Understanding and reporting Ransomware Attacks

Identifying Ransomware Threats: Understanding ransomware's telltale signs, its potential aftermath, and the need for immediate reporting and action.

Introduction: Basic understanding of ransomware and its impact

Ransomware depicts a type of malware (like Viruses, Trojans, etc.) that infects the computer systems of users and manipulates the infected system in a way, that the victim can not (partially or fully) use it and the data stored on it. The victim usually shortly after receives a blackmail note by pop-up, pressing the victim to pay a ransom (hence the name) to regain full access to the system and files. [1] Ransomware reaches computers and devices in various ways, including spam (with malicious file attachments or embedded links), compromised or specially crafted malicious websites or web pages, and exploit kits. There are two main classes of modern ransomware: lockers and crypto-ransomware [2]

Behaviors of ransomware have dramatically changed over the past years. In 2015, a shift in target was observed—operators started targeting businesses instead of individuals. This was made evident with a constant stream of reports of big companies succumbing to the threat. Apart from just infecting computers and mobile devices, ransomware also infects shared and removable drives and servers. Some families have also taken to encrypting chosen file types like tax-related and database files, ensuring bigger profits for their operators. [3]

This malware can lead to a variety of negative consequences, including [4]

- temporary or permanent loss of sensitive or proprietary information
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization’s reputation.
- Health risk. Cyberattacks targeting hospitals are so-called “threat-to-life crimes” [5]

References

[1] European Union Agency for Cybersecurity (ENISA), Ransomwarehttps://www.enisa.europa.eu/topics/incident-response/glossary/ransomware

[2] Yilmaz, Y., Cetin, O., Arief, B., & Hernandez-Castro, J. (2021). Investigating the impact of ransomware splash screens. Journal of Information Security and Applications, 61, 102934

[3] TrendLabs The Global Technical Support & R&D Center of TREND MICRO, Ransomware Past, Present, and Future, 2017 online: https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf

[4] University of California, https://security.berkeley.edu/faq/ransomware/what-possible-impact-ransomware

[5] VAN BOVEN, Liselotte S., et al. Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals. Annals of Emergency Medicine, 2023.

Precautionary measures

One possible explanation for the high rate of ransomware victimization among entrepreneurs is a lack of self-protective activity. Security measures, like firewalls, can be designed to counter cyber threats, and safe practices, including identifying suspicious requests and putting up warnings for suspicious activity, can be implemented. [1]

According to a study [2] on the effects of ransomware on hospitals, there is a need to develop three points a. Improved communication (between cyber-event planning and emergency management planning), b. Improved IT security (set up more secure log-in procedures, applied extensive limitations to remote system access, encrypted classified information), c. Improved contingency plans.

Despite the fact that ransomware attacks are increasing rapidly against enterprises a survey has shown that entrepreneurs generally perceive little risk of their businesses falling victim to ransomware attacks [1] therefore more information and awareness are needed.
Some of the most common ways people get infected by ransomware are [3]:

- Phishing emails
- Visiting corrupted websites (drive-by downloading)
- Downloading infected file extensions or malicious attachments
- System and network vulnerabilities
- Remote desktop protocol (RDP) attacks

There are numerous strategies to guard against being infected with ransomware. Since technology is always changing, it's critical to keep vigilant and adhere to fundamental cybersecurity procedures to ensure you are not ever at risk from ransomware attacks. Hwever, each organization should adapt its security strategy to its own needs and adopt measures that suit its requirements. It should also be emphasized that as technology evolves rapidly and the cyber environment is highly volatile, each process is systematically evaluated and modified accordingly.

For this reason, in this section, we will briefly mention only some general points for protection against ransomware [4] [5] [6] [7]

- Backup Data
- Keep All Systems And Software Updated
- Install Antivirus Software & Firewalls
- Network Segmentation (Because ransomware spreads swiftly across a network, in the event of an attack, it's critical to minimize its spread.)
- Email Protection (email phishing attacks are the leading cause of malware infections [8])
- Whitelisting determines which applications can be downloaded and executed on a network
- Limit User Access Privileges (limiting user access and permissions to only the data they need to work)
- Run Regular Security Testing
- Security Awareness Training.

It is worth emphasizing that one of the most serious threats to an organization's cybersecurity is human error. It is believed that up to 95% of successful cyber breaches are due to human error, highlighting the rapid shift to remote working in recent years during the pandemic as a particularly important factor [9]. For this reason, staff training should be an integral part of any security policy and should be given particular importance and attention.

References

[1] Bekkers, L., van't Hoff-de Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. Computers & Security, 127, 103099

[2] Van Boven, L. S., Kusters, R. W., Tin, D., van Osch, F. H., De Cauwer, H., Ketelings, L., ... & Barten, D. G. (2023). Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals. Annals of Emergency Medicine

[3] UpGuard, Kely Chin, 15 Nov. 2023, How to Prevent Ransomware Attacks: Top 10 Best Practices in 2023 online: https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks

[4] Europol, Tips & advice to prevent ransomware from infecting your electronic devices, online: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices

[5] UpGuard, Erward Kost, 15 nOV. 2023, online https://www.upguard.com/blog/protecting-employee-credentials-from-ransomware-compromise

[6] Microsoft, Protect your PC from ransomware, online: https://support.microsoft.com/en-us/windows/protect-your-pc-from-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3

[7] Kaspersky, Ransomware protection: How to keep your data safe in 2023, online: https://www.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

[8] FBI, FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics, online: https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

[9] Leah, J. (2022). 3 public sector cybersecurity threats – and how to prevent them. Available: https://www.hyve.com/insights/category/blog/#blog-navigation

Immediate Actions: What to do when you've identified a ransomware attack

The number one rule if you become infected with ransomware is never to pay the ransom, this is advice from LEA. All that does is give hackers more motivation to target you or another person with more cyberattacks. However, free decryptors might let you get access to some encrypted data. However, Not all ransomware families have had decryptors created for them, in many cases because the ransomware utilizes advanced and sophisticated encryption algorithms [1], in this case, a full system restore is necessary.

Take a photo of the ransomware message since this may contain useful information for the investigation of the incident, such as email address, bitcoin address, etc. Report it to the police and the payment processor involved. Collect any relevant logs for instance suspected command and control IP addresses, suspicious registry entries, or other relevant files detected The more information you give to the authorities, the more effectively they can disrupt the criminal infrastructure.

The IT department must be immediately informed, in order to take action as soon as possible. For example, cutting all connections, including inbound and outbound. Without an internet connection, no one can remotely access a computer and disconnect external storage devices [2] [3]. Passwords to all accounts and systems must be changed immediately. Furthermore, care must be taken when retrieving data for system restoration to avoid re-infecting clean systems.

Every employee must be informed about the situation, personally, check is significant in with each employee to make sure they are aware of the situation and know what to watch out for [4]. Because as already mentioned the infection can spread rapidly in the network. Malicious actors may keep an eye on the organization's activities or communications following an initial compromise to see if their actions have been discovered, [5] for this reason alternative ways of communication are demanded.

If the attack resulted in a data breach, the organization must inform the interested parties and report the incident to the Supervisory Authority in accordance with the applicable laws of each country. A data breach occurs when the data for which company/organisation is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity [6].

To conclude, the organization must refine—organizational policies, plans, and procedures and guide future exercises of the same also, should raise awareness the employees about cybercrime and safety policies frequently.

References

[1] Swapna, S., Keerthana, R., & Poojitha, P. (2019). Awareness of ransomware attacks-detection and prevention parameters. Think India Journal, 22(4), 8126-8134.

[2] National Cyber Security Centre, Mitigating malware and ransomware attacks online: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

[3] Microsoft, 18 Nov. 2022, 10 Things You Should Do After a Ransomware Attack online: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/10-things-you-should-do-after-a-ransomware-attack

[4] EJ Phillips, 2022 What to do AFTER a Ransomware Attack online: https://www.proactive-info.com/blog/what-to-do-after-a-ransomware-attack

[5] Stop Ransomware (An official website of the United States government), I've Been Hit By Ransomware, online: https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

[6] Europian Commission, What is a data breach and what do we have to do in case of a data breach, online: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en

Case Studies: Review of notable ransomware incidents

One characteristic illustration of the damage that can be brought about by a huge ransomware assault is the closure of the Frontier oil pipeline in the US. which led to panic buying and shortages. After the attack, Colonial Pipeline informed the public about the shutdown of their 5500 mile-long pipeline transporting 45% of the US East Coast's fuel supplies [1]. Joseph Blount, the chief executive of the pipeline company, said the company believes that the criminal hackers infiltrated Colonial's computers through an old virtual private network, commonly known as a V.P.N., "that was not intended to be in use." He added, "We are still trying to determine how the attackers gained the needed credentials to exploit it." [2]

The All India Institute of Medical Sciences (AIIMS), in New Delhi, had a ransomware attack on November 23, 2022, encrypting its healthcare information system's data and demanding a ransom of US$24.5 million. Patients and physicians at AIIMS experienced great distress as a result of the system's week-long shutdown. In a similar vein, on May 31, 2022, a ransomware assault compromised data from Costa Rica's Ministry of Finance, and restoration of the compromised data required US$15 million. The Costa Rican government shut down its online government services and proclaimed a state of emergency in the wake of this incident.

The biggest media company in Portugal, Impresa, was the target of one of the most notable ransomware attacks in history, carried out by the hacker collective Lapsus$ (Type of ransomware: Lapsus$). All of its websites, TV networks, and weekly newspapers were taken down by the attack. In addition, attackers took over the business's Twitter account and declared they had access to the AWS account. Impresa acknowledged the attack, according to news sources, but claimed there was no demand for ransom. Lapsus$, which claims that it gained access to Impresa's Amazon Web Services account, also sent a phishing e-mail to Expresso subscribers and tweeted from the newspaper's verified Twitter account.

One characteristic illustration of the damage that can be brought about by a huge ransomware assault is the closure of the Frontier oil pipeline in the US. which led to panic buying and shortages. After the attack, Colonial Pipeline informed the public about the shutdown of their 5500 mile-long pipeline transporting 45% of the US East Coast's fuel supplies [1]. Joseph Blount, the chief executive of the pipeline company, said the company believes that the criminal hackers infiltrated Colonial's computers through an old virtual private network, commonly known as a V.P.N., "that was not intended to be in use." He added, "We are still trying to determine how the attackers gained the needed credentials to exploit it." [2]

The All India Institute of Medical Sciences (AIIMS), in New Delhi, had a ransomware attack on November 23, 2022, encrypting its healthcare information system's data and demanding a ransom of US$24.5 million. Patients and physicians at AIIMS experienced great distress as a result of the system's week-long shutdown. In a similar vein, on May 31, 2022, a ransomware assault compromised data from Costa Rica's Ministry of Finance, and restoration of the compromised data required US$15 million. The Costa Rican government shut down its online government services and proclaimed a state of emergency in the wake of this incident.

The biggest media company in Portugal, Impresa, was the target of one of the most notable ransomware attacks in history, carried out by the hacker collective Lapsus$ (Type of ransomware: Lapsus$). All of its websites, TV networks, and weekly newspapers were taken down by the attack. In addition, attackers took over the business's Twitter account and declared they had access to the AWS account. Impresa acknowledged the attack, according to news sources, but claimed there was no demand for ransom. Lapsus$, which claims that it gained access to Impresa's Amazon Web Services account, also sent a phishing e-mail to Expresso subscribers and tweeted from the newspaper's verified Twitter account.

The REvil group emerged as a major ransomware threat in 2019, but their most disruptive operations started in 2020. Their strategies changed over time, but their primary approaches focused on software flaws or tricked victims into installing the ransomware via phishing emails or by taking use of vulnerabilities in the Remote Desktop Protocol (RDP). After entering a network, REvil proceeded laterally, acquiring administrative access, raising privileges, and encrypting files on the compromised host with the ransomware.

The 2021 Kaseya VSA supply-chain attack was one of their most notorious assaults. REvil took advantage of a zero-day vulnerability in the Kaseya VSA software, which is used by IT companies for infrastructure management and monitoring. They could infect up to 1,500 companies globally by spreading ransomware to a large number of Kaseya's customers by taking advantage of this vulnerability.

The biggest meat processor in the world, JBS, was the target of another noteworthy attack. In that instance, REvil gained access to the JBS networks through a successful spear-phishing attack, and JBS had to pay $11 million to stop the data breach. [5] [6].

References

[1] Greubel, A., Andres, D., & Hennecke, M. (2023). Analyzing Reporting on Ransomware Incidents: A Case Study. Social Sciences, 12(5), 265.

[2] New York Times, https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html

[3] Mary K. Pratt, 13 Sep. 2023, The 10 biggest ransomware attacks in history online: https://www.techtarget.com/searchsecurity/tip/The-biggest-ransomware-attacks-in-history

[4] Reuters, Portugal's Impresa media outlets hit by hackers, 3 Jan. 2022, online: https://www.reuters.com/business/media-telecom/portugals-impresa-media-outlets-hit-by-hackers-2022-01-03/.

[5] Cobalt, Jacob Fox, 24 Jul. 2023, 11 Biggest Ransomware Attacks in History, online: https://www.cobalt.io/blog/11-biggest-ransomware-attacks-in-history

[6] National Counterintelligence and Security Center, Kaseya VSA Supply Chain Ransomware Attack, 10 Aug 2021, online: www.NCSC.gov

This project was funded by the European Union’s Internal Security Fund - Police Programme under Grant Agreement No 101038738