Ransomware Attack: An Evolving Targeted Threat

Manuj Aggarwal
Ministry of Electronics & IT
Delhi, India
manuj.aggarwal@meity.gov.in

2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) | 979-8-3503-3509-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCNT56998.2023.10308249

***Abstract*— Ransomware typically locks the system to prevent users from accessing their own system or personal files. Only after receiving ransom demand by the attacker, the access is regranted to the user, without which data is permanently lost or, in some cases, made publicly available. In recent years there has been an exponential rise in number of ransomware cases. The attackers have evolved their techniques of attack and have become targeted in their attacks. The objective of this paper is to furnish an exhaustive understanding of ransomware's threat, present current trends, discuss current detecting techniques explored and summarize major ransomware groups active in recent years. Lastly, probable attack vectors, preventive measures and steps to respond in case of ransomware attack are discussed.**

***Keywords*— Ransomware, RaaS, Threat, Attacker, Ransom, Attack vector**

INTRODUCTION

Ransomware is a kind of malware that locks the system, thereby forbidding users from accessing their system or files. A ransom demand is made by the attacker in order to regain access. If the victim doesn't pay the ransom demand within a defined timeframe, the data is lost [1-3]. Extortion by ransomware is not new and has been active since the late 1980s; in initial cases, the payment was demanded via snail mail [4]. Targets can be generalised or specific to individuals, organizations or countries speaking a specific language. Majorly, the ransom is demanded in the form of cryptocurrency. Ransomware can be classified into the following four categories [4]:

Scareware: a pop-up message is received stating that a malware infection is discovered and that to remove it, a certain amount needs to be paid. If no action is taken, pop-ups will continue to be bombarded, but no harm to files is done.

Screen lockers: also known as non-encrypting ransomware, on starting up the system, a full-size window will appear with a logo from a government agency stating an illegal activity has been detected on the device and demands some amount. The user is not allowed to perform any work by locking the screen or flooding the device with pop-ups.

Encrypting ransomware: also known as crypto-ransomware, files are encrypted and taken out of the system. Payment is demanded in order to decrypt and redeliver.

Mobile ransomware - affects mobile devices via malicious apps or drive-by downloads. A message appears that due to some illegal activity, the device is locked and can be unlocked after paying a penalty. Due to the provision of automated cloud data backups, encryption of data does not benefit attackers.

Attackers have evolved their demand style over time to extort more money [5-8]. Earlier attackers encrypted data found on a system, and a ransom was demanded for decrypting it. This was referred to as single extortion. Attackers became more advanced and first exfiltrated the data to a separate location, then encrypted it. The organization is threatened of losing and exposing the data to the public domain if a ransom is not paid. This was referred to as double extortion. In Triple extortion attacks, the organisation is also threatened by a Distributed Denial of Service (DDoS) attack. Figure 1 shows the three types of exploitation by ransomware. Different attack vectors that can infect a device or network by a ransomware attack are as follows [4], [5]:

- Phishing emails, spear phishing and other social engineering attacks: Cybercriminals often pose as the Law enforcement agency with its logo in order to scare users into paying them money as a fine for doing some illegal activity.
- Malvertising and Drive-by downloads: on accessing an infected webpage without the need for the user's action, malicious code attacks the system. The code scans the browser to identify vulnerabilities that can be worked upon inject ransomware.
- Operating system and software vulnerabilities: unpatched vulnerabilities are used as an attack surface, and often ransomware is distributed with the name of patch, causing users to download and affect their device.
- Credential theft: attackers steal or crack authorised users' credentials to log into a device or network to deploy ransomware directly. RDP and Telnet are exploited to gain access to a computer remotely.
- Other malware: malware developed for other attacks is also used to deliver ransomware to a device. Conti ransomware was spread by Trickbot trojan, malware to steal banking credentials.

In this paper, ransomware's threat is discussed. Current trends in 2022 are presented, and major ransomware groups active in recent years are summarized. The rest of the paper is organised as follows: section II discusses related work in the field of ransomware and section III discusses current trends. In section IV, a summary of ransomware groups is provided. The paper concludes in section V.

RELATED WORK

Research has been done in the field of ransomware, mainly focusing on detection techniques and analysis of samples. Humayun et al. [9] have discussed Ransomware threats in IoT devices, while Yaqoob et al. [10] have presented some case studies to aware people of the vulnerability of IoT devices to ransomware attacks.

Researchers [11] have worked on detection methods for ransomware attacks. Monitoring unusual filesystem and registry entries helps in ransomware detection in Windows systems. In the Android environment, caution while granting access to Apps can help in avoiding ransomware attacks.

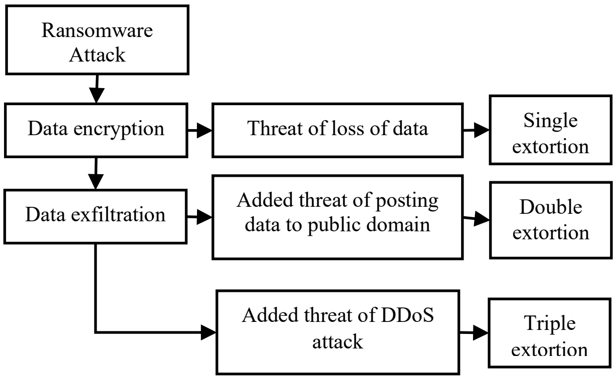

Fig. 1. Ransomware attacks types

Researchers [12–15] have exploited API calls to detect ransomware. Arabo et al. [12] developed a system which monitors API calls of each function used by DLLs to detect if the process is ransomware or not. Other details such as the disk usage and the thread count are also used in detection. The advantage of their system is that the signature database is not required and due to this zero-day ransomware attacks can also be detected. Hampton et al. [13] also exploited API calls to detect ransomware and claimed that calls to file system APIs and low-level drivers are unusual for processes. The authors supported their claim by presenting an analysis of 14 variants of ransomware. Qin et al. [15] exploited API calls and Natural Language Processing for ransomware detection. Almousa et al. [14] used API calls and machine learning techniques for the detection of ransomware.

Many researchers [14, 16–19] have used a machine learning approach to detect and analyse ransomware. Sgandurra et al. [16] dynamically analyze and classify ransomware using a machine learning approach. The authors claimed that different ransomware have a set of common features at run-time which helps in the early detection of new variants. Registry entry and API calls are two such classes with the most pertinent characteristics. However, the approach cannot detect ransomware samples that remain dormant for a time period, or wait for user action or do not perform any action in a sandbox environment. A reverse engineering framework using feature generation engines and supervised machine learning was developed by Poudyal et al. [18] to identify ransomware efficiently. Raw binaries, assembly codes, libraries, and function calls are analysed. The authors concluded that static level analysis at the ASM level and DLL level distinguish ransomware from normal binaries in a better way. Aljubory and Khammas [20] presented a method for detection and classifying ransomware based on machine learning algorithms. Hirano and Kobayashi [17] used a machine learning model on storage access patterns of ransomware and of a normal application and obtained effective behavioural models of ransomware.

Apart from machine learning, other techniques are also used by researchers. Cabaj and Mazurczyk [21] claimed that software-defined networking could help in avoiding ransomware, while Manavi and Hamzeh [22] used Convolutional Neural Networks for ransomware detection. Poudyal, S. and Dasgupta [23] used an AI-based ransomware detection framework. Moore [24] used a honeypot to detect ransomware activity.

A firmware-based Ransomware defence approach has been proposed by Baek et al. [25]. It needs to be embedded into an SSD controller as a form of firmware. Detection is based on the I/O patterns of a host system. The recovery algorithm is triggered on the identification of the encryption process by delaying the deletion feature of an SSD.

CURRENT TRENDS

It is not necessary to develop ransomware in order to perform ransomware attacks. Ransomware-as-a-service (RaaS) is a business model that provides the attacker with an easy entry into ransomware attacks by utilising ransomware developed by some other attacker/group [26-30]. The user purchases an already existing ransomware for carrying out attacks on their own and becomes an affiliate of the ransomware group. Ransom payment is shared with the developer. It also helps ransomware developers to focus better on upgrading the software and earn money for their creations without the need to take time and risk to distribute their threats. Most of the ransomware groups are providing RaaS service. Ransomware groups are spending money to attract affiliates with the ultimate aim of increasing their business. Ransomware are also available in the digital market or dark web for sale. In October 2020, REvil group spent USD 1 million on recruiting affiliates [5]. Apart from the RaaS model, there are threat actors who obtain login credentials of organizations and provide or sell them to other actors, referred to as Access brokers. In 2022, more than 2,500 access posts were observed, a 112% increase in comparison to 2021, indicating an increase in popularity [8].

Attackers have shifted to using existing tools in the operating system or via open-source applications sourced from various code repositories for attacks as it helps to avoid being caught. Cobalt Strike and Brute Ratel are used for such purposes. Microsoft Sysinternals utilities (PsExec) are used for lateral movements. Non-Sucking Service Manager is used to deploy an executable as a service [3].

Difficulty in tracing the money trail due to the use of cryptocurrency for ransom; availability of RaaS and lucrative advertising by ransomware groups; easy development tools to develop ransomware and use of new techniques of encryption have attracted a large number of attackers, including non-technical attackers into ransomware business; thereby resulting in exponential growth in ransomware incidents [26]. Figure 2 presents the number of ransomware attacks that occurred from 2019 to 2022. As can be observed, exponential growth is observed in the number of ransomware cases from 2020 to 2021. However, a slight decrease is observed from 2021 to 2022. The probable cause of the decline is due to attackers becoming more focused on attacking lucrative organisations rather than attacking any

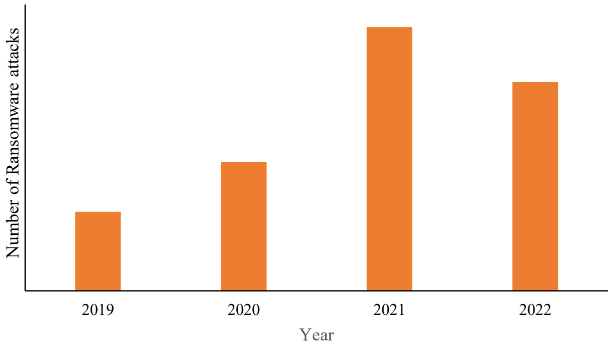

Fig. 2. Ransomware attacks count globally for the year 2019-2022 [31]

organisation. Also, organisations have adopted measures for cyber safety.

Figure 3 presents the number of ransomware attacks in top countries/regions in 2022. On comparing the data, it is observed that in 2022, the top country affected by ransomware was the US, with 1038 posts to extortion sites. Around 50% of the world's ransomware attacks were targeted at the US. Other top affected countries were of western Europe having developed economies and more resources that attract attackers of more chances of getting ransom. With an increased economic growth of Asian and South American countries, and due to increased usage of IT, these countries have become the next favourable choice of attackers. Brazil was ahead of India with 55 posts of extortion and India ranked ninth in the top 10 list with 41 posts to extortion [1]. In APAC and Japan region, India is second and follows Australia in the list and is then succeeded by Japan and Taiwan [32].

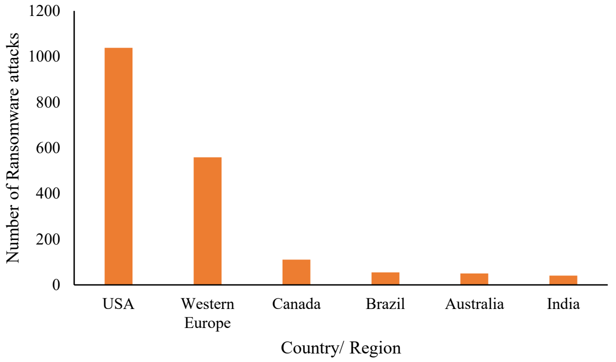

Fig. 3. Ransomware attacks count in top countries/regions in 2022 [27]

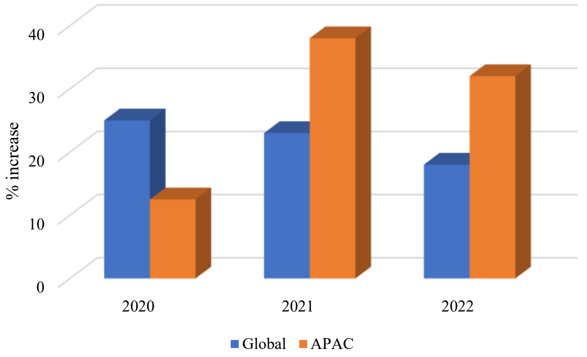

Fig. 4. Percentage increase in the number of ransomware attacks for the years 2020-2022 globally and in the APAC region [1]

In 2022, globally 18% of intrusions involved ransomware whereas for Asia-Pacific (APAC) countries, 32% of intrusions involved ransomware, signifying an increase in ransomware cases in the APAC region [1]. For India, a 53% rise in Ransomware incidents is observed in 2022. Figure 4 represents the percentage increase in the number of ransomware attacks for the years 2020-2022 globally and in the APAC countries group.

Once a ransomware attack has occurred, it is important to detect it, remove it and make the system back to normal at the earliest. Dwell time for a ransomware attack is defined as the number of days it takes to detect the attacker present in a compromised environment. The lower the dwell time, the more prepared the organization is. Intrusions involving ransomware had a median dwell time of 9 days in 2022, compared to 5 days in 2021 [1]. In India, for ransomware attacks dwell time is 10 days for large infrastructure networks and 3 days for smaller network infrastructure [3]. Figure 5 presents the dwell time of the APAC region, India and globally for the year 2022.

In the initial days, individual systems were easy targets of ransomware. Later, cybercriminals began attacking organisations and then realized their full potential in making easy money. Due to the impact on production, brand damage and fear of loss of data and revenue, organisations were compelled to pay ransom [4]. Attackers target almost all sectors of organisations, including hospitals, government agencies, and commercial institutions. The critical infrastructure sector is also targeted to disrupt critical services that compel them to pay a ransom.

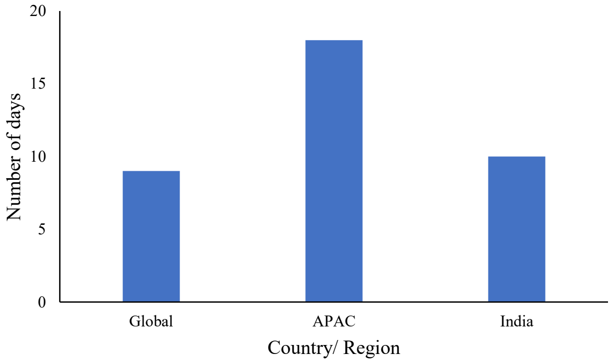

Fig. 5. Comparison of dwell time of APAC region, India and globally for the year 2022 [1], [3]

On the basis of the number of posts to extortion, in 2022 the manufacturing sector was the top sector affected by ransomware. 524 posts to extortion were observed in the manufacturing sector; while in 2021, 316 ransomware threat notes were observed in the manufacturing sector [1]. These attacks also include attacks on manufacturer suppliers as impacting suppliers severely affects the manufacturing sector. For example, Toyota's suppliers were affected in February 2022 and due to this, Toyota was forced to halt production. In the Indian context, in 2022 IT & IT enabled Services was the top sector affected by ransomware followed by Finance and Manufacturing [3].

On the basis of average ransom demand, in 2022 the business sector noted a maximum increase. The average ransom demand raised from an average of $8.4 million in 2021 to $13.2 million in 2022 [33]. On the basis of the average number of records impacted by ransomware attacks on businesses, the count raised from 100,000 in 2021 to almost 900,000 in 2022. On the basis of the number of records impacted by ransomware attacks, in 2022, around 115 million records were impacted as compared to 49.8 million records in 2021.

Worldwide, 2022 saw many ransomware attacks, some of them being TransUnion South Africa (54 million records affected) and a hack on the AirAsia Group (5 million records affected) [28, 33]. 30 organisations on the Forbes Global 2000 list suffered extortion attempts in 2022 [32]. The Top five Ransomware Attacks in 2022 [6]:

1. Costa Rica Government - In early April, Conti attacked the finance ministry, private import-export businesses, and government services and later in May, HIVE

affected the Costa Rican social security fund and the healthcare system which resulted in the declaration of a national emergency.

2. Nvidia - In February, Lapsus$ compromised the world's largest semiconductor chip company Nvidia and leaked one terabyte of employee credentials and proprietary information online. The ransom amount demanded was $1 million including a breach of confidential information.

3. Bernalillo County, New Mexico - On January 5, a ransomware attack hit the security controls in the Metropolitan Detention Center due to which convicts had to be restricted to their cells. This led to the de-compliance of the agreement and an emergency notice was filed in the federal court.

4. Toyota – During the first quarter of 2022, Toyota suppliers were hacked by Lockbit causing the suspension of operations at all lines at 14 domestic Japanese plants resulting in a dip in Toyota's overall production capacity.

5. SpiceJet - In May an attempted ransomware attack on India's SpiceJet airline impacted and slowed down SpiceJet flight departures by 6 hours and breached the data of 1.2 million passengers.

As per records, India is the ninth most affected country by ransomware. Recently in India, LockBit 3.0 attacked Fullerton India Credit Ltd., a non-banking financial company that claimed to have over 600 GB of sensitive data [27, 29, 34–37]. The group demanded a ransom of around INR 24 crores within a period of 5 days to erase all the exfiltrated data [37]. The top 5 Ransomware attacks in India [38] occurred are:

1. In February, Jawaharlal Nehru Port Container Terminal handling half of all the containers in India was reported to have begun turning away ships after a ransomware attack.

2. In May, Indian airline SpiceJet faced ransomware attacks on 24th, May or Tuesday night, which slowed the departure of flights the next morning. It troubles hundreds of passengers stuck in the airport and stranded in several locations in the country.

3. In July, A ransomware attack was carried out on Water Resources Department in Goa, responsible for flood monitoring systems across all over the regions of Goa.

4. In October, Tata Power, one of the leading power company, faced ransomware attacks on 14th Oct. These attacks impacted their IT infrastructure and system.

5. In November, India's leading public medical institute experienced a cyber-attack impacting primary healthcare services - discharge, billing, and patient admission system.

Nothing is safe from ransomware. Apart from Windows, Apple devices were also affected by ransomware. In 2016 KeRanger ransomware infected an app called Transmission and affected Apple devices until Apple released an update. In 2017 Findzip and MacRansom were discovered and in 2020, ThiefQuest (aka EvilQuest) exfiltrated the data and encrypted files but was unable to contact users to demand ransom. In early 2023, LockBit is observed to start targeting Apple devices [39, 40].

Data protection and insurance companies are also now in the picture. In April 2023, Data protection providers Rubrik and Zscaler partnered to enable enhanced ransomware protection. The companies integrated Rubrik's Sensitive Data Monitoring & Management SaaS-based data classification, discovering and reporting solutions with the data loss prevention (DLP) technology in Zscaler's data protection offering, which will be available to the two companies' mutual customers [41]. In April 2023, Rubrik, the Zero Trust Data Security Company doubled its Ransomware Recovery Warranty to $10 million for recovery-related costs [42].

Law enforcement agencies discourage ransom victims from paying ransom as it would motivate other attackers to perform ransom attacks. In some cases, it is legally required to report ransomware infections. For example, HIPAA compliance requires reporting any data breach. As per 2020 advisory from the US Treasury's Office of Foreign Assets Control, legal action would be taken if ransom is paid to attackers from countries under US economic sanctions. However, due to fear of losing or disclosure of data, organisations tend to pay a ransom. In IBM's Cyber Resilient Organization Study 2021, more than 60% of companies which experienced a ransomware attack, paid a ransom [5].

RANSOMWARE GROUPS

There are different ransomware groups active in cyber space. For the year 2022, top active ransomware groups by posts are LockBit, ALPHV/BlackCat, Conti, BlackBasta, Phobos, Hive and Karakurt [30]. Figure 6 shows the contribution of top 5 ransomware groups in 2022. The Hive ransomware group was reported to be the sixth-most active ransomware group in 2022 according to the volume of its ransomware notes [1]. For the Indian scenario, Lockbit, Makop and DJVU/Stop ransomware were the top ransomware. Lockbit, Hive and ALPHV/BlackCat, Black Basta targeted large organisations, while Makop and Phobos targeted medium and small organisations and at the individual level, Djvu/Stop was prevalent. New entries such as Vice Society, BlueSky etc. were also observed [3]. Table 1 gives a summary of prominent ransomware groups.

From the table, it can be observed that most of the ransomware groups are now providing the RaaS service. Some of the ransomware utilise the services of access brokers.

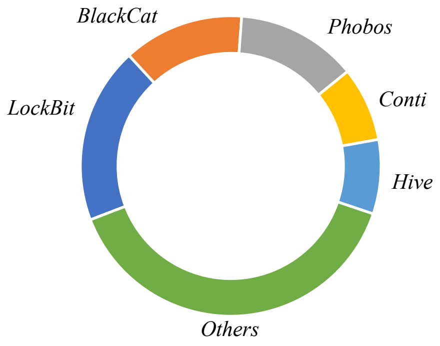

Fig. 6. Top 5 ransomware groups in 2022 [30]

TABLE 1: DIFFERENT RANSOMWARE ACTIVE IN RECENT YEARS

Ransomware	Active since year	Country of origin	Attack method	Main features
ALPHV/BlackCat	December 2021	Russian considered to be run by former members of the Darkside and Blackmatter	-It uses Rust programming language providing fast performance and cross-platform capabilities, enabling it to target on Apple and Linux as well. -to modify Windows Defender security settings, uses PowerShell throughout the victim network	-double-extortion -affiliates get up to 90% of any ransom collected.
Black Basta	April 2022.	Russian seems to a rebrand of conti and its affiliates	-uses the ChaCha20 algorithm and RSA-4096 to encrypt files. -uses Qakbot trojan and PrintNightmare exploit	-double-extortion -compromise organizations based in English-speaking countries -targeting businesses involved in technology, insurance, manufacturing, and utilities.
Conti	2020	Russia-based group	-uses customized AES-256 and multithreading that makes it much faster than most ransomware -remove Volume Shadow Copies, security checks and disable real time monitor -except .DLL, .exe, .sys and .lnk files, encrypts all files	-Mostly affected manufacturing industry -managing to obtain more than $50 Million.
CryptoLocker	September 2013	Not known	-targeted Windows systems -used phishing email and Gameover ZeuS botnet.	-Ransom of around $3 million was made.
DarkSide	August 2020	Likely to be Russian, but not state-sponsored code is similar to that of REvil,	-uninstalls certain security features and backup process. -based on a MAC address, a user ID is generated that is appended to each filename -algorithms- Salsa20 -Exploited vulnerabilities of VMware ESXi hypervisor	-Specifically avoids healthcare centres, schools, and non-profit organizations. -Checks system language settings and does not attack former Soviet-bloc countries and Syrian Arabic. -attacked the U.S. Colonial Pipeline in May 2021, leading to shut down of the pipeline supplying 45% of the U.S. East Coast's fuel.
Djvu/Stop	2018	Eastern Europe -variant of STOP ransomware	-uses multiple layers of obfuscation to slow verification and analysis. -focus on Windows operating systems -gains access to systems through compromised software downloads, whether pirated software or a software crack.	-second most detected ransomware -more than 222 ransomware variants. -Does not attack CIS countries and terminates itself.
Hive	June 2021	Russian organization	-Wide variety of initial access methods depending on affiliate. -Early versions were developed in GoLang -terminates backups, restores, anti-virus, antispyware, and file copies to avoid anti-malware. -To reduce forensic evidence, it creates batch files, containing commands to delete Hive's executable, disc backup copies, snapshots.	-Double-extortion -ransom note contains the login details for the HiveLeaks TOR website, which the victim can use to pay the ransom. -target healthcare and other Government Facilities, Communications, Critical Manufacturing and IT.
Karakurt	2021	Not known -indicated that KArakurt and conti are managed by the same party.	-doesn't encrypt data, but steals data -Threat to sell or post the data on dark web. -It uses extensive harassment campaigns against victims to shame them -Use access brokers	-prefers small organizations based in the US, the UK, Canada, and Germany. -targets organizations using single-factor Fortigate VPN servers using legitimate Active Directory credentials.
Lockbit	September 2019	Likely to be Russian	-attempts to encrypt data stored at any local or remote device -ability to self-propagate -conceals the executable encrypting file by hiding it as the image file.	- group does not target Russian organizations, or former Soviet countries. -targets include organizations in the US, China, India, Indonesia, Ukraine and Western Europe -attacks large enterprises in the healthcare and financial domains.
Makop	2020	Not known	-Infect through email attachments (macros), torrent websites, malicious ads. -uses custom-developed and off-the-shelf software tools	-target companies in Europe and Italy
Petya and NotPetya	March 2016	Russian government, the Sandworm group	-Impacts the system by encrypting the Master File Table of the NTFS file system -algorithms used- ECDH and SALSA20.	-In June 2017, a new variant of Petya exploiting EternalBlue appeared primarily targeting Ukraine. -NotPetya was a wiper with an inability to unlock systems once locked. -damages total nearly $10 billion
Phobos	2018	Not known - similar to Crysis and Dharma virus	-exploits incorrectly configured Remote Desktop Protocols (RDP), -phishing campaigns	-targets smaller organisations and individuals to avoid coming into the eyes of law enforcement agencies.
REvil also known	May 2020	Russian Believed to be an	-uses double-extortion attacks -exploited a Kaseya VSA zero-day vulnerability of the server platform.	-attacked a supplier of Apple and stole confidential schematics of their forthcoming products -group does not target Russian organizations, or

as Sodin or Sodinokibi		offshoot from GandCrab. DarkSide is an offshoot or a partner of REvil.	-delivered as a malicious update to the server platform.	former Soviet countries. -in 2021 attacks against the JBS USA and Kaseya Limited, $ 11 million ransom was paid as its entire U.S. beef processing operation was disrupted, and many of its customers observed significant downtime.
Ryuk	2018	Initially North Korean but later suspected of being Russian criminal groups	-uses Trickbot or Emotet to install itself after gaining access to a network's servers. -can defeat many anti-malware countermeasures -can disable backup files when stored on shared servers and system restore features.	-target large, public-entity Microsoft Windows cybersystems. -ransom demands averaging over $ 1 million. -reach is global and has affected U.S. hospitals shutting down access to patient records and U.S. school systems
Samsam also known as MSIL/Samas.A	2015	Eastern European hacker group	-exploit Windows servers and employed JexBoss Exploit Kit for accessing vulnerable JBoss applications. -Use access brokers and propagates through the RDP.	-Mostly targeted critical infrastructure industries mostly in the US, but also internationally -Directs victims to connect via a Tor hidden service site.

Preventive Measures and Incident Response

Ransomware attack starts by gaining access to the system, followed by Reconnaissance, in which Attackers identify files containing important data and additional credentials to move laterally throughout the network. After this, in the Activation phase, the Encryption process starts. Deletion of backups and disabling of system restore features is done in this phase. Lastly, a ransom note is left in the system often via a .txt file or through a pop-up message. It contains information to pay the ransom demand.

A. Protective measures to avoid attacks include:

It includes defence-in-depth by using layers of defence; secure email gateways to provide security from targeted attack; secure web gateways to scan and identify malicious traffic; monitoring tools for server and network to detect anomalies; maintaining proper and tested backups of sensitive data and system images on other devices disconnected from the network; applying the latest and tested patches; providing regular security awareness training and drills for users and implementing network protection policies such as least privilege, zero-trust architecture, segmentation of the network, etc.

B. Steps for responding to a ransomware

It is reported that 51% of organizations do not have a prescribed ransomware policy [37]. The human error turned out to be the primary cause of data breaches in more than 50% of cases. A tested Business Continuity Plan helps to avoid major operational disruption, without which it becomes tedious to analyze the harm made to the system and then restoration of the affected network. The following steps can be taken to minimize damage and quickly return to business as usual in case of ransomware attack [26].

- Isolate the infected device from the network to contain the infection.
- Disconnect all suspiciously behaving devices from the network to stop the spread of infection.
- Assess the damages by preparing a complete list of all affected systems and devices.
- Identify the entry point by checking for any alerts from any active monitoring platform and identify the ransomware by scanning encrypted files and ransom note.
- Reporting the ransomware attack to authorities is needed as per the rules of law enforcement agencies.
- Prioritize the restoration of systems by restoring the most critical ones first, followed by eradication of the threat from the network.
- If backup is available, restore the systems from a backup. Otherwise, try for decryption options available online.
- In case of unavailability of backups and a decryption key, start from scratch.

Conclusion

Ransomware attackers have evolved their techniques of attack from time to time. Starting from single extortion to triple extortion, and a target shift from individuals to organisations is observed. Now organisations from which large quantity of records and more ransom can be obtained are attacked. There is an exponential growth in ransomware attacks throughout the world. Although in 2022, a slight decrease is observed in ransomware attacks, due to more focused attacks, the amount of data compromised and ransom demand has increased. Researchers have different detection techniques, out of which analysis of API calls and use of machine learning techniques is most common. Different ransomware groups have been active in recent years, each having different methods of attack and different target organisations. Lastly, proper user awareness and preventive measures can only help in avoiding ransomware attacks.

References

[1] Mandiant, ‘M-Trends', 2023. [Online]. Available: https://www.mandiant.com/m-trends [Accessed May. 05, 2023].

[2] Kespersky, IT Security Economics 2022 Executive summary, 2022 [Online] Available: https://www.kaspersky.com/resource-center/threats/ransomware [Accessed May. 05, 2023].

[3] CERT-In, India Ransomware Report 2022 [Online]. Available: https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf [Accessed May. 05, 2023].

[4] Malwarebytes, All about ransomware attacks. https://www.malwarebytes.com/ransomware [Accessed May 05, 2023].

[5] IBM, What is ransomware? https://www.ibm.com/in-en/topics/ransomware [Accessed May 05, 2023].

[6] S. M. Kerner, “Ransomware trends, statistics and facts in 2023.” . https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts [Accessed May 05, 2023].

[7] A. Gabriella, “2022 Ransomware Statistics & The Biggest Ransomware Attacks.” https://heimdalsecurity.com/blog/ransomware-statistics/ [Accessed May 05, 2023].

[8] CrowdStrike, “2023 Global Threat Report.” [Online]. Available: https://go.crowdstrike.com/2023-global-threat-report.html [Accessed May. 05, 2023].

[9] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, “Internet of things and ransomware: Evolution, mitigation and prevention,” Egyptian Informatics Journal, vol. 22, no. 1, pp. 105–117, Mar. 01, 2021. doi: 10.1016/j.eij.2020.05.003.

[10] I. Yaqoob et al., “The rise of ransomware and emerging security challenges in the Internet of Things,” Computer Networks, vol. 129, pp. 444–458, Dec. 2017, doi: 10.1016/j.comnet.2017.09.003.

[11] Monika, P. Zavarsky, and D. Lindskog, “Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization,” in Procedia Computer Science, vol. 94, 2016, pp. 465–472. doi: 10.1016/j.procs.2016.08.072.

[12] A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier, “Detecting ransomware using process behavior analysis,” in Procedia Computer Science, vol. 168, 2020, pp. 289–296. doi: 10.1016/j.procs.2020.02.249.

[13] N. Hampton, Z. Baig, and S. Zeadally, “Ransomware behavioural analysis on Windows platforms,” Journal of Information Security and Applications, vol. 40, pp. 44–51, Jun. 2018, doi: 10.1016/j.jisa.2018.02.008.

[14] M. Almousa, S. Basavaraju, and M. Anwar, “API-Based Ransomware Detection Using Machine Learning-Based Threat Detection Models,” 2021 18th International Conference on Privacy, Security and Trust, IEEE, 2021. doi: 10.1109/PST52912.2021.9647816.

[15] B. Qin, Y. Wang, and C. Ma, “API Call Based Ransomware Dynamic Detection Approach Using TextCNN,” in Proceedings - 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering, ICBAIE 2020, IEEE, Jun. 2020, pp. 162–166. doi: 10.1109/ICBAIE49996.2020.00041.

[16] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, “Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection,” Sep. 2016, [Online]. Available: http://arxiv.org/abs/1609.03020

[17] M. Hirano and R. Kobayashi, “Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained From Live-forensic Hypervisor,” in Sixth International Conference on Internet of Things: Systems, Management and Security (IoTSMS) : Granada, Spain, October 22-25, 2019, 2019.

[18] S. Poudyal, K. P. Subedi, and D. Dasgupta, “A Framework for Analyzing Ransomware using Machine Learning,” 2018 IEEE symposium series on computational intelligence (SSCI), pp. 1692-1699, IEEE, 2018.

[19] G. Usha, P. Madhavan, M. Vimal Cruz, N. A. S. Vinoth, Veena, and M. Nancy, “Enhanced Ransomware Detection Techniques using Machine Learning Algorithms,” in Proceedings of the 2021 4th International Conference on Computing and Communications Technologies, ICCCT 2021, IEEE, 2021, pp. 52–58. doi: 10.1109/ICCCT53315.2021.9711906.

[20] N. Aljubory and B. M. Khammas, “Hybrid Evolutionary Approach in Feature Vector for Ransomware Detection,” in International Conference on Intelligent Technology, System and Service for Internet of Everything, ITSS-IoE 2021, IEEE, 2021. doi: 10.1109/ITSS-IoE53029.2021.9615344.

[21] K. Cabaj and W. Mazurczyk, “Using software-defined networking for ransomware mitigation: The case of cryptowall,” IEEE Netw, vol. 30, no. 6, pp. 14–20, Nov. 2016, doi: 10.1109/MNET.2016.1600110NM.

[22] F. Manavi and A. Hamzeh, “A New Method for Ransomware Detection Based on PE Header Using Convolutional Neural Networks,” in Proceedings of 17th International ISC Conference on Information Security and Cryptology, ISCISC 2020, IEEE, Sep. 2020, pp. 82–87. doi: 10.1109/ISCISC51277.2020.9261903.

[23] S. Poudyal and D. Dasgupta, “AI-Powered Ransomware Detection Framework,” in 2020 IEEE Symposium Series on Computational Intelligence, SSCI 2020, IEEE, Dec. 2020, pp. 1154–1161. doi: 10.1109/SSCI47803.2020.9308387.

[24] C. Moore, “Detecting ransomware with honeypot techniques,” in Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016, IEEE, Oct. 2016, pp. 77–81. doi: 10.1109/CCC.2016.14.

[25] S. Baek, Y. Jung, D. Mohaisen, S. Lee, and D. H. Nyang, “SSD-Assisted Ransomware Detection and Data Recovery Techniques,” IEEE Transactions on Computers, vol. 70, no. 10, pp. 1762–1776, Oct. 2021, doi: 10.1109/TC.2020.3011214.

[26] Trellix, What Is Ransomware? [Online]. Available: https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html [Accessed May 05, 2023].

[27] Recorded Future 2022 Annual Report. [Online]. Available: https://www.recordedfuture.com/2022-annual-report [Accessed May 05, 2023].

[28] Thales, 2023 Thales Data Threat Report. [Online]. Available: https://www.thalesgroup.com/en/worldwide/security/press_release/2023-thales-data-threat-report-reveals-increase-ransomware-attacks [Accessed May 05, 2023].

[29] BlackFog, 2022 Ransomware Attack Report, 2023. [Online]. Available: https://www.blackfog.com/2022-ransomware-attack-report [Accessed May 05, 2023].

[30] Sophos, Sophos 2023 Threat Report. [Online]. Available: https://www.sophos.com/en-us/content/security-threat-report [Accessed May 05, 2023].

[31] Annual number of ransomware attacks worldwide from 2017 to 2022. [Online]. Available: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ [Accessed May 05, 2023].

[32] India second most targeted country by ransomware in APAC and Japan region: Report. [Online]. Available: https://www.businesstoday.in/technology/story/india-second-most-targeted-country-by-ransomware-in-apac-and-japan-region-report-374338-2023-03-22 [Accessed May 05, 2023].

[33] Ransomware attacks declined in ’22 but more records being compromised. [Online]. Available: https://www.securityinfowatch.com/cybersecurity/article/21292765/ransomware-attacks-declined-in-22-but-more-records-being-compromised [Accessed May 05, 2023].

[34] ProofPoint, What Is Ransomware? [Online]. Available: https://www.proofpoint.com/us/threat-reference/ransomware [Accessed May 05, 2023].

[35] Mitigating malware and ransomware attacks. [Online]. Available: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks [Accessed May 05, 2023].

[36] NCSC, A guide to ransomware. [Online]. Available: https://www.ncsc.gov.uk/ransomware/home [Accessed May 05, 2023].

[37] Update: LockBit 3.0 Ransomware Targets Fullerton India: Company Reverts to Offline Operations as a Precaution. [Online]. Available: https://www.timesnownews.com/technology-science/lockbit-3-0-ransomware-targets-fullerton-india-demand-a-staggering-2400-crores-ransom-in-just-5-days-article-99721253 [Accessed May 05, 2023].

[38] Top 5 Ransomware Attacks in India to Watch Out for in 2023. [Online]. Available: https://www.linkedin.com/pulse/top-5-ransomware-attacks-india-watch-out-2023-ecscorp [Accessed May 05, 2023].

[39] N. Ahmed, Explained - What is LockBit ransomware and why is it targeting macOS?. [Online]. Available: https://www.thehindu.com/sci-tech/technology/explained-lockbit-ransomware-and-why-its-targeting-macos/article66766214.ece [Accessed May 05, 2023].

[40] L. Abrams, LockBit ransomware encryptors found targeting Mac devices. [Online]. Available: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-encryptors-found-targeting-mac-devices/ [Accessed May 05, 2023].

[41] J. Schwartz, Rubrik, Zscaler Partner to Double Down on Ransomware Protection. [Online]. Available: https://www.channelfutures.com/security/rubrik-zscaler-ransomware-protection [Accessed May 05, 2023].

[42] Rubrik, Rubrik Ups the Ante with $10 Million Ransomware Recovery Warranty. [Online]. Available: https://www.globenewswire.com/news-release/2023/04/24/2652758/0/en/Rubrik-Ups-the-Ante-with-10-Million-Ransomware-Recovery-Warranty.html [Accessed May 05, 2023].