PONDURANCE

3 Ways to Reduce Ransomware Attacks

pondurance.com

Introduction

Ransomware attacks have been around for decades, affecting organizations of all sizes and threatening the U.S. economy, commerce, and multiple industries. Ransomware gangs are becoming increasingly relentless in their tactics and have started encrypting backup files before encrypting live systems, making it even harder for organizations to avoid paying the ransom. The cost of ransomware attacks alone is expected to reach upwards of $20 billion in 2021.[1] It was recently reported that cyberattacks rose 400% since the start of the COVID-19 pandemic.[2] Opportunistic ransomware gangs seized on this opportunity and doubled down on their attacks against organizations during and after COVID-19. In this eBook, we will take a look at ways to identify and protect against ransomware.

What Is Ransomware?

Ransomware is a type of malware (malicious software) that gains access to files or systems and blocks users' access to those files and systems. Once malware is on a device, the malware is designed to encrypt files (encode and lock files with an encryption key) on a device, rendering any files and the systems that rely on them unusable.

Attackers then demand ransom in exchange for the decryption key that unlocks the files or devices. Ransomware groups often target and threaten to sell or leak exfiltrated data or authentication information if they do not receive a ransom payment. Businesses used to be able to rely on backups to restore their networks and files, but recently attackers have been encrypting the backup before the actual system.

How Ransomware Attacks Succeed

Carrying out a successful ransomware attack involves a variety of moving pieces. Ransomware gangs leverage botnets to carry out their attacks, while others buy lists of compromised credentials used for credential stuffing. Rogue developers sell ransomware software or direct network access on the dark web, making it easier to launch larger-scale ransomware attacks.

The best defense against ransomware is first to understand how attackers can access your organization's infrastructure. Some common trends we see attackers leverage include:

- **COVID-19** forced digitization within multiple industries, putting additional strain on IT resources as organizations implemented work-from-home policies. In addition, the Federal Trade Commission logged more than 517,500 consumer-related scams.[3] Of these scams, phishing and smishing messages plagued the internet with headlines relating to COVID-19 vaccines, federal stimulus payments, and more. If opened on work machines, phishing attacks could contribute to a ransomware infection, quickly spreading through a company's network.
- **Limited funding** is a leading factor in organizations being understaffed and underfunded when it comes to cybersecurity. As new techniques emerge, organizations need to invest in people, processes, and technology.
- **Ransomware-as-a-Service** (Raas) is a growing business model for rogue developers. Attackers buy or lease malware from these developers, and the developers get a portion of the ransom payment. RaaS allows low-level attackers to launch widespread ransomware campaigns.
- **Phishing** is frequently a gateway to ransomware. This type of attack can lead to an end-user clicking on a malicious link or can redirect to a phishing site that downloads malware to the user's computer.

Industries Most Affected By Ransomware Attacks

Healthcare organizations of all sizes continue to be prime targets for ransomware attacks, primarily due to the amount of patient data they process, outdated systems and devices, and lack of security awareness training. In 2020, ransomware attacks cost the healthcare industry $20.8 billion in downtime and affected 18 million patient records.[4] Ransomware gangs and their extensive network of accomplices pose multiple risks to healthcare organizations, including: 1) impact of patient care and safety; 2) disruption of business operations; and 3) disclosure of sensitive information.

Manufacturing is an industry that attracts ransomware attacks, and the financial impact is not the only effect of an attack. The ransomware attacks on the Colonial Pipeline and JBS meatpacking company demonstrate that attackers can negatively impact critical resources that U.S. citizens rely on to survive. In addition, the risk of losing intellectual property can affect business relationships.

Operational disruptions can significantly impact suppliers and create a chain reaction in supply chain penalties starting with contractual procurement. As downstream clients rely on manufacturers, downtime affects more than financial losses; it negatively impacts the relationships between client and customer. It is critical to have 24/7 visibility and security analysts to detect anomalous activity before attackers disrupt operations. According to resources, it can take 302 days to identify and contain a data breach for manufacturers.[5]

Education K-12 and Universities were no strangers to ransomware attacks. The FBI shared that 57% of cyberattacks reported were ransomware attacks that involved K-12 schools.[6] A group of **higher education institutions** confirmed they were victims of a data breach caused by a security flaw found within Accellion's file transfer software.[7] Supply chain attacks that exploit third-party software are becoming more common as attackers have increasing success gaining unauthorized access.

3 Ways To Protect Against Ransomware Attacks

Ransomware attackers are human, and they prey on human error to gain access to sensitive information. Educating your employees and implementing cyber hygiene practices are key to reducing human error, but investing in the right cybersecurity tools, hiring highly trained cybersecurity analysts, and implementing 24/7 monitoring will be key to mitigating ransomware attacks. Here are the top three ways you can combine people, processes, and technology to protect your business against ransomware attacks:

Identifying and managing vulnerabilities is a proactive approach to understanding your organization's risk. Analyzing your existing network, infrastructure, and digital landscape can help determine which gaps in your security program need to be filled. A vulnerability assessment and penetration test will generate a comprehensive report that will tell your security team where to focus its efforts to reduce ransomware attacks and other vulnerabilities that need to be patched.

360-degree monitoring of networks and devices, logs, and cloud infrastructure is key to eliminating blind spots. Logging alone is not enough. People, processes, and technology continue to be vital resources when developing a comprehensive cyberdefense program, and a holistic managed detection and response (MDR) service can help organizations achieve this much needed cybersecurity maturity. It's critical to leverage a 24/7 security operations center (SOC) to detect and mitigate threats in real-time. Implementing endpoint detection and response can provide more visibility into all endpoints such as laptops, computers, and other devices that are being used on the network.

Incident response planning is vital to responding to ransomware threats, minimizing losses, and preventing future attacks. An incident response plan should include responders, handlers, and forensic and malware specialists to scope, investigate, and orchestrate activities after an incident.

A comprehensive incident response plan should cover and include:

- **Identification** - Identify and detect an incident as soon as possible.
- **Containment** - Stop the incident and reduce the impact on corporate and consumer information, as well as business operations.
- **Eradication** - Eliminate the threat and prevent a recurrence.
- **Recovery** - Return to normal operations and conduct a post-breach investigation.

Conclusion

Ransomware affects more than financial loss. These attacks can affect business operations, intellectual property, personal identifiable information, and most importantly, your business's reputation. As budgets slowly increase, organizations turn to outsourced cybersecurity to help lessen the burden of stopping ransomware attacks. Organizations need to invest in a SOC that offers 24/7 monitoring and an MDR service that acts as an extension of its existing security team with guided recommendations on responding to a breach.

The odds of organizations recovering from a successful ransomware attack without paying a sizeable ransom are slim to none these days. It is critical to understand where your organization is most at risk to identify common patterns that lead to paralyzing ransomware attacks. Ransomware gangs want to get paid for their efforts, and their tactics are only getting more sophisticated.

PONDURANCE

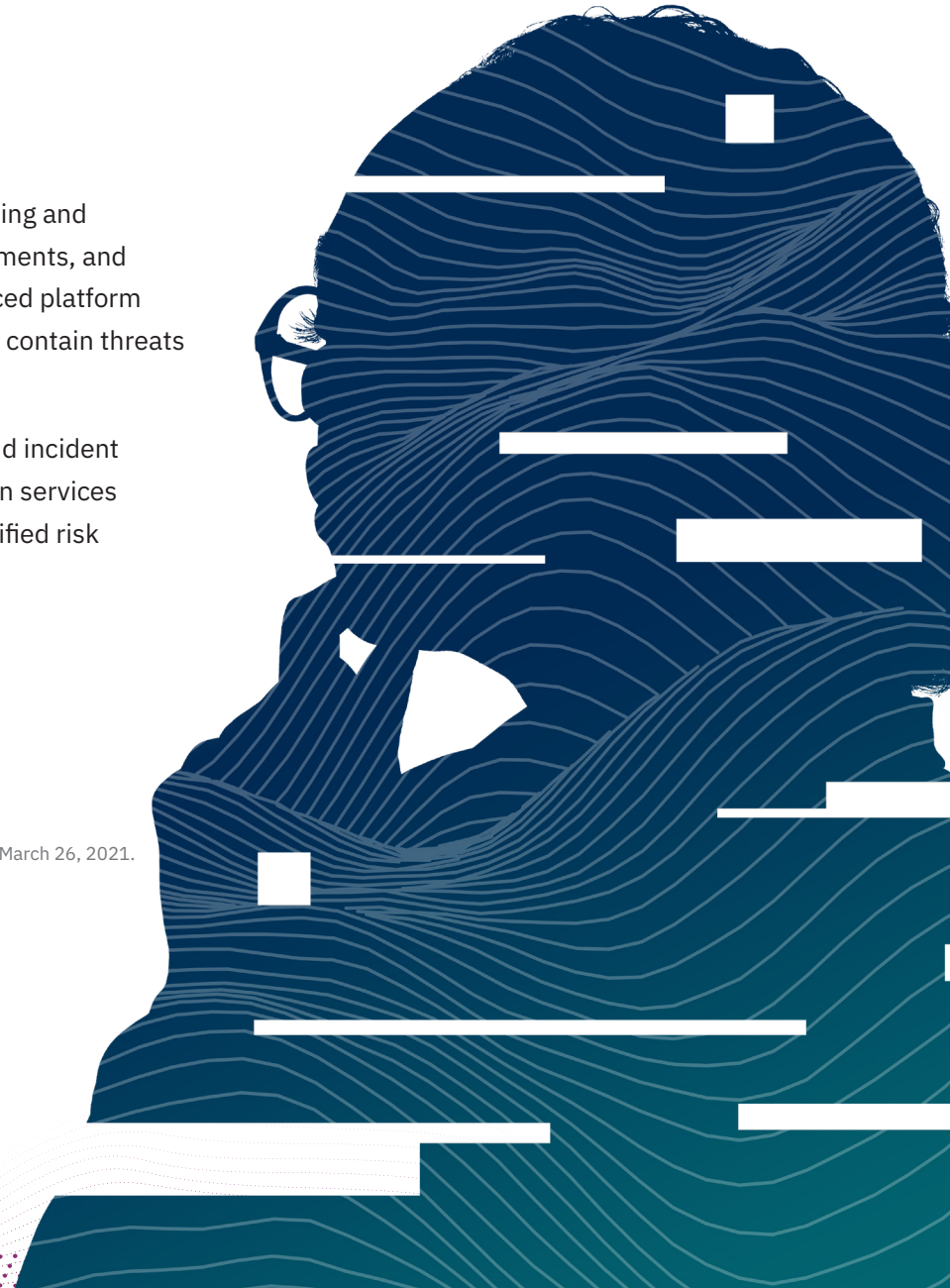
PONDURANCE

About Pondurance

Pondurance delivers world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.



1. Why Ransomware Costs Businesses Much More Than Money, Forbes, April 30 , 2021.
2. FBI Sees Spike In Cyber Crime Reports During Coronavirus Pandemic, The Hill, April 16, 2021.
3. Beware of Robocalls, Texts, and Emails Promising COVID-19 Cures or Stimulus Payments, AARP, June 15, 2021
4. 2020 offered a 'perfect storm' for cybercriminals with ransomware attacks costing the industry $21B, Fierce Healthcare, March 26, 2021.
5. 2020 Cost Of A Data Breach Report, IBM. 2021.
6. FBI Warns of Cyberattacks to Distance Learning, January 4, 2021, ABC News
7. Ransomware Targets Universities from California to Maryland in 2021, Pondurance, April 12, 2021.

pondurance.com

500 N. MERIDIAN ST., STE. 500
INDIANAPOLIS, IN 46204