ransomware attacks show no signs of stopping. The key to protecting healthcare IT against ransomware is to thwart the initial email phishing attacks.

An Ounce of Prevention Is Worth a Pound of Cure: Protecting Healthcare Enterprises Against Ransomware Attacks

January 2022

Written by: Lynne A. Dunbrack, Group Vice President, Public Sector

Introduction

In May 2021, the Cyber Division of the Federal Bureau of Investigation (FBI) issued a Flash Alert warning healthcare organizations and first responders, including law enforcement agencies, emergency medical services, 911 dispatch centers, and municipalities, that 16 Conti ransomware attacks were targeting their networks. Conti actors gained network access through malicious email links, attachments, and stolen Remote Desktop Protocol (RDP) credentials and then extorted ransom payments to restore access to essential IT systems and data. Preventing access to vital information impedes the ability of healthcare organizations and first responders to respond quickly to their patients' needs when time is of the essence.

In September 2021, *The Wall Street Journal* reported the first alleged ransomware death. The lawsuit filed by the infant's mother claims that the hospital did not tell her that its systems were under attack by ransomware and critical healthcare IT systems were shut down. Labor and delivery staff were unable to access key tests that would have shown that the umbilical cord was wrapped around the baby's neck. The baby was born with brain damage and died nine months later.

AT A GLANCE

KEY STATS

From January 1 to July 31, 2021, the IC3 received 2,084 ransomware complaints with over $16.8 million in losses, up from a total of 2,474 in 2020.

KEY TAKEAWAYS

- Bad actors are exploiting the pandemic crisis using tactics such as phishing and social engineering techniques to target and trick people.
- Once inside the network, the bad actor launches a ransomware attack and holds applications, networks, or data hostage unless a ransom is paid.
- It is critical to stop bad actors before the last mile of the attack when they have gained access to essential IT assets.

Cybercriminal activity increased significantly in 2020 and 2021 as bad actors exploited the global COVID-19 crisis during which normal business processes were upended as employers had to rapidly change how in-person processes were handled remotely. Furthermore, employees' personal home networks are more vulnerable to attack than corporate networks. In 2020, the FBI's Internet Criminal Complaint Center (IC3) received 791,790 complaints for a wide range of internet crime against U.S. targets — a 69% increase in total complaints over 2019 — and reported losses exceeded $4.1 billion. From January 1 to July 31, 2021, the IC3 received 2,084 ransomware complaints with over $16.8 million in losses, up from a total of 2,474 in 2020. The actual number of incidents could be higher as the IC3 figures include only victims who reported the ransomware attack to IC3.

Cybercriminals are pivoting to exploits that are the easiest to pull off and have the largest payoff. Ransomware targets people to essentially deliver the malware to networks by unwittingly clicking on malicious links and attachments that then compromise healthcare IT systems and data. As a result, tactics such as social engineering, email compromise, and phishing have become more sophisticated, leading to more ransomware attacks, which are easier to carry out and more productive than early brute-force attacks. Ransomware clearly pays off for bad actors, as evidenced by the growing number of attacks and successful collection of ransom payments.

What Is Ransomware?

Ransomware is a more destructive form of malware that takes IT systems hostage. In the healthcare industry, cybercriminals extort healthcare organizations for ransom payments (hence the name of the attack) for the key to unencrypt data and systems or for a promise by the bad actors not to publicly disclose the seized data. In many cases, the healthcare organizations have to revert to manual processes because their healthcare IT systems have been shut down either by the bad actor or by IT to prevent further damage. An operational failure can occur, leading healthcare organizations to turn away patients and divert them to other facilities, including their competitors. Ransomware payments along with remediation costs can run in the millions of dollars. Thus, ransomware has a disastrous impact not only on the brand and financial health of the attacked institution but also, more importantly, on patient care.

Anatomy of a Ransomware Attack

Ransomware attacks will continue in 2022 because they have proven to be lucrative for cybercriminals. To build an unfailing defense strategy, healthcare organizations must understand the fundamental steps of a ransomware attack.

1. **Distribution.** Email and web are the most common ransomware attack vectors among cybercriminals and hostile nation-states. For example, attackers will trick users into accessing malicious software using phishing emails, social engineering, fake websites with malicious links, and infected external storage devices such as USB sticks. In many cases, ransomware is a secondary payload delivered to already compromised systems.
2. **Infection.** The person under attack unknowingly downloads an executable (downloader) that installs the ransomware.
3. **Staging.** The ransomware payload dropped by the file conceals and embeds itself in the system.
4. **Scanning and encryption.** Once inside the network, the attacker will launch malicious software that encrypts systems, applications, or data.
5. **Ransom note.** The attacker will inform the healthcare organization that its systems, applications, or data are no longer accessible until the ransom is paid.

Extortion can come in the form of ransom payment for the key to unencrypt the healthcare IT systems or the data or, in the latter case, to prevent the bad actor from making the data publicly available on the internet or selling it to a third party. A new, disturbing twist to ransomware attacks is to also blackmail patients by threatening to reveal their sensitive health information if they don't pay the ransom demanded. Hacktivists, who are motivated by political or social causes, may threaten to delete data. There is no guarantee that once the ransom payment is made, typically in untraceable cryptocurrency, that the key will be sent or the data will not be further compromised through unauthorized disclosure or deletion.

Protecting Against Ransomware Attacks

Protection Against Phishing Attacks

Strong email hygiene is critical for protecting IT assets against ransomware attacks because bad actors typically target email as the initial infection point to access the networks of healthcare organizations. Cybercriminals' phishing emails have become more sophisticated over time. The tone, content, and look and feel of phishing emails closely mimic those of emails from valid senders. Often, even tech-savvy healthcare staff are duped into clicking links or downloading attached documents that launch further malware attacks.

Application of Rigorous Granular Access Policies

Network borders have become increasingly porous as a result of the growth of cloud and edge computing and the increased use of mobile devices in healthcare. The rapid shift to remote work during the early days of the pandemic eroded any sense of tightly controlled LAN and WAN perimeters. To protect seemingly borderless networks, healthcare organizations are adopting a zero-trust approach to security — "never trust, always verify." No level of trust is automatically granted to any end users or to any computing or network resources. Every device, user, network connection, and data exchanged is authenticated before access to data and apps is granted to authorized users. This enforcement of a rigorous granular access policy, augmented by a robust cloud security framework, helps prevent a ransomware attack from spreading across the network should a cybercriminal gain access to an application or a system.

Comprehensive Holistic Approach to Security

The best defense against ransomware attacks is a layered approach that combines strong email hygiene and zero trust network access controls and identifying staff who are being targeted for phishing emails and are more likely to click on a malicious link or attachment. The last mile of cybersecurity protection includes awareness training to mitigate the initial phishing attack, and then isolation technology provides a containerized environment for protected interaction with third-party messaging tools and cloud apps.

Cybercrime Is Constantly Evolving and Becoming More Insidious

Cybercriminals are clever about finding new people to attack who will be vulnerable to their phishing exploits and more willing to click on malicious links and attachments, often carrying ransomware. During the global pandemic, healthcare organizations became even more vulnerable to cyberattacks, especially ransomware, as staff shifted to working from home and as in-person processes such as procurement and payment processing became completely digital.

Phishing as a Ransomware Precursor

The early cyberattacks relied on brute force such as spam and denial-of-service attacks, which were successful only 10% of the time. Over time, bad actors evolved to stealing sensitive information such as credit cards, social security numbers, and protected health information — all available for sale on the dark web — to commit financial or medical identify theft for monetary gain. The next step in the evolving attacks is cybercriminals engaging in phishing through social engineering, including spear phishing (highly targeted attacks) and whaling (targeting senior executives), to steal credentials to gain access to the network. Success rates using various phishing attacks to get into the network, exfiltrate data, and conduct financial fraud can run as high as 75%. The stakes get higher when phishing and whaling attacks include ransomware to extort large sums of money from healthcare organizations to be paid in cryptocurrency.

Ransomware Delivered via Cloud File Sharing Applications

With many employees working remotely during the pandemic, file sharing services became the primary means of sharing large data files that were too large to be sent by email over personal networks. They also became a vector for ransomware attacks. Security researchers have identified a significant uptick in exploitation of legitimate file sharing services such as Box, Google Drive, OneDrive, and SharePoint from which bad actors launched email-based attacks to distribute malware and ransomware. Attackers exploit file sharing services to bypass domain reputation checks. The use of nested email is even more difficult to detect. In this scenario, an email containing malicious content or a malicious link is sent as an email thread of the initial email. If the unsuspecting user clicks on the secondary email content or link, the malware is released.

Ransomware in the Supply Chain

Cybercrime is big business. Organized crime syndicates and hostile nation-states are laser focused on how to successfully exploit their targets to achieve a positive return on their investments in acquiring or developing malicious software. The COVID-19 pandemic made it painfully clear how vulnerable the global supply chain is. Supply chain managers and their staff conduct high volumes of financial transactions between the healthcare organization and third-party suppliers that can run into six figures. A vast supply chain network in healthcare makes it a popular — and lucrative — target for cybercriminals. Bad actors recognized this quickly, launching various fraud attacks as healthcare users struggled to procure personal protective equipment, ventilators, and other essential medical supplies for treating COVID-19 patients.

Patience Is a Virtue for Cybercriminals

Complex, multistage phishing lures that maximize the value of compromised credentials take time for cybercriminals to cast. Using legitimate credentials to gain access to the healthcare organization's network, cybercriminals may lurk inside undetected for months to analyze employees' communication styles with internal colleagues and third parties. Once inside, bad actors can monitor network traffic, determine how to cause the most damage, start to exfiltrate data including protected health information, encrypt important IT resources and, ultimately, launch a ransomware attack.

Considering Proofpoint

Founded in 2002 by Eric Hahn, former CTO of Netscape, and headquartered in Sunnyvale, California, Proofpoint Inc. is a leading cybersecurity company serving 8,000+ enterprise customers worldwide. On average, Proofpoint analyzes 2.2 billion+ emails, 35 billion+ URLs, and 200 million+ attachments per day and monitors 22 million+ cloud accounts per day using advanced artificial intelligence and machine learning to deliver insights into its clients' security posture, including people-centric risk. Financial services and healthcare are the company's largest customer segments.

Proofpoint offers an integrated, people-centric approach to reduce the risk of ransomware attacks by layering controls that:

- **Prevent the initial attack.** Three out of four ransomware attacks start with email phishing or malware downloaders. Proofpoint Threat Protection Platform stops ransomware attacks by blocking malicious email, shifting defenses further up the ransomware attack chain. The platform uses machine learning-based engines and advanced sandboxing to analyze evasion techniques and URL- and attachment-based threats. Email-focused security orchestration automation and response (mSOAR) automates remediation of user-reported malicious or suspicious email.

- **Identify users who are most susceptible to phishing emails.** Proofpoint's in-depth analysis of user behavior provides people-centric insights about a healthcare organization's most targeted employees. Again, stopping ransomware from being launched is key to thwarting these attacks. By understanding which users are being aggressively targeted or may be more apt to fall for a phishing email, security teams can work with the business stakeholders to deploy adaptive security controls. The controls include greater user awareness training as well as browser isolation, which provides additional URL protection in corporate email.
- **Contain ransomware threats by automating threat detection and response processes.** Proofpoint automates processes such as blocking end-user access to cloud apps from risky locations or known threat actors and confirming a user's identity and preventing risky access using contextual data. Web security and isolation technology blocks connections to compromised sites.
- **Prevent data exfiltration.** Proofpoint Cloud Security's Web Security and Browser Isolation delivers risk-aware data security that can perform data loss prevention (DLP) in real time. Proofpoint protects sensitive data in cloud apps and blocks sensitive content from being exfiltrated via command and control, downloaded to unmanaged devices, and emailed out.
- **Train users to be more resilient to phishing.** Proofpoint security awareness training helps change behavior and reduce risk. First, it makes employees more aware of potential email attacks. More importantly, it changes behavior by teaching employees what to do if they receive a phishing email. User resilience is critical. Phishing attacks are becoming more frequent and sophisticated. These attacks are increasingly a means of delivering ransomware.

  The Proofpoint targeted training program first assesses the healthcare organization's risk profile by asking:

  - Which users are most heavily targeted by threat actors?
  - What are the most common attacks the healthcare organization faces?
  - What risky behavior and knowledge gaps need to be addressed?

  Short, focused videos and interactive, game-based training modules cover specific gaps. Online quizzes and gaming techniques engage users and help them retain their training. Organizations can further reinforce the training with healthcare-specific educational material. Proofpoint provides posters, mouse pads, screensavers, and other content to keep security top of mind.

Challenges and Marketing Opportunities

The market challenges that Proofpoint and its customers face can also present opportunities for a company with strong healthcare experience and a broad product portfolio:

- **Phishing attacks becoming more advanced and persistent.** The increasing volume of phishing attacks and high-profile security breaches inside and outside the healthcare industry is creating a heightened demand for security products and services. This is both an opportunity and a challenge for Proofpoint to keep up with the demand for its services and to stay ahead of the cybercriminals whose attacks are becoming more sophisticated and pernicious.

- **Cybercriminals constantly evolving their craft to exploit new crises and vulnerabilities.** Bad actors are highly responsive to new opportunities to exploit healthcare organizations. The spike in scams and cybercrime since the early days of the global pandemic are illustrative of the creativity bad actors apply to finding new vectors and creating exploits for very specific targets. Over time, they fine-tune their attacks using more distribution channels and advanced tactics such that even tech-savvy users fall prey to them.
- **More lucrative targets.** The increase in online financial transactions for life-saving medical equipment due to a shift in work from home for nonessential workers has made supply chain and financial managers/executives more lucrative targets. Redirecting financial transactions that can run in the tens to hundreds to even thousands of dollars creates a significant financial windfall for bad actors.
- **Pseudonymity through Bitcoin and other digital currencies.** The inherent nature of digital currency makes it attractive to cybercriminals. Since cryptocurrency is outside the purview of governments and federal agencies, anti-money laundering and know-your-customer requirements are typically not applicable to financial transactions using digital currency. The limited financial security protocols make it easier for cybercriminals not only to extort and collect ransom payments but also to conduct business with other cybercriminals.
- **Heightened demand for security products and professionals.** The growing volume of phishing and other cybercriminal attacks inside and outside the healthcare industry increases the demand for security products and professionals. This higher demand also makes it harder for healthcare organizations to attract and retain highly skilled IT security talent. As such, they lean on their security vendors to provide managed security services. A vicious cycle ensues.
- **Balancing robust security and user access to IT systems and data.** There is a constant struggle between IT security teams that want to lock down access to IT systems and line-of-business executives who want ready access to the data in those systems. If security protocols are too strict, end users will find ways around them, often making end users more vulnerable to social engineering and IT systems more prone to attack.
- **Employees working from home during the pandemic using personal devices for work.** Although many healthcare organization employees have returned to their offices for work, the way we work is shifting, and more employees will continue to work at home on an ongoing basis. Their personal devices and email accounts may not be well protected, putting not only themselves but also the healthcare organization's systems at risk.

Conclusion

Ransomware attacks show no signs of stopping — quite simply because they work. The financial rewards are significant and yet difficult to trace back to the bad actor who launched the attack because the ransom was paid in cryptocurrency. Cybercriminals will continue to evolve their technology and strategies to develop new ransomware attacks while avoiding detection by IT security.

The key to protecting healthcare IT against ransomware is to thwart the initial email phishing attacks. Ransomware is the weapon that is deployed after bad actors have successfully stolen legitimate credentials, gained access to the network, and begun wreaking havoc by encrypting and/or exfiltrating data. Healthcare organizations must

Ransomware is the weapon that is deployed after bad actors have stolen legitimate credentials, gained access to the network, and begun wreaking havoc.

focus on the beginning of the attack chain, not the end when the most damage has been done to the their systems, processes, and reputation. Because people are the conduit to data, employees will remain a primary target for attackers. Thus, healthcare organizations will need to be vigilant about conducting regular security training and awareness programs for employees. In addition, healthcare organizations should:

- Use robust email security, including authentication capability such as DMARC to verify who is sending emails to an employee or on behalf of that employee
- Deploy isolation technology for "happy clickers" (e.g., those who work in vulnerable ways, those who are heavily targeted by cybercriminals)
- Implement a DLP solution to protect against data exfiltration in the event of a breach

The best defense against ransomware is a strong offense. It's not a matter of if a hospital will be attacked; it's a matter of when. By taking a holistic approach of robust security technology and employee security awareness training, healthcare organizations can mount an effective defense to protect themselves against ransomware.

About the Analyst

Lynne A. Dunbrack, *Group Vice President, Public Sector*

Lynne Dunbrack is Group Vice President for Public Sector, which includes IDC Government Insights and IDC Health Insights. She manages a group of analysts who provide research-based advisory and consulting services for payers, providers, accountable care organizations, IT service providers, and the IT suppliers that serve those markets. Lynne also leads the IDC Health Insights Connected Health IT Strategies program.

MESSAGE FROM THE SPONSOR

About Proofpoint

Proofpoint, Inc is a leading cybersecurity and compliance company that provides health institutions protection and visibility for their greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps healthcare stop targeted threats, safeguard their patient data and intellectual property, and make their users more resilient against cyberattacks. Leading healthcare organizations of all sizes, including more than two-thirds of the Fortune 1000 healthcare institutions, rely on Proofpoint for people-centric security solutions that mitigate their most critical risks across email, the cloud, social media, and the web before they cause lasting harm. More information is available at www.proofpoint.com/healthcare.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com