TREXIN INSIGHT PAPER

March 2, 2022

RANSOMWARE

Understanding cybersecurity basics to better defend individuals, businesses, and teams.

Due to the COVID-19 pandemic, malicious email attacks have increased up to 600%[1]. In these attacks, ransomware still ranks as the most prominent malware threat to your personal and organizational data. Attacks can impact businesses of any size across all sectors; however, nearly 50%[2] of healthcare breaches were caused by ransomware attacks in 2020 alone. What's most shocking—despite attacks on healthcare costing more than any other industry at $408[3] per second—healthcare organizations only dedicate around 6%[4] of their budget to cybersecurity measures. With a limited budget and minimal attention on cybersecurity, healthcare organizations remain vulnerable to online attacks. No matter the industry or role within, it is crucial to understand cybersecurity basics to better defend individuals, businesses, and teams.

To further understand what ransomware is, how it occurs, and why you and your organization should care, Isabelle Primer, a member of Trexin's Healthcare & Life Sciences Practice, partnered with Chief Security Officer and Technology Capability Lead, Glenn Kapetansky, to break down the 'five W's and one H' of the rapidly growing issue of ransomware.

WHAT IS RANSOMWARE AND WHEN CAN AN ATTACKER STRIKE?

Ransomware is a type of malware that threatens to block access or publish an individual/organization's data unless the attacker is paid in some form. Historically, the hacker demands payment from the victim before restoring access to the hostage files. More recently, hackers threaten to publish the compromised data. Either way, these attacks often begin as phishing emails; the most recognizable are those that pique the receiver's interest even if they have details that don't seem quite right. These suspicious emails usually contain some sort of action that must be complete by the end-user – such as guiding users to open attachments or links.

In addition to email phishing, another popular attack is drive-by downloading. In this scenario, a user unknowingly visits an infected website where malware is downloaded and installed onto their device without the user's knowledge. Crypto-ransomware, a variant of malware that encrypts files, can spread through phishing emails or drive-by-downloading, but now has evolved to spread through social media and SMS messaging as well.

These are only a few of the many ways data can be held hostage through ransomware. Like viruses in the real world, as technology evolves, ransomware and malware evolve in parallel and create variants.

WHY DOES THIS HAPPEN? WHAT'S THE MOTIVE?

Over the course of 2021, cybersecurity specialists noted multiple troubling trends occurred—but ransomware continued to top the list. Albeit far from new, this issue is now more common than ever before—nearing a 151% year-over-year increase compared to 2020[5]. One driver for this continued growth is that ransomware *works.* Attackers have greater incentive and variety of successful tactics from which to choose, compared to other exploits.

Whether motivated financially or politically, attackers' incentives have grown due to the pandemic-driven shift in attention towards vulnerable industries and organizations' willingness to pay. Specifically, the healthcare, governmental, and educational sectors have been hit the hardest. In September 2020 alone, cyber criminals infiltrated and stole 9.7 million medical records[6]; Cyberattacks against K-12 schools rose 18%[7]; and 33% of all attacks on governmental bodies were ransomware[8].

In addition, an attacker's opportunity for success has also increased due to anonymity with cryptocurrency and the rise in Ransomware as a Service (RaaS). With RaaS, even inexperienced attackers can leverage world-class ready-made ransomware tools to better enable and carry out their attacks. Furthermore, during the height of the COVID-19 pandemic, cybercriminals had more free time to build or purchase these RaaS tools, thus bolstering the already high percentage of attacks.

WHO SHOULD CARE?

Considering the different flavors of ransomware above and based on the different motivations of the malicious actors and technology vectors for exploiting, the unfortunate answer is "everybody". A business might be better able (and willing) to pay, but a private individual in a position of leverage within a company can be attacked on a personal level for the cybercriminal to later gain access to their organization. Glenn Kapetansky speaks on this issue:

> **Advice from Glenn:** Don't think "just because" you're apart of a small organization or obscure industry that you're safe. In fact, in 2019, 63% of SMBs reported experiencing a data breach within the last 12 months—spending on average nearly $3 million per incident[9]. We now live in an interconnected world (consider SolarWinds and Log4j as recent examples), and "security through obscurity" is no longer a playable strategy. Your smaller organization or industry may be sideswiped by a malicious actor on the way to larger prey, or a guinea pig to practice on.

WHO CAN HELP?

The answer to this has shifted significantly, just in the past couple years.

> **Advice from Glenn**: Traditionally, if a business is approached for ransomware, the Secret Service is the appropriate agency because of its mission to protect commerce. And of course, the local police should be notified in all cases, or the FBI in cases involving national scope. So (again, traditionally) a business group connected to all three (such as InfraGard) is an efficient way to notify law enforcement.

But here's where it gets tricky. If you have a cyber insurance policy, it's recommended as a first step to contact your insurer and follow their very specific steps to coordinate the response with law enforcement and with the Ransomers, through negotiation and payment. Coverage can include the cost of restoring systems, data, access, and forensic efforts and compliance reporting.

> **Advice from Glenn:** It all adds up and you don't want to forego reimbursement by not following your insurer's procedures! However… even before contacting your insurance, you should contact your legal counsel (who you have on speed dial of course, starting right after you read this), because every email and communication has legal/compliance ramifications. There are very clear protocols for communicating with customers, vendors, and appropriate government agencies. Even internal communications need to be tightly managed, so as not to accidentally incur additional liability with imprecise language or incomplete information.

I'VE BEEN ATTACKED! HOW SHOULD I RESPOND? SHOULD I PAY THE ATTACKER?

The answer is… absolutely not. For several reasons:

- This signals that you are willing to pay ransom any time it is asked. There are several cases where companies, especially those who have an abundance of wealth, are hit repeatedly. A 2021 report by Cybereason found 80% of organizations that previously paid ransom demands confirmed they were exposed to a second attack.
- Even after paying ransom, the sheer scale of decrypting large amounts of data (e.g. Colonial Pipeline) can be slower than restoring from backups.
- Paying ransom is illegal in many jurisdictions, so can only be done under specific coordination with law enforcement (via your legal counsel and insurance agent—Remember Glenn's advice from earlier?).

Advice from Glenn: But, of course, the real-world hates absolutes. So, the answer is please, please prepare ahead of time with the proper expertise, backups, and procedures tested and lined up, so you can afford to say no.

This TIP is an expansion of a recently published interview with Glenn Kapetansky. For more information, refer to the Authority Magazine article here.

In addition, to learn more about Trexin's Cybersecurity Practice Area and how we can help you prepare for or recover from a ransomware attack, click here.

References

[1] https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542

[2] https://www.hhs.gov/sites/default/files/2021-hph-cybersecurity-forecast.pdf

[3] https://www.hipaajournal.com/ransomware-attacks-have-cost-the-healthcare-industry-at-least-157-million-since-2016/

[4] https://www.fiercehealthcare.com/tech/could-patients-be-at-risk-during-a-hospital-cyber-attack-it-depends-how-far-hackers-are

[5] https://threatpost.com/ransomware-volumes-record-highs-2021/168327/

[6] https://www.hipaajournal.com/september-2020-healthcare-data-breach-report-9-7-million-records-compromised/

[7] https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf

[8] https://securityintelligence.com/posts/threat-actors-targeted-industries-2020-finance-manufacturing-energy/

[9] https://www.thesslstore.com/blog/15-small-business-cyber-security-statistics-that-you-need-to-know/


This TIP was written by Isabelle Primer and Glenn Kapetansky. Isabelle and Glenn welcome comments and discussion on this topic and can be reached at isabelle.primer@trexin.com and glenn.kapetansky@trexin.com.