GSJ: Volume 11, Issue 5, May 2023, Online: ISSN 2320-9186
www.globalscientificjournal.com

RANSOMWARE – TREND ANALYSIS AND FUTURE INSIGHTS

[1]*Omenka Ugochukwu E* [2]*Luke-Odoemena Ijeoma* [3]*Nlemadin Anuli L* [4]*Onyike Obinna G*

[5]*Nwoduh Udochukwu* [6]*Iwuoha Obioha* [7]*Emeagi Ijeoma nee Agwamba*

[1.2,3,4,5,6,7] *Department of Computer Science , Federal Polytechnic Nekede, Owerrri, Imo State*

Abstract: Ransomware is malware that uses password protection and cryptography to hijack a victims files or computer system, deny user access, and demand a ransom payment. This report comprehensively analyzes the ransomware threat, its evolution, and trends. Ransomware attacks date back to the late 90s but became a more severe threat to cybersecurity in 2017 due to the cryptocurrency boom, leading to notable attacks such as the WannaCry ransomware attack. Ransomware assaults have escalated dramatically in recent years, with the number of attacks globally increasing by 62% in 2020, 105% in 2021, and falling by 23% in 2022. It examines the types of ransomware, its lifecycle, and its critical associated trends. It also highlights potential future directions for ransomware attacks and their possible implications for cybersecurity. Understanding the anatomy of a ransomware assault can assist businesses in better preparing for these risks.

Keywords*: Ransomware, Cryptocurrency, Cybersecurity*

INTRODUCTION

Ransomware is a type of malware that uses diverse methods to infect a victim's computer system, delivering a malicious payload. The malicious payload employs password protection and cryptography to hijack a victim's files or computer system, denies the user access, and then demands a ransom be paid for the process to be reversed.

In recent times, most ransomware has been engineered to threaten sensitive and private data exposure if demands are not met. Even when demands are met the attacker might continue threats

of information leakage, with a view to further extort the victim, or eventually sell the information from the leak on the dark web in a bid to make more profits.

This report provides a comprehensive awareness of the ransomware threat, highlighting the critical trends that have emerged over the years and emphasizing the potential future directions of ransomware attacks with the possible implications for cybersecurity.

BACKGROUND

Ransomware attacks date back to the late 90's when the internet and the web where still in their budding ages. The mid 2000's ushered in a modern era in ransomware evolution, when attacks utilized advances in cryptography and leveraged on services of the internet for propagation. Figure 1 shows a timeline of attacks from inception to present (Warikoo, 2023). It is pertinent to note that ransomware attacks where never seen as severe threats to cybersecurity until the year 2017 when several remarkable attacks were recorded. The success of these numerous attacks are been linked to the cryptocurrency boom of 2017. Among the attacks of 2017 was a very notable one known as the WannaCry ransomware attack. This was a worldwide cyberattack that affected over 200,000 in more than 150 nations around the globe. This malicious attack targeted a Microsoft Windows Operating System vulnerability known as 'Eternal Blue' which existed in unpatched Windows Operating Systems. A lack of sensitization on the importance of security updates made this attack successful, Microsoft had earlier released a patch to tackle this vulnerability, but it was ignored by many users and organizations. In the UK, it hit the health sector hard enough to make NHS lose around £92million (Griffiths, 2023).

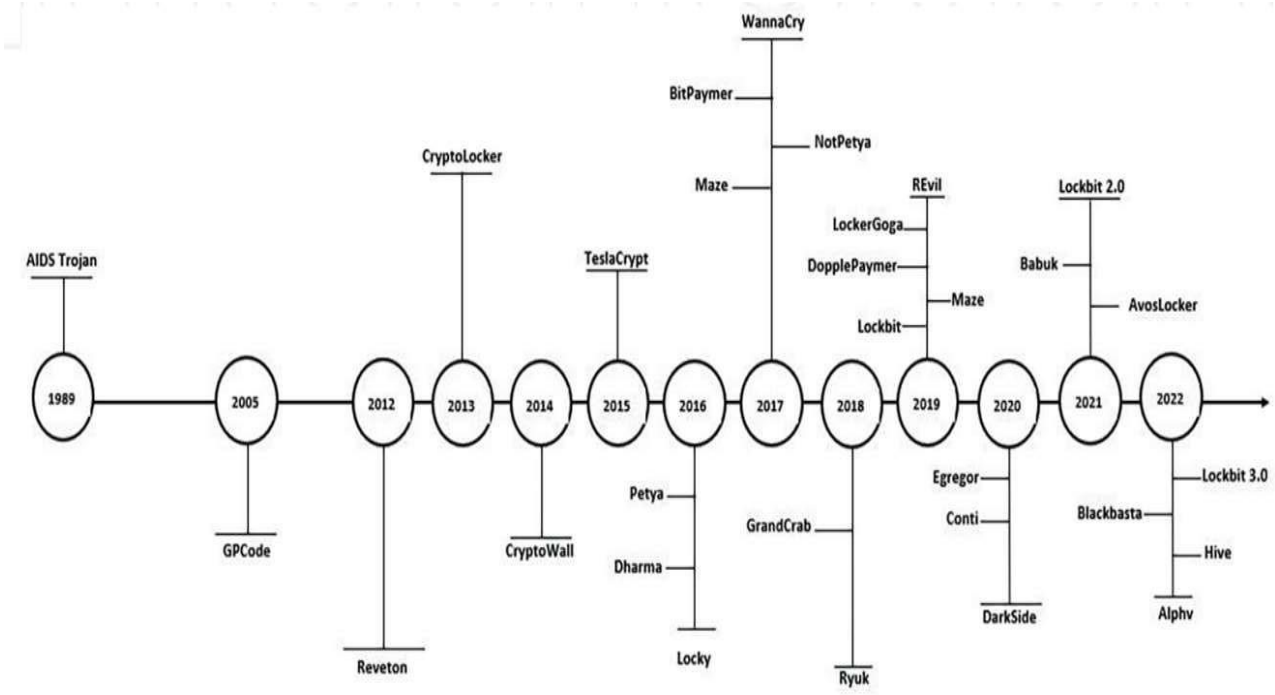

Fig. 1 Chronological Evolution of Ransomware. (Warikoo, 2023)

Ransomware assaults have escalated dramatically in recent years, which has made ransomware one of the most alarming cybersecurity threats. The number of ransomware assaults worldwide increased by 62% in 2020 capping the figure at 304.6 million. In 2021, there were 623.3 million ransomware assaults globally, a 105% increase over 2020 numbers and in 2022, the number of ransomware assaults fell by 23%, rounding off at 236.1 million as seen in Figure 2 (Petrosyan, 2022). This recent drastic rise and fall can be explained thus, in 2020 the world experienced a pandemic that partially halt the operations of business and organizations. Companies had to operate online to ensure the stay in business and this increased the amount of dependency on technology, especially the internet and its services. In 2021, Post pandemic companies combined remote work and physical presence to usher in the hybrid type of services which still maintained the dependency. This brought about an atmosphere with new technologies and processes that were prone to attacks. By 2022, most companies have become cyber aware, and governments have increased scrutiny also.

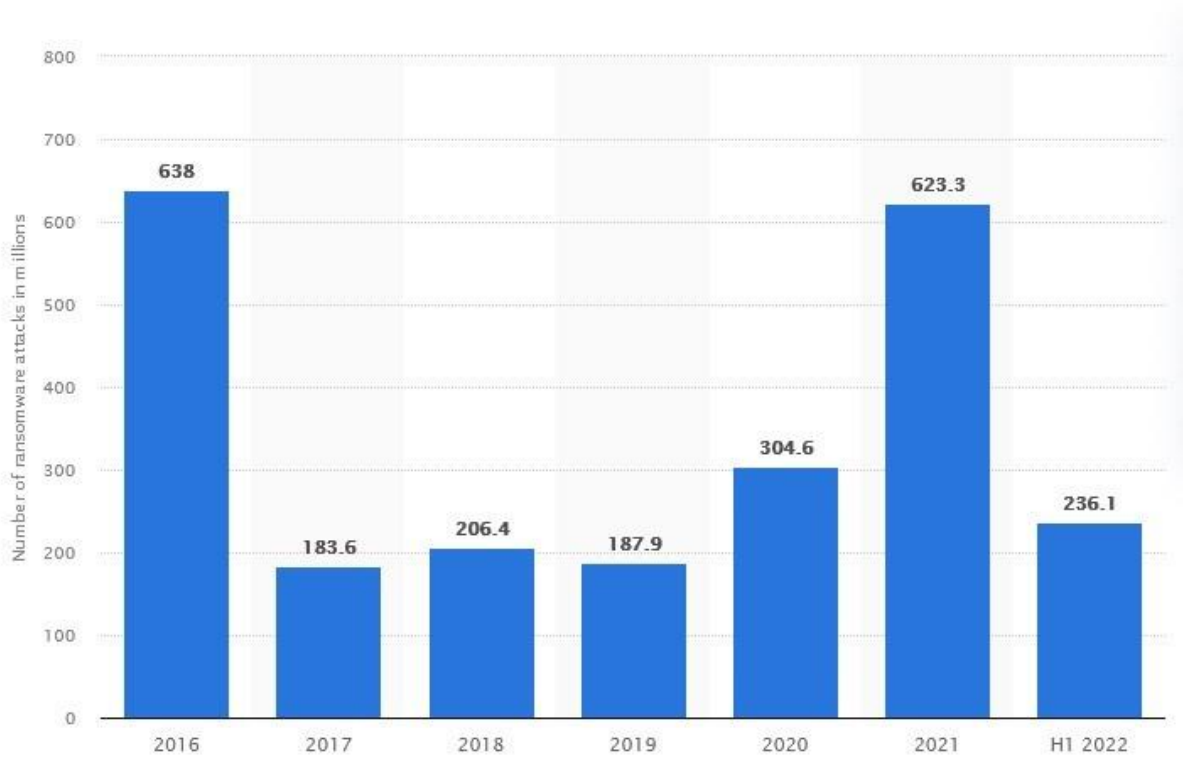

Fig 2 Annual number of ransomware attacks worldwide from 2016 to first half 2022. (Petrosyan, 2022)

Critical Analysis of Current Trends

Before we delve into the critical analysis phase of the current trends in ransomware, there is a need to understand the types and basic operation of ransomware.

The most traditional types of ransomware are:

- Lockers - locks a machine, making data and apps unavailable. The ransom demand is shown on a lock screen, sometimes with a countdown clock to build urgency and force victims to act.
- Encryptors - encrypts a system's files and data, the contents remain inaccessible until ransom is paid, and a decryption key is sent. This is the most malicious and common type of ransomware.
- Scareware - fake software that claims to have identified a virus or other problem on a computer and then asks for payment to fix it. Some lock the computer, while others just flood the screen with pop-up notifications (Beaman et al, 2021).

Knowing the anatomy of a ransomware assault can assist businesses in better preparing for these risks. If you understand how the ransomware lifecycle works, you may be able to prevent hazards before they cause significant impact.

Distribution

The network is usually infiltrated; this can be by a phishing email, an exploit, or a worm etc.

Command and Control

Once inside, the ransomware connects to the attacker's command and control server to obtain instructions.

Credential Access

While remaining undiscovered, the virus continues to lay the groundwork for its assault by collecting credentials and obtaining access to more accounts throughout the network.

Search and Encrypt

The malware looks for data to encrypt on the local workstation as well as any networks it has obtained.

Extortion

Attackers start stealing and/or encrypting local and network files. The attacker requests money to decrypt or return the files to the company (JPMorgan, 2022).

Double Extortion Tactics

The rising use of double extortion methods in ransomware attacks is a crucial trend. Cybercriminals employ this strategy by encrypting the victim's data, stealing data, and threatening to publicly disclose it unless the ransom is paid. This method has shown to be highly effective since victims are typically willing to pay to avoid public disclosure of sensitive information.

The addition of double extortion marks a watershed moment in the continued evolution of ransomware. Current ransomware attacks follow the same pattern: encrypt the data of the targeted companies and demand money in exchange for access restoration. Yet, because there is no assurance that hackers would follow their promise, some firms choose not to pay ransom, particularly if backup data are kept regardless (Agcaoili et al.,2012). Just like the plan isn't horrible enough, ransomware operators are increasingly employing multilayer extortion strategies such as deploying distributed denial-of-service (DDoS) assaults and/or hounding victim enterprises' customers and stakeholders as seen in Figure 3.

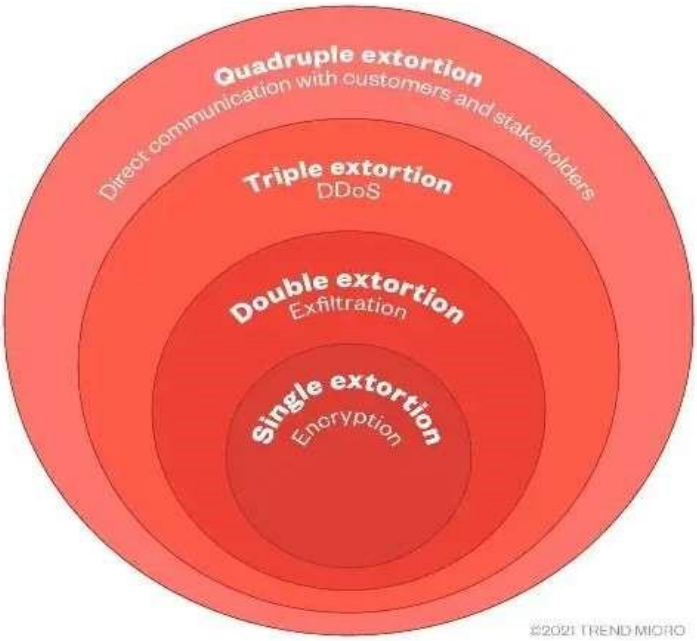

Fig. 3 Ransomware extortion phases (Agcaoili et al.,2012).

The Stages include Encrypt Organizations Data, Leak their data on the internet, Launch a denial of service attack on their online presence and directly contact their customers to tell them of the compromise.

Ransomware as a Service

Ransomware as a service (RaaS) is a subscription-based model that allows affiliates to conduct ransomware attacks using pre-developed ransomware tools. Associates profit from each successful ransom payment. Ransomware as a Service (RaaS) is a business concept that is similar to Software as a Service (SaaS). RaaS customers, like other SaaS users, do not need to be trained or even experienced to utilise the product effectively (Kost, 2023). RaaS technologies, as a result, enable even the most inexperienced hackers to carry out very intricate cyberattacks as shown in Figure 4.

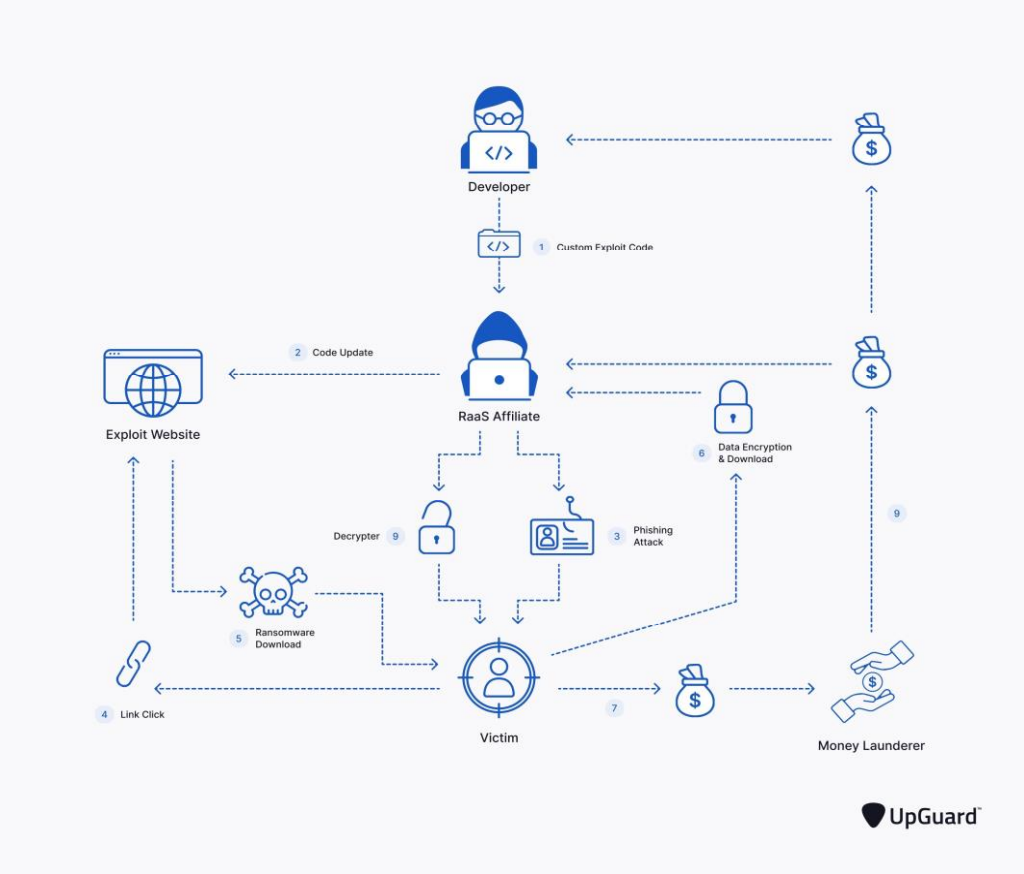

Fig. 4 Anatomy of RaaS (Kost, 2023)

DISCUSSION

Ransomware threats have a dismal future, with cybercriminals likely to evolve and discover new ways to strike victims. The use of artificial intelligence (AI) to launch more sophisticated attacks is one potential future trend. AI may be used to automate assaults and develop unique malware that is resistant to detection. Devoteam (2003.) stated that AI is used by cybercriminals to construct increasingly sophisticated and difficult-to-detect phishing attempts. They can, for example, utilise AI to build convincing false emails or websites that appear real. In a couple of seconds, AI can clone any website and customise it depending on the original to provide the appearance of genuine access to an internal resource.

Also the attack on Critical infrastructure such as Industrial Control System, including all kinds of cyber physical systems. Many ransomware attacks on industrial and critical infrastructure businesses expose operational technology (OT) data that threat actors might utilise, including to perform cyber-physical assaults. A cyber-physical assault is a breach in cyberspace that affects

physical processes, possibly inflicting property damage and endangering safety or life. Renewable and hydroelectric energy providers, manufacturers of automobile and industrial equipment, oil and gas companies, control system integrators, satellite monitoring service and most recently healthcare are among those affected(Kovacs, 2022).

CONCLUSION

Ransomware is a major problem for individuals, businesses, and governments, and it is predicted to become more prevalent in the future. As technology evolves, cybercriminals will continue to devise new methods of conducting attacks. To counteract ransomware attacks, organisations and individuals must work to improve their cybersecurity posture. Governments must also step up efforts to track down and prosecute cybercriminals to deter future assaults.

REFERENCES

Agcaoili J., Ang M.,Earnshaw E., Gelera B.&Tamana N. (2021, June 15)Ransomware Double Extortion and Beyond: REvil, Clop, and Conti, Trend Micro Incorporated.Retrieve March 26th, 2023, from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digitalthreats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers & security, 111, 102490. https://doi.org/10.1016/j.cose.2021.102490

Devoteam (2003.). Dangers and challenges of AI in cybersecurity. Are you prepared? Retrieved March 26, 2023, from https://www.devoteam.com/expert-view/dangersand-challenges-of-ai-in-cybersecurity/

Griffiths, C. (2023, March 11). The Latest 2023 Ransomware Statistics (updated March 2023). Retrieved from AAG: https://aag-it.com/the-latest-ransomwarestatistics/#:~:text=There%20were%20623.3%20million%20ransomware,all%20cyber%20crimes%20in%202022.

JP Morgan (2022, September 7). The anatomy of a ransomware attack.JP Morgan Chase & Co. Retrieved March 25, 2023, from https://www.jpmorgan.com/commercialbanking/insights/the-anatomy-of-a-ransomware-attack

Kost, E. (2023, July 27). What is Ransomware as a Service (RaaS)? The Dangerous Threat to World Security. Upguard. Retrieved March 26, 2023, from https://www.upguard.com/blog/what-is-ransomware-as-a-service

Kovacs, E. (2022, January 31). OT Data Stolen by Ransomware Gangs Can Facilitate Cyber-Physical Attacks. Security Week Network. Retrieved March 26, 2023, from https://www.securityweek.com/ot-data-stolen-ransomware-gangs-can-facilitate-cyberphysical-attacks/

Petrosyan, A. (2022, August 3). Annual number of ransomware attacks worldwide from 2016 to first half 2022. Statista. https://www.statista.com/statistics/494947/ransomwareattacks-per-year-worldwide/

Warikoo, Arun. (2023). Perspective Chapter: Ransomware. 10.5772/intechopen.108433. Retrieve from https://www.researchgate.net/publication/367641107_Perspective_Chapter_Ransomw are