HicksZilla Security Consulting Group

Cyber Threat Analysis Report: Ransomware

Date: 15 June 2023

Executive Summary:

This report presents a detailed analysis of ransomware, a malicious software that encrypts files and demands ransom payments to decrypt. The analysis covers the technical aspects of ransomware, including attack vectors, notable ransomware families, malware analysis, attribution challenges, and estimated monetary losses. The information in this report is based on publicly available data.

Introduction:

Ransomware attacks pose a significant threat to organizations worldwide, causing severe financial losses, operational disruptions, and reputational damage. Understanding the technical intricacies and strategies employed by ransomware actors is crucial for developing robust cybersecurity defenses and effective incident response plans.

Ransomware Overview:

Ransomware is a type of malware that actively encrypts files, rendering them inaccessible until a ransom payment is made. Cybercriminals gain unauthorized access to victim systems through various attack vectors, such as phishing emails, exploit kits, or compromised systems. Once the system is infected, the ransomware employs strong encryption algorithms to lock the victim's files, while simultaneously displaying a ransom note with instructions for payment.

Common Attack Vectors:

- Phishing Emails: Cybercriminals skillfully employ social engineering techniques to deceive users into clicking on malicious links or opening infected attachments.
- Exploit Kits: Ransomware takes advantage of known vulnerabilities in software or operating systems to exploit and gain unauthorized access to systems.
- Remote Desktop Protocol (RDP) Attacks: Attackers specifically target systems with exposed RDP services, attempting to gain illicit access.

- Malicious Downloads: Ransomware is distributed through malicious websites or compromised legitimate websites, exploiting user trust to trick them into unknowingly downloading infected files.

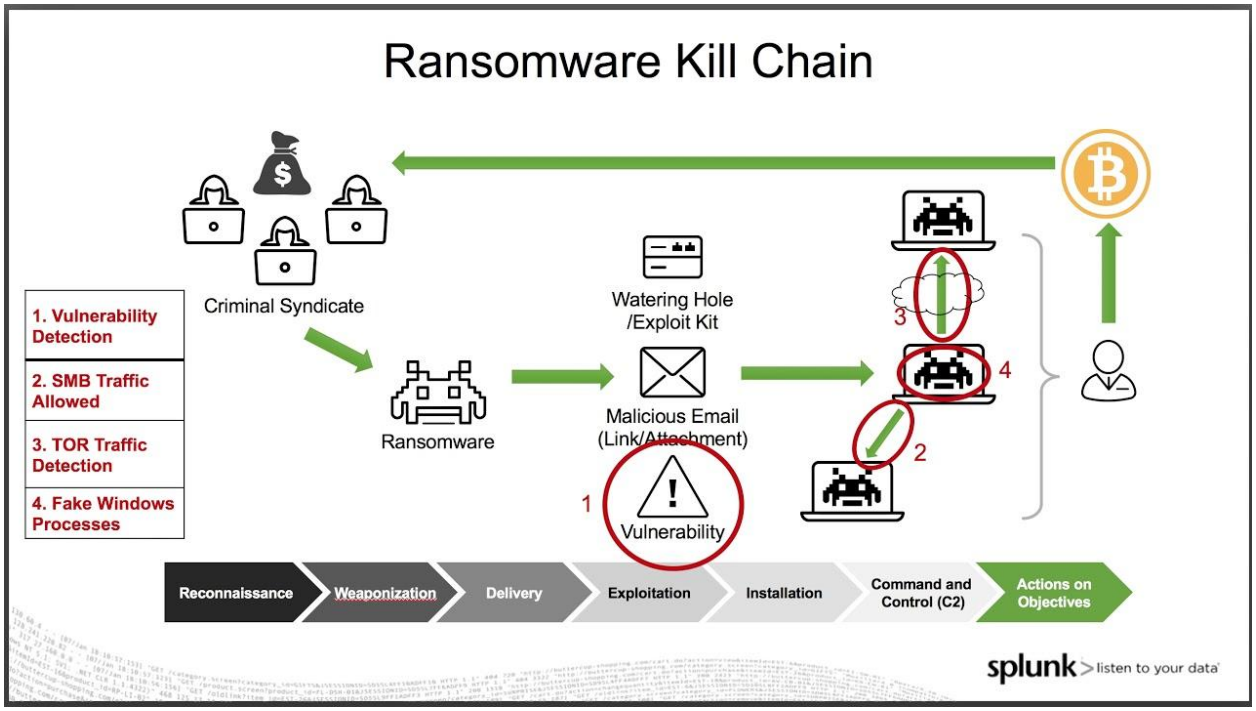

Fig 1 - Ransomware Killchain

Notable Ransomware Families and Variants:

- WannaCry (CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147): WannaCry exploited vulnerabilities in the Microsoft Windows SMB protocol, causing widespread impact across thousands of systems globally.
- Ryuk (CVE-2018-8453, CVE-2019-1069): This ransomware strain is often associated with the Lazarus Group, an advanced persistent threat (APT) group allegedly linked to North Korea.
- GandCrab (CVE-2019-3396, CVE-2017-10271): Known for its ransomware-as-a-service (RaaS) model, GandCrab enabled multiple threat actors to conduct their own ransomware campaigns.
- REvil/Sodinokibi (CVE-2018-8453): Infamous for targeting high-profile victims and demanding exorbitant ransom payments.

Attribution of Advanced Persistent Threats (APTs):

- The "WannaCry" malware is primarily associated with the Lazarus Group, an Advanced Persistent Threat (APT) group that is allegedly linked to North Korea. The Lazarus

Group is known for conducting sophisticated cyberattacks with political and financial motivations.

- The "Ryuk" malware is associated with an APT group known as Wizard Spider. This APT is a highly organized cybercriminal group believed to operate out of Eastern Europe, with some potential links to Russia.
- The exact attribution of GandCrab to a specific Advanced Persistent Threat (APT) group remains uncertain. Unlike many other ransomware strains, GandCrab was distributed through a ransomware-as-a-service (RaaS) model, allowing multiple threat actors to use the ransomware for their own campaigns.
- The attribution of REvil/Sodinokibi to a specific APT group or individuals is still a subject of ongoing investigation and analysis. The ransomware has been linked to a cybercriminal group known by various names, including Gold Southfield, Sodin, and Pinchy Spider. This cybercriminal group operates as a ransomware-as-a-service (RaaS) model, providing the REvil/Sodinokibi ransomware to other threat actors.

Malware Analysis:

Mitigating the threat of ransomware attacks requires the utilization of various malware signatures, which act as identifiers for specific ransomware variants. These signatures can be integrated into antivirus and intrusion detection systems, enabling real-time scanning and alerting for ransomware detection. By incorporating malware signatures into security measures and staying updated with the latest signatures, organizations can effectively defend against ransomware and prevent the encryption of critical files.

WannaCry		
Hashes	MD5	0A73291D3AF071E9E3A147BFA7DDB8B6
	SHA1	EFE992B14B07B9BBBC6D5C63D632D05CA142472F
	SHA256	24D004A104D4D54034DBC530D80AC77C6BB5D0AFC5FE7FABAC5FAC4A85C1BBC3

IDS/IPS Signatures	YARA Rule	rule WannaCry_Ransomware { meta: description = "Yara rule for WannaCry ransomware" strings: $string1 = { 45 6E 63 72 79 70 74 65 64 20 46 69 6C 65 3A 20 } $string2 = { 57 61 6E 6E 61 43 72 79 70 74 6F 72 3A 20 } condition: any of them }
	Snort Signature	alert tcp any any -> any any (msg:"WannaCry Ransomware Activity"; content:"|09|O|0A|O|0A|G|0A|I|0A|Q|0A|Y|0A|O|0A|D|0A|"; flow:to_server; sid:10000001;)
	Suricata Signature	alert tcp any any -> any any (msg:"WannaCry Ransomware Activity"; content:"|09|O|0A|O|0A|G|0A|I|0A|Q|0A|Y|0A|O|0A|D|0A|"; flow:to_server; sid:10000001;)
Antivirus Signatures	Symantec	Ransom.Wannacr
	McAfee	Ransom-WannaCry!055CC374D03A
	Avast	Win32:WanaCryptor-D

Ryuk		
Hashes	MD5	2e9a8df2dc0e98b7110fdd2af29d50a6
	SHA1	4e7be37f52f2aa2e27206d8e4b509de8fda292f7
	SHA256	811E0882F1AA5D4BEEB9253FA795F8264D525A12A388B15BB33E202E71E8D64F
IDS/IPS Signatures	YARA Rule	rule Ryuk_Ransomware { meta: description = "Yara rule for Ryuk ransomware" strings: $string1 = "ryuk.exe" $string2 = "ryukReadMe.html" condition: all of them }
	Snort Signature	alert tcp any any -> any any (msg:"Ryuk Ransomware Activity"; content:"ryuk.exe"; content:"ryukReadMe.html"; sid:10000002;)
	Suricata Signature	alert tcp any any -> any any (msg:"Ryuk Ransomware Activity"; content:"ryuk.exe"; content:"ryukReadMe.html"; sid:10000002;)
Antivirus Signatures	Symantec	Ransom.Ryuk

	McAfee	Ransom-Ryuk!2E9A8DF2DC0E
	Avast	Win32:Ryuk-ACR

GandCrab		
Hashes	MD5	A57EE189D5D8C6342A147A4D46D0426E
	SHA1	C16B2464EDDE42182C78B2D42122C93DE61D6B9B
	SHA256	0FA0C052DB4DD04B2D5A8EE079A8ED53C6C10557C30EDFDC2D1FCB1BDAE2DC8F
IDS/IPS Signatures	YARA Rule	GandCrab_Ransomware { meta: description = "Yara rule for GandCrab ransomware" strings: $string1 = "CRAB-Decrypt.txt" $string2 = "CRAB-DECRYPT.txt" condition: any of them }

	Snort Signature	alert tcp any any -> any any (msg:"GandCrab Ransomware Activity"; content:"CRAB-Decrypt.txt"; flow:to_server; sid:10000003;)
	Suricata Signature	alert tcp any any -> any any (msg:"GandCrab Ransomware Activity"; content:"CRAB-Decrypt.txt"; flow:to_server; sid:10000003;)
Antivirus Signatures	Symantec	Ransom.GandCrab
	McAfee	Ransom-GandCrab!A57EE189D5D8
	Avast	Win32:GandCrab-A

REvil / Sodinokibi		
Hashes	MD5	0A7E1D8AFAA1694B53B95FDD74EE4C1C
	SHA1	F47A9F77CD3D3AAE0DD6528622D135BE203D3C80

	SHA256	1F9807247E85BFD55F2AC4185803657C7A4B78C707CEE5C24AE4AB3FED6828E5
IDS/IPS Signatures	YARA Rule	REvil_Ransomware { meta: description = "Yara rule for REvil (Sodinokibi) ransomware" strings: $string1 = "RECOVERY_KEY" $string2 = "Sodinokibi" condition: any of them }
	Snort Signature	alert tcp any any -> any any (msg:"REvil (Sodinokibi) Ransomware Activity"; content:"RECOVERY_KEY"; flow:to_server; sid:10000004;)
	Suricata Signature	alert tcp any any -> any any (msg:"REvil (Sodinokibi) Ransomware Activity"; content:"RECOVERY_KEY"; flow:to_server; sid:10000004;)
Antivirus Signatures	Symantec	Ransom.REvil
	McAfee	Ransom-REvil!0A7E1D8AFAA1
	Avast	Win32:RansomX-gen [Ransom]

Business Impact : Monetary Losses

Ransomware attacks have caused significant financial losses for individuals, businesses, and even governments worldwide. Determining the exact monetary losses caused by ransomware attacks is challenging due to underreported incidents. However, industry reports estimate that annual losses due to ransomware attacks reach billions of dollars. These losses encompass ransom payments, system downtime, recovery efforts, reputational damage, legal fees, and regulatory fines.

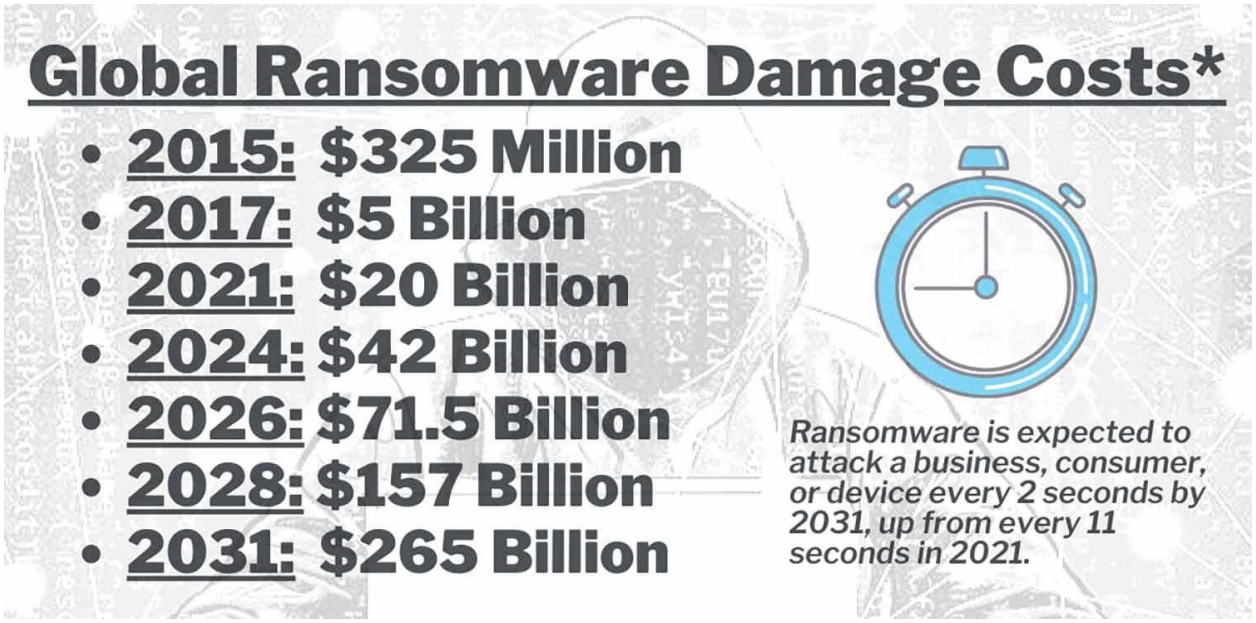

Fig 2 - Ransomware expected financial impact

The following paragraphs provide a summary of the monetary losses associated with various ransomware strains, including WannaCry, Ryuk, GandCrab, and REvil/Sodinokibi.

1. WannaCry:
   WannaCry, which emerged in 2017, caused widespread disruption and financial damages. It infected hundreds of thousands of systems across 150 countries. The estimated monetary losses resulting from WannaCry are staggering, with figures ranging from hundreds of millions to billions of dollars. The attack impacted critical sectors such as healthcare, government, and finance, leading to operational disruptions, data loss, and costly recovery efforts.
2. Ryuk:
   Ryuk ransomware, first identified in 2018, has targeted organizations of all sizes, with a particular focus on enterprises. Its operators employ advanced techniques and carefully select high-value targets for maximum financial gain. Monetary losses attributed to Ryuk attacks are difficult to quantify precisely due to the decentralized nature of ransom payments. However, various reports suggest that Ryuk has extorted hundreds of millions, if not billions, of dollars from victims globally.

3. GandCrab:
   GandCrab was one of the most prevalent ransomware families until its operators retired in 2019. During its active period, GandCrab infected numerous organizations, including small businesses, and demanded ransom payments in cryptocurrency. The exact monetary losses caused by GandCrab are challenging to determine definitively. However, industry reports estimate that it generated tens to hundreds of millions of dollars in ransom payments before its operators ceased their activities.
4. REvil/Sodinokibi:
   REvil, also known as Sodinokibi, has emerged as a prominent ransomware-as-a-service (RaaS) operation. Its sophisticated infrastructure and tactics have resulted in significant financial damages. REvil attacks have targeted high-profile victims, including large corporations and organizations, demanding exorbitant ransom amounts. The monetary losses associated with REvil attacks are substantial, with some reports estimating them to be in the hundreds of millions, if not billions, of dollars.

These figures represent a cumulative impact across multiple victims and incidents. It's important to note that the financial losses resulting from ransomware attacks extend beyond ransom payments. They include costs associated with incident response, recovery, reputation damage, legal fees, and potential regulatory penalties. Additionally, the intangible losses, such as trust, customer confidence, and operational disruptions, can have long-lasting effects on affected entities.

Recommendations and Conclusion:

To mitigate the risk of ransomware attacks, organizations should implement a multi-layered defense strategy. The following paragraphs outline several key strategies that organizations can implement to mitigate the threat of ransomware:

1. Regular Backups and Data Recovery Planning:
   Maintaining regular backups of critical data is crucial. Organizations should follow the 3-2-1 backup rule, which means having at least three copies of data stored on two different media types, with one copy stored offsite. This ensures the ability to recover data without paying a ransom. Additionally, organizations should develop and test data recovery plans to ensure a smooth and efficient restoration process in case of an attack.
2. Employee Education and Awareness:
   Educating employees about ransomware risks and best practices is vital. Regular training programs should cover topics such as identifying phishing emails, suspicious links, and downloading files from trusted sources only. Employees should be aware of the potential consequences of clicking on malicious links or opening infected attachments. Encouraging a culture of cybersecurity awareness can significantly reduce the likelihood of successful ransomware attacks.

3. Robust Endpoint Protection:
   Deploying and regularly updating reliable endpoint protection software, including antivirus and anti-malware solutions, is essential. These tools can help detect and block known ransomware variants. Implementing advanced endpoint protection measures such as behavior monitoring, machine learning, and threat intelligence can enhance detection capabilities and prevent emerging threats.
4. Patch Management and Vulnerability Assessments:
   Promptly applying software patches and updates is critical for preventing ransomware attacks. Regular vulnerability assessments can identify weaknesses in the IT infrastructure that could be exploited by attackers. Establishing a robust patch management process, which includes timely patch deployment and vulnerability remediation, minimizes the risk of ransomware exploiting known vulnerabilities.
5. Network Segmentation and Access Controls:
   Segmenting networks into isolated zones and employing strict access controls can limit the lateral movement of ransomware within an organization's infrastructure. By separating critical systems and implementing access restrictions based on the principle of least privilege, organizations can minimize the impact of a ransomware infection and prevent its spread to sensitive areas.
6. Incident Response Planning:
   Developing and regularly testing an incident response plan specific to ransomware incidents is essential. This plan should include predefined steps for isolating infected systems, notifying relevant stakeholders, engaging law enforcement if necessary, and restoring operations from backups. Having a well-defined response strategy helps organizations minimize downtime, limit financial losses, and effectively recover from a ransomware attack.

Implementing these mitigation strategies, in conjunction with a comprehensive cybersecurity program, can significantly reduce the risk and impact of ransomware attacks. It's important to adapt and update these measures as new threats and attack techniques evolve. Additionally, staying informed about emerging ransomware trends and collaborating with industry peers and security experts can further enhance an organization's defense against ransomware threats.