FORTINET

POINT OF VIEW

Stop Ransomware With Ongoing Preparation

Executive Summary

Reports of successful ransomware breaches continue to rise at an alarming rate. New malware strains and advanced extortion techniques have made an impact on businesses of all sizes and in every industry sector. As organizations face the reality that ransomware could very well reach their enterprises, many are currently ill-prepared and under-resourced for the latest attacks in terms of people, processes, and technologies.

Ransomware Responses Are Falling Short

It seems every day, incident response (IR) teams heed the call of another enterprise hit with ransomware. Understanding the lessons from these casualties of ransomware, and the commonalities across them, can provide insight into what to avoid, what to improve, and inform an organization's security strategy.

"The fastest ransomware can encrypt roughly 100,000 files in just four minutes and nine seconds."[1]

IR teams provide many critical services to ransomware victims. In this work, they see several recurring issues with regard to lapses in cybersecurity best practices. A common problem is the lack of a ransomware playbook. When there are playbooks, often the team hasn't exercised against them recently. Maybe there's been turnover, and the newer members of the team are unaware. Whatever the reason, the processes laid out in the playbook aren't followed, and the playbook may as well not exist.

When a ransomware attack is successful, things can become chaotic without the appropriate strategies and structures in place. Multiple roles and job functions across the organization need to be involved in responding to a breach. This may include the chief information officer (CIO); the sales organization to talk to customers if any private data is compromised; the chief financial officer (CFO) to address the market if it's a publicly traded company; and the chief marketing officer (CMO) to formulate a public-relations plan.

Nobody wants to inform the executive team that an adversary has infiltrated the company, but the extent of the impact on systems or what data may have been encrypted or exfiltrated is unknown. Mitigating the damages of a ransomware attack is an ongoing cycle of preparation. This is where many organizations are surrendering a huge advantage to their cyber adversaries.

Targeting Under-resourced Areas

To counter ransomware attacks, security leaders need better preparation and resources. Specifically, many organizations are currently lacking in the following areas:

- **People.** Organizations need to do a better job of providing ongoing and updated employee awareness to detect malicious emails and network behavior. They also often fall short of providing 24/7 security coverage and the skills to monitor, review, and act on events or suspicious behavior.

- **Processes.** Incorrect product configurations present opportunities for ransomware attacks. Many organizations also don't have appropriate logging capabilities for suspicious or malicious behavior, nor do they manage access according to the "least privilege" principle—where a subject should be given only those privileges needed for it to complete its task.[2]
- **Technology.** Organizations need appropriate protections on all devices, not just those deemed critical. Many businesses lack endpoint detection and response (EDR) technology that can learn and prevent malicious behaviors. These include ransomware-related file downloads, command-and-control attacks, and lateral (east-west) threat movement. EDR can be used by IR teams to play back an attack and take immediate action to terminate processes, block execution, and isolate machines at the outset of investigation. Organizations may also benefit from additional security controls that block known IPs, file hashes, and other identifiable characteristics.

> "Preparing for ransomware with a tabletop exercise can identify potential gaps and ensure the right process is in place to mitigate and recover from a potential attack."[3]

Actions Needed for Greater Resilience

While governments, law enforcement, and regulators continue to grapple with ransomware issues, companies need to ensure they remain resilient by focusing on ransomware prevention, preparation, response, and recovery strategies.[4]

Prepare. Organizations need to use proactive assessment tools such as ransomware assessments and tabletop exercises to help ensure that their ransomware playbooks are up to date. They also need an engaging security awareness training program that regularly educates employees across the organization based on realistic scenarios. To ensure that security teams are regularly refreshed on the latest ransomware best practices, organizations should also invest in professional cybersecurity training and certification programs for security staff.

Maintain. To protect an enterprise 24/7, consider outsourcing as a short-term solution or as part of an overall long-term strategy. A security operations center-as-a-service (SOCaaS) or managed detection and response (MDR) service can provide this kind of 24/7 expert coverage.

Respond. Having an experienced IR team on retainer can be an additional safeguard in the event of a ransomware attack. These dedicated experts can help stop further damage in a live attack situation and also help evaluate security program gaps as part of their final report.

Getting in Front of Evolving Threats

To stay ahead of escalating ransomware risks, enterprises must revisit evolving best practices through regular security assessments and tabletop exercises. Organizations of all sizes and industries have to do more to maintain employee awareness as well as the latest technologies for monitoring, detecting, and analyzing threats at all times. Updated playbooks and well-tested IR plans can also help the broader organization respond to incidents swiftly and shield the company from compounding risks. In the event of an attack, involving an expert IR team can help mitigate damages, restore operations, and guide remediation efforts.

[1] Nathaniel Mott, "Ransomware Can Encrypt 100,000 Files in Minutes," PC Mag, March 26, 2022.

[2] "Least Privilege," CISA, accessed August 5, 2022.

[3] Chuck Brooks, "Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know," Forbes, June 3, 2022.

[4] "Ransomware prevention: How organizations can fight back," McKinsey & Company, February 14, 2022.

www.fortinet.com

August 24, 2022 9:07 AM

1689014-0-0-EN