Snort Alert Analysis using SGUIL via Security Onion

January 12, 2024

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.

Initial Indicator of Compromise

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:

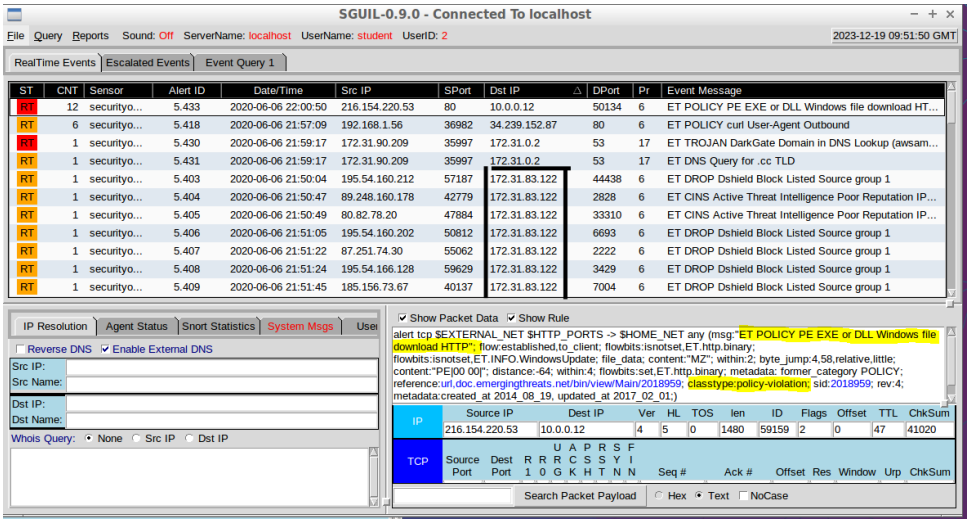


Figure 1: Reviewing Imported Network Traffic in Sguil

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 DST IP column. as shown. It is now easy to identify the initial indicator of compromise as:

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

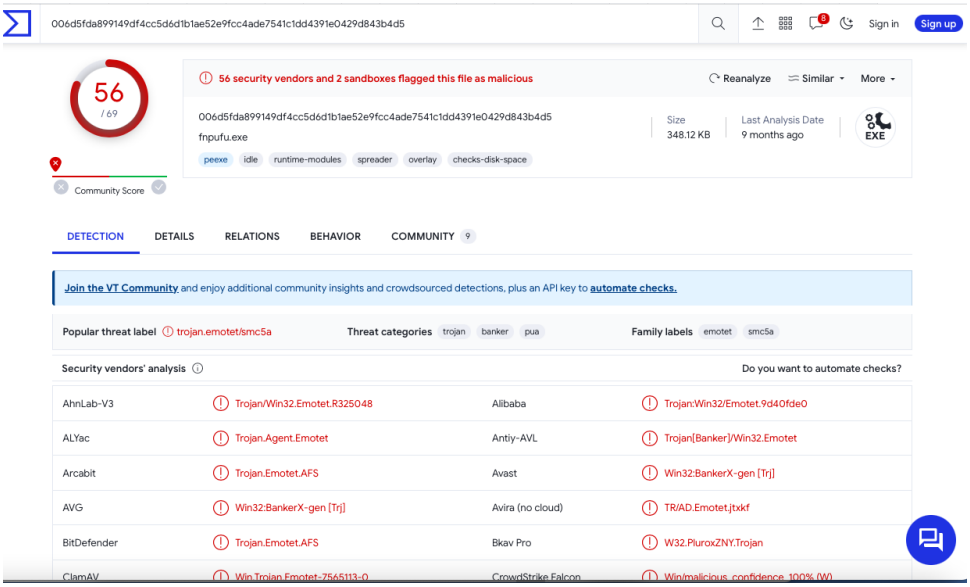


Figure 2: Result on VirusTotal, shows the file is a malware Trojan Emotet AFS

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 the Tanu's rules are not well written to capture all the threats.

We will now use Wireshark to review related HTTP network traffics to identify interesting signs of post-infection activity from the malware download.

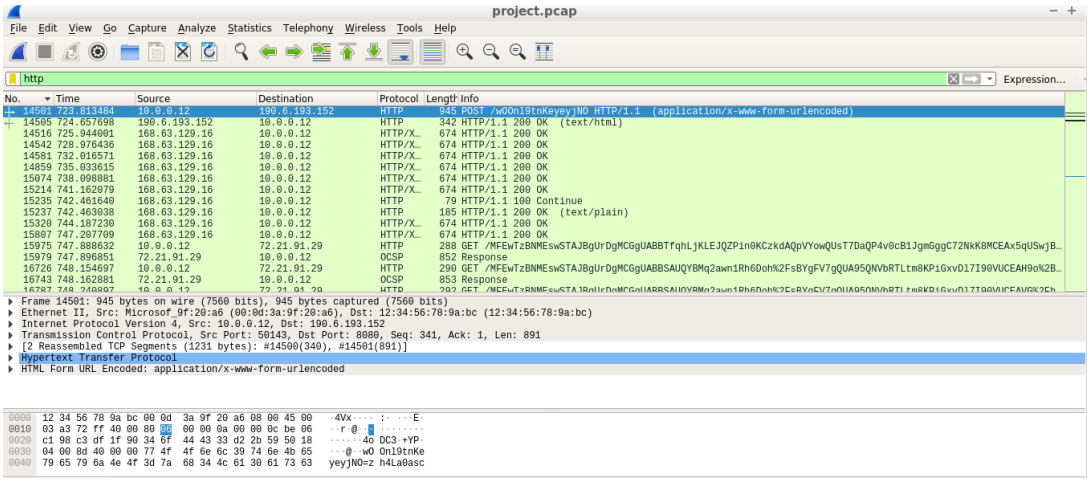


Figure 3: Reviewing the network packet file on Wireshark

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

Looking up the Destination IP address on VirusTotal,

1 Live Packet Capture

Multiple Snort alerts were triggered by a single DNS request.

Identify the DNS request in Sguil that triggered multiple alerts. Record the same request from the Security Onion VM using tcpdump. Save the file to dns.pcap and include this file in your project submission.

2 Read and Analyze Packet Captures

Malware will frequently check in with a command-and-control server shortly after it is installed.

Even after applying filters, the file may still have thousands of records. Are there any connections that appear particularly unusual that may be related to the network IDS alert? Investigate the IP addresses involved.

3 Collecting and analyzing data with Splunk

Find the Zeek conn.log entry related to the suspicious activity identified in Step 1. Take a screenshot of the search query with the search result (there should be only one result) and save it as search.png

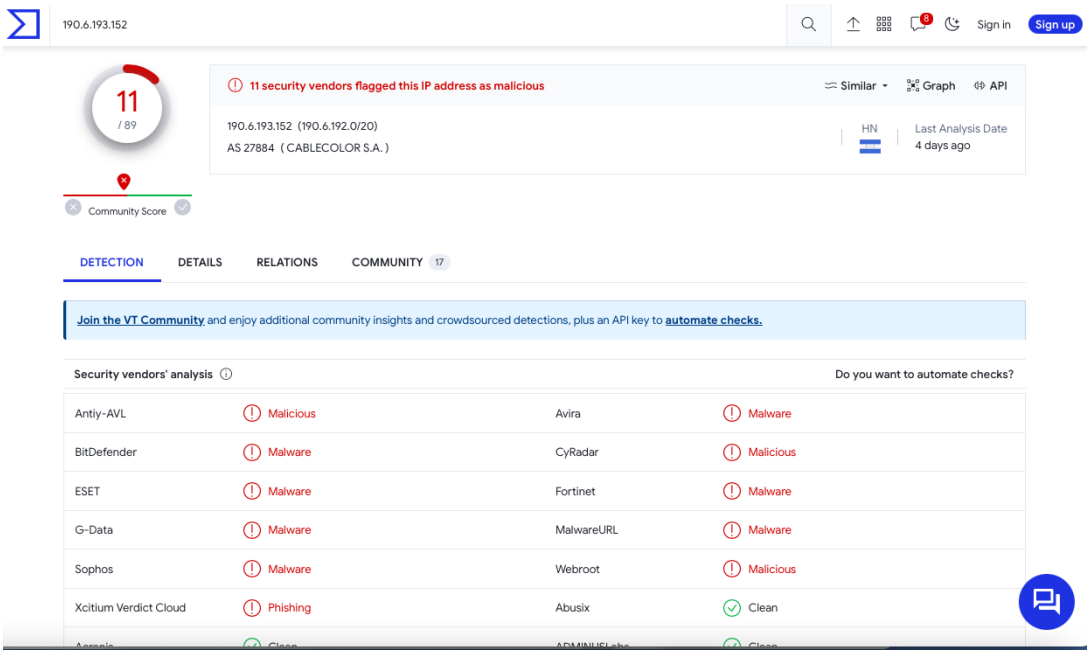
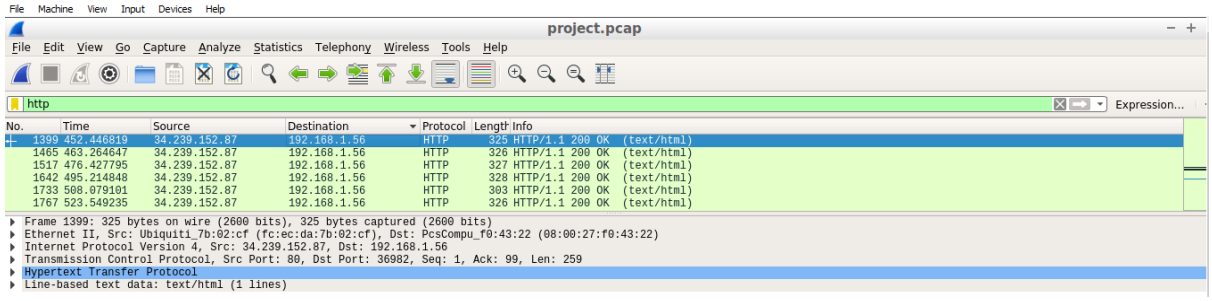


Figure 4: VirusTotal result shows 11 vendors had flagged the IP address as malicious



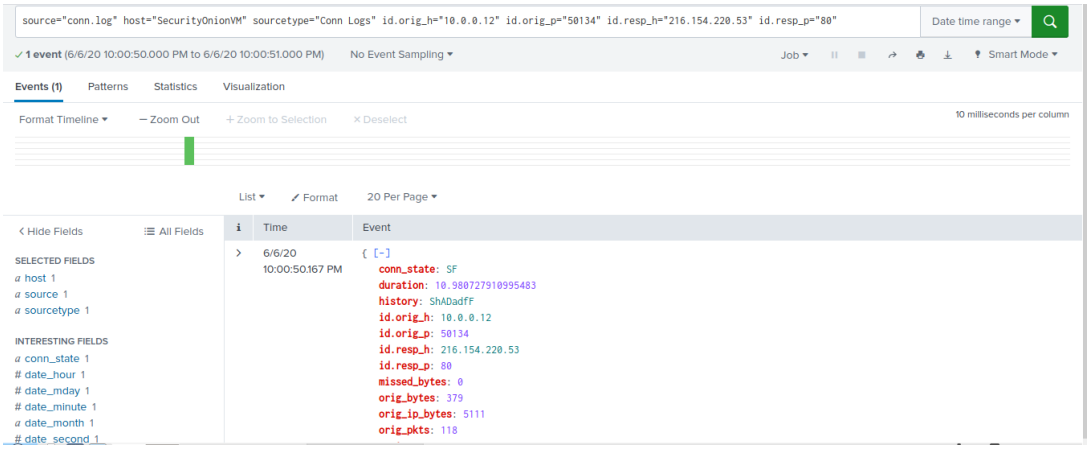


Figure 5: Snapshot of

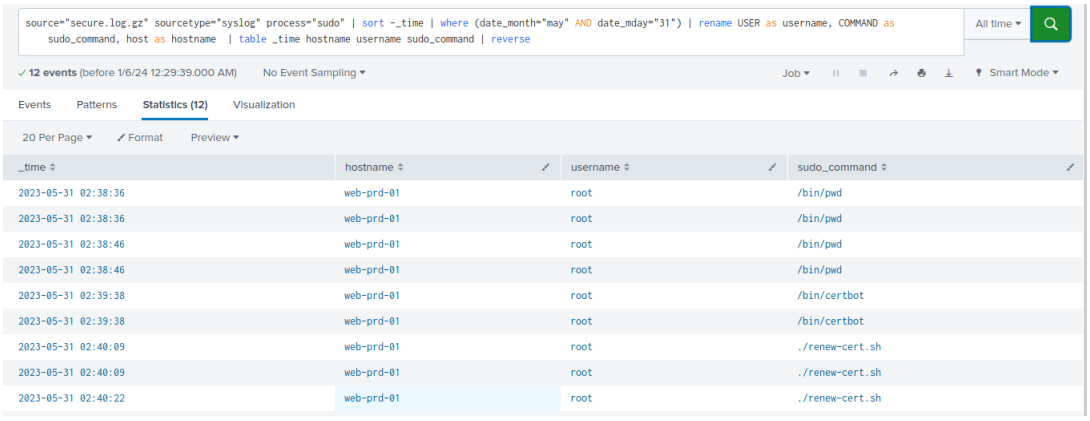


Figure 6: Privilege escalation

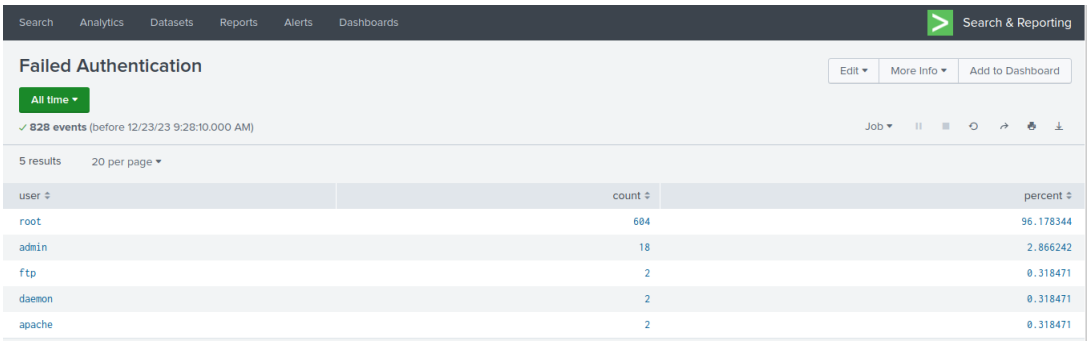


Figure 7: Failed Authentication

4 Containment:

- We are identifying the infected assets(s) and physically disconnect them from the network:
- 22:10 The Network Operations Center (616-555-4662) has been contacted and the on-call staff has been asked to disable network access to the wall jack (desktop) or network switch (data center).
- Copies of the malicious code, affected systems and any identified artefacts for further investigation are secured.
- Business continuity options for users affected by such disconnection include: a) Replacing disconnected devices with fresh builds from IT, where stocks permit (ensuring they first have relevant updates applied). b) Directing users whose devices are disconnected to work from an alternative location; such as another office, a Disaster Recovery facility or from home.
- The account passwords for any system users will be reset, including local and administrative accounts. Help Desk (616-555-4357) will assist with this.
- Login credentials of suspected compromised accounts are suspended

5 Analysis (other compromised hosts, lateral movement, data exfiltration, etc.)

We are monitoring for any new infections which might suggest that the malware is spreading across the infrastructure. The latest malware definitions have been deployed across the antimalware solution.

An estate-wide anti-malware scan is initiated. We will determine whether the malware appeared to be communicating with outside parties and take steps to block any such communication. We will Inform business data owner(s) and stakeholders of the progress of containment activities.

6 Recovery:

Complete malware scanning of all systems, across the estate. Re-image systems. Re-set the credentials of all involved system(s) and users account details. Restore any corrupted or destroyed data. Restore any suspended services Post-incident recommendations: Draft a post-incident report that includes the following details as a minimum: Details of the cyber incident identified and remediated across the network to include timings, type and location of incident as well as the effect on users; Activities that were undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to be resumed; Recommendations where any aspects of people, process or technology could be improved across the organization to help prevent a similar cyber incident from reoccurring, as part of a formalized lessons identified process. Complete the formal lessons identified process to feedback into future preparation activities. Consider sharing lessons identified with the wider stakeholders. Conduct root cause analysis to identify and remediate underlying vulnerabilities. Publish internal communications in line with the communications strategy to inform and educate employees on malware attacks and security awareness