FINAL REPORT

CYB550 - ANALYZE AND EVALUATE MALWARE

Jorge, Nsundidi
CANISIUS UNIVERSITY | 2001 MAIN ST, BUFFALO, NY 14208

Table of Contents

Introduction

This report provides a detailed analysis of five malware samples, focusing on their behavior, analysis methods, and insights gained from both static and dynamic analyses. The samples were selected based on their prevalence and impact in the cybersecurity landscape.

Malware Samples Overview

Sample 1: Trojan.Win64.Injects

- **Overview**: This sample is a file infector is a type of malware that has the capability to propagate by attaching its code to other programs or files. It is designed to steal sensitive information from the infected system.
- **Behavior**: Upon execution, it utilizes the Firefox browser process for potential data exfiltration while employing TASKKILL.EXE to terminate browser processes, disrupting normal operations to facilitate its malicious activities.

Sample 2: Zusy.Generic

- **Overview**: This Ransomware encrypts files on the victim's machine and demands a ransom for the decryption key, while also exhibiting behaviors indicative of personal data exfiltration.
- **Behavior**: It employs sophisticated execution methods via WMI, modifies files in the Chrome extension folder, and creates files in both the system drive root and user directory, all while checking for supported languages to customize its ransom note.

Sample 3: trojan.generic

- **Overview**: This Trojan appears to be a benign application, as the analysis reveals no malicious or suspicious behaviors typically associated with harmful software.
- **Behavior**: It retrieves the computer name and checks for supported languages, which may be used for identification and to customize user interactions, while the detection of PyInstaller indicates that it may have been packaged as a standalone executable, suggesting a potentially legitimate origin.

Sample 4: trojan.zusy/themida

- **Overview**: This Trojan appears to be a potentially benign application, as no malicious behaviors were detected during analysis.
- **Behavior**: It reads the BIOS version, retrieves the computer name, checks for supported languages, and sends debugging messages, though the context of its execution raises some suspicion.

Sample 5: trojan.symmi

- **Overview**: This is a computer Trojan horse that could perform several actions on your system where your personal information is put at risk of being stolen.
- **Behavior**: It runs in the background, attempting to steal personal data and web credentials, while connecting to a command-and-control server to exfiltrate information and receive instructions. Additionally, it engages in suspicious activities such as reading the BIOS version and contacting servers without host names, indicating potential evasion tactics.

Comprehensive Static Analysis

SAMPLE 1: TROJAN.WIN64.INJECTS

1. File Type and Signature

- **Filename:** file.exe
- **Size:** 946 KiB (968704 bytes)
- **Type:** PE32 executable (GUI) Intel 80386, for MS Windows
- **SHA256:** 3cb9ced1b227371eff8b97286b40871f10525c2261ac8af10c99af863ef28cdb

2. Imports and Exports

- **Imports:** The malware imports various Windows APIs from the following DLLs:
  - ADVAPI32.dll
  - COMCTL32.dll
  - COMDLG32.dll
  - GDI32.dll
  - IPHLPAPI.DLL
  - KERNEL32.dll
  - MPR.dll
  - ole32.dll
  - OLEAUT32.dll
  - PSAPI.DLL
  - SHELL32.dll
  - USER32.dll
  - USERENV.dll
  - UxTheme.dll
  - VERSION.dll
  - WININET.dll
  - WINMM.dll
  - WSOCK32.dll
- **Exports:** The malware does not appear to export any functions.

3. Strings and Resources Found in the Binary

- **Strings:** The binary contains numerous strings, including:
  - URLs related to Google and YouTube, indicating potential phishing or data exfiltration. *https://youtube.com/account?=https://accounts.google.com/v3/signin/challenge/pwd*
  - API calls related to process management, memory manipulation, and user authentication.

- **Resources:** The binary includes various resources such as:
  - Icons (RT_ICON)
  - Menus (RT_MENU)
  - Dialogs (RT_DIALOG)
  - Version information (RT_VERSION)
  - Manifest (RT_MANIFEST)

4. Basic Structure of the Code

- **Sections:**
  - **.text:** Contains executable code.
  - **.rdata:** Contains read-only data, including imported function names.
  - **.data:** Contains initialized data.
  - **.rsrc:** Contains resources.
  - **.reloc:** Contains relocation information.

- **Entrypoint:** The entry point of the executable is located at 0x420577 in the .text section.

Analyze and Findings

Immediate Insights

- The malware is identified as a **Trojan.Win64.Injects**, indicating its capability to inject code into other processes.
- It exhibits spyware characteristics, including the ability to capture keystrokes and take screenshots.
- The malware demonstrates evasive techniques, such as terminating processes and using high entropy sections to avoid detection.
- It communicates with multiple domains and hosts, suggesting a command-and-control (C2) infrastructure.

Challenges Faced During Analysis

- **Complexity of Code**: The presence of high entropy sections and obfuscation techniques made it challenging to analyze the code structure and functionality.

SAMPLE 2: ZUSY.GENERIC

1. File Type and Signature

- **Filename**: f11b60b273e2606e91832edbb014ad229563f5c537ddab11dba80018c11364dd
- **Type**: PE32+ executable (GUI) x86-64, for MS Windows
- **SHA256**: f11b60b273e2606e91832edbb014ad229563f5c537ddab11dba80018c11364dd

2. Imports and Exports

- **Imports**: The malware imports various Windows APIs from the following DLLs:
  - **KERNEL32.dll**
  - **MPR.dll**
  - **ole32.dll**
  - **OLEAUT32.dll**
  - **RstrtMgr.DLL**
  - **SHELL32.dll**
  - **SHLWAPI.dll**
  - **WS2_32.dll**
  - **WTSAPI32.dll**
- **Exports**: The malware does not appear to export any functions.

3. Strings and Resources Found in the Binary

- **Strings**: The binary contains numerous strings, including:
  - PowerShell commands for removing shadow copies.
  - References to WMI (Windows Management Instrumentation) for querying system information.
  - Strings indicating potential ransomware behavior, including negotiation messages and instructions for victims.
- **Resources**: The binary includes various resources such as:
  - Manifest (RT_MANIFEST)
  - Other resource types that may include icons and version information.

4. Basic Structure of the Code

- **Sections**:
  - **.text**
  - **.rdata**
  - **.data**
  - **.pdata**
  - **.rsrc**
  - **.reloc**

- **Entrypoint**: The entry point of the executable is located at **0x14008d058** in the **.text** section.

Analyze and Findings

Immediate Insights

- The malware is identified as **Ransomware**, capable of removing shadow copies using PowerShell, which is a common tactic to prevent recovery of encrypted files.
- The malware demonstrates **evasive techniques**, such as marking files for deletion and using high entropy sections to avoid detection.
- It communicates with potential command-and-control (C2) infrastructure, as indicated by the presence of Tor URLs and references to remote access.

Challenges Faced During Analysis

- **Complexity of Code**: The presence obfuscation made it challenging to analyze the code.

SAMPLE 3: TROJAN.GENERIC

1. File Type and Signature

- **Filename**: ce2833e73db1f6dff7f6f2d90caeabf0aa1b31a519466f87580a418323a5f10e.exe
- **File Type**: Win32 EXE executable
- **SHA256**: ce2833e73db1f6dff7f6f2d90caeabf0aa1b31a519466f87580a418323a5f10e

2. Imports and Exports

- **Imports**: The malware imports various Windows APIs from the following DLLs:
  - **USER32.dll**
  - **COMCTL32.dll**
  - **KERNEL32.dll**
  - **ADVAPI32.dll**
  - **GDI32.dll**
- **Exports**: The malware does not appear to export any functions.

3. Strings and Resources Found in the Binary

- **Strings**: The binary contains numerous strings, including:
  - References to PowerShell commands, indicating potential malicious behavior.
  - Strings related to the malware's functionality, such as file manipulation and system queries.
- **Resources**: The binary includes various resources such as:
  - Icons (RT_ICON)
  - Group icons (RT_GROUP_ICON)
  - Manifest (RT_MANIFEST)

4. Basic Structure of the Code

- **Sections**:
  - **.text**: Contains executable code.
  - **.rdata**: Contains read-only data, including imported function names.
  - **.data**: Contains initialized data.
  - **.pdata**: Contains exception handling data.
- **Entrypoint**: The entry point of the executable is located at **0x0000C3B0** (offset 49904).

Analyze and Findings

Immediate Insights

- The malware is identified as a **potentially malicious executable**, with characteristics suggesting it may perform actions typical of ransomware or other malicious software.
- The presence of PowerShell commands indicates that the malware may attempt to execute commands that could manipulate system settings or files.

Challenges Faced During Analysis

- **Obfuscation**: The high entropy sections and potential use of packing techniques complicate the analysis, making it difficult to discern the true functionality of the code without further dynamic analysis.

SAMPLE 4: TROJAN.ZUSY/THEMIDA

1. File Type and Signature

- **Filename:** defOff.exe
- **File Type:** Win32 EXE executable
- **SHA256:** 2490ae736012809e367980cefd58a8e6e64855c063b96e92b9b6560dcf92fb1b

2. Imports and Exports

- **Imports:** The malware imports various Windows APIs from the following DLL:
  - kernel32.dll
- **Exports:** The malware does not appear to export any functions.

3. Strings and Resources Found in the Binary

- **Strings:** The binary may contain strings related to its functionality, including potential commands or messages that indicate its purpose.

- **Resources:** The binary includes various resources such as:
  - (RT_VERSION)
  - (RT_MANIFEST)

4. Basic Structure of the Code

- **Sections:**
  - **The executable contains 6 sections, including:**
    - An unnamed section with high entropy, indicating potential obfuscation or packed code.
    - .rsrc
    - .idata
    - Other sections that may contain executable code or data.
- **Entrypoint:** The entry point of the executable is located at offset 0x2A0000 (2777088).

Analyze and Findings

Immediate Insights

- The malware is identified as a potentially malicious executable, with characteristics suggesting it may perform actions typical of malware.
- The presence of high entropy in sections indicates that the code may be obfuscated or packed, which is a common tactic to evade detection.
- The lack of a digital signature suggests that the file may not be from a trusted source.

Challenges Faced During Analysis

- **Obfuscation**: The high entropy sections complicate the analysis, making it difficult to discern the true functionality of the code without further dynamic analysis.

SAMPLE 5: TROJAN.SYMMI

1. File Type and Signature

- **Filename**: 2e0320.exe
- **File Type**: Win32 EXE executable
- **SHA256**: 61f4cdf248de59f1bb1c40ec647816f2a2add0ecbac6f575318d598bd87a67e7

2. Imports and Exports

- **Imports**: The malware imports various Windows APIs from the following DLL:
  - **kernel32.dll**
- **Exports**: The malware does not appear to export any functions.

3. Strings and Resources Found in the Binary

- **Strings**: The binary may contain strings related to its functionality, including potential commands or messages that indicate its purpose.
- **Resources**: The binary includes various resources such as:
  - Manifest (RT_MANIFEST)

4. Basic Structure of the Code

- **Sections**:
  - The executable contains 7 sections, including:
    - An unnamed section with high entropy, indicating potential obfuscation or packed code.
    - **.rsrc**
    - **.idata**
- **Entrypoint**: The entry point of the executable is located at offset **0x00000000** (4734976).

Analyze and Findings

Immediate Insights

- The malware is identified as a **potentially malicious executable**, with characteristics suggesting it may perform actions typical of malware.
- The presence of high entropy in sections indicates that the code is obfuscated or packed, which is a common tactic to evade detection.

Challenges Faced During Analysis

- **Obfuscation**: The high entropy sections complicate the analysis, making it difficult to discern the true functionality of the code without further dynamic analysis.

Comprehensive Dynamic Analysis

SAMPLE 1: TROJAN.WIN64.INJECTS

Behavioral Observations

1. System Changes:

- **Files Created:**
    - Multiple files were created in the following directory:
        - **C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating**
        - Notable files include:
            - **content-track-digest256-1.vlpset**
            - **content-track-digest256.sbstore**
            - **google-trackwhite-digest256.sbstore**
            - **social-tracking-protection-linkedin-digest256-1.vlpset**
            - **base-fingerprinting-track-digest256-1.sbstore**
            - Additional files related to tracking and fingerprinting were also created, indicating a focus on monitoring user behavior.
- **Files Modified:**
    - Existing files in the Firefox profile directory were likely modified, as the malware appears to overwrite or drop new content into these files, potentially compromising the integrity of the browser's data.
- **Files Deleted:**
    - No specific deletions were identified.

2. Network Activity:

- **Connections Made:**
    - This malware established connections to multiple IP addresses, including:
        - 34.120.158.37
        - 35.244.181.201
        - 34.160.144.191
        - 35.201.103.21
    - These connections suggest potential communication with command and control (C2) servers, likely for data exfiltration or to receive additional payloads.

- **Data Sent:**
    - While specific data exfiltration attempts were not detailed, the malware's focus on stealing sensitive information accessed through the Firefox browser indicates that it likely sent user credentials or other sensitive data to the established connections.

3. Processes Spawned During Execution:

- **Processes:**
    - The malware spawned the following processes:
        - **trojan.atraps/silentall.exe** (PID: 6388): This is the main malware executable responsible for executing malicious actions, including process termination and file manipulation.
        - **firefox.exe** (PID: 3560 and PID: 1356): The malware utilized the Firefox browser process as a potential vector for data exfiltration or credential theft, indicating that it may have injected itself into the browser's execution context.
- **Process Termination:**
    - The malware employed **TASKKILL.EXE** to terminate various processes, including:
        - Web browsers (e.g., Firefox, Chrome, Microsoft Edge, Opera, Brave), indicating an attempt to disrupt user activities and prevent detection by security software.

Conclusion:

The behavioral observations of the malware sample **trojan.atraps/silentall** reveal a sophisticated approach to data theft and system compromise. The creation and modification of files within the Firefox profile, extensive network activity with multiple connections, and the spawning of processes designed to manipulate user behavior highlight the malware's intent to maintain control over the infected system while evading detection. Immediate remediation actions are recommended to mitigate the risks associated with this malware.

SAMPLE 2: ZUSY.GENERIC

Behavioral Observations

1. System Changes:

- **Files Created:**
    - Multiple files were created in various directories, including:
        - Temporary directories.
        - The root directory of the system drive.
        - User directory
        - An encrypted Visual Basic Script
    - These files are likely used for staging, executing additional malicious components, or establishing persistence.
- **Files Modified:**
    - Files within the Chrome extension directory were modified, indicating an attempt to manipulate browser functionality or install malicious extensions.
- **Files Deleted:**
    - No specific deletions were identified**.**

2. Network Activity:

- **Connections Made:**
    - The ransomware established connections to multiple IP addresses:
        - 192.168.100.255:137
        - 2.16.164.49:80
        - 51.124.78.146:443
        - 95.101.149.131:80
    - It suggesting potential communication with command and control (C2) servers for data exfiltration or to receive additional payloads.
- **Data Sent:**
    - While specific data exfiltration attempts were not detailed, the malware's behavior suggests it may have sent sensitive information to the established connections, potentially leveraging stolen personal data**.**

3. Processes Spawned During Execution:

- **Processes:**
    - The malware spawned the following processes:
        - ransomware.exe (PID: 556): This is the main ransomware executable responsible for encrypting user files and executing malicious actions.
        - powershell.exe (PID: 6160): Used for executing commands and scripts, indicating a sophisticated method of launching the malware.
- **Process Termination:**
    - The malware may have employed techniques to terminate security-related processes, although specific instances were not detailed.

Conclusion

The behavioral observations of the ransomware sample AKIRA/Zusy reveal a clear pattern of malicious activity characterized by file modification, potential data theft, and sophisticated execution methods. The creation and modification of files, along with the use of known indicators, highlight the malware's intent to encrypt user data and demand a ransom for decryption. Immediate remediation actions are recommended to mitigate the risks associated with this ransomware and to protect affected systems.

SAMPLE 3: TROJAN.GENERIC

Behavioral Observations

1. System Changes:

- **Files Created:**
    - No specific files were created during the execution of the sample, indicating a lack of file manipulation typically associated with malicious behavior.
- **Files Modified:**
    - No existing files were modified, suggesting that the sample does not interfere with system integrity or user data.
- **Files Deleted:**
    - No specific deletions were identified.

2. Network Activity:

- **Connections Made:**
    - 40.127.240.158:443
    - 192.168.100.255:137
    - 40.127.240.158:443
    - 40.127.240.158:443
    - 23.216.77.28:80
    - 192.168.100.255:138
- **Data Sent:**
    - No data transmission was observed, further supporting the benign nature of the sample.

3. Processes Spawned During Execution:

- **Processes:**
    - The following process was observed:
        - **sample3.exe** (PID: 6300): This is the main executable of the sample, which did not exhibit any malicious or suspicious behaviors during the analysis.
- **Process Termination:**
    - No process termination activities were noted, indicating that the sample does not attempt to disrupt other applications or services.

Conclusion

The dynamic analysis of Sample 3 reveals no malicious or suspicious behaviors, indicating that the sample may not pose a threat. However, the detection of PyInstaller and the retrieval of the computer name suggest that the sample may be a legitimate application or a benign script. Further context regarding the sample's intended functionality would be beneficial to fully assess its impact and purpose.

SAMPLE 4: TROJAN.ZUSY/THEMIDA

Behavioral Observations

1. System Changes:

- **Files Created:**
    - No specific files were created during the execution of the sample, indicating a lack of file manipulation typically associated with malicious behavior.
- **Files Modified:**
    - No existing files were modified, suggesting that the sample does not interfere with system integrity or user data.
- **Files Deleted:**
    - No specific deletions were identified.

2. Network Activity:

- **Connections Made:**
    - The sample established multiples **connections** to various IP addresses from different countries.
        - 40.127.240.158:443
        - 192.168.100.255:138
        - 40.127.240.158:443
        - This behavior may warrant further investigation to determine the nature of these connections and whether they are benign or indicative of malicious activity.
- **Data Sent:**
    - The data sent in these requests typically includes the certificate information being validated, such as the certificate serial number and the issuer's details. The responses from the OCSP or CRL servers will indicate whether the certificate is valid, revoked, or unknown.
    - The HTTP code 200 indicates that the requests were successful, meaning the processes were able to communicate with the certificate validation servers without issues.

3. Processes Spawned During Execution:

- **Processes:**
    - The following process was observed:

        - **sample4.exe** (PID: 5208): This is the main executable of the sample, which did not exhibit any malicious behaviors during the analysis.

- **Process Termination:**
    - No process termination activities were noted, indicating that the sample does not attempt to disrupt other applications or services.

Conclusion

The dynamic analysis of Sample 4 reveals no malicious behaviors, indicating that the sample may not pose a direct threat. However, the suspicious activity of reading the BIOS version, along with the informational activities of reading the computer name, checking supported languages, and sending debugging messages, suggests that the sample may be a legitimate application or a diagnostic tool.

The execution of sample4.exe from the temporary directory and the establishment of multiple connections necessitate further analysis to fully assess its impact and purpose. Additional context regarding the sample's intended functionality would be beneficial for a comprehensive evaluation.

SAMPLE 5: TROJAN.SYMMI

Behavioral Observations

1. **System Changes:**
    - **Files Created:**
        - The analysis did not specify any particular files created by the sample, but the presence of the executable **sample5.exe** indicates that it may have created additional files or artifacts during its execution.
    - **Files Modified:**
        - Existing files may have been modified as the sample operates, particularly those related to user credentials and browser data, although specific modifications were not detailed.
    - **Files Deleted:**
        - No specific deletions were identified during the analysis.
2. **Network Activity:**
    - **Connections Made:**
        - The malware established connections to multiple IP addresses, including:
            - 188.114.97.3
            - 20.223.36.55
            - 20.242.39.171
            - 20.223.35.26
            - 185.215.113.16
            - 4.175.87.197
        - These connections suggest potential communication with command-and-control (CnC) servers, likely for data exfiltration or to receive additional payloads.
    - **Data Sent:**
        - The sample made a GET request to the URL **http://185.215.113.16/off/def.exe** with a response code of 200, indicating that it may have attempted to download or communicate with a remote server. While specific data exfiltration attempts were not detailed, the malware's focus on stealing

sensitive information suggests that it likely sent user credentials or other sensitive data to the established connections.

3. **Processes Spawned During Execution:**
    - **Processes:**
        - The malware spawned the following processes:
            - **sample5.exe (PID: 1016):** This is the main malware executable responsible for executing malicious actions, including data theft and communication with CnC servers.
            - **svchost.exe (PID: 2192):** This legitimate Windows process may have been utilized by the malware to facilitate its operations or to mask its activities.
    - **Process Termination:**
        - The analysis did not specify any process termination actions taken by the malware, but the potential for it to disrupt legitimate processes to evade detection exists.

Conclusion

The behavioral observations of the malware sample Trojan.Symmi reveal significant malicious activities, including data theft, credential harvesting, and communication with command-and-control servers. The established network connections and the GET request to a remote server indicate a clear intent to exfiltrate sensitive information. The lack of specific file creation or modification details does not diminish the threat posed by this sample, as its primary focus appears to be on stealing data and maintaining control over the infected system. Immediate remediation actions are recommended to mitigate the risks associated with this malware, including isolation of affected systems and further investigation into its impact on network security.

Conclusion

The analysis of the five malware samples reveals a diverse range of techniques and behaviors, each exhibiting unique characteristics identified through both static and dynamic analyses. This variety emphasizes the importance of a comprehensive approach to malware investigation, as it yields critical insights into potential threats and indicators of compromise.

The Trojan.Win64.Injects sample showcases sophisticated data exfiltration methods, leveraging browser processes and command-and-control communications to capture sensitive information. In contrast, the Zusy.Generic ransomware is designed to encrypt user files and demand a ransom, employing evasive tactics to hinder recovery efforts.

Meanwhile, the Trojan.Generic and Trojan.Zusy/Themida samples, although appearing benign, raise concerns due to their obfuscation and potential for malicious intent. Lastly, the Trojan.Symmi sample underscores the ongoing risk of data theft and credential harvesting through its established network connections.

Collectively, these findings underscore the constant need for organizations to monitor and enhance their security measures to effectively address the evolving threats posed by these malware variants. Maintaining vigilance and adopting proactive cybersecurity strategies are essential to mitigate the risks associated with such sophisticated malware attacks.

References

1. Microsoft. (n.d.). *WMI start page*. Retrieved from https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

2. Abuse.ch. (n.d.). *Malware Bazaar*. Retrieved from https://bazaar.abuse.ch/browse/

3. PCRisk. (n.d.). *Themida Trojan removal guide*. Retrieved from https://www.pcrisk.com/removal-guides/24108-themida-trojan