DivIHN

In Service, with
Excellence and Grace

Ransomware Threat Management

March 2020

Contents

Introduction

Ransomware continues to be a real threat to business operations across all industries, no organization is safe from this threat. The combination of widely available exploit kits on the dark web, limited resources and skills needed to execute attacks, and potential financial gain makes ransomware attractive to bad actors.

The intent of this guidance is to provide insight into the ransomware threat and the actions that should be taken to reduce it. Below are a few statistics[1] to frame the ransomware threat. These statistics aren't based on surveys; instead, they are derived using data collected from ransomware incidents Coveware has responded to.

Interesting Ransomware Statistics

- Dharma, Ryuk, and GrandCrab are the most common ransomware types. The type of ransomware used in attacks continually shifts. Sodinokibi was not used in Q1 2019 but it surfaced in Q3 2019 targeting several Texas cities.
- Remote Desktop Protocol (RDP) (64%), Phishing (30%), and software vulnerabilities (6%) are the attack vectors used by the ransomware types.
- Of those who decided to pay ransom, 96% received the decryption tools. The type of ransomware is an indicator of success rate.
- The decryption process can result in data loss – 10-20% on the high end. Files and file systems can be damaged during the encryption process. Success is determined by the ransomware variant used.
- Downtime averages 5-10 times the cost of the ransom amount.
- The average time to recover from a ransomware incident is 7.3 days.
- Cloud computing providers (supply chain) will be increasingly targeted. The iNSYNQ incident is an example of what may become more of a challenge in the future.

Ransom payment is a much talked about issue. The 96% success rate (see above) in receipt of decryption tools doesn't imply ransom payment should be pursued as this decision is different for each organization. Some organizations are adamant that ransom will not be paid, and this is viable if you have the ability to recover. On the other hand, if recovery will take two weeks and the business is losing $10 mil in revenue daily, ransom payment may be a consideration. (DivIHN is not advocating either approach.) Before paying ransom consider the ransomware type to measure the probability of success. If you chose this path, don't go it alone when negotiating ransom payment, engage a partner that's experienced in navigating ransomware incident response.

[1] Source of ransomware statistics: Coveware

Ransomware Threat Management

A holistic approach is needed to effectively manage the ransomware threat and protect company assets. Holistic ransomware threat management requires a focus on four key areas: inventory, protection, monitoring/detection, and response. You may recognize these categories from the NIST Cybersecurity Framework. The considerations below represent the basics that apply to most technology environments. Where to start and what level of controls to implement depends on the maturity of the organization and risk to the business, respectively.

Ransomware Threat Management Considerations

Inventory

Establish an understanding of what systems/applications are deployed and what's critical to the business (e.g., revenue generation). This information is used to enable effective protection of assets.

- *Critical Systems and Data* – Identify critical systems and important data needed to maintain business operations. Critical systems and associated data must be given priority when mitigating ransomware risk (see Protection and Backups). Focus on what's important to the business.
- *Asset Inventory* – For many organizations establishing and maintaining a full system inventory is a challenge. Start with a technology inventory of critical systems and hosts exposed to the internet.

Protection

Deploy the right to security controls to protect data and technology.

- *Awareness Training* – Educating employees to ensure they don't fall victim to phishing attacks is critical to managing ransomware threats. Provide ongoing training and awareness to keep this community informed. Google's Jigsaw project provides a great phishing awareness tool.
- *Anti-virus Software* – Endpoints and servers must be protected using anti-virus software. The effectiveness of signature-based detection has been debated for some time but remains a staple in endpoint protection. However, it can be complemented by next generation solutions such as Cybereason, Crowdstrike, or Carbon Black to enhance protection in this constantly evolving threat landscape.
- *RDP Services* – As Coveware identified, RDP is a commonly used attack vector. Leading practices should be used to secure these services – restrict network access (change listening ports and restrict IP addresses), manage administrative access, implement two-factor authentication (avoid SMS), and consider implementing RDP gateways. Reference this article for additional insight.

- *Vulnerability Management* – Ransomware often takes advantage of known vulnerabilities. Patch critical and high vulnerabilities in a timely manner. Organizations developing custom software must implement secure development practices and perform security testing throughout the development process – static application security testing (SAST), manual code reviews, dynamic application security testing (DAST), and interactive application security testing (IAST).
- *Restrict Privileges* – Limit administrative access on end points to restrict software installation. In addition to restricting privileges consider whitelisting applications. These actions can prevent the execution of malware. However, implementation can be controversial due to the impact on user productivity. Understand the business and user needs, and proceed as appropriate. At a minimum, these countermeasures should be implemented on community end points and operational (e.g., shop floor) workstations.
- *Isolation* – Segregate systems to restrict lateral movement of attacks. This ranges from segregating critical systems to removing unnecessary file system mounts to managing privileged access as described in restricting privileges. Isolating systems can reduce ransomware damage by restricting lateral movement.

Monitoring/Detection

Detect of threats and attacks early in the kill chain.

- *Threat Detection* – Network and host-based intrusion detection should be performed. Most threat detection systems use Indicators of Compromise (IOCs) to detect threats but systems that use Tactics, Techniques, and Procedures (TTPs) are preferred due to increased accuracy. This capability is needed to thwart ransomware attacks before they infect the environment.
- *Dark Web Monitoring* – Dark web monitoring can be a controversial topic and not appropriate for all organizations. High value targets such as government institutions, hospitals, and financial companies should monitor the dark web to understand the ransomware market and evolving TTPs. At a minimum, subscribe to a threat intelligence feed to receive actionable information on known threats. Refer to cyberthreat for a listing of threat intelligence feeds. Ransomware attacks are unpredictable. This increases the importance of threat intelligence to understand and prepare for shifts.

Response

Establish a response in the event systems and data are compromised.

- *Incident Response* – A strong response plan is needed to minimize business disruption. In addition to addressing the basics (identification, containment, eradication, and recovery) a clear process to take a decision on ransom payment is required. Identify a partner to help you navigate a ransomware incident. The partner should be experienced with ransomware negotiations, forensics, and recovery.
- *Resiliency/Recovery/DR* – Ensure the appropriate recovery capability is in place. This includes validating recovery timing meets current business recovery time objectives (RTOs). At a minimum, ensure backups images are isolated and can't be encrypted along with

other data sets should ransomware hit. Additionally, ensure the backups provide for full system state recovery.

Below are additional resources that can be used to manage the ransomware threat.

- *No More Ransom* – No More Ransom is a good source to reference for ransomware response. The resource provides tools to decrypt well-known ransomware. Their objective is to enable decryption of data without paying bad actors.
- ID Ransomware – The tool can be used to identify the type of ransomware used in the attack.

Conclusion

Taking action in the highlighted areas will greatly reduce the risk of ransomware. If infection should occur, the business impact will be diminished by effective detection and response. Remain vigilant as ransomware is real threat that must be understood and mitigated.