Nama : Mochammad Aldo Rizky

Kelas : SIB4C

Lab - Attack Analysis

Objectives

Part 1: Investigate IOCs

Part 2: Investigate the Malicious Activity

Part 3: Investigate the More Malicious Activity

Introduction

Once an alert has been reported and validated, the digital forensics and incident response analysis must be completed. In a large organization, members of the incident response team (i.e., CSIRT) are responsible for this process. The response team typically consists of veteran threat hunters and select cybersecurity analysts and technicians. To help the incident response team, various tools and resources are available.

In this lab, you will use the ANY.RUN online interactive malware hunting service and the Mitre ATT&CK Matrix to investigate potential malicious activity.

ANY.RUN offers a free service in which community users can upload suspected malware files for analysis. It provides a very rich set of analyses features that lets you safely investigate the behavior of malware. The ANY.RUN sandbox can dynamically run the malware and display details of what the malware does in safe and secure analysis interface.

Note: You will use the free version of ANY.RUN which has limited features and can only run malware samples on a 32-bit Windows 7 virtual machine. Two more advanced versions are available for a monthly subscription. The Searcher and Hunter versions provide access advanced features and other operating systems (e.g., Windows 10).

Scenario

You are working a cyber technician and you have been selected to work with the incident response team at XYZ, Inc. A cybersecurity analyst has asked you to evaluate hash values from security alerts that have been generated by the Intrusion Prevention System (IPS). The IPS has flagged a series of events as potentially malicious.

You will use the ANY.RUN online tool and Mitre ATT&CK Matrix to perform forensic analysis based on the provided hash values.

Required Resources

- A device with internet access

Instructions

Part 1: Investigate IOCs

In this part, you will use the ANY.RUN website to categorize identified hash values to see if they are malicious, suspicious, or benign.

Step 1: Explore the ANY.RUN site

a. Open a web browser and navigate to the **ANY.RUN** webpage.

b. At the top of webpage are available links starting with “WHY US”. Click **SERVICE** from the horizontal menu to move to the sandbox service interface.

c. Click one of the countries in the map to show the list of public submissions from that country. Community users can view a detailed analysis for each submission.

d. Explore and become familiar with this dashboard. The ANY.RUN tool has many options available that will be of great value to a cybersecurity analyst. Use this opportunity to learn more about the tool.

Step 2: Validate Suspicious Hashes

In this step, you will investigate some MD5 hash of files that the cybersecurity analyst has identified in the table below. You will verify if they are potentially malicious, suspicious, or benign.

a. To search hash values, click **Public Tasks** in the menu on the left.

This opens the **Public submissions** page which displays a list of public tasks arranged by the most recent submission. Notice that each task is labelled with the analysis verdict identifying the submission as no threat detected (i.e., benign), suspicious activity, or malicious activity.

b. The Cybersecurity analyst has asked you to validate several hash values. Complete the following table by copying and pasting the identified MD5 hash value in the search box in the upper right of the window and press **Enter**.

IOCs MD5 Hash Values	Malicious / Suspicious / Benign	Associated Filename
2fd03624e271ec70349ce56fb30f563b		
c419df63e0121d72411285780c2fc6cc		
3acf52e5a62d50bdcedcb89174bf5492		
766b774626947000e67e0b318f558e94		
422a6ca28a7e4d8e5e498523c6f049f4		
b497845beb135740e6caed03a2020036		

Note: These malicious hash values will also be used in Part 2 and 3.

IOCs MD5 Hash Values	Malicious / Suspicious / Benign	Associated Filename
2fd03624e271ec70349ce56fb30f563b	Malicious	wireframe.exe
c419df63e0121d72411285780c2fc6cc	Suspicious	Updreg.EXE
3acf52e5a62d50bdcedcb89174bf5492	Benign	BACs_Payment2847.html
766b774626947000e67e0b318f558e94	Malicious	gh2st.exe
422a6ca28a7e4d8e5e498523c6f049f4	Malicious	file1.exe
b497845beb135740e6caed03a2020036	Suspicious	winlogon.exe

Part 2: Investigate the Malicious Activity

In this part, you will use the ANY.RUN website to investigate the malicious activity identified in the previous part. From the ANY.RUN tool, you will pivot to different tools to examine the malicious activity. Finally, you will use the Mitre ATT&K Matrix to identify the tactics and techniques used by the threat actors.

Step 1: Investigate the first malicious hash process tree.

a. From the ANY.RUN Public submissions page, search for the first identified malicious hash value in Part 1, Step 2b.

b. Click the resulting entry to open it in the ANY.RUN sandbox. The ANY.RUN analysis interface provides insights to many aspects of the malware behavior.

Note: If more than one submission is displayed, then click the submission with the **wireframe.exe** filename.

c. On the right-hand side of the screen, you will see the process tree which displays a group of horizontal blue bars in a nested tree-like structure. It shows all the software processes that were used in the exploit. Some of them are windows software components, and others are part of the malware.

What are the names of the processes used in this activity?

Based on the instructions and the information provided, the names of the processes involved in this activity are:

wireframe.exe

cmd.exe

timeout.exe

NvidiaGPU.exe

wireframe.exe, cmd.exe, timeout.exe, and NvidiaGPU.exe.

Step 2: Investigate the malicious activity text report.

Above the process tree are three text boxes labelled “Text report”, “Processes graph”, and ATT&CK matrix.

a. Click the **Text report** to open a report in a new web browser window.

b. Scroll through the document to see the generated report.

What is the SHA256 value associated with this activity?

The SHA256 value associated with this activity is:

9C83A89EA0E56D5AF9AA37D2DABED20B2412DB8C9694A13128EA173A73557487

9C83A89EA0E56D5AF9AA37D2DABED20B2412DB8C9694A13128EA173A73557487

Step 3: Investigate the malicious activity processes graph.

a. Return to the analysis webpage and click the **Processes graph**.

Which process was executed first?

The first process executed in this activity is:

wireframe.exe

wireframe.exe

What is the process name in the red highlighted box?

The process name in the red highlighted box is:

nvidiagpu.exe

nvidiagpu.exe

b. Click the red highlighted box.

What is the identified danger?

The identified danger is:

ASYNCRAT was detected

ASYNCRAT was detected

Step 4: Investigate the malicious activity in the ATT&CK matrix

a. Return to the analysis webpage and click the **ATT&CK matrix** to open the Mitre ATT&CK Matrix page.

How many Tactics, Techniques, and Events are there related to this malicious activity?

There are:

4 tactics

5 techniques

16 events

4 tactics, 5 techniques, and 16 events.

What are the tactics that were used by the threat actors?

Execution, Persistence, Privilege escalation, and Discovery

b. Click the various techniques that were used.

Which technique is identified as a Danger?

The tactics used by the threat actors are:

Execution

Persistence

Privilege Escalation

Discovery

Boot or Logon Autostart Execution

Part 3: Investigate the More Malicious Activity

In this part, you will repeat the steps in Part 2 to examine the other two malicious entries discovered in Part 1.

Step 1: Investigate the second malicious hash process tree.

a. Return to the ANY.RUN Public submissions page, and search for the second identified malicious hash value discovered in Part 1, Step 2b.

b. Click the resulting entry to open it in the ANY.RUN sandbox.

What is the name in the process tree of the process used in this activity?

The name of the process used in this activity, as shown in the process tree, is:

gh2st.exe

gh2st.exe

c. Open the Text report.

What is the SHA256 value associated with this activity?

The SHA256 value associated with this activity is:

88DD2037D0C43ABACEBAD866DF3F8CCD2EE7D64B01405AA6756A3A1C2FAC28FA

88DD2037D0C43ABACEBAD866DF3F8CCD2EE7D64B01405AA6756A3A1C2FAC28FA

d. Return to the analysis webpage and open the **Processes graph**.

What are the identified dangers?

The identified dangers are:

Steals credentials from Web Browsers

Stealing of credential data

Actions look like stealing of personal data

Connects to CnC server

REDLINE was detected

Steals credentials from Web Browsers, Stealing of credential data, Actions looks like stealing of personal data, Connects to CnC server, and REDLINE was detected.

e. Return to the analysis webpage open the **ATT&CK matrix**.

How many Tactics, Techniques, and Events are there related to this malicious activity?

There are:

3 tactics

7 techniques

245 events

3 tactics, 7 techniques, and 245 events.

What are the tactics that were used by the threat actors?

The tactics used by the threat actors are:

Credential Access

Discovery

Collection

Credential access, Discovery, and Collection

c. Click the various techniques that were used.

d. Which techniques are identified as a Danger?

The techniques identified as a danger are:

Credential from Password Stores

Unsecured Credentials

Software Discovery

Email Collection

Credential from Password Stores, Unsecured Credentials, Software Discovery, and Email Collection

Step 2: Investigate the third malicious hash process tree

a. Return to the ANY.RUN Public submissions page, and search for the third identified malicious hash value discovered in Part 1, Step 2b.

b. Click the resulting entry to open it in the ANY.RUN sandbox.

What is the name in the process tree of the process used in this activity?

The name of the process used in this activity, as shown in the process tree, is:

file1.exe

file1.exe

c. Open the **Text report**.

What is the SHA256 value associated with this activity?

The SHA256 value associated with this activity is:

F7B1639B6C4CA677BA279B945A94C5F6D67E6C4C89FD39CD8BE882A8A7CDFCAA

F7B1639B6C4CA677BA279B945A94C5F6D67E6C4C89FD39CD8BE882A8A7CDFCAA

d. Return to the analysis webpage and open the **Processes graph**.

What Dangers does it display?

The dangers displayed in the Processes graph are:

Steals credentials from Web Browsers

Stealing of credential data

Actions look like stealing of personal data

Connects to CnC server

REDLINE was detected

Steals credentials from Web Browsers, Stealing of credential data, Actions looks like stealing of personal data, Connects to CnC server, REDLINE was detected.

e. Return to the analysis webpage open the **ATT&CK matrix**.

How many Tactics, Techniques, and Events are there related to this malicious activity?

There are:

3 tactics

7 techniques

1525 events

3 tactics, 7 techniques, and 1525 events.

What are the tactics that were used by the threat actors?

The tactics used by the threat actors are:

Credential Access

Discovery

Collection

Credential Access, Discovery, and Collection

Reflection Questions

1. Explain how forensic analysis and incident response is very much like law enforcement trying to solve a criminal case.

Forensic analysis and incident response are indeed similar to law enforcement's approach to solving a criminal case. Here's a detailed explanation:

1. **Validation of the Incident: Just as a police detective must first confirm that a crime has occurred, cybersecurity professionals must verify that a security incident has taken place. This involves assessing alerts, logs, and other indicators to ensure that the reported event is legitimate and requires further investigation.**

2. **Evidence Collection: Once an incident is validated, both law enforcement and forensic analysts gather evidence. In criminal cases, detectives collect physical evidence from the crime scene, witness statements, and surveillance footage. In cybersecurity, analysts collect logs, file system data, network traffic, and malware samples to understand the extent of the breach and the methods used by attackers.**

3. **Preservation of Evidence: Just as detectives must secure evidence to prevent contamination or loss, forensic analysts ensure that digital evidence is preserved in a forensically sound manner. This often involves creating images of hard drives or isolating systems to prevent further compromise.**

4. **Analysis of Evidence: In a criminal investigation, detectives analyze the gathered evidence to identify suspects, motives, and methods. Similarly, in incident response, analysts examine the collected data to understand how the breach occurred, what vulnerabilities were exploited, and what data may have been compromised.**

5. **Reporting Findings: Law enforcement prepares reports detailing their findings, which may be used in court. Forensic analysts also document their processes and findings in detailed reports, which can be used for legal proceedings, compliance requirements, or internal reviews.**

6. **Remediation and Prevention: After resolving a criminal case, law enforcement often takes steps to prevent future crimes. In cybersecurity, incident responders not only mitigate the immediate threat but also analyze the incident to improve defenses, implement new security measures, and develop strategies to prevent similar attacks in the future.**

Like a police detective, you must validate that a crime has happened, collect all of the possible evidence, and analyze the result.

2. Two of our malicious activities referred to Redline. What is Redline?

RedLine Stealer is a malicious program designed to collect sensitive user information. Here's a more detailed overview:

Data Collection: RedLine is primarily focused on gathering confidential data from various sources, including web browsers, installed software, and system configurations. It can capture usernames, passwords, credit card information, cookies, and autofill data.

Browser Targeting: The malware targets multiple web browsers, such as Chrome, Firefox, and Edge, allowing it to extract stored credentials and other personal data directly from users' sessions.

Installation of Additional Malware: In addition to stealing data, RedLine can facilitate the installation of other types of malware onto the infected system, further compromising the victim's security and privacy.

Distribution: RedLine is often distributed through phishing campaigns, malicious attachments, or exploit kits, making it a significant threat in the realm of cybercrime.

Impact: The information collected by RedLine can be used for identity theft, financial fraud, or sold on dark web marketplaces, making it a tool of choice for cybercriminals looking to exploit stolen data.

RedLine Stealer is a malicious program that collects users' confidential data from browsers, systems, and installed software. It also infects operating systems with other malware.