Ransomware Attacks: Simulation and Prevention

CSCE 5550: Group 21

Group members:
Sai Sathwika Guntupalli
Meghana Kesani
Lakshmi Naveenareddy Pasam
Saurav Narsing Shinde

Abstract:

This project aims to simulate the delivery of ransomware through phishing emails to test the vulnerability of targeted users. The simulation will mimic the stages of a real ransomware attack, from phishing delivery to the presentation of a simulated ransom demand. The primary goal is to assess user susceptibility, improve awareness, and enhance organizational defenses.

Introduction:

With the rapid development of technology, ransomware has become one of the most common and harmful forms of cybercrime, exploiting technical vulnerabilities and human weaknesses Unlike previous studies that focus on hindsight in particular, our work takes a different approach by analyzing ransomware attacks from the attacker's perspective of view This work highlights the various stages of the attack until the execution Objective To develop the basics for creating ransomware scenarios that mimic the world self-attack, identifying the tools, techniques and techniques used by cybercriminals Thus aiming to assess the effectiveness of existing security measures and suggesting improvements to enhance the security of the organization forward and protect individual users They continue to grow exponentially

Scope of the Project:

The main goal of this project is to simulate and prevent phishing attacks to strengthen security awareness across the organization.

- Target Audience: This project will focus on university staff or organization members, with the possibility to include students and external stakeholders later.
- Simulations: I will conduct phishing simulations via email, voice phishing (vishing), and SMS phishing (smishing).
- Key Components: The project includes designing realistic phishing emails, creating fake landing pages, and setting up a system for users to report suspicious emails.
- Metrics: I will monitor user interactions with phishing emails and track how many suspicious emails are reported.

This methodical technique for simulating ransomware threats through phishing attacks is provided. This strategy concentrates on phishing techniques while adhering to the standard stages of a ransomware attack:

Phases of a Ransomware Attack Simulation:

1. Planning and objectives: Define the objectives of the simulation, such as assessing the organization's vulnerability to phishing attacks delivering ransomware We will also identify target audiences, focusing on specific departments or functions.
2. Creating content: Create authentic phishing content that mimics common ransomware techniques, such as fake content or malicious add-ons. The scenarios will be tailored to the organization's reference to known software or internal processes to maximize reliability.
3. Email planning: Create phishing emails with strong calls to action, encouraging recipients to click links or open attachments. These emails will include things like urgency or potential to increase the chances of user engagement.
4. Simulation Execution: Send phishing emails to selected participants and monitor their communication. Using tracking tools, we will collect data on email opens, link clicks, and downloads to evaluate the effectiveness of the simulation.
5. Analysis of the results: We will analyze the data collected from the simulation to evaluate the success of the phishing attempt. This includes identifying patterns or weaknesses in specific departments or functions within the organization.
6. Reporting and feedback: We will provide a detailed report to the staff, summarizing the results and highlighting any areas of concern. Participants who have been in contact with the phishing effort will receive personalized information on the risks of ransomware.
7. Increased awareness and training: Conduct training programs to educate employees to recognize phishing attacks and understand ransomware risks. This will include resources with tips on how to avoid falling prey to phishing scams.
8. Evaluation and follow-up: We will develop a follow-up sampling plan to evaluate the effectiveness of the training and monitor progress. Phishing scenarios will be updated based on the latest techniques used by ransomware attackers.
9. Optimizing security culture: Integrate our findings into organizational security measures to improve defense against ransomware. Encouraging a culture of security awareness will help ensure that employees remain alert to future threats

Tools and Technologies:

- VirtualBox: To simulate the environment for the ransomware attack.
- Python: For scripting the encryption, decryption, and monitoring system activities.
- AES and RSA: Encryption algorithms for securing and decrypting files.
- SMTP: For sending phishing emails with the ransomware payload.
- Scapy: For monitoring network traffic and detecting suspicious activity.
- pyinotify/os: For monitoring file changes and detecting unusual activity.