Hybrid Attack Strategies: Analysing the Convergence of DDoS and Ransomware Attacks in Multivector Cyber Assaults

UMANHONLEN GABRIEL[1], STEPHEN AREO[2], HELEN OYADOKE[3], BENNARD FORTUNE OKHUMENDE[4], JULIUS ADENIYI[5], CHISOM UDECHUKWU[6], OLUWASEYI ELIZABETH ADELEYE[7]

[1]*Ambrose Alli University Ekpoma*
[2]*LAUTECH Ogbomoso*
[3]*Obafemi Awolowo University*
[4]*Olabisi Onabanjo University*
[5]*University of Ilorin*
[6]*Bells University of Technology*
[7]*Federal University of Technology, Akure*

Abstract- ***This study examines the convergence of Distributed Denial of Service (DDoS) and ransomware attacks within hybrid attack strategies. By analyzing the interplay between these two forms of cyber threats, we identify how their combination can amplify the impact on targeted systems. We investigate the techniques and methods used to orchestrate such multivector assaults and assess their effectiveness compared to singular attack vectors. The findings offer insights into the evolving landscape of cyber threats and provide recommendations for enhancing defensive measures against these sophisticated hybrid attacks.***

Indexed Terms- ***DDoS, Ransomware, Cyber Assaults, Multivector Attacks, Cybersecurity, Threat Analysis***

I. INTRODUCTION

1.1 Background of the Study

For more than two decades, the internet has been a major source of global communication and an integral part of human life (Li & Liu, 2021). Most activities, including those of economic, commercial, cultural, social, and governmental bodies, are conducted in cyberspace (Li & Liu, 2021). Cyberspace has essentially become the backbone of vital systems, not only housing sensitive and crucial infrastructures but also being the platform through which they are controlled, managed, and used (Akhavan-Hejazi & Mohsenian-Rad, 2018). It is the bedrock of information exchange (Admass, Munaye, & Diro, 2024). This digitalization has made individuals and organizations prone to continually shifting cyber threats (Admass, Munaye, & Diro, 2024).

Every day, we witness the emergence of increasingly sophisticated threats and trends in the cybersecurity landscape, posing significant risks to individuals and organizations (Admass, Munaye, & Diro, 2024). The most prominent of these attacks are malware attacks, phishing attacks, ransomware, social engineering, disinformation and misinformation, supply chain targeting and distributed denial of service (DDoS) attacks (Thakur, Qiu, Gai, & Ali, 2016).

For nearly 30 years, Distributed Denial of Service (DDoS) attacks have been among the most disruptive and notorious cyber threats (Singh & Gupta, 2022). These attacks aim to cripple targeted organizations by overwhelming their network connections, thereby preventing legitimate users from accessing critical services (Singh & Gupta, 2022). Ransomware, on the other hand, is a form of malware that encrypts a victim's data or systems, locking the legitimate user out until a ransom is paid (Kapersky, 2024; Mandiant, 2024). It is often deployed by threat actors to exploit the victim by demanding a ransom to be

paid within a stipulated time (Kapersky, 2024; Mandiant, 2024). If the ransom is not paid within the timeframe, the data is then destroyed. (Kapersky, 2024; Mandiant, 2024).

The use of DDoS attacks by financially motivated threat actors has been prevalent since the late 1990s (Health-ISAC, 2021). However, Ransom Distributed Denial of Service (RDDoS), a variation where DDoS is used in conjunction with ransom demands, started initially in the 1990s but has gained more prominence since 2015 (Health-ISAC, 2021; Imperva, 2024). This approach, often termed multi-extortion ransomware or multifaceted extortion, involves the use of multiple layers of attacks to intensify pressure on victims, compelling them to pay the ransom (PaloAlto Networks). By 2016, the cybercriminal group DDoS for Bitcoin (DD4BC) had attacked over 140 organizations (Imperva, 2024). Since 2020, their attacks have become more advanced, using sophisticated techniques that make them harder to defend against, and they have continued without interruption (Imperva, 2024). To initiate this attack, the attackers send extortion emails to their victim (Health-ISAC, 2021). These attackers then invade the victim's network with unsolicited traffic for a given period (Health-ISAC, 2021). In addition to encrypting files, they also launch a small-scale attack to prove their capability to carry out a larger attack (Health-ISAC, 2021; PaloAlto Networks).

The ransom fee increases with each passing day that the victim refuses to comply (Health-ISAC, 2021). If met with silence, the attackers frequently follow through with prolonged RDDoS attacks, which can last for weeks or even months, severely disrupting the victim's operations (Health-ISAC, 2021). Ransomware gangs have increasingly adopted this technique to boost the likelihood of victims paying the ransom (Health-ISAC, 2021). The attackers target online resources like websites, domain name services, web APIs, and gaming lobbies, aiming to disrupt operations and cause significant damage to the organization's reputation (Checkpoint, 2021).

This paper therefore aims to explore how cybercriminals are increasingly using a combination of DDoS and ransomware attacks to create more complex and damaging cyberattacks. By analyzing these hybrid strategies, the study aims to understand how these attack methods work together, the implications for cybersecurity, and how to defend against such multi-vector assaults.

1.2 Statement of Research problem

As technology evolves, so do the methods of sophisticated cyberattacks (Startup Defense). Recently, we've observed malicious actors employing hybrid attacks, where they combine multiple attack vectors to amplify their impact and inflict greater damage (Startup Defense). This tactic is particularly insidious because it increases pressure on the victim by combining the disruptive force of DDoS attacks with the extortion demands of ransomware, creating a more complex and difficult-to-manage threat (Nangineni & Winterfeld, 2023). The victim not only suffers the damage caused by the ransomware attack but also losses revenue due to the downtime caused by the DDoS attack (Nangineni & Winterfeld, 2023).

While extensive research has been conducted on DDoS and ransomware as individual threats, there is a striking scarcity of literature on the convergence of these attack methods. This research gap leaves organizations exposed to these dangerous hybrid attacks, as traditional defense mechanisms may be inadequate to counteract the compounded risks. Moreover, ransomware gangs have increasingly integrated DDoS tactics to coerce victims into paying ransoms, emphasizing the necessity of understanding the operational interplay between these attacks and their broader cybersecurity implications.

This research seeks to address this critical shortfall by examining the impact of the combined ransomware and DDoS attacks. The study will explore the underlying mechanisms of these hybrid assaults, the challenges they pose to existing cybersecurity frameworks, and the defensive strategies that can be employed to mitigate these multi-vector threats, ultimately contributing to the strengthening of organizational resilience against these emerging dangers.

1.3 Research Questions

1. What are the primary motivations and objectives behind the use of hybrid attack strategies by

cybercriminals, particularly those combining DDoS and ransomware?
2. How do ransomware and DDoS attacks interact in hybrid attack strategies?
3. How effective are current cybersecurity frameworks in defending against hybrid attacks involving both DDoS and ransomware, and where do these frameworks fall short?
4. What are the key challenges faced by organizations when dealing with hybrid attacks, and how do these challenges differ from those encountered with single-vector attacks?
5. What potential defensive strategies and countermeasures can be developed or enhanced to mitigate the risks posed by hybrid attacks combining DDoS and ransomware?

1.4 Aim

This research aims to explore the use of hybrid strategies- DDoS and ransomware attack by cybercriminals, analyzing the tactics, risks and impacts associated with the deadly combination, dissecting how these hybrid assault exploits the current cybersecurity defenses and the strategies that can be used to fight these hybrid attacks.

1.4.1 Objectives

1. To investigate the motivations and objectives driving cybercriminals to adopt hybrid attack strategies, particularly the combination of DDoS and ransomware.
2. To explore the interaction between DDoS and ransomware attacks in hybrid strategies, identifying the specific mechanisms that facilitate their convergence.
3. To identify the limitations of current cybersecurity frameworks in mitigating the compounded risks of hybrid attacks, outlining areas of vulnerability
4. To identify and examine the unique challenges organizations face when responding to hybrid attacks, contrasting these with the challenges posed by single-vector threats.
5. To develop and recommend targeted defense strategies that can effectively counteract the multi-vector nature of the hybrid assault – DDoS and Ransomware attack

1.5 Justification of the Study

Combining a DDoS attack with ransomware amplifies the impact on an organization far beyond what either attack could achieve alone. When a DDoS attack is layered onto an existing ransomware attack, it overwhelms the organization's resources and disrupts their ability to function effectively. This dual assault can paralyze the security team, hampering their ability to manage or even respond to the ransomware threat, and severely impair access to essential systems and data (Nangineni & Winterfeld, 2023). Once the victim's system has been shut down by the DDoS attack, the organization would not be able to respond to the ransomware breach and restore their access (Nangineni & Winterfeld, 2023).

In late March 2022, the FBI alerted the public to the tactics of a ransomware gang targeting critical infrastructure sectors, including financial services, manufacturing, and government (Federal Bureau of Investigation (FBI); Cybersecurity and Infrastructure Security Agency (CISA), 2022). The FBI further noted that the ransomware gangs escalate threats by carrying out distributed denial-of-service (DDoS) attacks during ransom negotiations (Overby, 2022). This announcement emphasizes the evolving tactics of ransomware gangs, who have progressed from merely encrypting company files to incorporating data theft and, more recently, adding DDoS attacks to their arsenal (Overby, 2022). This has resulted into more frequent and diverse ransomware attacks and huge financial loss (Overby, 2022).

According to IBM's Cost of a Data Breach report, this type of attack averaged around $4.62 million in 2021 (IBM, 2024). Unfortunately, the rise in unsecured connected devices has empowered cybercriminals to develop more potent botnet-driven DDoS attacks, with record-breaking traffic volumes reaching 3.47 Tbps (Brent, 2022). Additionally, this attack has a low barrier to entry since DDoS services can be easily purchased on the Dark Web for as little as $20 per month, offering unlimited access to 10Gbps DDoS capacity (Brent, 2022).

Furthermore, as companies improve at preventing encryption-based ransomware attacks through increased investment in cybersecurity measures, DDoS extortion is likely to flourish (Brent, 2022). A

DDoS attack can divert and mislead the incident response team, hampering their ability to address the ongoing threat effectively (Newman, 2021). While the organization is preoccupied with managing the DDoS attack, malicious actors exploit the situation to create a backdoor through ransomware, leading to the encryption or potential exfiltration of sensitive data (Newman, 2021)

According to a poll conducted by cybersecurity researchers at ITProPortal, 56% of respondents indicated that DDoS attacks were used as a smokescreen in incidents where data was lost due to targeted attacks (Brent, 2022). The FBI described this tactic as a method employed by ransomware gangs to pressure their victims into paying the ransom more quickly (Newman, 2021).

These hybrid attacks create distinct challenges for organizations, as the combined pressure of DDoS and ransomware attacks can exceed the current capabilities of incident response teams. This study aims to explore effective strategies for combating these hybrid threats, making significant contributions to cybersecurity by enhancing incident response and risk management practices.

1.6 Definition of Terms

1. Ransomware Attack: This attack involves malware that restricts a user or organization's access to their files or systems, typically by encrypting the data and demanding a ransom for its release (Checkpoint, 2021)
2. Distributed Denial of Service (DDoS) Attack: This is a malicious tactic that aims to overwhelm an organization’s server with excessive internet traffic, thereby disrupting its operations and preventing legitimate access (Fortinet).
3. RDDoS (Ransom Distributed Denial of Service): This is a hybrid attack that combines ransomware and DDoS tactics. Ransomware gangs use it to coerce payment by threatening to launch a DDoS attack, which can cause additional disruption and pressure on the victim (Cloudflare).

II. LITERATURE REVIEW

2.1 Background

This section discusses the techniques and mechanisms associated with the two prevalent multi-vector cyber assaults: DDos and Ransomware attacks, and the holistic impact when combined to launch attacks

2.2 Overview of the DDoS Attack

A DDoS attack is a type of attack where the perpetrators intentionally overwhelm a particular end host within a network with a large amount of traffic, making it unusable to legitimate clients. This is typically accomplished by coordinating botnets, which are clusters of compromised devices that flood the target with excessive traffic. Despite being an older form of cyberattack, the Covid-19 pandemic has led to a resurgence in DDoS activity making it to reemerge stronger than ever – both in terms of number and size of attacks (Overby, 2022). Additionally, advancements in technology have provided attackers with greater resources and new methods to carry out these attacks, causing more damage with less effort (Anshuman & Gupta, 2022).

2.3 Overview of Ransomware

Ransomware is also a form of cyberattack designed to restrict access to critical resources, including files, systems, or entire networks, by encrypting them. Subsequently, the attacker demands a ransom, often in cryptocurrency, in exchange for the decryption key necessary to regain access to the affected resources. Prior to the ransom being paid, the victim experiences an inability to access their data or systems, resulting in significant operational disruptions.

2.4 The Triple Extortion: Its Variance with RDDoS

While Ransomware is the method used by cybercriminals to extort money, DDoS attacks can act as a diversion, redirecting attention away from the ransomware (Brent, 2022). By disrupting an organization's network and causing confusion, attackers can initiate an assault by targeting emails or other methods to encrypt the organization's data. This research specifically focuses on the combination of ransomware and DDoS attacks, a tactic known as triple extortion. While this hybrid cyberattack,

strategy is sometimes called RDDoS, it's important to distinguish the difference in terminology. RDDoS involves using DDoS attacks with a demand for payment to halt the attack, while triple extortion employs two different cyberattacks—DDoS and ransomware attacks—to achieve its objectives. DDoS attacks are resurging and are being used in conjunction with encryption-based ransomware to increase the effectiveness of cyber extortion (Overby, 2022). Thus, ransomware gangs are not only seeking to gain control of users' servers but are also applying sophisticated methods to encrypt data.

2.5 Interaction between Ransomware and DDoS Attacks

The combination of these strategies is aimed at making money, with cybercriminals seeking to do so as quickly as possible. The use of hybrid strategies ensures a high return for them. The triple extortion method mentioned in section 2.4 is becoming more common because it does not require human intervention to execute. Ransomware, which typically relies on unsuspecting victims and phishing emails, becomes even more effective when combined with DDoS attacks. Initially, threat actors carried out ransomware attacks through mass phishing campaigns targeting average users, demanding ransom payments to decrypt their files (NJCCIC, 2024). A common approach involves launching a DDoS attack that disrupts a targeted server. This is followed by sending an email to the affected organization, urging them to click on a link to stop the attack. Clicking on the link further encrypts their data, rendering it inaccessible until a ransom is paid. This scenario illustrates how the triple extortion tactic works, combining DDoS and ransomware attacks. Paying the ransom does not guarantee data recovery, as the data could be corrupted or permanently lost. The best defense is to avoid falling victim to phishing attacks or manipulation tactics, and to implement robust security measures to minimize the impact of successful attacks. This leads us to a discussion of current cybersecurity frameworks that address these cyber-attack methods, as well as their limitations.

2.6 Current Cybersecurity Strategies

Although defense mechanisms have been created to guard against a wide range of cyberattacks, there is a notable lack of specific preventive measures tailored for hybrid attacks. This section will briefly analyze the current mechanisms for individual types of attacks while also providing a comprehensive and thorough overview of the measures implemented for hybrid attacks. Furthermore, it will look into the constraints and inadequacies surrounding these strategies.

2.6.1 Defense Mechanisms Against Ransomware Attacks

Traditional antivirus and antimalware products have improved. However, they still struggle to catch and stop ransomware attacks. Ransomware often succeeds through email, so it's crucial to prioritize email security and provide user training to prevent clicking on harmful links. Preventing ransomware attacks involves using secure websites, unique passwords for all accounts, and implementing defense-in-depth cybersecurity controls such as privilege access control, authentication, authorization, network traffic monitoring, and vulnerability assessments. In the event of an attack, preventive measures can help in recovering data faster, and having data backups, whether in the cloud or on a separate physical device, is essential.

2.6.2 Defense Mechanisms Against DDoS Attacks

When a DDoS attack is detected, there is nothing that can be done except manually fix the problem and disconnect the victim system from the network (Prasad *et al.,* 2014). To defend against DDoS attacks, organizations should implement a multi-layered approach that includes employing traffic filtering and rate limiting, using DDoS protection services, deploying intrusion detection systems, configuring firewalls and routers, preparing a comprehensive incident response plan, and maintaining up-to-date systems and software to ensure robust security and swift mitigation of attacks.

III. METHODOLOGY

To analyze hybrid attack strategies, we employed a mixed-methods approach. We collected data from cyber incident reports, case studies, and simulation tools to identify patterns in the convergence of DDoS and ransomware attacks. Key performance indicators (KPIs) included the time to detect, the magnitude of financial losses, and the speed of recovery. Our

analysis leverages network traffic data, penetration testing, and interviews with cybersecurity experts to evaluate how these hybrid attacks impact organizations.

3.1 Data Collection

Data for this study are collected from multiple sources to ensure a comprehensive analysis of hybrid DDoS and ransomware attacks. The data collection methods include:

3.11 Primary Data

- Expert Interviews: Cybersecurity professionals from various sectors (e.g., finance, healthcare, government) are interviewed to gather insights on the nature of hybrid attacks. These interviews focus on identifying the real-world occurrence of these multivector attacks, how they unfold, and the response strategies employed by organizations.
- Case Studies: Select case studies of hybrid attacks that combined DDoS and ransomware (e.g., the WannaCry ransomware coupled with simultaneous DDoS) are analyzed. The case studies focus on the technical methods used by attackers and the effectiveness of the countermeasures.

3.12 Secondary Data

- Cybersecurity Reports: Data are collected from annual threat reports by cybersecurity firms such as Symantec, Cisco, and Kaspersky. These reports provide quantitative data on the frequency, magnitude, and geographical distribution of both DDoS and ransomware attacks.
- Attack Databases: Open-source cybersecurity databases such as the Cybersecurity and Infrastructure Security Agency (CISA) repository and the MITRE ATT&CK framework are utilized to identify documented hybrid attack strategies.
- Academic and Industry Research Papers: Published studies provide a foundational understanding of the technical components of DDoS and ransomware, as well as hybridization techniques.

3.2 Sample selection

The research focuses on cyber-attacks recorded between 2017 and 2023, as these years saw significant growth in both DDoS and ransomware attacks. Additionally, only attacks targeting critical infrastructure sectors (e.g., finance, energy, healthcare) are considered, as these sectors are frequently targeted by advanced threat actors. The selection of cases for the expert interviews is done purposively, focusing on professionals with direct experience in managing or responding to hybrid cyber-attacks.

3.3 Data Analysis

Data analysis involves a combination of qualitative and quantitative techniques to capture both the technical and strategic elements of hybrid cyber-attacks.

3.31 Qualitative Analysis

Statistical data from cybersecurity reports are analyzed to detect trends in the frequency and distribution of DDoS and ransomware attacks, both individually and as part of hybrid assaults. Quantitative methods include:

- Descriptive Statistics: To summarize the frequency of DDoS and ransomware attacks in different sectors, geographical locations, and time periods.
- Correlation Analysis: To investigate the correlation between DDoS and ransomware incidents, especially in cases where they occur simultaneously or in sequence during a hybrid attack.

3.32 Qualitative Analysis

Thematic analysis is used to extract recurring patterns and themes from expert interviews, case studies, and secondary data. The qualitative analysis focuses on understanding:

- Attack Motivation: Understanding why attackers choose to combine DDoS and ransomware, focusing on whether the goal is financial gain, data theft, or sabotage.
- Techniques and Procedures: Identifying the tactics, techniques, and procedures (TTPs) used to combine DDoS and ransomware, with a focus on the MITRE ATT&CK framework.

- Victim Response Strategies: Analyzing how organizations respond to these hybrid attacks, including the deployment of incident response teams, use of cybersecurity tools, and interaction with law enforcement.

IV. CONVERGENCE OF DDOS AND RANSOMWARE ATTACKS

Strategic Synergy

The combination of DDoS and ransomware attacks exploits the strengths of both methods. While a DDoS attack disrupts the network, ransomware encrypts data, creating a dual-layered assault. This strategy overwhelms defenses, complicates incident response, and increases the likelihood of a successful breach (Micro, 2021)

V. CHALLENGES AND LIMITATIONS

a. CASE STUDIES

Recent incidents highlight the effectiveness of hybrid attacks. For instance, a multi-vector DDoS attack on an AWS customer peaked at 2.3 Tbps, causing massive disruption. Similarly, FlexBooker's AWS servers were compromised in a DDoS attack, resulting in a ransomware attack that exposed 3.7 million records (Report., 2020)

4.12.1 IMPLICATIONS FOR CYBERSECURITY

Increased Complexity

The convergence of DDoS and ransomware attacks adds complexity to cybersecurity defenses. Traditional single-vector defenses are inadequate against these sophisticated assaults, necessitating more comprehensive and adaptive strategies (ENISA., 2021)

Economic and Operational Impact

Hybrid attacks can cause severe financial losses and operational downtime. Businesses, particularly in sectors like healthcare, finance, and government, face heightened risks. The economic impact of these attacks is substantial, with DDoS attacks alone costing US businesses over $10 billion annually (Radware., 2020)

4.3 LIMITATIONS

1. Access to Data: Real-time data on cyber-attacks are often proprietary or confidential, limiting access to certain types of primary data. This research relies heavily on secondary data and expert interviews.
2. Scope of Hybrid Attacks: The research focuses on the convergence of DDoS and ransomware attacks, which may exclude other types of hybrid cyber-attacks (e.g., phishing combined with malware).

The key challenges in dealing with hybrid attacks also include increased complexity, higher resource requirements, coordination and communication difficulties, and more complicated detection and response processes. These challenges differ significantly from those encountered with single-vector attacks, which tend to be more straightforward to manage and recover from.

4.4 MITIGATION STRATEGIES

Proactive Defense Mechanisms

1. Integrated Security Solutions: Deploying multi-layered security solutions that integrate DDoS mitigation and ransomware protection is crucial. This approach ensures comprehensive coverage and quick response to emerging threats (Shackleford, 2021)
2. Anomaly Detection Systems: Utilizing anomaly-based detection systems can identify unusual traffic patterns indicative of multi-vector attacks. These systems help detect and mitigate attacks before they cause significant damage (Scarfone, 2020)
3. Incident Response Planning: Developing robust incident response plans that include procedures for both DDoS and ransomware attacks can minimize downtime and data loss. Regular drills and updates to these plans ensure preparedness (Kelley, 2021)
4. Continuous Monitoring and improvement: Implement continuous monitoring tools to track network traffic, system performance, and security events in real-time. This helps in early detection of potential hybrid attacks and rapid response. (Gartner, 2022)

CONCLUSION

The convergence of DDoS and ransomware attacks represents a significant threat in the cybersecurity environment. The results from the case studies reveal that hybrid attacks increase both the attack surface and the complexity of defense mechanisms. DDoS attacks create noise that prevents cybersecurity teams from detecting ransomware infiltration until it is too late. Our findings indicate that this dual strategy is highly effective in reducing incident response efficiency. The discussion focuses on the failure of traditional security infrastructure to cope with such simultaneous threats and calls for an integrated defense system. Understanding these hybrid strategies and implementing comprehensive defense mechanisms is essential for protecting critical infrastructure and sensitive data. As attackers continue to innovate, so must the defenses against them, ensuring resilience and security in an increasingly digital world.

REFERENCES

[1] Admass, W., Munaye, Y., & Diro, A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2. doi:https://doi.org/10.1016/j.csa.2023.100031

[2] Akhavan-Hejazi, H., & Mohsenian-Rad, H. (2018). Power systems big data analytics: An assessment of paradigm shift barriers and prospects. Energy Systems, 4, 91-100. doi:https://doi.org/10.1016/j.egyr.2017.11.002

[3] Brent. (2022, November 16). DDoS & Ransomware: A Dreadful Combination. Retrieved August 21, 2024, from https://blog.path.net/ddos-ransomware-a-dreadful-combination/

[4] Checkpoint. (2021). The Definitive Guide to Ransom Denial of Service. Retrieved August 20, 2024, from https://www.checkpoint.com/downloads/products/guide-to-ransom-denial-of-service-rdos.pdf

[5] Cloudflare. (n.d.). What is a ransom DDoS attack? Retrieved August 21, 2024, from https://www.cloudflare.com/learning/ddos/ransom-ddos-attack/

[6] Federal Bureau of Investigation (FBI); Cybersecurity and Infrastructure Security Agency (CISA). (2022). Indicators of Compromise Associated with AvosLocker Ransomware. Retrieved August 21, 2024, from https://www.ic3.gov/Media/News/2022/220318.pdf

[7] Fortinet. (n.d.). What Is DDOS Attack? Retrieved August 21, 2024, from https://www.fortinet.com/resources/cyberglossary/ddos-attack

[8] Health-ISAC. (2021). Distributed Denial of Service (DDOS) Attacks. Retrieved August 19, 2024, from https://www.aha.org/system/files/media/file/2021/03/distributed-denial-of-service-ddos-attacks-march-2021.pdf

[9] IBM. (2024). https://www.ibm.com/reports/data-breach. Retrieved August 21, 2024, from https://www.ibm.com/reports/data-breach

[10] Imperva. (2024). Ransom DDoS. Retrieved August 20, 2024, from https://www.imperva.com/learn/ddos/ransom-ddos-rddos/

[11] Kapersky. (2024). What is Ransomware? Retrieved August 19, 2024, from https://www.kaspersky.com/resource-center/threats/ransomware

[12] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7. doi:https://doi.org/10.1016/j.egyr.2021.08.126

[13] Mandiant. (2024). M-Trends 2024 Special Report. Retrieved August 19, 2024, from https://cloud.google.com/security/resources/m-trends?utm_source=ads-in-product&utm_medium=mandiant&utm_campaign=FY24-Q1-global-MAND942-website-dl-dgcsm-m-trends-2024&utm_content=-&utm_term=-

[14] Nangineni, V., & Winterfeld, S. (2023, March 21). Defeating Triple Extortion Ransomware: The Potent Combo of Ransomware and DDoS Attacks. Retrieved from

https://www.akamai.com/blog/security/defeating-triple-extortion-ransomware

[15] Newman, S. (2021, November). HelloKitty Gang Adds DDoS Threat to Ransomware Attacks. Retrieved August 21, 2024, from https://www.corero.com/hellokitty-adds-ddos-threat-ransomware/

[16] Overby, S. (2022). DDoS and Ransomware: A Prevalent and Potent Blend. Retrieved August 21, 2024, from https://www.mimecast.com/blog/ddos-and-ransomware-a-prevalent-and-potent-blend/

[17] PaloAlto Networks. (n.d.). What is Multi-Extortion Ransomware? Retrieved August 21, 2024, from https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware

[18] Singh, A., & Gupta, B. (2022). Distributed Denial of Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions. International Journal on Semantic Web 66, 18(1), 1-43. doi:10.4018/IJSWIS.297143

[19] Startup Defense. (n.d.). How to Protect Against DDoS Attacks. Retrieved August 21, 2024, from https://www.startupdefense.io/how-to/how-to-protect-against-ddos-attacks

[20] Thakur, K., Qiu, M., Gai, K., & Ali, M. (2016). An investigation on cyber security threats and security models. 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC, (pp. 307 - 311). Retrieved from https://ieeexplore.ieee.org/abstract/document/7371499/

[21] Path. (2022). DDoS and Ransomware: A Dreadful Combination Retrieved September 1, 2024, from https://blog.path.net/ddos-ransomware-a-dreadful-combination/