Ransomware and its Evolution with the Covid-19 Pandemic.

Rohan Mahesh
Information Technology
(Bachelors in Engineering)
Shah and Anchor Kutchhi Engineering College
(Affiliated with Mumbai University)
Mumbai, India

Khushi Jain
Information Technology
(Bachelors in Engineering)
Shah and Anchor Kutchhi Engineering College
(Affiliated with Mumbai University)
Mumbai, India

Nidhi Adatiya
Information Technology
(Bachelors in Engineering)
Shah and Anchor Kutchhi Engineering College
(Affiliated with Mumbai University)
Mumbai, India

Ms. Bhargavi Dalal
Information Technology
(Assistant Professor)
Shah and Anchor Kutchhi Engineering College
(Affiliated with Mumbai University)
Mumbai, India

Dr.Nilakshi Jain
Information Technology
(Associate Professor and guide)
Shah and Anchor Kutchhi Engineering College
(Affiliated with Mumbai University)
Mumbai, India

***Abstract*—**In this paper, we discuss different cyber threats to corporate infrastructure. Our primary focus is Ransomware(RW), its types, along with its evolution. With the COVID-19 pandemic, the number of cyber attacks have steeply increased due to the home-office working situation. Cases of Ransomware (RW) have doubled as shown by cyber security research conducted in Q1 2020. Traditional network antimalware software and several other packet filtering techniques have also been ineffective against these attacks, this paper also tries to delve into the types of attacks, spread of the malware to multiple systems along with protective measures that can be undertaken to limit its potential of infecting all the systems within a network. We have also tried to show the evolutionary nature of the malware with recent cases showing a different type of attack that emphasizes blended extortion Ransomware attacks where hackers steal confidential information before encrypting it. If victims chose not to pay for a decryption key, attackers will then threaten to release stolen information publicly. This intern results in a catch-22 problem where the target is vulnerable even after backing up systems.

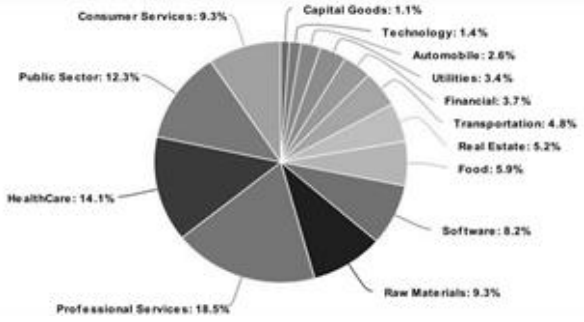
Keywords*—(Ransomware, Zero-day, vulnerabilities, RaaS, exploit, Sodinokibi, obfuscated, SN AKE, Tycoon***)**

I. INTRODUCTION

Firstly, we look into various types of Ransomware(RW) attacks and its advent with the recent pandemic. Newer iterations of this attack have been detected throughout the world. Its primary goal however, still remains the same, which is to deny access of data to the owner of the target machine and ask the network owner for a ransom that is made using cryptocurrency, in order to allow access to their own data. An ideal target is usually any enterprise that has weaker network protocols which can be exploited for its vulnerabilities. Research conducted by the IBM security X-Force suggests that the hardest hit industry is the manufacturing sector, followed closely by professional services. This is mainly due to the victims having high sensitivity towards network downtime, making it crucial for them to pay the ransom as time reliable operations require zero to no downtime of the network infrastructure. Therefore, the owners of the network will prefer paying the ransom rather than losing productivity.

With the Covid-19 pandemic, these industries are already facing severe losses in terms of productivity due to reduced demand and presence of a solid workforce. This has been a great opportunity for hackers to exploit the vulnerabilities of these networks as the necessary security teams are not present onsite for a quick response to the attacks.

Newer samples of the RW attacks have seen a growth of about 72% in 2020 alone according to a report by Security magazine (issue of Jul 2020).Altogether, the normal ransoms made for the second quarter of 2020 was $178,254, a 60 percent expansion from the first leg. 20,000+ new incident reports anticipated for 2020, breaking past records. 50% expansion in portable device attacks featuring threats of obscuring line among corporate and individual organizations. Ransomware flourishes during COVID-19 pandemic, with new examples expanding by 72 percent. Targeting basic frameworks has become rampant, which include medical services organizations and professional services as depicted by the chart of common sectors affected.



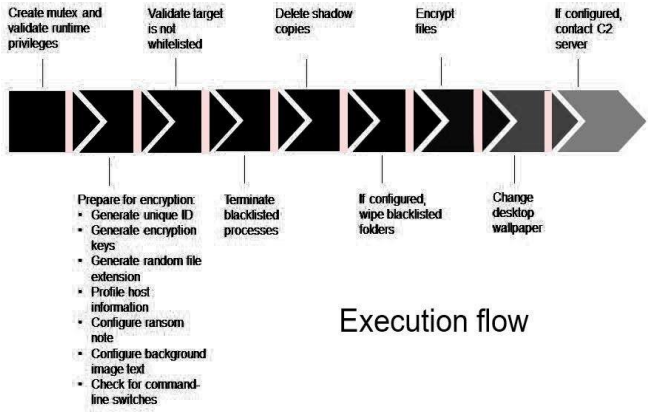
II. TYPES OF RANSOMWARE

Since April of 2020, we have witnessed several types of Ransomware, the most common ones are as follows.

A. REvil/Sodinokibi Ransomware

This is a type of complex file encrypting strain that is also a Ransom as a Service (RaaS). It has been detected in several countries throughout the globe. Initially this type of Ransomware spread through a zero-day vulnerability within the Oracle WebLogic Server. Many systems that deployed Oracle software were updated with an infected patch. Even though this was later fixed, the systems that had applied the updates already had the malware.

This resulted in the progressive spread of *Revil* ransomware through spam, phishing mails and RDP attacks. Eventually, making REvil, one of the most common types of attacks. As Covid-19 forces security teams to work from home, this attack has become the most prolific, with overall affected systems giving it the 4th position amongst the most deadly malwares of all time.



Sodinokibi is a flavour of REvil ransomware which has recently gained popularity, the attack starts out as an obfuscated Javascript file that is injected into the target system, this file is not detected by antimalware applications as the code is difficult to decipher by itself. After entering the host machine, the malware begins executing its Javascript files.

The process flow typically includes-

- Tweaking privileges using the CVE-2018-8453 weakness
- Resource manipulation by voiding blacklisted operations.
- Locking out server files that are not on the whitelist.
- Data transfer from the target to the attacker.

B. MAZE Ransomware

The MAZE ransomware dispatched on different fronts, focusing on numerous associations across industry areas including accounting, medical care, data storage (IT), and government. Like other ransomware strains, it encodes documents in a network framework, and requests a payment from its casualties to retrieve these records. Notwithstanding, what separates it from other common ransomware has been its 'novel' blackmail strategies to likewise take victims' information and initiate steps to freely deliver them except if the payment is made. As MAZE ransomware works under an associate model, it can grow its activities generally across various topographical areas and industries.

The release of company data to the public is known as Data exfiltration, has become a prevalent tactic in Q1 2020, whereas this method was virtually non-existent in the last quarter. This tactic has shown rapid growth during the pandemic and is projected to increase as the groups try to inflate the conversion rates on their exchanges. MAZE has shown to exfiltrate data 99 percent of the time. This data is either used as news material by the group to interest the world or being directly sent to customers so that the company's reputation can directly be tarnished if the ransom is not paid.

There has also been a radical shift in by attackers using this ransomware towards a post compromise distribution. Unlike the conventional approach of leveraging data for money or cryptocurrency and the hacker trying to distribute the attack throughout a wide array of systems, this method prioritizes gaining privilege access to a particular system, with the motive of trying to target a critical system within the network. This information is later used to extract personal data before the deployment of the ransomware within the target.

C. SNAKE (EKANS) Ransomware

The infamous SNAKE (EKANS) ransomware is notorious for targeting large businesses that require massive network equipment for their operations. In early June 2020, this ransomware was detected in the servers of the Japanese automaker Honda. According to Information Security specialists, the technical difficulties being faced by the company's customer and financial services was likely due to an infected server. This inturn resulted in the company halting it's services for a few days so that internal security audits could be done to remedy the situation.

Recently, the developers of the MAZE ransomware announced their "retirement" from the malware development industry. Therefore, many attackers are turning to SNAKE as a viable alternative. SNAKE tends to work a little differently as the files that are encrypted by the malware are renamed to files with randomized extensions such as ".WNgh, .NdWfEr".Along with this a ransom note is added which is mostly named as "RECOVER-FILES.txt". This text file specifies that the enterprise

network has been compromised and the victim has 3 days to pay the ransom and failure to do so would lead to the documents being published online.

An analysis report of the incident at Honda indicated that the malware was launched using a "nmon.bat" file. EKANS is a ransomware variant written in the Go programming language, first observed in commercial malware repositories in late December 2019. There are very few relevant samples to analyze. Therefore, EKANS poses a unique and unforeseen risk to equipment used by the industry.

D. TYCOON Ransomware

The Tycoon Ransomware is a relatively new strain of malware that was found by security professionals from Blackberry and KPMG's intelligence department. Initially, it starts out in the form of a ZIP archive which contains the malware. It uses a Trojanised Java image file which is stored in one of the modules, so it can evade any antimalware programs that may have been deployed within the system. So, this method of escaping detection is relatively new and JRE images designed to be used by the Java Virtual Machine at runtime. Unlike the popular Java Archive format JIMAGE is mostly internal to the JDK and rarely used by developers as it does not belong to the standard Java library. Its primary objective however, still remains the same, which is to lock the administrator out of the system.

The technical analysis of the files revealed that there were five essential parts within the configuration files of the Tycoon Ransomware. It mainly consisted of-

1. The hacker's email address for communication.
2. Public Key of the RSA encryption that was applied to the AES keys.
3. A main note that contains the address where the ransom is supposed to be sent, along with some other information.
4. Names of systems that are excluded from the attack.
5. Commands that are to be executed.

The uniqueness of the malware stems from the fact that experts have found the malware within the Java Runtime Environment with code that contains scripts targeting linux servers, thereby concluding that it is able to infect both Windows and Linux systems. Adding to the list of deadly features, Tycoon also contains a built-in persistence mechanism that is handled by an operation called Image File Execution Option. This is a type of file, that is found within the windows registry results in a combined feature set of advanced targeting and persistence mechanisms, making the program virtually untraceable.

Due to the utilization of RSA to scramble the safely produced AES keys, the decoding process requires getting the assailant's private RSA key. Considering a 1024-digit RSA key, albeit hypothetically possible, has not been accomplished at this point and would require exceptional levels of computation.

Therefore, all enterprises that have a mid sized network are advised to have robust auditing strategies to confirm the credentials of the connection, constant updations of the operating systems, along with web servers. Recently though, a well known company released a group of Decryption keys publicly that they had paid a ransom for, when this key was used with other cases of affected files, the key seemed to work for all the files rendering the malware powerless.

III. Combating Ransomware

Several steps have already been taken to combat Ransomware with varied results. Essentially, there is no set procedure to reverse the damage and companies can ensure network safety by implementing certain precautionary steps to make sure that their networks are safe or limit the monetary damage, in case of an attack. With fewer people in the workforce during the pandemic, this task becomes exponentially difficult.

Keeping in mind the recent changes in the workplace environment, we found some unconventional but effective ways to limit Ransomware.

A. Outsourced Security Operations Center (SOC)

We came across this rapidly growing approach of outsourcing the inhouse security team's job of handling real-time attacks and replacing it with a third party security company that has a dedicated Security Operations Center. This method ensures that the response time in case of an attack is quick and a timely incident report is generated along with possible fixes to mitigate the problem.

The company can limit their downtime by simply incorporating an incident response plan, this plan could prove beneficial against some of the common Ransomwares, however, it will still not be very efficient, as newer attacks are being discovered constantly and a more dynamic plan is required. In this case, a third party security team will be able to effectively lessen downtime by implementing a dynamic incident response plan. Not only will they be able to quickly identify the breached sector and isolate it, but also save time while carrying out the entire process, effectively stopping its spread.This also mitigates the overall in monetary and productivity losses incurred by the company due to the incident. Following the attack, the team will be able to efficiently restore or backup essential files and reinstall it onto the network while the in-house security team can keep the day-to-day operations running smoothly.

An independent survey reflected that ransomware has heavily impacted the industry with at least 48% of all enterprises being hit with an attack. This totals up to an average company being hit at least 6 times each. Deploying a SoCaaS can lessen the burden of the organisation's security team especially the ones working from home. The report also showed that an average of 33 hours were wasted in the recovery process from an attack. Dedicating this task to an external company saves money in the long run. They also employ experienced industry professionals that know how to use the most up-to-date technology, monitor and respond to any threats effectively stopping the attack at its tracks.

Although the system might seem simple first, there are certain challenges that an organisation might face if they outsource. There is always a great security risk while having company data outside the premises, if correct measures are not implemented. We also cannot neglect the fact that an external expert is not very familiar with the company specific infrastructure. In this case, the company taking the contract has to dedicate time to getting to know the company's network. Finally, we also have the problem of reversibility if the company taking the contract uses proprietary equipment.

B. Detection using Machine Learning Algorithms

In AI, a work process is an iterative cycle that includes gathering accessible information, cleaning and setting up the information, building models, approving and then making the final product.There are two basic ways to deal with malware investigation: Static examination: Static investigation includes inspecting the malware without running it,Dynamic examination: Dynamic investigation includes running the malware.considering the type of input of the networks,Hybrid examination: Includes an amalgamation of both approaches.

These examination techniques are carried out using using various deep learning approaches which are also grouped according to the type of input in the network:

(1) Employing feature engineering to extract a vector feature representing the executable.

(2) Techniques for the representative gray scale of an executable as input.

(3) Functions that are fed a sequence of API function invocations;

(4) An approach that takes the model of a program as a sequence of instructions

(5) Representing a computer program as a sequence of bytes

(6) Classification of programs on the basis of network .

These techniques show great promise in detection of Ransomware but also have their own challenges. There are laws that restrict sharing of binaries and they become a hurdle to the research being conducted in the field. There is also the universal problem of concept drift that changes the underlying relationships of data.

C.Actively training staff on links

The main reason for the spread of Ransomware still remains human error. Phishing messages were a highly effective method for the spread of malware in 2020. Therefore employees need to be trained on links they can trust. In this way, we can be somewhat wary of email messages being sent over the web. Certain precautionary steps can be taken to curb the influence of malware on infrastructure security.

- Broadcast all messages for known malware strains, and keep firewalls and endpoint securities fully informed regarding the most recent known malware marks.
- Informing clients about any breaches and spreading caution.
- Giving VPNs to clients to use outside of the organization
- As a company, realizing that employees will click the wrong link is important.

The high number of phishing messages sent each day and the wide array of attack methods imply that a few messages will make it to the worker's inbox. Preparing representatives to perceive and react fittingly to these messages can help limit an association's exposure to ransomware.

D. Maintaining a Dual Backup of the data

For a company, dual backups of data are quite beneficial. One of the backups should ideally be on the cloud while the other should be internal. This approach ensures that in the event of data loss, a persistent backup is being created that keeps data safe even if one of the backup fails. With the case of a Ransomware the quickest way of getting rid of the malware is flushing the disk and restoring an active backup of data, thereby ensuring that the spread is limited. Working with a reputed cloud solutions provider can also greatly benefit recovery from any attack.

E. Securing Server Data

The access to data within the server should be restricted. Features like Dynamic access control, limit the information access by any digital hacker. Organization division will guarantee that the organization security in general isn't undermined, if there is an occurrence of an attack. The benefit of this technology is that access to records and documents on Active Directory credits can be controlled. The objective is to offer the ability to go past a conventional permit/deny depending on the client

F. Whitelisting:

Whitelisting the connections that are deemed legitimate is one of the most common ways of protecting against malwares. This method uses a technique of only allowing certain programs to run unlike blacklisting which actively blocks unwanted connection.The termination of any unauthorised data packet will ensure that only legitimate packets are entertained by the network.This will also prevent any unknown files from executing in the background as only the knows packets are allowed to. This method can also be used effectively against Ransomware as the primary working still remains the same.

G. Honeyfile Approach:

This is an unconventional approach that is proposed by a developer named Gomez Hernandez, who tries to detect existing ransomware within the system by deploying a honey file design of the Linux system to immediately isolate the ransomware from the canary file when there is unauthorised access to data, thus allowing it to maintain the rest of the data. Along with finding the cause of the malware, this program also has features that remove the process from the system.The system works on a file with three essential components, a main FIFO, the links that are used for file access along with a monitoring process that acts as a server.

This type of system also has its flaws which include the fact that the complete file system is not protected. When installed in fewer numbers, the efficiency of this elaborate trap reduces significantly. The defence mechanism can also be overrun by the removal of the central trap. There can also be partial bypass wherein all the files within a particular directory can be blocked before the process is shut down.

IV. CONCLUSION

We observed the different types of Ransomware that were commonly used to attack networks in 2020. These include three main types of attacks REvil,MAZE and SNAKE along with their specific features and different ways they affect corporate infrastructure. We also observed that the use of these tools has spiked with the Covid pandemic due to the absence of emergency security teams within the enterprise campus. It is also noted that only a few precautionary steps can be taken to prevent Ransomware and as of now, research on a remedial measure is still being conducted.

V. ACKNOWLEDGMENT

We would like to express our gratitude towards Dr. Nilakshi Jain for her thoughtful insight using her years of industry experience on the subject, throughout the course of research, Ms.Bhargavi Dalal for briefing us about the process of paper publishing . We would also like to thank our principal Dr. Bhavesh Patel for his support towards our endeavour and providing us with invaluable resources in terms of his suggestions and feedback. We also greatly appreciate all the efforts taken by the Research Cell at Shah and Anchor Kutchhi Engineering College.

VI. REFERENCES

[1] D. Gonzalez and T. Hayajneh, "Detection and prevention of crypto Ransomware(RW)," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, 2017, pp. 472-478, doi: 10.1109/UEMCON.2017.8249052.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] KPMG's report on the rise of Ransomware(RW) during the COVID-19 pandemic

[3] https://www.coveware.com/blog/q1-2020-ransomware-m arketplace-report.

[4] DXC Technology, Security Threat Report, July-August 2020

Daniel Gibert, Carles Mateu, Jordi Planes, The rise of machine learning for detection and classification of malware: Research developments, trends and challenges, Journal of Network and Computer Applications, Volume 153,2020,102526,ISSN 1084-8045.

[5] N. Aldaraani and Z. Begum, "Understanding the impact of Ransomware: A Survey on its Evolution, Mitigation and Prevention Techniques," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, 2018.

[6] S. Sharmeen, Y. A. Ahmed, S. Huda, B. Ş. Koçer and M. M. Hassan, "Avoiding Future Digital Extortion Through Robust Protection Against Ransomware Threats Using Deep Learning Based Adaptive Approaches," in IEEE Access, vol. 8, pp. 24522-24534, 2020.

[7] S. Saxena and H. K. Soni, "Strategies for RansomwareRemoval and Prevention," 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2018, pp. 1-4, doi: 10.1109/AEEICB.2018.8480941

[8] S. R. Zahra and M. Ahsan Chishti, "RansomWare and Internet of Things: A New Security Nightmare," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2019, pp. 551-555, doi: 10.1109/CONFLUENCE.2019.8776926.

[9] S. Z. Sajal, I. Jahan and K. E. Nygard, "A Survey on Cyber Security Threats and Challenges in Modem Society," 2019 IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 2019, pp. 525-528, doi: 10.1109/EIT.2019.8833829.

[10] I. Nadir and T. Bakhshi, "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques," 2018 International Conference on Computing, Mathematics

and Engineering Technologies (iCoMET), Sukkur, 2018, pp. 1-7, doi: 10.1109/ICOMET.2018.8346329.

[11] K. R. Dalal and M. Rele, "Cyber Security: Threat Detection Model based on Machine learning Algorithm," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2018, pp. 239-243, doi: 10.1109/CESYS.2018.8724096.

[12] Hakak, S., Khan, W. Z., Imran, M., Choo, K.-K. R., & Shoaib, M. (2020). Have you been a victim of COVID-19-related Cyber incidents? Survey, taxonomy, and mitigation strategies. IEEE Access, 1–1. doi:10.1109/access.2020.3006172.

[13] F. Ullah et al., "Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach," in IEEE Access, vol. 7, pp. 124379-124389, 2019, doi: 10.1109/ACCESS.2019.2937347.

[14] V. Chamola, V. Hassija, V. Gupta and M. Guizani, "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact," in IEEE Access, vol. 8, pp. 90225-90265, 2020, doi: 10.1109/ACCESS.2020.2992341.

[15] R. Punia, L. Kumar, M. Mujahid and R. Rohilla, "Computer Vision and Radiology for COVID-19 Detection," 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, pp. 1-5, doi: 10.1109/INCET49848.2020.9154088.

[16] Y. Liu, H. Qin, Z. Chen, C. Shi, R. Zhang and W. Chen, "Research on Cyber Security Defense Technology of Power Generation Acquisition Terminal in New Energy Plant," 2019 IEEE International Conference on Energy Internet (ICEI), Nanjing, China, 2019, pp. 25-30, doi: 10.1109/ICEI.2019.00011.

[17] M. Satheesh Kumar, J. Ben-Othman and K. G. Srinivasagan, "An Investigation on Wannacry Ransomware and its Detection," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, 2018, pp. 1-6, doi: 10.1109/ISCC.2018.8538354.

[18] A. AlSabeh, H. Safa, E. Bou-Harb and J. Crichigno, "Exploiting Ransomware Paranoia For Execution Prevention," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9149005.

[19] S. Saeed, N. Jhanjhi, M. Naqvi, M. Humayun and S. Ahmed, "Ransomware: A Framework for Security Challenges in Internet of Things," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/ICCIS49240.2020.9257660.