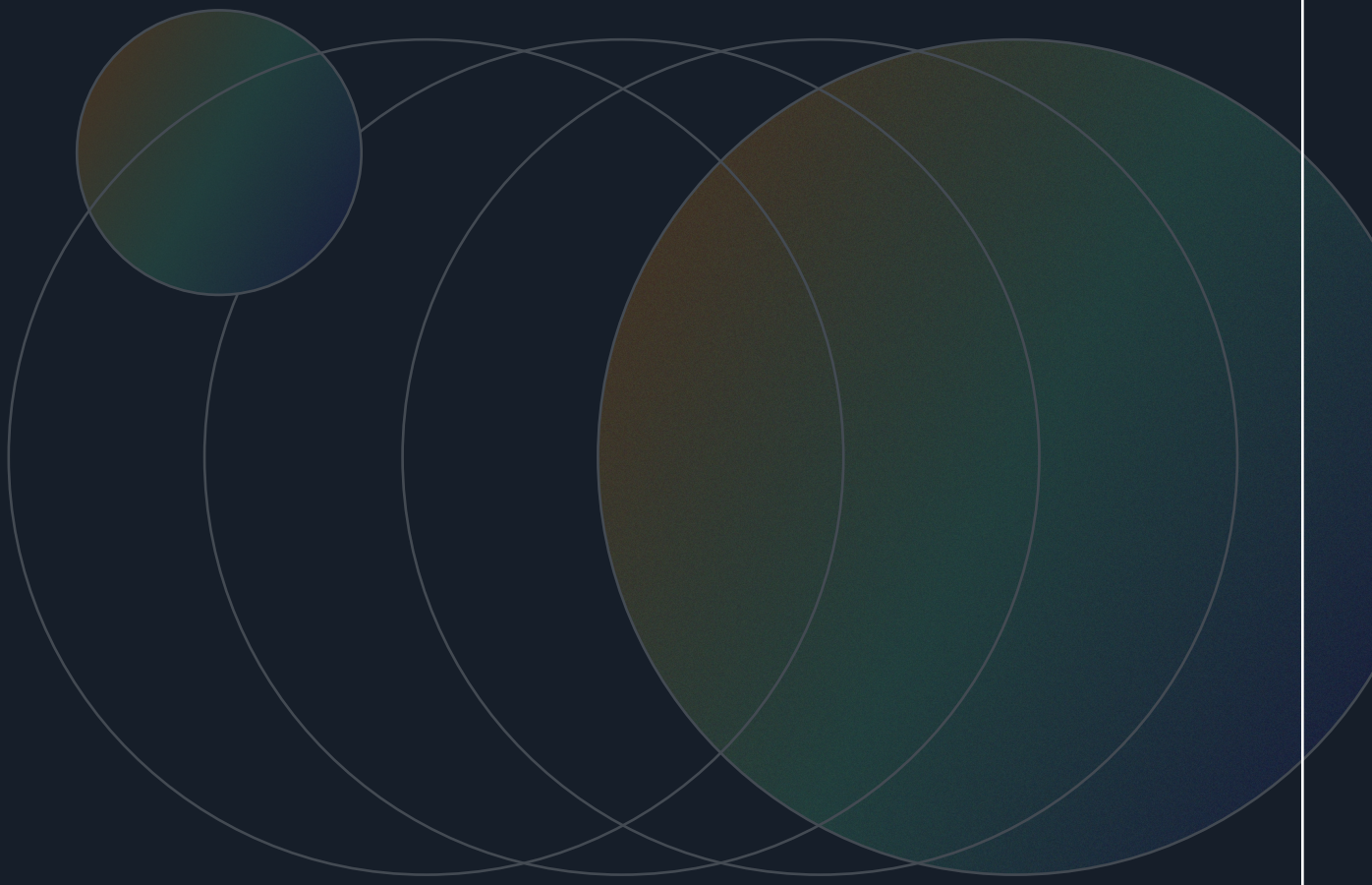
RSI | *Whitepaper*

Ransomware



858.999.3030 | info@rsisecurity.com
2022

TABLE OF CONTENTS

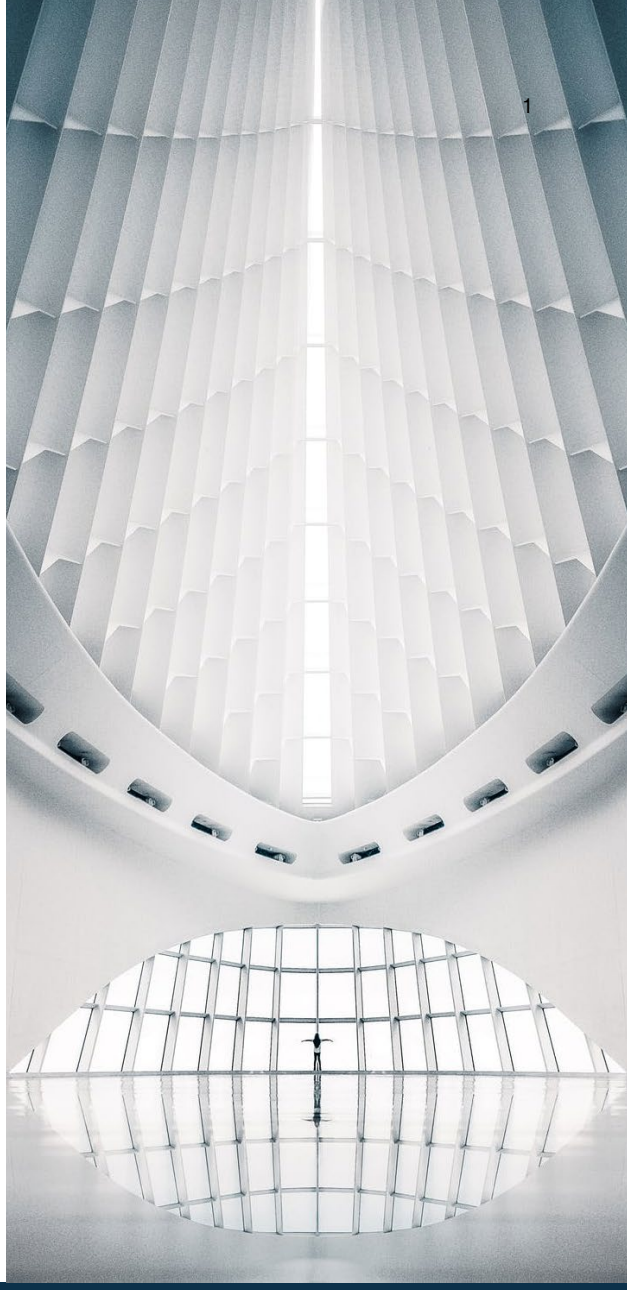
Executive Summary

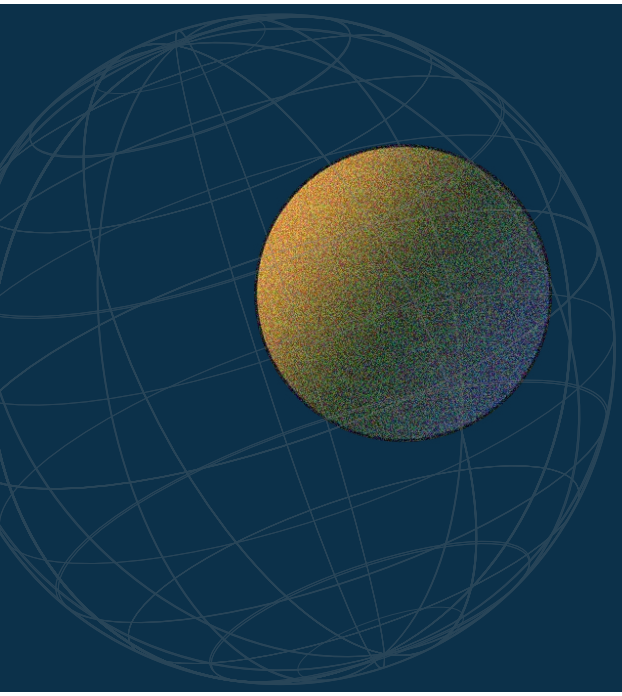
Ransomware is one of the most common, and dangerous, types of cyber attack. It refers to a type of malicious software that blocks a user from accessing their system or files once it infects their computer system. The files or system is held “hostage” until the victim performs an act, such as paying in exchange for the decryption key. To better understand what ransomware is and how to prevent it from victimizing your organization, we’ll first explore one of the earliest recorded cases of ransomware. Then, we’ll quickly dive into some basic techniques for ransomware defense that have withstood the test of time before diving more deeply into comprehensive solutions for modern ransomware attacks. Finally, we’ll look at the legal considerations surrounding ransomware and what the future holds for cybersecurity.

Ransomware’s Origins and History

Ransomware has roots going back to 1989 when diskettes containing information on AIDS were compromised. They were to be used at a conference coordinated by the World Health Organization (WHO). The attackers encrypted file names on the victims’ computers and hid directories. To decrypt them, victims had to pay $189 to a mailbox in Panama.

Over time, ransomware attacks have evolved due to changing technology in computer systems as well as payment methods. And with the advent of cryptocurrency, the proliferation of illegal online activity due to the benefits of anonymity presented by the payment system has thrust ransomware into a new phase. Businesses, individuals, governments, and other organizations have devised mechanisms to cope with the new threats. Apart from direct financial costs associated with paying a ransom, victims experience disruptions to their normal activities.





Ransomware is typically malicious software that can encrypt a person’s data before demanding a ransom or particular fee to unlock the same. According to Slayton (2018), it remains the worst form of data breach besides denial of service. Plus, it is the widely used form of a cybersecurity breach in most institutions, including the healthcare facilities like hospitals. More specifically, recent studies approximate that it accounts for 46% of all data breaches across different sectors (Corradini & Nardelli, 2018). Previous studies show that between 2015 and 2020, several institutions suffered from cyberattacks in the US and around the world (Slayton, 2018). For example, a healthcare facility in Maryland, US, suffered a major ransomware attack that paralyzed operations in the facility for a whole month (Slayton, 2018). Similarly, multiple institutions cutting across health and financial sectors suffered different attacks in many US states.

Time-Tested Mitigation Tactics

Several basic measures can be taken to protect systems from ransomware. These practices have withstood the test of time, remaining effective throughout all generations of ransomware:

- First, it is essential to use an antivirus at all times. This is the first line of defense in detecting ransomware and all other forms of malicious software.
- It is also essential to keep all computers fully patched. Configuring operating systems to allow only authorized software to run on computers prevents malware from working.
- Finally, physical controls such as restriction of personal devices from accessing a system's network reduce the probability of infecting an organizational system with ransomware.

These activities can be carried out to supplement a dedicated ransomware protection system.

Ransomware Defense Architecture

The first line of defense against ransomware consists of perimeter protections. Of these, the most essential component is a firewall. While it is a basic component of many computer systems, it is essential to ensure it has egress and ingress filtering to control what communications get in and out of the system. In this case, systems that do not need to communicate with outside servers are restricted from sending or receiving data.

Further, should ransomware get into the network, it can be restricted from sending data back to its source by a complex firewall or filtering system. Proxy server and web filter mechanisms are used to block off access to known malicious websites. A spam filter system detects emails with potential malware before it hits the client's server. Remote Access or Virtual Private Network approaches are another perimeter defense component. It is essential to limit remote access to just the necessary accounts. Two-factor authentication systems can be used to mitigate damage caused by compromised access credentials.

Anti-Ransomware Network Defense

One network defense approach is a DNS sinkhole that supplements the perimeter defense to prevent connections to certain domains by deceiving DNS requests that arise from domains in the sinkhole. Network segmentation is used to ensure that if a malware infection succeeds, it remains isolated on the network segment the infected endpoint is on. This ensures that the ransomware does not spread throughout the organization.

However, virtual machine segmentation ensures that virtual machine communications are controllable within the network security mechanisms similar to those of physical systems. Network Intrusion Detection System allows early detection of exploit attempts and alerts network administrators of possible outbreaks.

Anti-Ransomware Endpoint Defense

Endpoint protections are employed on desktop PCs and other end-user systems. One protection requires the system to have no unnecessary applications and services. Correct monitoring of administrative rights reduces the probability of attacks succeeding in computers.

Next-generation antivirus systems use machine learning and cloud-based file execution approaches to detect zero-day attacks and novel strains of ransomware. Host-Based Intrusion Detection systems detect suspicious changes to system files that are of acritical nature. These can be used to identify early outbreaks and counter certain attempted exploits. Web and Spam filtering approaches at the endpoint work to prevent access to known malicious websites and to stop the users from accessing emails from malicious senders. It is also essential to regulate support for Macros and allow access based on user needs.

NAS Servers vs. Ransomware

A denial-of-service attack, usually abbreviated as DoS, is among Protecting systems from infection via the Network-Attached Storage (NAS) server requires file permissions policies that allow access on a least-privilege basis. The risk for infection increases with scope creeps as permission enforcement is relaxed with time. Shadow copies created as point-in-time snapshots of data allow recovery to previous versions of files in case of an infection. This approach is also employed for virtual machine snapshots.

Data inventories are useful during recovery and remediation phases post-attack.

Data Backup and Ransomware

A backup and recovery plan sets out a defined recovery timeline and points for each critical asset. As such, backup policies should outline backup schedules, how data is recovered, and who is responsible for recovery. Storage snapshots on servers allow for a rollback of a storage volume to a previous state before infection. Offline backups ensure that the recovery data does not become encrypted by an attack. It is also essential to test the backup and recovery systems to gauge the potential impacts of an attack on the entire system's infrastructure.

Legal Considerations for Ransomware

At the moment, there is no federal or state law requiring or prohibiting ransom payment to an attacker. Responses are discretionary, but best practices typically dictate avoiding a payment.

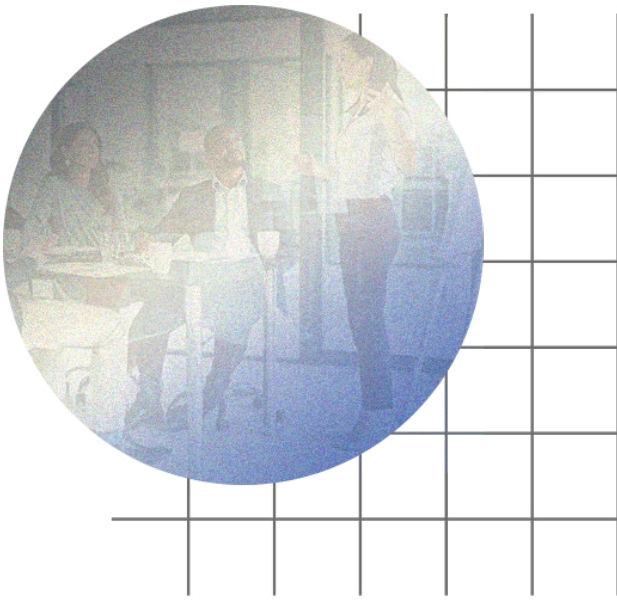
Nevertheless, a victim has to consider various laws when paying a ransom. These include the Trading with the Enemy Act and the International Emergency Economic Powers Act, which give the US President final say on all economic payments to declared enemies in wartime and under other vectors of duress, respectively. The Electronic Communications Privacy Act and the Computer Fraud and Abuse act are other federal laws used to handle ransomware cases.

Regulations Impacting Ransomware

Government entities such as the Federal Bureau of investigation have discouraged ransom payments in the case of attacks. This arises from the implications of paying ransoms to possible terrorist groups, criminal organizations, and other criminal entities.

The Office of Foreign Assets Control holds that companies may risk violating its regulations by paying ransoms. This is especially the case if the perpetrator of an attack is in the specially designated nationals or blocked persons lists. These include entities from countries such as Syria, North Korea, and Iran. The HHS's Office for Civil Rights requires health care entities to maximize their compliance programs and employ computer forensics to find out the cause and nature of an attack, then report on these to all impacted parties, as appropriate. State laws generally discourage ransomware payments as they fuel the vicious cycle of ransomware.

Ransomware, Crypto, and CCSS



Cryptocurrency has risen in prominence over the past decade from a fringe hobby to a force impacting every sector of the economy. One area in which crypto's impact has been especially relevant is cybersecurity, and specifically ransomware and all related extortion schemes.

Because the blockchain can offer near-complete anonymity, hackers tend to request ransom payments in cryptocurrencies such as Bitcoin. A joint task force of US governmental agencies has estimated that over $140 million in Bitcoin was paid out to ransomware scams from 2013 to 2019. That figure encompasses transactions large and small, as forensics can often determine that a crypto payment is a ransom, but not to whom the ransom payment is being paid. Crypto ransoms and aggregate totals from targeted schemes can be quite large. In one 2021 case, the US Department of Justice seized $2.3 million in Bitcoins paid to the hacker group Darkside.

An organization does not need to deal in crypto to be targeted in this kind of attack. However, one way to prepare for a crypto-related ransomware scheme is to ramp up crypto safety, whether or not the organization in questions processes cryptocurrency. To that effect, all organizations should target Cryptocurrency Security Standard (CCSS) implementation. Cybersecurity safeguards required for Level I, II, and III compliance will make a ransomware attack less likely; they also ensure that secure payment, in crypto, is easier to manage if that solution is deemed appropriate. All future crypto transactions will also be significantly safer.

What the Future Will Look Like

Given the complexity of the legal framework that victims must navigate to comply with laws when paying a ransom, the best approach is to have a robust and dynamic protection system that reduces the likelihood of a ransomware attack actualizing. Ransomware attacks result in:

- Loss of productivity
- Business disruption and downtime
- Destruction of crucial information
- Damage to hostage systems
- Loss of reputation for the victim

What the Future Will Look Like

Thus, it is essential to have protection systems with capabilities such as file server auditing, file analysis, data risk assessment, cloud protection and data leak prevention. Furthermore, having a recovery plan remains a vital component of the protection framework. This includes backups in online and offline systems and regular system analysis to identify potential weaknesses. A comprehensive ransomware security framework of the future will have several tasks:

- First, it is essential to use an antivirus at all times. This is the first line of defense in detecting ransomware and all other forms of malicious software.
- It is also essential to keep all computers fully patched. Configuring operating systems to allow only authorized software to run on computers prevents malware from working.
- Finally, physical controls such as restriction of personal devices from accessing a system's network reduce the probability of infecting an organizational system with ransomware.

Overall, responding to an attack requires response planning, communications, mitigation, and improvement planning.

Key Takeaways:

Ransomware has been a thorn in the side of cybersecurity specialists since the dawn of modern computing. It's remained essentially the same since its inception, adapting to new technologies and using contemporary trends (like cryptocurrency) to exploit unwitting businesses more effectively. However, the best defenses against ransomware have also remained relatively unchanged. Organizations need to build ourt robust defense architecture, including perimeter, network, NAS server, and backup protocols. They should also ensure that these systems comply with applicable ransomware and cryptography standards and regulations. Resisting evolving threats of ransomware in the future will require scalable, comprehensive visibility and reporting infrastructure, ideally with the help of a managed security service provider.

REFERENCES

Ronny Richardson and Max North, "Ransomware: Evolution, Mitigation, and Prevention," International Management Review 13 no.1 (2017), https://digitalcommons.kennesaw.edu/facpubs/4276/

Nikolai Hampton and Zubair Baig, "Ransomware: Emergence of the Cyber-Extortion Menace," Australian Information Security Management Conference (2015), https://doi.org/10.4225/75/57b69aa9d938b

Manveer Patyal et al., "Multi-Layered Defense Architecture Against Ransomware," International Journal of Business & Cyber Security 1 no. 2 (2017), https://www.researchgate.net/publication/315471509

Alex Fagioli, "Zero-Day Recovery: The Key to Mitigating the Ransomware Threat," Computer Fraud & Security, 2019 no.1, https://www.magonlinelibrary.com/doi/abs/10.1016/S1361-3723%2819%2930006-5

Jammie Smith, "Ransomware Incident Response for Law Enforcement" (thesis, Utica College, 2017), https://www.proquest.com/openview/316198b643eb477647d0e4b4e59439fa/1.pdf

Mario Conti et al., "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective," Computers & Security 79 (2018), https://arxiv.org/pdf/1804.01341.pdf

FBI, "The National Cyber Investigative Joint Task Force Releases Ransomware Fact Sheet," FBI News, https://www.fbi.gov/news/pressrel/press-releases/the-national-cyber-investigative-joint-task-force-releases-ransomware-fact-sheet

DOJ, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," DOJ Office of Publice Affairs (2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

Shaila Sharmeen et al., "Avoiding Future Digital Extortion Through Robust Protection Against Ransomware Threats Using Deep Learning Based Adaptive Approaches," IEEE Access 8 (2020), https://ieeexplore.ieee.org/document/8976152