Technical Report 2024-09-03
Internetworking and Media Communications Research Laboratories
Department of Computer Science, Kent State University
http://medianet.kent.edu/technicalreports.html

Ransomware Modelling: Attack Process Reference Modeling On Petri-Net (Part-III)

Javed I. Khan & Fred Kembamba
e-mail: Javed@ kent.edu | fkembamb@ kent.edu

CARE Lab
Internetworking and Media Communications Research Laboratories
Department of Computer Science

Kent State University
233 MSB, Kent, OH 44242
September 2024

Abstract

Ransomware attacks pose an escalating threat to organizations across industries, with the potential to severely disrupt operations, encrypt critical data, and demand ransom for restoration. These attacks often leave long-lasting impacts on affected entities. This technical report provides an in-depth examination of the ransomware attack lifecycle, detailing the stages attackers follow, from system infiltration to ransomware deployment and execution. By breaking down each phase of the attack, this paper offers a comprehensive step-by-step design of the methods used by cybercriminals, providing valuable insights into the strategies needed for effective defense. It uses petri-NET to describe the process.

1. Key Words

Ransomware, Cybersecurity, Markov Chain, Network Architecture, System Vulnerabilities, Attack Modeling, Probabilistic Analysis, Defense Strategies.

2. Introduction

Ransomware, one of the most pervasive and destructive types of cyberattacks, continues to evolve in both sophistication and scope. Modern ransomware attacks are no longer confined to small-scale incidents; they now pose significant threats to enterprises, critical infrastructure, and even governmental bodies. These attacks have been characterized by their ability to cripple operations, extort significant sums of money, and cause irreversible damage to both data integrity and organizational trust.

To effectively mitigate such threats, understanding the structure and phases of a ransomware attack is paramount. Ransomware Attack Modeling is an analytical approach that helps security professionals, organizations, and researchers identify, simulate, and anticipate the various stages of a ransomware attack. This modeling provides a detailed, step-by-step representation of the progression of an attack, from the initial infiltration of a network to the final deployment of the ransomware payload and the subsequent ransom demand.

Before conducting the analysis, several components are required: (a) a scenario of an institutional network model, along with the key computing systems involved in both the attack and defense, (b) a list of common vulnerabilities, safety measures, and their relationships in the various systems that play a role in the attack, and (c) the common steps used in a typical ransomware attack. This technical report presents component (c), while the remaining items are covered in associated technical reports [1] and [2]. These reports are not specific to any particular analysis. Any researcher can use these reference models for their analysis.

3. Formal Problem definition

The core problem addressed in this study is to present the steps involved in a ransomware attack, focusing on how attackers progress through different stages of the attack process. The ransomware lifecycle typically includes phases such as reconnaissance, phishing, initial compromise, lateral movement, data encryption, and ransom demands. By outlining these stages, we aim to highlight critical points where defenses can be strengthened to prevent the attack from advancing.

Ransomware attacks exploit system vulnerabilities, often taking advantage of poor adherence to cybersecurity best practices. This study addresses two primary challenges: first, understanding the sequence of actions attackers follow during a ransomware attack, and second, assessing how well safety practices can prevent or mitigate the attack at various stages.

The goal is to provide a detailed model that evaluates the resilience of a system against ransomware by analyzing how effective security measures can disrupt or prevent each step of the attack process. This study focuses on the stages leading up to the ransomware deployment and ransom demand, rather than the execution or spread of ransomware itself.

4. SOLUTIONS

The complexity of ransomware attacks necessitates a structured reference model that captures the full lifecycle of an attack. By examining key stages such as reconnaissance, initial compromise, lateral movement, data encryption, and ransom demands, this reference model provides a foundation for analyzing how ransomware attacks unfold and progress. It serves as a crucial tool for identifying intervention points where defensive measures can be applied to disrupt the attack.

This reference model encapsulates the entire ransomware lifecycle, offering cybersecurity professionals a systematic way to understand each stage. It enables experts to simulate attack sequences in controlled environments, providing valuable insights into both prevention and mitigation strategies. By applying this model during real-world analysis, organizations can better prepare for potential threats, fortify their defenses, and minimize the risk of an attack progressing to its final stages.

The model serves as a baseline for future, more detailed analysis, including simulations and probabilistic evaluations, and helps in identifying critical vulnerabilities where proactive safety measures can be deployed effectively.

5. Methodology

This section is about a detailed analysis of the various phases involved in ransomware attacks, starting from early reconnaissance and phishing attempts to later stages like lateral movement within networks and the deployment of ransomware. The methodology focuses on demonstrating how systematic application of preventive and reactive safety practices can significantly increase system resilience during such attacks. By utilizing Markov Chain modeling, the methodology provides a robust framework to simulate and understand the dynamic progression of ransomware attacks. This approach helps to identify critical vulnerabilities and offers insights into strengthening organizational defenses against these evolving cyber threats.

5.1. SYSTEM INFILTRATION ATTACK

5.1.1. System Reconnaissance:

System reconnaissance is often the initial phase undertaken by an attacker before launching an actual attack. This reconnaissance process involves analyzing and identifying a target system for potential vulnerabilities. To accomplish this, attackers typically leverage various tools commonly employed by legal penetration testers, such as Nmap, Shodan, and Maltego, among others. These tools aid in vulnerability scanning, enabling the identification of weaknesses within the system's defenses. The reconnaissance effort extends to scanning the target system to uncover open ports, ascertain installed services, determine the hosting operating system, and pinpoint potential vulnerabilities.

In some cases, attackers may resort to social engineering tactics to gather additional information that could aid in the decision-making process regarding whether to proceed with the attack. Furthermore, attackers may scour online sources to gather valuable intelligence that could provide insight into the target system's infrastructure and potential weak points. This comprehensive reconnaissance phase lays the groundwork for subsequent stages of the attack, allowing attackers to devise more informed and targeted strategies.

The success of this attack stage is made possible by the existence of many vulnerabilities, some of which include uncontrolled open ports, lack of port scan security, and exposure of the organization’s crucial information. Ultimately, the goal of this reconnaissance phase is to collect enough information to facilitate the attacker in launching a successful attack.

5.1.2. Send Phishing Attack:

Phishing attacks capitalize on the wealth of information gathered during the reconnaissance phase, particularly the collection of emails and identification of potential system vulnerabilities. Armed with this data, attackers craft tailored emails designed to deceive recipients into downloading and installing malicious payloads. These phishing emails are carefully crafted to appear legitimate, often impersonating trusted entities such as financial institutions, government agencies, or well-known companies.

The success of a phishing campaign hinges on the manipulation of human psychology and the exploitation of trust. Attackers employ various tactics to entice recipients to take the desired action, such as clicking on malicious links or downloading attachments. Once the recipient interacts with the phishing email and executes the payload, the attacker gains unauthorized access to the victim's system, enabling further exploitation and potential compromise of sensitive data.

Phishing attacks are a potent threat to organizations and individuals, as they exploit the weakest link in the security chain: human behavior. It is crucial for organizations to implement robust security awareness training programs and deploy technologies capable of detecting and mitigating phishing attempts. Additionally, users must remain vigilant and exercise caution when interacting with unsolicited emails or suspicious attachments to avoid falling victim to phishing scams.

5.1.3. Successful Phishing Attack:

If the recipients fall for the phishing attack and interact with the malicious content, the attackers exploit this trust to facilitate the unwitting download and execution of malware.

Once the malware infiltrates the target system, it establishes a foothold within the network, granting attackers the opportunity to execute a range of malicious activities. The success of malware installation hinges on the effectiveness of the phishing attack in acquiring access credentials or sensitive information, as well as the attackers' ability to deploy and execute malware without detection.

Upon clicking the download link, the malware activates Sysinternal tools, enabling remote access for the attackers and providing a backdoor into the system. Additionally, another payload, LaZagne malware, is deployed and executed to recover passwords stored on the local computer, further enhancing the attackers' ability to escalate privileges and access sensitive information.

5.1.4. Check the Type of Computing System:

Upon successful compromise, the attacker checks the type of computing system they have infiltrated. A key objective during this phase is to ascertain the presence of Active Directory (AD) as the centralized authentication and authorization mechanism. Recognizing AD's pivotal role in network infrastructure, the attacker gains crucial insights into potential attack vectors and systems hosting valuable data. To facilitate this reconnaissance endeavor, the attacker deploys BloodHound, a legitimate tool designed for AD analysis, onto the compromised system. Leveraging BloodHound's capabilities, the attacker conducts thorough analysis of AD configurations, user permissions, group memberships, and trust relationships. This comprehensive assessment enables the attacker to map out the network topology, identify privileged accounts, and pinpoint critical assets within the AD environment. By meticulously analyzing the information gathered through BloodHound, the attacker lays the foundation for subsequent stages of the attack, armed with valuable intelligence necessary for devising targeted and effective strategies. This phase of computer identification empowers the attacker to further exploit vulnerabilities within the AD infrastructure and potentially compromise sensitive data with precision and efficiency.

5.1.5. Perform Security Evasion:

In security evasion, the attacker employs a sophisticated method to bypass detection mechanisms and execute malicious code within the target system. By meticulously identifying a legitimate process, the attacker covertly injects the malicious code, typically in the form of a Dynamic Link Library (DLL), into the target space. This technique allows the attacker to camouflage the malicious activity within a seemingly benign process, thereby evading detection by traditional security measures. By leveraging this method, the attacker can execute a wide range of malicious activities, including data exfiltration, privilege escalation, and remote access, while remaining undetected by antivirus software and intrusion detection systems. This evasion tactic underscores the importance of implementing advanced threat detection and response mechanisms, such as behavior-based anomaly detection and endpoint monitoring, to detect and mitigate sophisticated attacks aimed at compromising system integrity and confidentiality.

5.1.6. Credential Extraction:

In the credential extraction attack phase, the attacker exploits vulnerabilities uncovered in preceding stages to infiltrate other computers within the network. Leveraging legitimate tools like LaZagne and additional malware such as keyloggers, the attacker initiates password recovery processes on compromised systems to extract stored credentials. LaZagne, a versatile password retrieval tool, enables the attacker to recover passwords stored on the local computer, providing access to a wealth of sensitive information.

In parallel, the attacker deploys keyloggers on compromised systems to capture keystrokes and log user activities. Keyloggers silently monitor user input, recording keystrokes, login credentials, and other sensitive information entered by unsuspecting users. By complementing LaZagne's capabilities with keylogging functionality, the attacker gains a comprehensive means of capturing passwords and other credentials, even those that may not be stored locally.

The successful deployment of both LaZagne and keyloggers underscores the sophistication of the attack and the attacker's determination to gather valuable credentials for further exploitation. Organizations must implement robust security measures, including regular malware scans and intrusion detection systems, to detect and mitigate such multifaceted attacks effectively.

5.1.7. Lateral Movement:

In the lateral movement attack phase, the attacker capitalizes on the vulnerability created in previous stages to extend their reach within the network. Leveraging the compromised system's access, the attacker seeks to infiltrate other computers across the network. Initially, they utilize the credentials obtained from the compromised system to attempt access to additional computers within the network. By leveraging these credentials, the attacker aims to escalate privileges on other systems, exploiting any weaknesses in their security defenses. Additionally, the attacker may resort to brute-force attacks or social engineering tactics to gain unauthorized access to other computers. Through these methods, the attacker seeks to expand their foothold within the network, moving laterally from one system to another. This lateral movement strategy allows the attacker to explore and exploit various network resources, potentially compromising critical assets and escalating the overall impact of the attack.

5.1.8. Sell the Compromised System:

In some cases, rather than immediately deploying ransomware or directly monetizing the compromised system, the attacker may choose to sell access to the compromised system or network to other malicious actors on underground forums or dark web marketplaces. This allows other attackers to exploit the compromised system for their own malicious purposes, such as launching additional attacks, stealing data, or conducting espionage.

The first phase of ransomware attack modeling provides insights into the initial steps and processes involved in the attacker's journey, from reconnaissance and phishing to successful compromise, security evasion, and lateral movement within the target environment. Understanding these phases is critical for developing effective defense strategies and mitigating the risk of ransomware attacks.

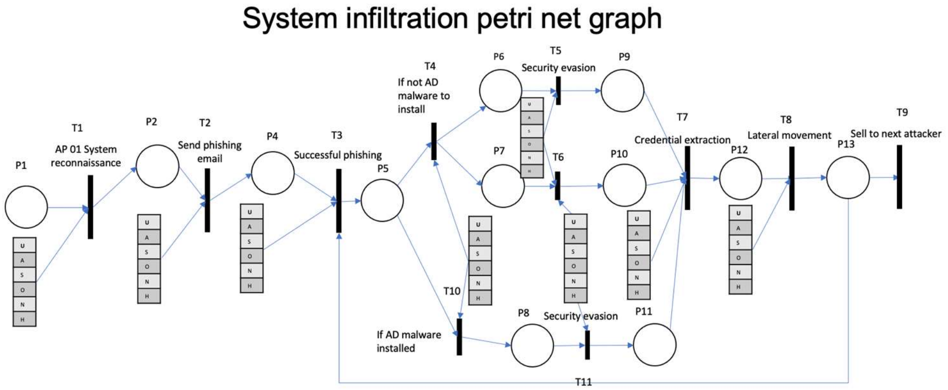

Fig 1 System infiltration petri net graph

The next phases of the ransomware attack model involve the deployment of ransomware and subsequent actions taken by the attacker:

5.2. Ransomware Deployment Stage

5.2.1. Data Reconnaissance:

After gaining initial access and establishing a foothold within the target environment, the attacker conducts data reconnaissance to identify valuable or sensitive data stored on compromised systems. This may involve scanning file systems, databases, or other data repositories to locate files containing personally identifiable information (PII), financial records, intellectual property, or other valuable assets.

5.2.2. Identify Target Systems:

The attacker identifies target systems or computers within the network that contain valuable or critical data. This may include servers hosting databases, file shares containing sensitive documents, or workstations used by key personnel. By prioritizing target systems, the attacker can maximize the impact of the ransomware attack and increase the likelihood of extorting a ransom payment from the victim organization.

5.2.3. Harden Vulnerabilities:

To harden the vulnerability and fortify their access to the compromised system, the attacker undertakes a series of strategic activities. Firstly, the attacker enables SSH (Secure Shell) for remote access, granting them persistent access to the system for executing commands and transferring files remotely. This serves as a critical component of their backdoor access strategy, ensuring continued access to the compromised system even after initial infiltration. Additionally, the attacker creates a backdoor, establishing a covert entry point into the system that bypasses normal authentication mechanisms. By embedding this backdoor, the attacker can stealthily access the system at will, evading detection and maintaining a foothold for future exploitation. To further enhance their stealth and evade detection, the attacker implements sophisticated security evasion techniques. These techniques may include obfuscation, polymorphism, or encryption of malicious code to evade detection by antivirus software and intrusion detection systems. By employing these evasion tactics, the attacker aims to conceal their presence, prolong their access, and maximize the effectiveness of their malicious activities. Collectively, these measures bolster the attacker's control over the compromised system, enabling them to persistently exploit the vulnerability while minimizing the risk of detection or mitigation by defenders.

5.2.4. Deploy Ransomware:

In the ransomware deployment phase, the attacker leverages the vulnerabilities identified and exploited in previous stages, including the process of increasing system weaknesses and creating a backdoor for future access. With the target systems compromised and access secured, the attacker proceeds to deploy ransomware across the network, spanning from System #1 to #12. This deployment is carefully orchestrated, with the attacker waiting for the opportune moment to initiate the ransomware payload. Once activated, the ransomware swiftly encrypts critical files and directories on the compromised systems, rendering them inaccessible to legitimate users. The success of this phase relies on the attacker's ability to infiltrate the target systems undetected and deploy the ransomware payload effectively, establishing a foothold for subsequent malicious activities.

5.2.5. Sell to the Next Attacker:

In some cases, rather than directly monetizing the ransomware attack by extorting a ransom payment from the victim organization, the attacker may choose to sell access to the compromised systems or network to other malicious actors on underground forums or dark web marketplaces. This allows other attackers to leverage the compromised infrastructure for their own malicious purposes, such as launching additional attacks, stealing data, or conducting espionage.

The deployment of ransomware and subsequent actions taken by the attacker represents a critical phase in the ransomware attack lifecycle.

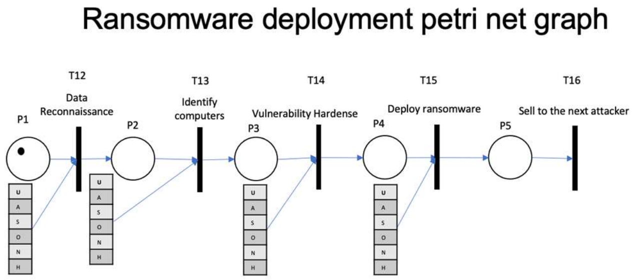

Fig 2 Ransomware deployment petri net graph

5.3. RANSOMWARE EXECUTION STAGE

5.3.1. Exfiltrate Data

In the data exfiltration phase, the attacker strategically targets specific systems within the network, namely System #04, #06, #07, #08, and #10, for the purpose of extracting sensitive data. Leveraging the compromised systems, the attacker initiates the exfiltration process to copy data from these identified sources to their own computers, employing the Megasync tool for efficient data transfer. This tool allows for seamless synchronization of files between the compromised systems and the attacker's computers, enabling the swift and covert extraction of valuable information. By selectively targeting these systems and utilizing Megasync, the attacker aims to circumvent detection mechanisms and successfully exfiltrate data without raising suspicion. This phase underscores the importance of robust data protection measures and continuous monitoring to detect and mitigate unauthorized data access and transfer within organizational networks.

5.3.2. Business Reconnaissance

In the business reconnaissance attack path, the attacker conducts a meticulous analysis of the data exfiltrated from the compromised systems to inform their approach for orchestrating a ransomware attack. By scrutinizing the exfiltrated data, the attacker gains valuable insights into the organization's operations, sensitive information, and potential areas of vulnerability. This reconnaissance effort allows the attacker to assess the criticality of the data, identify high-value assets, and understand the potential impact of a ransomware attack on the organization's operations and reputation. Based on the findings from the business reconnaissance phase, the attacker formulates a comprehensive attack plan, outlining the specific targets, timing, and methods for launching the ransomware attack. This attack plan serves as a strategic roadmap for the attacker, guiding their actions and ensuring maximum impact and effectiveness in achieving their malicious objectives. Ultimately, the business reconnaissance phase plays a crucial role in the attacker's decision-making process, enabling them to tailor their ransomware attack to maximize disruption, financial gain, or other nefarious goals.

5.3.3. Check Up Exfiltration

Once data exfiltration is attempted, the attacker will verify whether the exfiltration was successful. If the attacker detects any issues—such as incomplete transfers or disrupted connections—they will attempt the exfiltration process again until it succeeds. This step ensures that the attacker has a significant amount of valuable data in hand, which can later be used to exert more pressure on the victim to pay the ransom by threatening to release sensitive information publicly.

5.3.4. Delete Database

In the "Delete Database Backup" attack path, the attacker's objective is to sabotage data recovery efforts by targeting and deleting database backups. This action is intended to make it significantly more challenging for the organization to recover from potential data loss or system compromise incidents.

To execute this attack, the attacker first identifies the location of the database backups within the organization's network infrastructure. This may involve reconnaissance activities to locate backup repositories, identify backup schedules, and ascertain access controls governing backup files.

Once the database backup files are located, the attacker gains unauthorized access to the backup storage systems or directories. This may involve exploiting vulnerabilities in backup server software, leveraging stolen credentials obtained through previous attacks, or employing social engineering tactics to trick authorized users into granting access.

With access to the backup files, the attacker proceeds to delete or corrupt the data stored in the backup repositories. This may involve overwriting backup files with random data, deleting backup snapshots, or executing commands to remove backup files from storage devices.

By deleting database backups, the attacker aims to undermine the organization's ability to restore critical data in the event of a security incident or data loss event. This can have severe consequences for the organization, potentially leading to extended downtime, loss of important data, and financial losses.

The success of this attack path hinges on the attacker's ability to gain unauthorized access to backup systems, identify and delete backup files without detection, and evade detection by security monitoring mechanisms. Organizations must implement robust access controls, encryption mechanisms, and backup integrity checks to mitigate the risk posed by such attacks and ensure the resilience of their data backup and recovery processes.

5.3.5. Set Up Payment Method

Before the ransomware is fully launched, the attacker sets up a payment channel, usually in the form of cryptocurrency wallets (e.g., Bitcoin or Monero), which provide anonymity for financial transactions. This step ensures that when the ransom demand is made, the victim has a clear and secure way to transfer the funds. The payment method setup is crucial to ensuring the attacker receives the ransom while maintaining their anonymity and avoiding law enforcement detection.

5.3.6. Erase Remaining Traces

In the "Erase Trace" attack path, the attacker's objective is to eliminate any remaining traces of their presence within the compromised systems and network environment. This activity is crucial for covering their tracks and evading detection by security personnel or forensic investigators. To accomplish this goal, the attacker employs various techniques and tools designed to erase digital footprints, logs, and other artifacts that could reveal their activities. This may include deleting log files, wiping system logs, clearing event logs, and removing any forensic evidence left behind during the intrusion.

Additionally, the attacker may attempt to disable or circumvent security monitoring and logging mechanisms to prevent the detection of their actions. This may involve tampering with intrusion detection systems, firewall logs, and security event monitoring tools to avoid triggering alerts or notifications. Furthermore, the attacker may leverage privileged access obtained during earlier stages of the attack to manipulate system configurations, modify access controls, and cover their tracks more effectively. This could involve altering file timestamps, modifying registry entries, and deleting incriminating files or directories.

By erasing traces of their presence, the attacker aims to thwart any forensic investigation attempts and evade attribution by concealing their identity and activities. This increases the difficulty for incident responders and forensic analysts to reconstruct the attack timeline, identify the attacker's tactics, techniques, and procedures (TTPs), and attribute the intrusion to a specific threat actor or group. Organizations must implement comprehensive logging and monitoring solutions, conduct regular security audits, and employ proactive threat hunting techniques to detect and respond to malicious activity effectively. Additionally, implementing strong access controls, enforcing the principle of least privilege, and deploying endpoint detection and response (EDR) solutions can help mitigate the risk posed by attackers attempting to erase traces of their presence.

5.3.7. Launch Ransomware

This is the moment when the ransomware itself is deployed, encrypting data across the victim's network. Files, databases, and other critical systems are locked behind strong encryption algorithms, rendering them inaccessible to the victim. The ransomware may spread laterally through the network, affecting not only the initial target but also connected devices and systems. The encryption of data is the core of the ransomware attack, ensuring that the victim is crippled and must consider paying the ransom to regain access.

5.3.8. Announce Ransomware

After the ransomware is launched, the attacker formally announces the attack to the victim. This typically occurs via a ransom note displayed on the victim's computer screens or sent via email. The note includes instructions on how to pay the ransom, often along with threats of data deletion or exposure if the ransom is not paid within a specific time frame. The announcement marks the beginning of the negotiation phase, where the victim must decide whether to meet the attacker's demands or attempt alternative recovery methods.

5.3.9. Remote DB Backup

If the victim has a remote backup system in place, they may attempt to restore their data from these backups instead of paying the ransom. The effectiveness of this step depends on the attacker's ability to disable or corrupt the victim's backup systems. If the backups are intact and usable, the victim may be able to reset their system and recover from the attack without meeting the ransom demands, rendering the attack unsuccessful for the attacker.

5.3.10. Attacker Proves Ransomware Seriousness

If the victim attempts to restore from backups or refuses to pay the ransom, the attacker may take additional steps to demonstrate their control and the seriousness of their threats. This could involve releasing small portions of stolen data publicly, deleting files irreversibly, or escalating the ransom demand. The goal is to convince the victim that paying the ransom is the only viable option to avoid further damage or data exposure.

5.3.11. Pay Ransomware (If paid)

If the victim decides to comply with the attacker's demands and pays the ransom, the attacker typically provides decryption keys or recovery tools. The payment is usually made through an anonymous method like cryptocurrency to ensure the attacker cannot be traced. Once payment is confirmed, the attacker sends instructions on how to decrypt the files or recover access to the encrypted systems. This step is the resolution of the attack if the victim opts to meet the ransom demand.

5.3.12. Provide Decryption and Recovery Tools

After the ransom is paid, the attacker provides the necessary tools or keys to decrypt the victim's data and restore normal operations. The process of decryption may vary depending on the complexity of the ransomware and the specific conditions set by the attacker. While some attackers honor their word and release the decryption tools, others may not, leaving the victim without a way to recover their data even after payment.

5.3.13. Pay Ransomware (If Not Paid)

If the victim refuses to pay the ransom, the attacker may leave the encrypted data as-is or take further punitive measures. In some cases, the attacker will delete the encrypted data altogether, making recovery impossible without backups. In other scenarios, the attacker may simply move on, leaving the victim with encrypted data that can no longer be accessed, thus paralyzing business operations indefinitely.

5.3.14. Delete/Keep It As Is

In the case where the ransom remains unpaid, the attacker has a final decision to make. They can either delete the encrypted data to cause maximum damage to the victim, or they can leave it encrypted and move on to the next target. Some attackers may keep the data encrypted indefinitely, providing no way for the victim to recover their files, while others may eventually release the decryption key after a certain period as part of a strategy to show future victims that paying the ransom is essential.

5.3.15. Ransomware Phase 2

In more sophisticated attacks, there may be a second phase to the ransomware campaign. This could involve re-infecting the victim's systems after they have started recovering, or launching a new wave of encryption that targets additional areas of the network. Phase 2 attacks are often designed to exploit weaknesses in the victim's recovery efforts, catching them off-guard after they believe the worst is over. This phase demonstrates how relentless some attackers can be, especially if they perceive that more damage or ransom can be extracted.

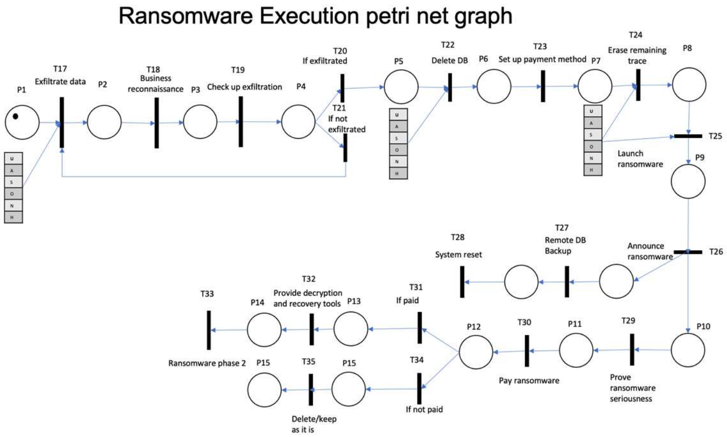

Fig 3 Ransomware Execution petri net graph

6. Conclusion

This technical report provides a comprehensive breakdown of the ransomware attack lifecycle, illustrating how attackers can exploit system vulnerabilities through a series of deliberate and coordinated steps. By understanding each phase of a ransomware attack, beginning with system reconnaissance and concluding with ransom demands; organizations can better prepare and fortify their defenses. The reference model outlined here serves as a critical tool for cybersecurity professionals, enabling a clearer understanding of how attacks progress and identifying crucial intervention points.

This technical report emphasizes the importance of structured defensive strategies and the need for robust safety practices to mitigate risks at each stage of the attack. Although this study does not delve into the probabilistic modeling of attacks, the provided reference model lays the groundwork for future analysis and simulations. In conclusion, this approach equips organizations with a foundational understanding necessary to enhance their security posture and minimize the potential impact of ransomware attacks.

References

[1] **Khan, J. I., & Kembamba, F.** (2024). *RANSOMWARE MODELLING: A REFERENCE CYBERINFRASTRUCTURE MODEL FOR RANSOMWARE ATTACH ANALYSIS (PART-I)* . Medianet Technical Report, Technical Report 2024-09-02. Internetworking and Media Communications Research Laboratories, Department of Computer Science, Kent State University. Available at: https://www.medianet.cs.kent.edu/techreports/TR-2024-09-01-RansomeWareCyberInfrastructure-KK.pdf

[2] **Khan, J. I., & Kembamba, F.** (2024). *RANSOMWARE ATTACK MODELING: KEY SYSTEMIC VULNERABILITIES AND SAFETY PRACTICES EXPLOITS (PART-II).* Medianet Technical Report, Technical Report 2024-09-02. Internetworking and Media Communications Research Laboratories, Department of Computer Science, Kent State University. Available at: https://www.medianet.cs.kent.edu/techreports/TR-2024-09-02-RansomeWareExploits-KK.pdf

[3] **Khan, J. I., & Kembamba, F.** (2024). *RANSOMWARE MODELLING: ATTACK PROCESS REFERENCE MODELING ON PETRI-NET (PART-III)*. Medianet Technical Report, Technical Report 2024-09-03. Internetworking and Media Communications Research Laboratories, Department of Computer Science, Kent State University. Available at: https://www.medianet.cs.kent.edu/techreports/TR-2024-09-03-RansomeWareProcess-KK.pdf