Snort Alert Analysis using SGUIL via Security Onion

January 13, 2024

Content

1 Introduction

Snort can be configured to alert administrators or actively block malicious traffic, providing a crucial layer of defense against various cyber threats. Snort is a common Network Analysis tool. It excels at identifying signature-based threats. In network intrusion detection/prevention mode, Snort can analyze packets and compare them with a set of rules that define malicious or suspicious behavior. If a rule matches, Snort can generate an alert or perform an action, such as blocking the packet, modifying the packet, or sending a response.

1.1 Initial Indicator of Compromise

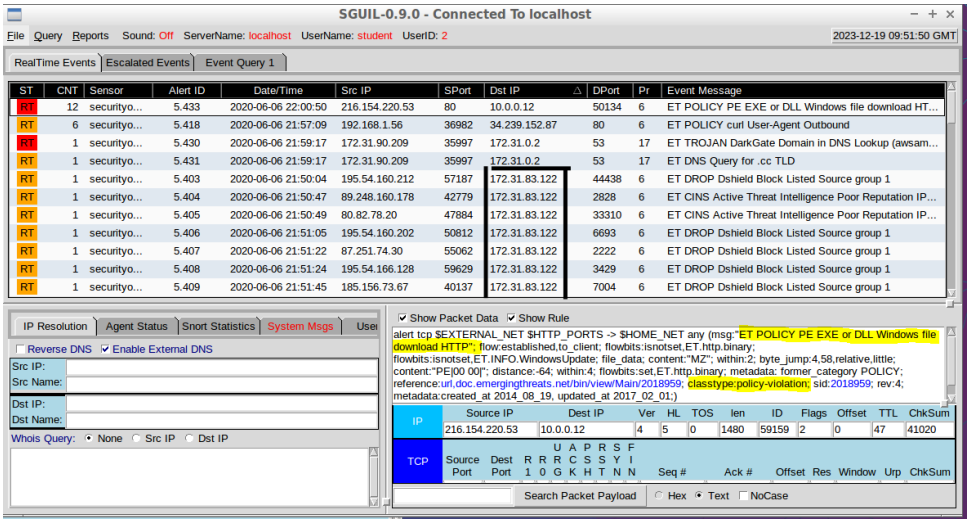

Figure 1: Reviewing Imported Network Traffic in Sguil

We have a network packet file project.pcap for our analysis. Let us take a look at the alert generated from the network intrusion detection system (IDS)

- Import PCAP file into Security Onion via terminal using the command.

```
sudo so-import-pcap
```

- Open Sguil and login with your credentials to view imported network traffic as shown below:

What Is A Honeypot?

In cybersecurity, a honeypot is a server that presents one or more seemingly-vulnerable services.

- Attracts attackers
- Provides threat intelligence
- Informs defensive measures
- Typically placed on an isolated network segment and excluded from IDS

In FIG 1, I have filtered out alerts related to the honeypot by sorting the Destination IP column. as shown. much traffic with different sources but moving to the same destination 172.31.83.122 (Honey pot destination). This is because probably honeypot is vulnerable and many attackers are trying it.

We can see an initial indicator of compromise:

```
2020-Jun-06 22:00:50 216.154.220.53:80 --> 10.0.0.12:50134
```

where

- 216.154.220.53 is the source IP and 80 is the source port
- 10.0.0.12 is Destination IP and 50134 is Destination port

Common indicators are:

- Alert content: "ET POLICY PE EXE or DLL Windows file download HTTP"
- Alert classtype: policy-violation, which is of high priority.
- network count: 12 >> 1
- Unusual time of day (non work hour). It may not be enough evidence on its own, but it makes it more suspicious.
- Downloaded object named fnpufu.exe, the request made with an unusual user-agent.

Given that the alert is coming from an external source IP "216.154.220.53", let us verify the status on VirusTotal. A check on **VirusTotal** revealed no flag.

Additional analysis: The source IP is not malicious, but we can:

- extract the detected object **fnpufu.exe**.
- calculate its SHA-256 hash value using the command:
  ```
  >> sha256sum fnpufu.exe
  output: 006d5fda899149df4cc5d6d1b1ae52e9fcc4ade7541c1dd4391e0429d843b4d5
  ```
- check the the resulting hash value against VirusTotal.

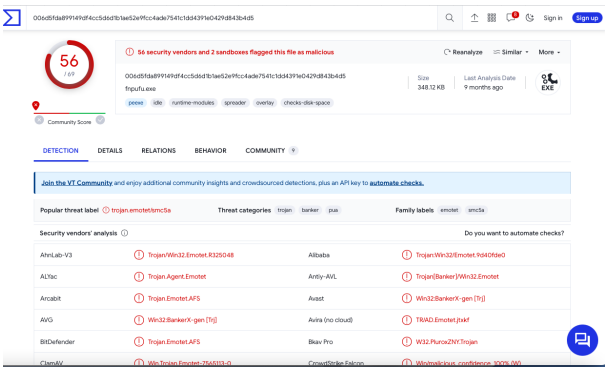

Figure 2: Result on VirusTotal, shows the file is a malware Trojan Emotet AFS

Figure 2 shows the result of looking up the hash value on VirusTotal, flagged by 56 vendors as malicious.

1.2 Additional Indicators of compromise

The Snort alerts may not tell the entire story. Remember that Snort:

- Can only alert on previously identified threats: new and unknown threats will not appear in Sguil!
- Network IDS Logs (Snort) only provide data for packets that match threat signatures. It is likely that Tanu's rules are not well written to capture all the threats.

We will review the network packet on Wireshark, checking HTTP network traffics to identify interesting signs of post-infection activity from the malicious malware.

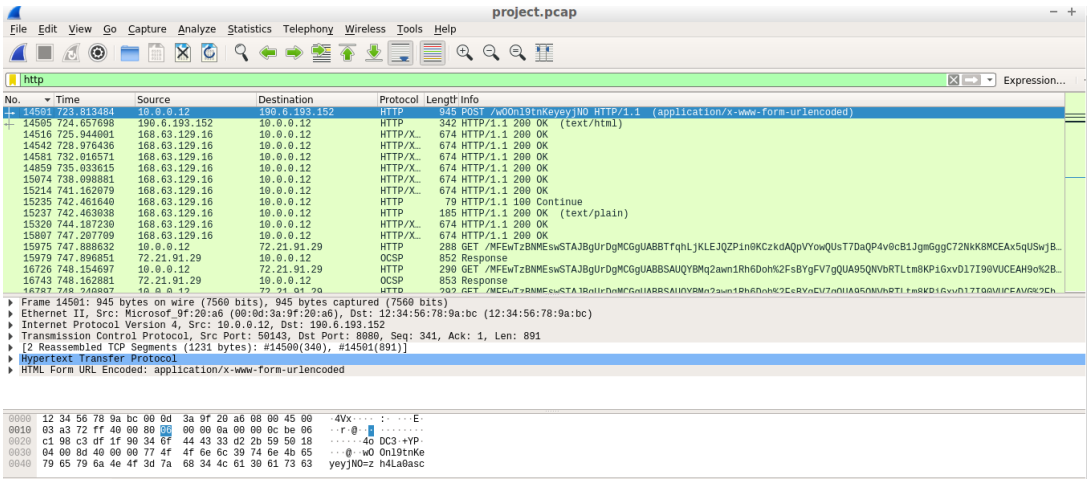

Figure 3: Reviewing the network packet file on Wireshark

The alert:

```
10.0.0.12 —> 190.6.193.152 POST /w00n19tnKeyeyjNO HTTP/1.1
Content-Type: application/x-www-form-urelencoded
```

where

- 10.0.0.12 is src IP and 50143 src port, 190.6.193.152 is dst IP and 8080 is the dst port

looks suspicious. Let's examine the Destination IP address on VirusTotal,

2 Discussion

The alert **ET POLICY PE EXE or DLL Windows file download HTTP**, is from the Emerging Threats (ET) ruleset, specifically from the "Policy" category, and it indicates a potential policy violation related to the download of a Windows PE (Portable Executable) file, which can be an executable (EXE) or dynamic link library (DLL), via HTTP.

Breaking down the alert:

- **ET POLICY**: This prefix signifies that the alert is related to a policy violation, meaning it's not necessarily an attack but could indicate an activity that violates a security policy or best practices.
- **PE EXE or DLL**: This part specifies the type of file being downloaded. PE refers to Portable Executable, the file format for executable files and DLLs on Windows.
- **Windows file download**: This clarifies that the alert is specifically related to the download of a file on a Windows system.
- **HTTP**: Indicates that the download occurred over the HTTP protocol.

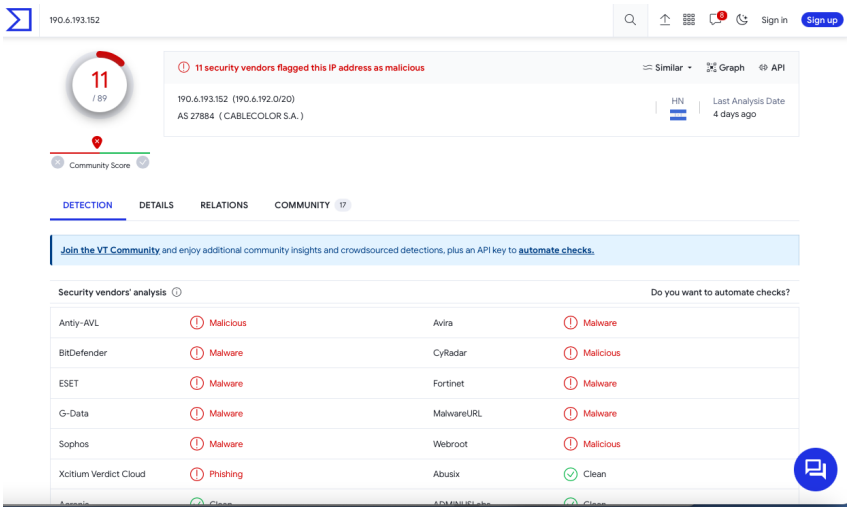

Figure 4: VirusTotal result shows 11 vendors had flagged the IP address as malicious

In simpler terms, this alert is triggered when there's an attempt to download a Windows executable (either an EXE or DLL file) over HTTP. Such alerts can be significant because executable files downloaded from the internet can pose a security risk. As we saw in our analysis, the alert is true positive - a malicious activity associated with malware.

3 Command and Control (C2)

Command and Control (C2) refers to a technique used by attackers to maintain control over compromised systems. In the context of a downloaded executable serving as a payload for C2.

The downloaded executable fnpufu.exe from our analysis is a payload designed to establish a connection with a command and control server **190.6.193.152** , enabling attackers to control the compromised system remotely.

here's how it typically works:

- **Delivery of Malicious Payload**: The attackers created the malicious payload: fnpufu.exe
- **Execution on the Target System**: fnpufu.exe was delivered to the target system through various means such as phishing emails, drive-by downloads, or other exploitation techniques (we do not know yet). Once on the system, a user (216.154.220.53 in our case) inadvertently tried to execute the malicious file.
- **Payload Establishes Connection**: Upon execution, the fnpufu.exe initiates a connection to a Command and Control server **190.6.193.152** operated by the attackers. This connection is typically established over the internet (HTTP).

The compromised system, now under the control of the attackers, is likely to send beacons or signals, commands instructing the malware or the compromised system to perform specific actions, data exfiltration, persistence and control, ensuring that it continues to run even after reboots. This persistence allows the attackers to maintain control over the system for an extended period.

Conclusion

As a security analyst monitoring network traffic, I have investigated alerts to determine whether the download is legitimate or if it requires further scrutiny. I analyzed the specific file being downloaded, the source and destination IP addresses, the associated URLs, and other relevant details to assess the potential risk and take appropriate actions if necessary.

Please go to other files in this folder to see how we are able to identify isntances of data exfiltration, persistence of the attackers in this or