2024

Malware Simulation

NETWORKS & CYBER - II

ABDUL SAMI QASIM I22-1725

AHMAD ABDULLAH I22 -1609

Table of Contents

Group Members

- Ahmad Abdullah (22i-1609)
- Abdul Sami Qasim (22i-1725)

Introduction

In this assignment, we were asked to make malware for a Windows system which does the following:

- Scans the Windows directory structure
- Identifies files and folders with specified names
- Replace these files and folders with garbage data (placeholder files)
- Logging mechanism in the malware

These were the basic requirements of the assigned task.

Documentation

Summary of Malware Actions

To perform this task, we created a PowerShell script (.ps1) that had the following functions in it:

1. Scan-Directory
2. Log-Action
3. Generate Garbage Data
4. Replace With Garbage Data

We also included an array **targetFileAndFolderName** that contained the names of the folders/files that are to be targeted by the malware.

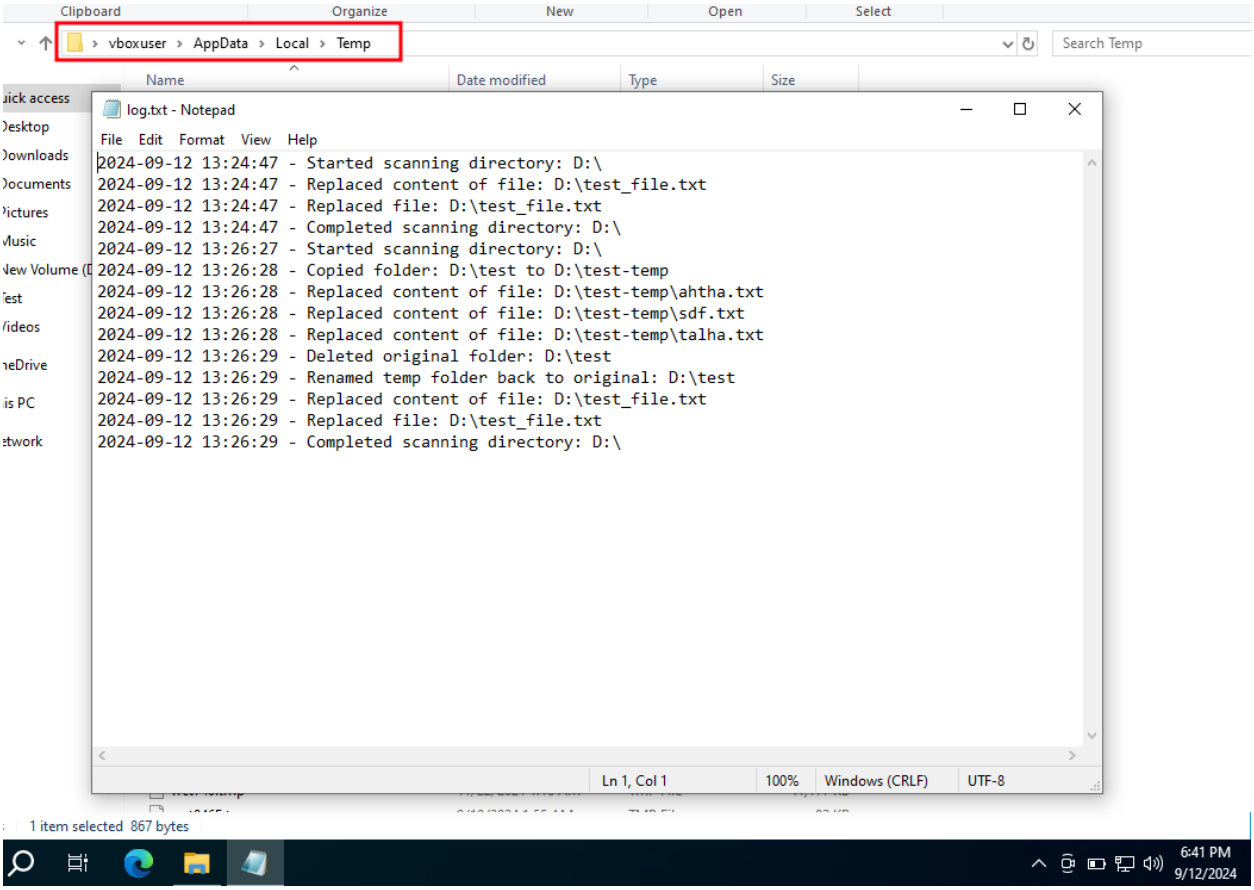
Scan Directory:

Scan directory recursively scans the given directory (D:\) to find the items mentioned in the target names array. Upon finding the targeted folder, it copies the folder to another path, deletes the original folder and then fills the newly created folder's files with garbage values.

If a file is found, it just replaces its information with garbage values.

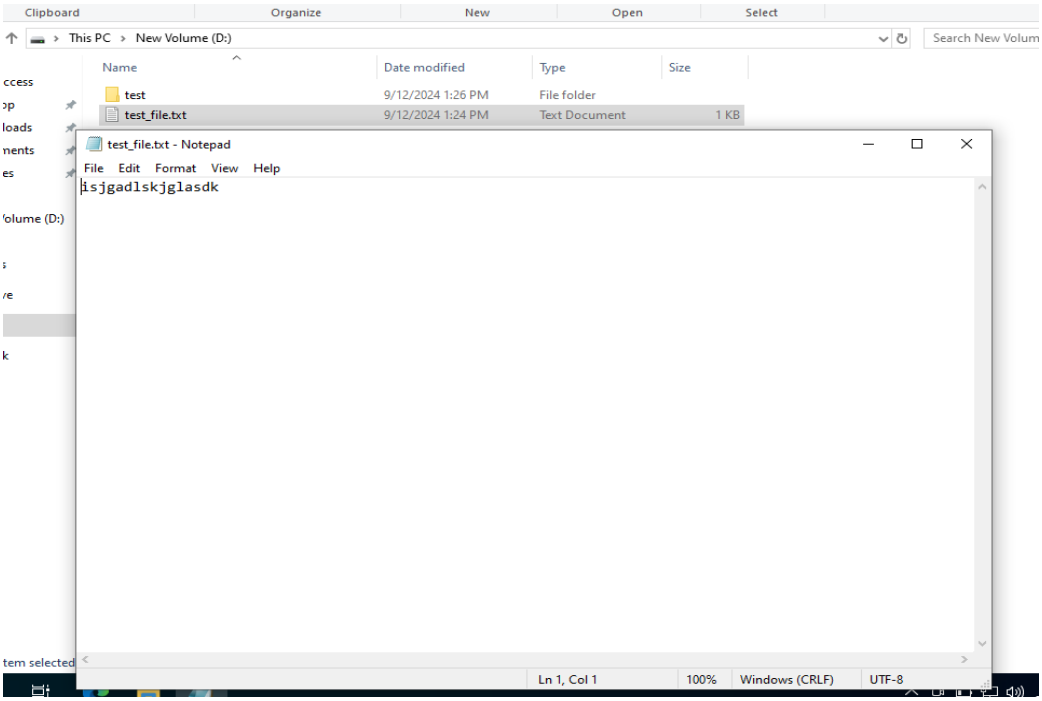
Log-Action:

Log-Action logs the performed actions into a file located at **\AppData\Local\Temp\log.txt** in the current user's folder along with their timestamp.

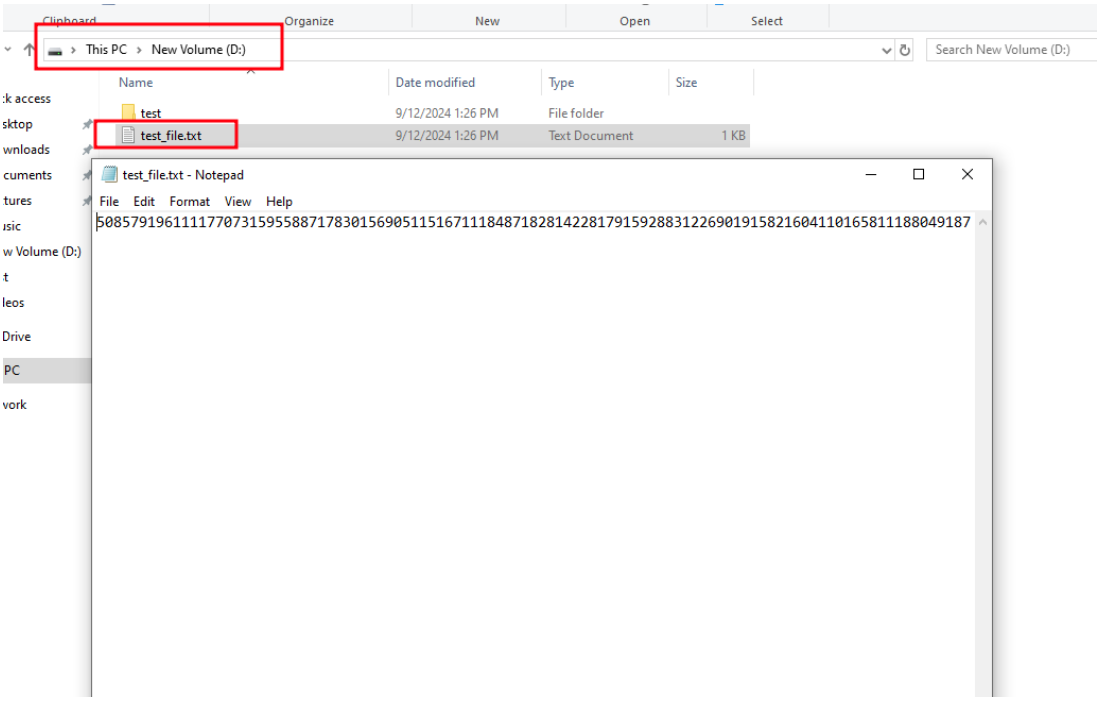


Garbage Data

Generates garbage values of the required size which are random numbers and replaces the contents of a file with the newly created garbage values.



Before Running the Script



After Running the Script

Sequence of Events

1. The target names array is created
2. The scan directory function is called
3. The scan directory function finds the targeted folders/files
4. The function calls the garbage generation, and the data replacement functions
5. All the functions call the Log-Action function which creates a log entry in the log file created

Impacts

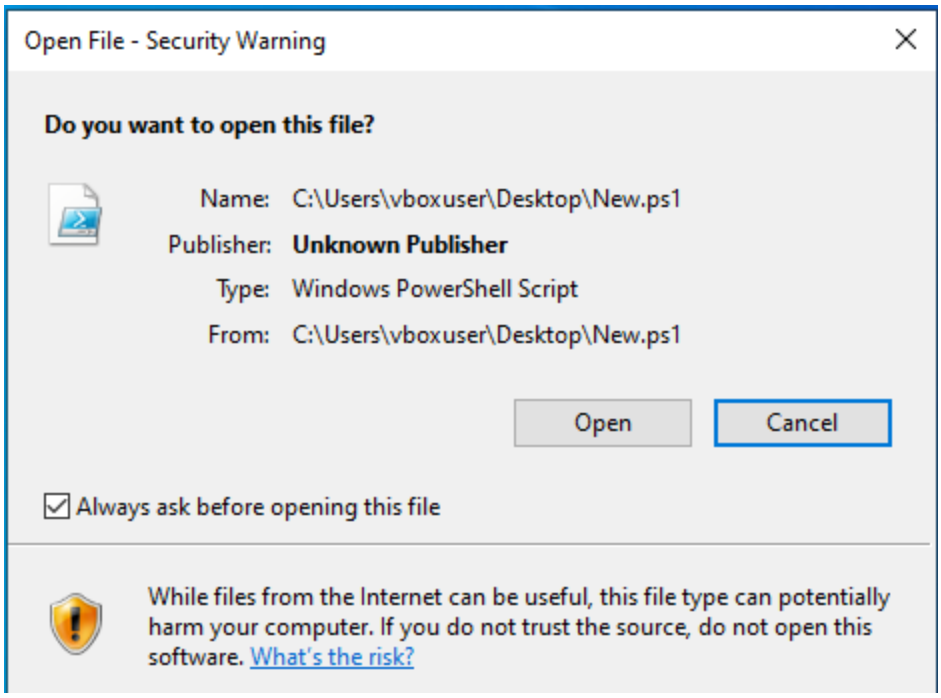
A small script such as this one wouldn't do much damage to a system where only a few bytes of data are altered but on a larger scale, this type of malware could cause great damage to important data residing on any of the disks.

For example, if a threat actor tries to do this to a large organization having TBs of data this could bring the whole business down depending on the damage. Not only large organizations but also small businesses where keeping records of daily business activity is important could be affected if this type of malware finds its way into their system.

Counter Measures

To mitigate such attacks, the first and foremost thing that we, as Cyber Security Engineers, need to do is to implement the best resources that the business can afford, such as a good antivirus, updated firewall policies and restricted access control to people based on their roles.

Secondly, we need to educate the personnel, people who will be interacting with the system daily, about some major cyber threats that cause cybercrime such as phishing emails, as most of the cyber attacks are done through social engineering. Reading antivirus-generated warnings such as the one given below before running any program on a computer whether it is personal or corporate. In case of finding any suspicious file or program, one should contact the Security Operations Centre (SOC) team to analyze the system before anything.



Key Takeaways

Ensuring file and folder integrity is crucial to prevent unauthorized tampering, as demonstrated by malware that replaces files with garbage data. Proper logging mechanisms are essential for tracking malicious activities, providing valuable insights for investigation and mitigation. Even small-scale scripts can have a substantial impact when executed on a larger scale, highlighting the importance of monitoring and defending systems effectively.

Regular training and awareness programs for personnel help reduce human error by enabling them to recognize potential cyber threats, such as phishing. Implementing strict access control and role-based permissions can minimize the damage malware can cause by restricting access to critical system areas.

A robust defence strategy, including up-to-date antivirus software, firewalls, and proactive threat detection, plays a vital role in preventing malware attacks. Lastly, early contact with the Security Operations Centre (SOC) team upon noticing suspicious activity is crucial in preventing small threats from escalating into major incidents.