Ransomware

CBER701-Fall2023-Sec002-Group 5

Submitted to: Professor John Tziotzis

CENTENNIAL COLLEGE

Submitted by:

Syed

Kryselle Matienzo

Rashin Ghodrat Zadeh Zeighami

Suhasini Shashi Kumar Manchineela

Ampem Darko

December 8, 2023

Abstract

Ransomware, a malicious software encrypting files with demands for payment, poses a severe threat to individuals, businesses, and governments. This paper delves into common ransomware types, its evolution across generations, and the prevailing encryption schemes. It explores propagation methods and outlines potential responses when attacked. The impact on businesses, exemplified by the WannaCry attack's $4 billion estimate, is discussed alongside notable cases like ExPetr/NotPetya and Black Basta. The WannaCry timeline reveals its global impact, eventual cessation through a domain discovery, and attribution to the Lazarus Group. Technical details on WannaCry's encryption model and communication through the Tor network are provided. Current concerns, such as DeepFake ransomware and remote work vulnerabilities, suggest future research directions. The Toronto Public Library's recent Black Basta incident underscores the ongoing threat.

Contents

List of Figures

List of Tables

1. Introduction

Ransomware is a type of malicious software that encrypts a victim's files. The attackers then demand a ransom from the victim to restore access to the files. This form of cyber threat has become increasingly prevalent, targeting individuals, businesses, and even government institutions. The problem lies in the disruptive and often financially damaging impact ransomware attacks have on various entities.

Understanding and addressing ransomware is crucial due to its widespread and severe consequences. Ransomware attacks not only result in financial losses for victims but also pose a threat to data integrity, privacy, and the functioning of critical systems. As technology continues to advance, combating ransomware becomes essential to safeguarding digital ecosystems and ensuring the trust and security of online activities.

1.1 Common types of ransomware attacks

a. **Locker Ransomware:** Locks victims out of their devices, displaying a ransom note demanding payment to regain access. It targets the operating system, restricting functionality.
b. **Crypto Ransomware:** Encrypts important files, holding them hostage until a ransom is paid for the decryption key. Attackers often provide countdowns and warnings about potential data deletion.
c. **Scareware:** Involves coercing users into downloading software by bombarding them with pop-ups and alarming messages, creating a false sense of urgency.
d. **Leakware (Exfiltration/Doxware):** Threatens to release sensitive data online, aiming to extort money by exploiting individuals or businesses' desire to protect confidential information.
e. **Ransomware-as-a-Service (RaaS):** Operates as a dark web business model, streamlining ransomware attacks by automating various aspects, including deployment, payment collection, and user access restoration.

1.2 Evolution of ransomware

The classification categorizes crypto ransomware based on its propagation capabilities and generation.

Generation I: Early variants of crypto ransomware (before 2013) had limited propagation capabilities. They couldn't efficiently spread on networks and were often confined to a single infected machine. **Examples:** AIDS Information, GPCoder.

Generation II: Emerged in 2013, Generation II crypto ransomware gained the ability to propagate through network paths. It could encrypt devices physically and logically connected to the infected machine, including those with 'write' access to server shares. **Examples:** CryptoLocker, CryptoWall, CryptoDefence.

Generation III.a (Trojans): This type, appearing in 2016, utilizes various tools and exploits network weaknesses for propagation. Generation III.a crypto ransomware can infect entire networks, severely disrupting organizational functions. It often enters via vulnerable servers. **Examples:** Samas, BitPaymer.

Generation III.b (Worms): Emerging in 2017, Generation III.b, also known as 'crypto worms,' exploits software vulnerabilities for propagation. Similar to Trojans, they can infect entire networks, with examples like WannaCry and NotPetya.

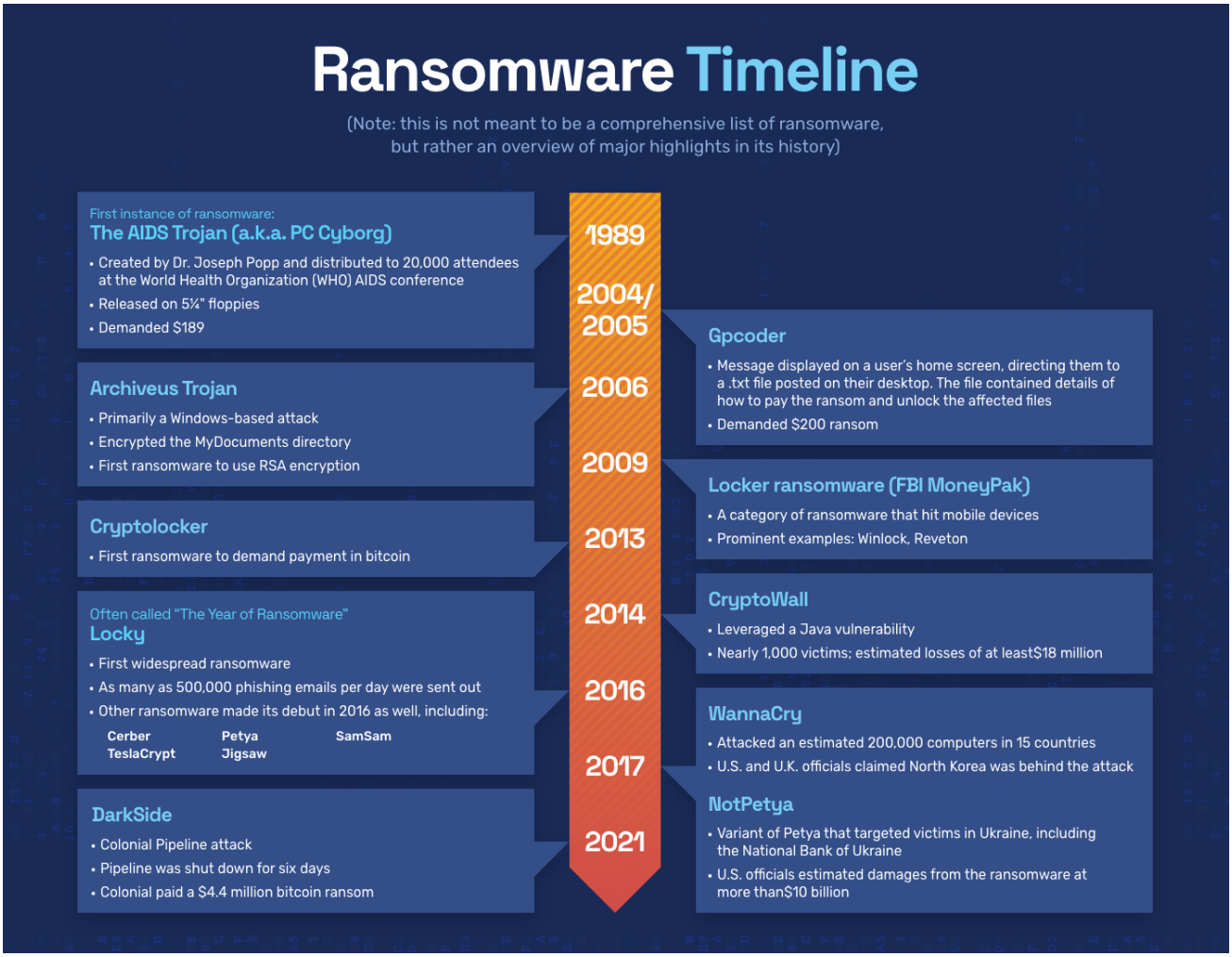

Figure 1 - Evolution of Ransomware

2. Overview of Ransomware

Crypto ransomware typically employs one of three encryption schemes: symmetric, asymmetric, or hybrid. The symmetric approach, embedding the encryption key in the ransomware, is vulnerable to reverse engineering. Asymmetric encryption, though more secure, is slow for larger files. The most effective is hybrid encryption, combining both methods. The ransomware creates a random symmetric key to encrypt files, and a public-private key pair is generated on a

command-and-control (C&C) server. The public key encrypts the symmetric key, with the private key held by the server. After ransom payment, the private key decrypts the symmetric key, recovering the victim's files. Unique key pairs per infection prevent key sharing among victims.

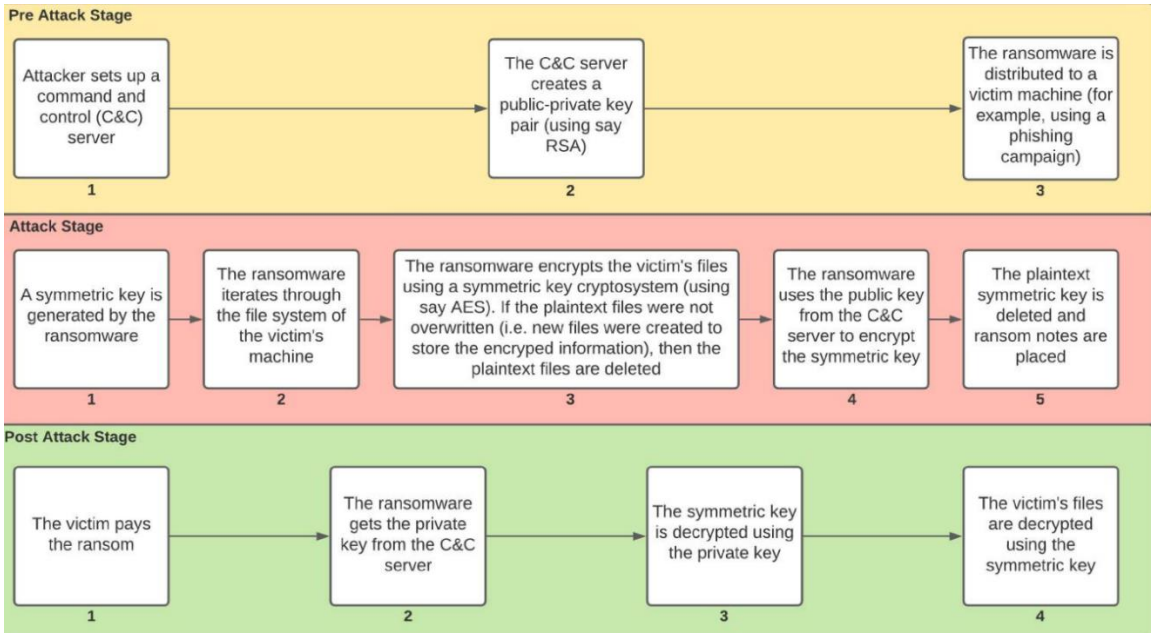

Figure 2 - Hybrid Approach of Ransomware

Table 1- Common ways Ransomware spreads

Method	Description
Email Attachments	Phishing emails use deceptive attachments, posing as legitimate files, to trick users into activating ransomware upon opening
Malicious URLs	Phishing emails redirect users to fake websites, impersonating trusted entities, where unwitting victims input credentials, leading to ransomware attacks.
Remote Desktop Protocol (RDP)	Exploiting RDP vulnerabilities or social engineering, attackers gain remote access, enabling them to implant ransomware through system weaknesses.
Pirated Software	Illegitimate software, often sourced from untrusted platforms, carries malware, and lack of updates heightens susceptibility to ransomware infections.
Removable Devices	Ransomware can spread via infected USB devices strategically placed in public areas, tempting users to plug them in and compromising systems upon file access

When a user's system is infected with ransomware, organizations typically face four primary options:

- **Pay the Ransom:** Some victims may consider paying the ransom to regain access to their files or systems. However, cybersecurity experts and law enforcement agencies discourage this, as there is no guarantee of receiving the decryption key, and paying the ransom supports criminal activities.

- **Restore from Backup:** The safest option is to restore affected files from a backup created before the ransomware infection occurred. Regularly backing up data is crucial to mitigate the impact of ransomware attacks.
- **Lose the Files:** If the user lacks a backup and chooses not to pay the ransom, they may accept the loss of their files. However, this can be a significant setback, especially if the files contain important or irreplaceable data.
- **Brute Force the Key:** Brute forcing a ransomware decryption key involves attempting all combinations, but the process is computationally infeasible due to the key's complexity. With a 617-digit number, it would take about 6.4 quadrillion years on a standard desktop computer to decipher, highlighting the formidable strength of ransomware encryption, making it practically impossible to break within a reasonable timeframe, even with powerful computers.

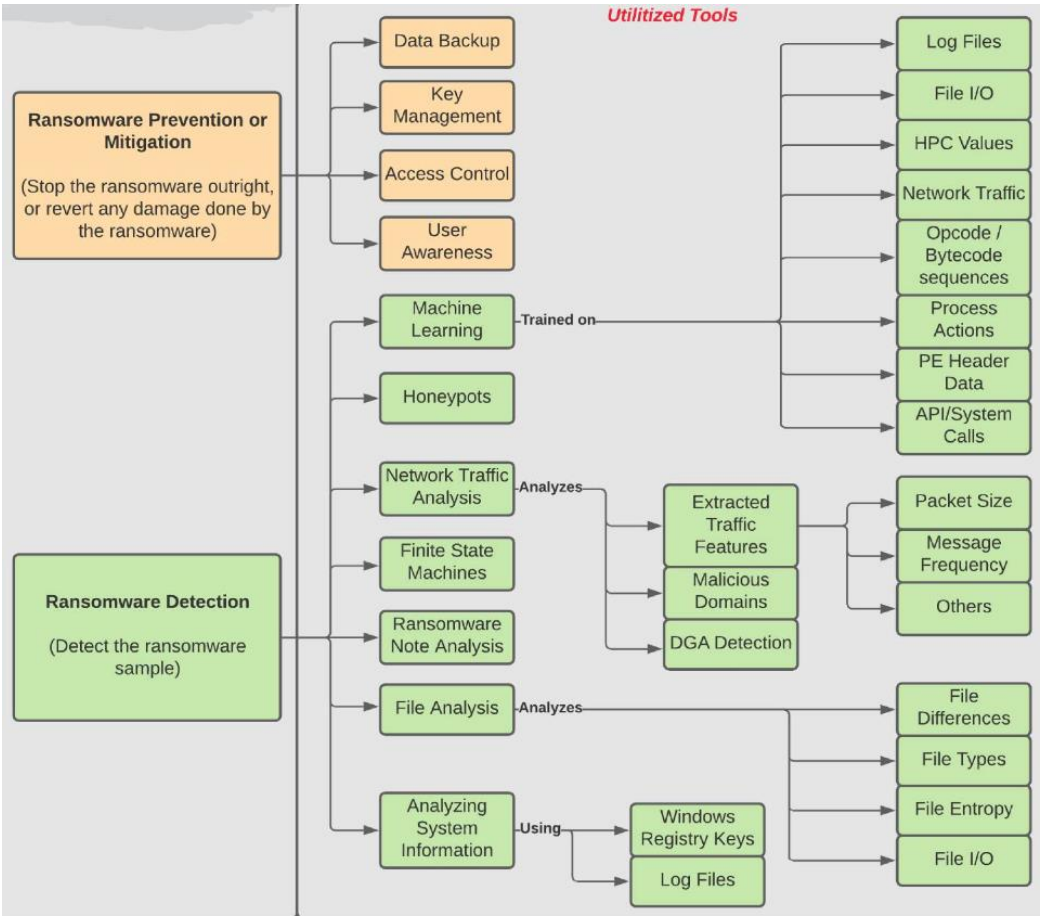

Figure 3 - Ransomware Prevention and Detection

Table 2 - Impact of Ransomware on Businesses

Impact	Description
Extended Downtime	Ransomware often leads to prolonged business disruptions as organizations struggle to restore systems and operations.

Damage to Brand Reputation	Ransomware attacks can tarnish a company's image, eroding customer trust and confidence in the brand.
Sensitive Data Exposure	Businesses may face data breaches and the potential exposure of sensitive information, leading to regulatory and legal consequences
Financial Impact of Ransom Payments	Paying ransoms can impose significant financial burdens on organizations, with no guarantee of recovering encrypted data or preventing future attacks.
Ransomware as a Gateway for Future Attacks	Successful ransomware incidents can make businesses vulnerable to subsequent cyber threats and exploitation by attackers.

3. WannaCry/WannaCrypt

Type of Attack: Ransomware (vulnerability in SMB protocol)
Attackers: Believed to be the Lazarus Group
Target Company: Multiple (global attack); Microsoft Windows users
Monetary Impact: Estimated $4 billion.

The WannaCry ransomware, which emerged in May 2017 and affected nearly 5 million devices by May 2019, targeted Microsoft Windows systems, encrypting data and demanding Bitcoin ransom payments. The WannaCry malware is a crypto ransomware that affected over 200,000 computers globally, employing a computer worm component to spread across the internet in August 2017. Crypto ransomware encrypts user files for extortion, and WannaCry utilizes Bitcoin for anonymous ransom payments to evade law enforcement. It also employed the Tor network for Command-and-control communications, enabling anonymous internet interactions between the malware operator and the malware itself.

3.1 Timeline of WannaCry

- *NSA Discovers SMB Protocol Vulnerability:* The NSA identifies a vulnerability in the SMB protocol and develops the EternalBlue exploit.
- *Shadow Brokers Steal NSA Tools:* In January 2017, the hacking group Shadow Brokers steals NSA tools, including the EternalBlue code.
- *Microsoft Cancels February 2017 Patch Cycle:* Microsoft breaks its usual patch cycle in February 2017.
- *Microsoft Releases SMB Protocol Patch:* On March 14, 2017, Microsoft releases a patch addressing the SMB protocol vulnerability.
- *Shadow Brokers Release Vulnerability:* Shadow Brokers publicly releases the vulnerability on April 14, 2017, one month after the patch, indicating potential communications with Microsoft.
- *WannaCry Outbreak:* WannaCry ransomware spreads globally on May 12, 2017. Malware exploited a vulnerability in the Server Message Block (SMB) protocol, specifically targeting SMB Version 1 and TCP port 445 on Windows systems.

- *Discovery of Kill Switch:* On the same day, a kill switch is discovered, leading to the registration of a domain name to halt the malware's spread.
- *Ransom Money Withdrawal:* On August 2, 2017, the ransom money from three bitcoin accounts is withdrawn, potentially involving a Bitcoin mixer for money laundering.
- *US Government Accuses North Korea:* On December 19, 2017, the US government publicly accuses North Korea of orchestrating the WannaCry attack.
- *US Justice Department Charges Park Jin Hyok:* On September 6, 2018, the US Justice Department charged Park Jin Hyok, believed to be a high-profile member of the Lazarus group, for launching the WannaCry attack.

3.2 How was it stopped?

The WannaCry attack was stopped when a security researcher named Marcus Hutchins discovered an unusual function in the ransomware's code. Before executing, WannaCry would query the domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, which did not exist. Hutchins registered the domain, causing copies of WannaCry to stop executing. This domain query function was likely included in WannaCry to check if it was inside a sandbox, an anti-malware tool. Sandboxes generate fake responses to domain queries, and by sending a query to a hard-coded domain, WannaCry could be tricked into thinking it was in a sandbox and shut down. Another possibility is that the ransomware was unfinished, and the domain was meant to be replaced later. Overall, the registration of the domain disrupted WannaCry's ability to continue spreading and executing.

3.3 How does WannaCry work?

The ransomware utilizes a hybrid cryptographic model, combining asymmetric and symmetric cryptography.

- It has two hardcoded keys: an AES key used to encrypt random files on the victim's desktop, demonstrating the decryption capability, and an RSA public key (Attacker's public key or APU).
- The malware generates a 2048-bit RSA key pair (Victim's key pair or VPU VPR), encrypts the victim's private key (VPR) with the attacker's public key (APU), and stores it as 00000000.pky, destroying the original VPR.
- Unique AES keys are generated for each file, used to encrypt the victim's files.
- The ransomware then encrypts all AES keys using the VPU and appends ".WNCRYT" extension to each file before wiping the originals.

To decrypt files, one needs the attacker's private key (APR) to decrypt VPR, VPR to decrypt AES keys, and AES to decrypt the files. Since the attacker's private key is unknown, the only way to decrypt files is to request the attackers to decrypt the victim's private key.

WannaCry employs the Tor network for its Command and Control (C&C) communications, attempting connections to hardcoded IP addresses associated with Tor Hidden Services. Tor Hidden Services are websites accessible only through the Tor network, operated by anonymous

individuals. The communication occurs over port numbers 443 and 9001. The C&C's purpose is to enable attackers to gather basic information about victims, such as the number of infected computers and their IP addresses, facilitating the measurement of the attack's impact.

Figure 4 - WannaCry extrotion message

3.4 Other famous ransomware

June 2017: ExPetr / NotPetya

Type of Attack: Ransomware (A wiper exploiting an SMB vulnerability)
Attackers: Likely Russian-sponsored threat actors
Target Company: Various, but severely impacted Maersk and Merck
Monetary Impact: Estimated $10 billion

The NotPetya variant, although categorized as ransomware, primarily acts as wiperware with a focus on file destruction instead of monetary gain. Similar to its predecessor Petya, NotPetya encrypts the Master Boot Record (MBR) and Master File Table (MFT). Unlike Petya, after encryption, it destroys the device's content. Even if victims pay the ransom, they never get their files back.

October 2023: Black Basta Ransomware

Type of Attack: Ransomware
Attackers: Black Basta Group
Target Company: Toronto Public Library
Monetary Impact: Investigation ongoing

The Black Basta ransomware, operating since April 2022, employs a double extortion tactic by encrypting data and threatening to publish it unless a ransom is paid. Primarily targeting large organizations in the US, Canada, the UK, Australia, and New Zealand, the group uses a highly targeted approach, avoiding a spray-and-pray method. The ransomware is written in C++, impacting both Windows and Linux systems, utilizing AES and RSA encryption algorithms. It encrypts data in chunks to speed up the process and is distributed through exploits, RDP brute forcing, and phishing emails.

Figure 5 - Black Basta displays a ransomware note as the victim's wallpaper directing them to a .txt file with more details

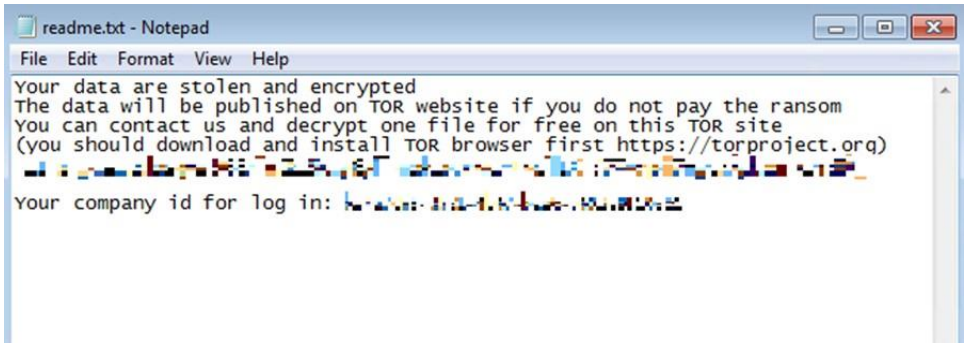

Figure 6 - An example of the contents of the ransom note .txt file

The Toronto Public Library (TPL) Canada's largest public library system confirmed that data was stolen in a recent Black Basta ransomware attack on October 27th, 2023.

4. Future research directions:

1. **DeepFake Ransomware:** Anticipating the potential rise of DeepFake-based ransomware, where attackers generate manipulated content of victims engaging in false or incriminatory actions. Mitigating such attacks poses challenges due to the rapid dissemination of content through various social media channels.
2. **Remote Working Vulnerabilities:** With the increased prevalence of remote work and BYOD policies, there is a need to address vulnerabilities exploited during the COVID-19 pandemic. Research should focus on mitigating ransomware attacks that saw a 72 percent growth during this period.

3. **Blockchain-based Countermeasures:** Exploring the use of blockchain, an immutable decentralized ledger, as a countermeasure against ransomware attacks. The decentralized nature, linked hash function, timestamp function, and consensus mechanism of blockchain offer potential.

5. Conclusion

In conclusion, the escalating threat of ransomware demands a comprehensive understanding of its types, evolution, and encryption mechanisms. The impact on businesses, exemplified by notorious cases like WannaCry, ExPetr/NotPetya, and the recent Black Basta attack on the Toronto Public Library, underscores the financial, reputational, and operational risks associated with these cyber incidents. The evolving nature of ransomware, evidenced by its generational progression and adaptation to new vulnerabilities, necessitates continual vigilance and proactive cybersecurity measures.

The WannaCry case, with its global reach and eventual disruption through a unique domain discovery, serves as a stark reminder of the need for robust cybersecurity practices. As businesses grapple with the consequences of extended downtime, compromised data integrity, and financial burdens from ransom payments, the importance of preventive strategies, including regular data backups and employee training, cannot be overstated.

Looking ahead, emerging threats like DeepFake ransomware and vulnerabilities associated with remote work during the COVID-19 pandemic highlight the dynamic landscape of cybersecurity challenges. The potential role of blockchain-based countermeasures offers a promising avenue for research and development in fortifying digital ecosystems against ransomware attacks. Ultimately, a collaborative effort involving technological advancements, regulatory frameworks, and user awareness is crucial to effectively combatting the persistent and evolving threat of ransomware in our increasingly digitalized world.

References

202303151200 Black Basta Threat Profile tlpclear - hhs.gov. (n.d.-a). https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf

Alraddadi, W., & Sarvotham, H. (n.d.). A comprehensive analysis of WannaCry: Technical analysis ... - people. https://people-ece.vse.gmu.edu/coursewebpages/ECE/ECE646/F20/project/F18_presentations/Session_III/Session_III_Report_3.pdf

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021, December). *Ransomware: Recent advances, analysis, challenges and future research directions*. Computers & security. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8463105/

The history of Ransomware? understand: Prevent: Recover. Ransomware.org. (2023, May 8). https://ransomware.org/what-is-ransomware/the-history-of-ransomware/

Kaspersky. (2023, July 6). *What is WannaCry ransomware?*. www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

What was the WannaCry ransomware attack? | cloudflare. (n.d.-b). https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/