Technical Report 2024-09-01
Internetworking and Media Communications Research Laboratories
Department of Computer Science, Kent State University
http://medianet.kent.edu/technicalreports.html

Ransomware Modelling: A Reference Cyberinfrastructure Model for Ransomware Attach Analysis (Part-I)

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

Exact, actionable and usable analysis of a sophisticated attack like ransomware attack requires specific model of the network encompassing all multitude of systems, networks, software, and people including attacker, the victim and the intermediaries involved. A reference model is badly needed for any analysis which are specific enough to accommodate all the key elements in the most sophisticated attacks, as well as general enough to capture most of the attacked organization. This document presents a reference model including language and methodology for organizations to describe their computing systems and network architecture for ransomware analysis. By applying this model, organizations can quantify the risk of ransomware attacks and evaluate the effectiveness of their defense strategies, leading to improved cybersecurity measures.

1. Key Words

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

2. INTRODUCTION

Ransomware attacks pose a significant threat to organizations by exploiting system vulnerabilities and user behaviors to gain unauthorized access and encrypt critical data. Although there has been extensive research on various aspects of ransomware, a gap exists in the literature regarding the application of mathematical modeling and simulation to analyze these attacks and provide a quantitative assessment of system status. This study aims to fill that gap by developing a comprehensive model that simulates ransomware attacks and quantifies the state of a system both during and after an attack.

The scope of this model includes identifying key system vulnerabilities, simulating different attack scenarios, and evaluating the effectiveness of defense strategies. The model operates under certain assumptions, including a static network architecture and consistent user behavior patterns. Ultimately, this model is designed to benefit organizations by offering actionable insights to enhance their cybersecurity measures.

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 (a), while the remaining items are covered in associated technical reports [2] and [3]. These reports are not specific to any particular analysis. Any researcher can use these reference models for their analysis.

3. Why IS A REFERENCE MODEL Needed?

A reference model is crucial for ransomware analysis because it provides a standardized framework to represent complex network architectures, system vulnerabilities, and attack patterns. Without such a model, it becomes difficult to quantify risks or to evaluate the effectiveness of different defense strategies. By establishing a baseline, organizations can simulate attack scenarios under controlled conditions, allowing them to identify weaknesses and prioritize mitigation efforts. Furthermore, a reference model facilitates communication across teams and stakeholders by providing a clear and consistent understanding of the system's architecture, vulnerabilities, and defenses. This shared understanding is essential when designing targeted responses to potential ransomware threats.

4. Network and Data Flow

A clear illustration of the network topology and data flow within the organization. This should include all the communication paths, protocols used, and the interactions between different devices and servers. An example is depicted in the following diagram:

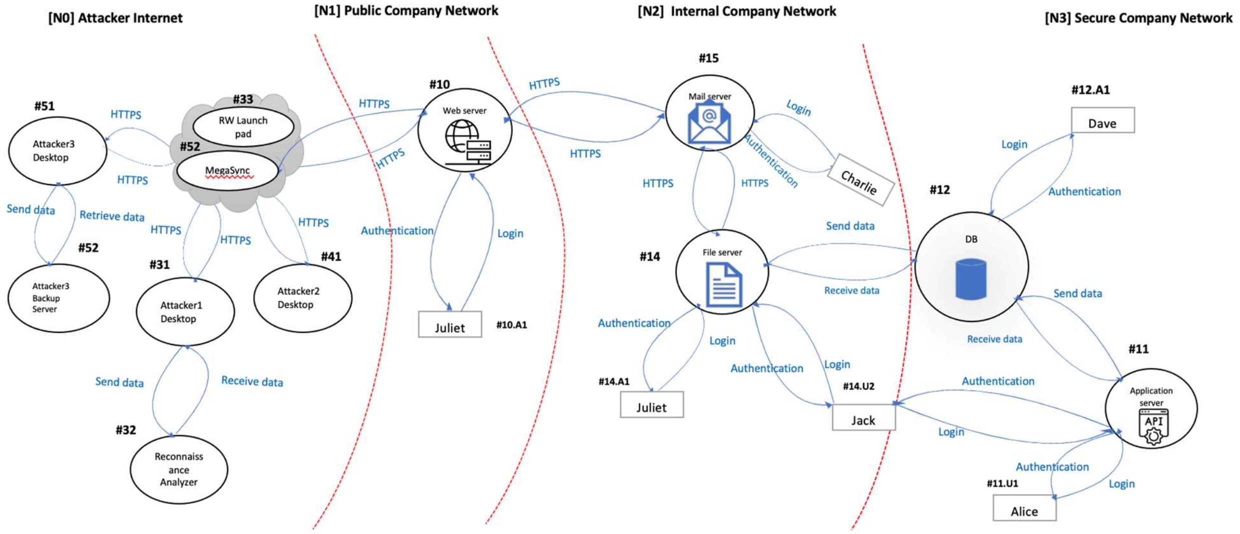

Fig 2. Network structure and data flow

The diagram illustrates a multi-network attack scenario, showing interactions between different networks and entities during a cyberattack, particularly involving ransomware. Here's a description of the diagram based on the labels and the logical flow of entities:

i. [N0] Attacker's Network

This section represents the environment controlled by the attackers and is divided into two key areas:

Cloud Environment:

The **Ransomware Launch Pad** (#15) serves as the central hub from which the ransomware is prepared and deployed.

Megasync functions as an Online Secure Data Warehouse, where the attackers store the exfiltrated data after it has been collected during the attack. It is a critical component for managing stolen data.

Local Environment (Attacker Infrastructure):

The attackers utilize three desktops labeled **Attacker1**, **Attacker2**, and **Attacker3**, from which they coordinate and execute malicious activities. Each desktop plays a role in different stages of the attack process.
There is also a Backup Server connected to the infrastructure, which is likely used to store backups of stolen data or as a contingency in case other parts of their infrastructure are compromised.
Additionally, the Reconnaissance Analyzer (#14) is used to gather intelligence on the target network and identify vulnerabilities. This information is crucial for planning and executing the attack efficiently.
The local infrastructure and cloud environment work in tandem, facilitating reconnaissance, ransomware deployment, and data exfiltration to ensure the success of the attack.

ii. [N1] Public Company Network:

This network is the public-facing part of the company, exposed to external access, likely including web servers or services accessible to external users. There is a Web server (#5) where an entity named Juliet is interacting through Login and Authentication.

iii. [N2] Internal Company Network:

This represents the company's internal network, presumably shielded from the public-facing part. It contains a Mail server (#8) and a File server (#10). Users like Charlie, Jack, and Juliet are logging in and interacting with these resources. Data is exchanged across different components within this internal network.

iv. [N3] Secure Company Network:

This is the most secure section of the company's infrastructure, involving critical data.
It includes a DB (#9) (database) and an Application server (#6) where high-level users like Alice and Dave authenticate and send/receive data.

Attack Path Flow

The attack originates from the [N0] Attacker Internet environment, where the attackers are operating using two devices, Attacker1 Desktop and Attacker2 Desktop. Juliet, a user in the Public Company Network [N1], is interacting with the Web Server (#5). The attackers might be attempting to exploit this interaction, possibly through phishing or other forms of compromise.
Data flows between the attacker's infrastructure and Juliet's session on the Web Server. Following this, the ransomware spreads into the Internal Company Network [N2], where it compromises File Servers (#10) and Mail Servers (#8). Users within the internal network, including Juliet, Jack, and Charlie, are affected or involved in the attack chain.
The attack then progresses into the [N3] Secure Company Network, where the goal may be to compromise the Database (#9) or sensitive applications on the Application Server (#6). A detailed explanation of this attack can be found in technical report [3].

Connections and Actions

Each arrow represents an action or data flow:

- **HTTPS** and **Login** connections are shown where users log in to servers and services.
- **Authentication** is required at different points, such as accessing the **File Server**, **DB**, and **Application Server**.
- The **Attacker's infrastructure** communicates with compromised systems in the **Public Company Network** and **Internal Company Network**, sending and receiving data.

The diagram demonstrates a multi-stage ransomware attack targeting a company's infrastructure. While organizations may have different network structures, we have selected this generic structure to explain the ransomware attack. It illustrates how attackers penetrate through multiple layers of the company's network, starting from a public-facing server and progressing through to more secure internal systems. The diagram focuses on how vulnerabilities are exploited across different network zones, ultimately aiming to compromise sensitive company assets such as databases and servers.

5. Example Cyberinfrastructure Description

To perform the ransomware analysis, the organization must describe its computing system and network architecture. Here is an example of a computing system structure:

Computing System Structure: Detailed information about each device within the network, including user details, installed applications, operating systems, hardware specifications, and network interfaces. An example of such a structure is shown below:

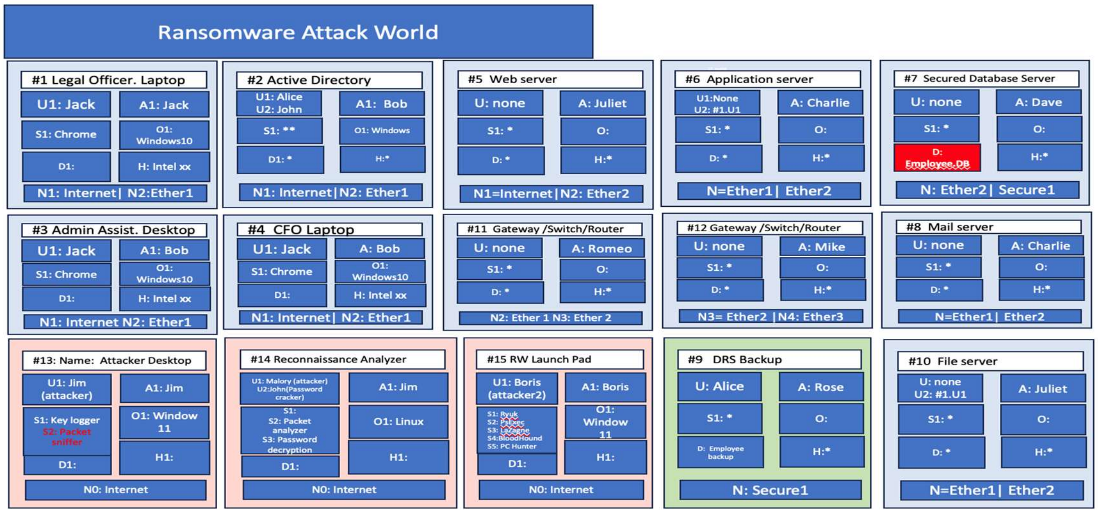

Fig 1 Computing system description

Defining Abbreviations in the Diagram:

- **U1, U2, etc. (User)**:
  - **U1**: Refers to "User 1." It typically indicates the primary user associated with a device or system. For example, "U1: Jack" would indicate that Jack is the primary user of that device.
  - **U2**: Refers to "User 2," indicating an additional user associated with the device.
- **S1, S2, etc. (Software)**:
  - **S1**: Refers to "Software 1," typically indicating the primary software installed or running on the system. For example, "S1: Chrome" means Chrome is the primary software running on that device.
  - **S2**: Refers to secondary software, if any.
- **D1, D2, etc. (Data)**:
  - **D1**: Refers to "Data 1," which usually points to the primary set of data on the device. For example, "D1: Intel.xlsx" indicates that there is a significant file or dataset on that system, often important for the scenario.
  - **D2**: Could indicate secondary or additional important data.
- **N1, N2, etc. (Network Interface)**:

  - **N1**: Refers to "Network Interface 1." This represents the primary network connection for the device. For example, "N1: Internet" shows that the device is connected to the internet via a specific network interface.
  - **N2**: Refers to the secondary network connection, if there are multiple interfaces or if it is segmented (e.g., Ethernet, Secure networks).
- **A1, A2, etc. (Admin/Administrator)**:
  - **A1**: Refers to "Admin 1," typically indicating the main administrator or person responsible for managing that system. For instance, "A1: Bob" suggests that Bob is the administrator of that device.
  - **A2**: Refers to a secondary administrator, if there are multiple administrators.
- **O1, O2, etc. (Operating System)**:
  - **O1**: Refers to "Operating System 1." It indicates the primary operating system running on the machine. For example, "O1: Windows 10" indicates that the device is using Windows 10.
  - **O2**: Could refer to an alternate or secondary operating system.
- **H1, H2, etc. (Hardware)**:
  - **H1**: Refers to the hardware associated with the system. This could represent the primary hardware components, like the CPU, storage, or any significant hardware details relevant to the system's security or function.
- **N1, N2, etc. (Network Interface)**:
  - This typically represents the network inteface that the computer is connected to. For example,
  - **"N1**: Internet" could imply that this system is connected to the internet through a network device.
  - **"N2**: Internet" could indicate that the system is connected to wireless internet .

The description of computing system depicted in Figure 1 is structured into two distinct groups: attacker computers and victim computers. The attacker group comprises of six computers, specifically numbered #13, #14, #15, #16, #17, and #18. These computers are configured to simulate various attack vectors and malicious activities aimed at compromising the system. On the other hand, the victim group consists of twelve computers, numbered from #1 to #12. These computers represent the targets of the simulated attacks, showcasing how different vulnerabilities and defenses respond under ransomware attack conditions. The model provides a comprehensive framework for studying and modeling ransomware attacks, and the interactions between attacker and victim systems.

6. CONCLUSIONS

This report has introduced a reference model for ransomware analysis, designed to help organizations understand and simulate potential attack scenarios within their network architectures. By utilizing a Markov chain model, the framework provides a quantitative assessment of system status during and after ransomware attacks. The model is beneficial for identifying key vulnerabilities, evaluating different attack scenarios, and assessing the effectiveness of defense strategies.

However, this model comes with certain limitations. Firstly, it operates under the assumption of a static network architecture, which may not accurately reflect the dynamic nature of real-world environments. Additionally, the model assumes consistent user behavior patterns, which might not capture the complexity of human factors in cybersecurity incidents. These assumptions limit the model's adaptability to evolving threats and the fast-paced changes that occur within organizational networks.

To expand and improve the reference model, future work could focus on introducing more dynamic elements, such as adapting to changes in network topologies or user behaviors in real-time. Incorporating machine learning techniques could allow for the detection of evolving attack patterns and system vulnerabilities. Furthermore, extending the model to cover additional types of malware beyond ransomware, such as advanced persistent threats (APTs) or zero-day exploits, would make it more versatile and comprehensive. Expanding the dataset of vulnerabilities and attack vectors would also enhance the accuracy and predictive power of the model, offering deeper insights into an organization's cybersecurity posture.

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