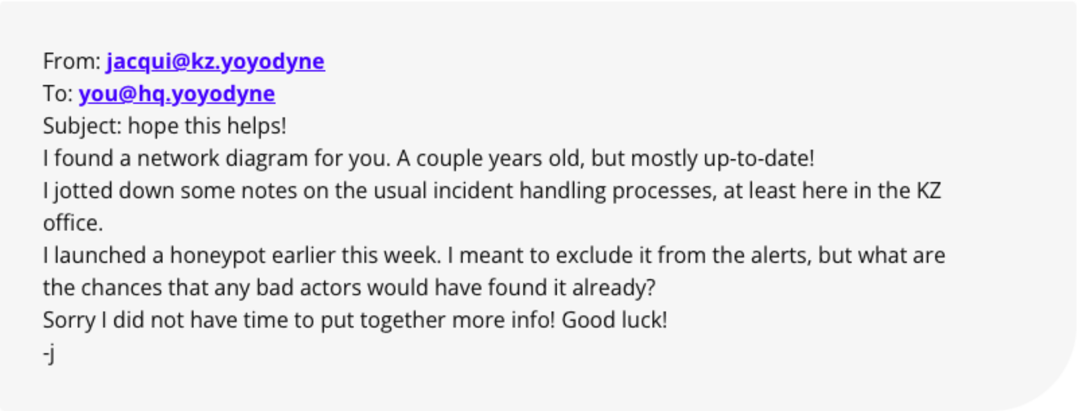
Incident Detection and Response

December 21, 2023

Introduction

Part of the job we do as security analyst is monitoring and analyzing alerts, and responding to security incidents. In this project, I will be filling in for Jacqui, a colleague at Yoyodyne's satellite office in Kalamazoo who is on vacation.

The Scenario



From: jacqui@kz.yoyodyne
To: you@hq.yoyodyne
Subject: hope this helps!
I found a network diagram for you. A couple years old, but mostly up-to-date!
I jotted down some notes on the usual incident handling processes, at least here in the KZ office.
I launched a honeypot earlier this week. I meant to exclude it from the alerts, but what are the chances that any bad actors would have found it already?
Sorry I did not have time to put together more info! Good luck!
-j

Here is the project outline:

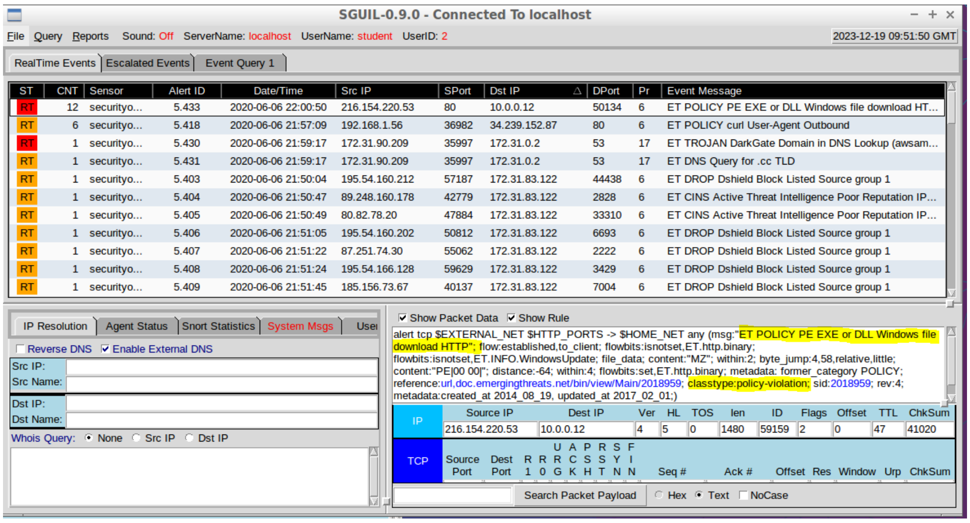
Outline

- Analyze Alerts from the Intrusion Detection System using Sguil.
- Live Packet Capture with tcpdump
- Read and Analyze Packet Captures with wireshark
- Create a Snort rule
- Use Splunk to Collect and Analyze Data
- Use Incident Response playbooks to Determine the Next Steps

1 IDS Alert Analysis using SGUIL via Security Onion

First analyzing a PCAP file that captured network alerts based on the snort rule written by Jacqui.

- 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.



SGUIL-0.9.0 - Connected To localhost
File Query Reports
RealTime Events | Escalated Events | Event Query 1
IP Resolution | Agent Status | Snort Statistics | System Msgs | User
Search Packet Payload

Sound: Off ServerName: localhost UserName: student UserID: 2 2023-12-19 09:51:50 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	12	securityo...	5.433	2020-06-06 22:00:50	216.154.220.53	80	10.0.0.12	50134	6	ET POLICY PE EXE or DLL Windows file download HT...
RT	6	securityo...	5.418	2020-06-06 21:57:09	192.168.1.56	36982	34.239.152.87	80	6	ET POLICY curl User-Agent Outbound
RT	1	securityo...	5.430	2020-06-06 21:59:17	172.31.90.209	35997	172.31.0.2	53	17	ET TROJAN DarkGate Domain in DNS Lookup (awsam...
RT	1	securityo...	5.431	2020-06-06 21:59:17	172.31.90.209	35997	172.31.0.2	53	17	ET DNS Query for .cc TLD
RT	1	securityo...	5.403	2020-06-06 21:50:04	195.54.160.212	57187	172.31.83.122	44438	6	ET DROP Dshield Block Listed Source group 1
RT	1	securityo...	5.404	2020-06-06 21:50:47	89.248.160.178	42779	172.31.83.122	2828	6	ET CINS Active Threat Intelligence Poor Reputation IP...
RT	1	securityo...	5.405	2020-06-06 21:50:49	80.82.78.20	47884	172.31.83.122	33310	6	ET CINS Active Threat Intelligence Poor Reputation IP...
RT	1	securityo...	5.406	2020-06-06 21:51:05	195.54.160.202	50812	172.31.83.122	6693	6	ET DROP Dshield Block Listed Source group 1
RT	1	securityo...	5.407	2020-06-06 21:51:22	87.251.74.30	55062	172.31.83.122	2222	6	ET DROP Dshield Block Listed Source group 1
RT	1	securityo...	5.408	2020-06-06 21:51:24	195.54.166.128	59629	172.31.83.122	3429	6	ET DROP Dshield Block Listed Source group 1
RT	1	securityo...	5.409	2020-06-06 21:51:45	185.156.73.67	40137	172.31.83.122	7004	6	ET DROP Dshield Block Listed Source group 1

☐ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY PE EXE or DLL Windows file download HTTP"; flow:established,to_client; flowbits:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate; file_data; content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"PE|00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary; metadata: former_category POLICY; reference:url,doc.emergingthreats.net/bin/view/Main/2018959; classtype:policy-violation; sid:2018959; rev:4; metadata:created_at 2014_08_19, updated_at 2017_02_01;)
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	216.154.220.53	10.0.0.12	4	5	0	1480	59159	2	0	47	41020

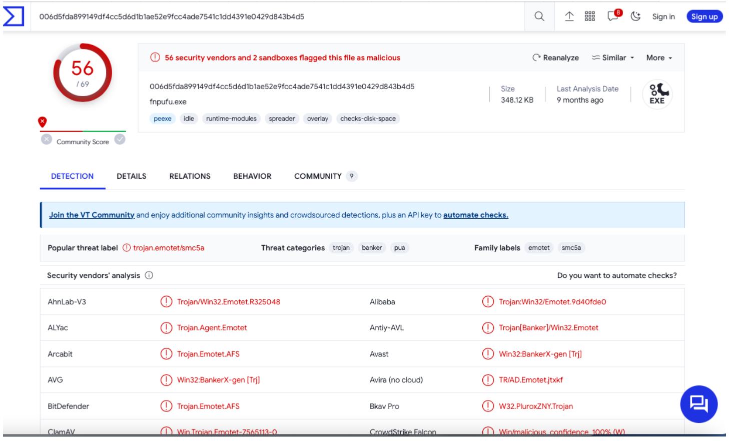
TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum

○ Hex ● Text ☐ NoCase

Figure 1: Reviewing Imported Network Traffic in Sguil

The first alert "ET POLICY PE EXE or DLL Windows file download HTTP", is suspicious.

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



006d5fda899149df4cc5d6d1b1ae52e9fcc4ade7541c1dd4391e0429d843b4d5

56 / 69

56 security vendors and 2 sandboxes flagged this file as malicious

006d5fda899149df4cc5d6d1b1ae52e9fcc4ade7541c1dd4391e0429d843b4d5
fnpufu.exe
peexe idle runtime-modules spreader overlay checks-disk-space

Size 348.12 KB
Last Analysis Date 9 months ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.emotet/smc5a Threat categories trojan banker pua Family labels emotet smc5a

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Emotet.R325048	Alibaba	Trojan:Win32/Emotet.9d40fde0
ALYac	Trojan.Agent.Emotet	Antiy-AVL	Trojan[Banker]/Win32.Emotet
Arcabit	Trojan.Emotet.AFS	Avast	Win32:BankerX-gen [Trj]
AVG	Win32:BankerX-gen [Trj]	Avira (no cloud)	TR/AD.Emotet.jtxkf
BitDefender	Trojan.Emotet.AFS	Bkav Pro	W32.PluroxZNY.Trojan
ClamAV	Win.Trojan.Emotet-7565113-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)

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

Common indicators are:

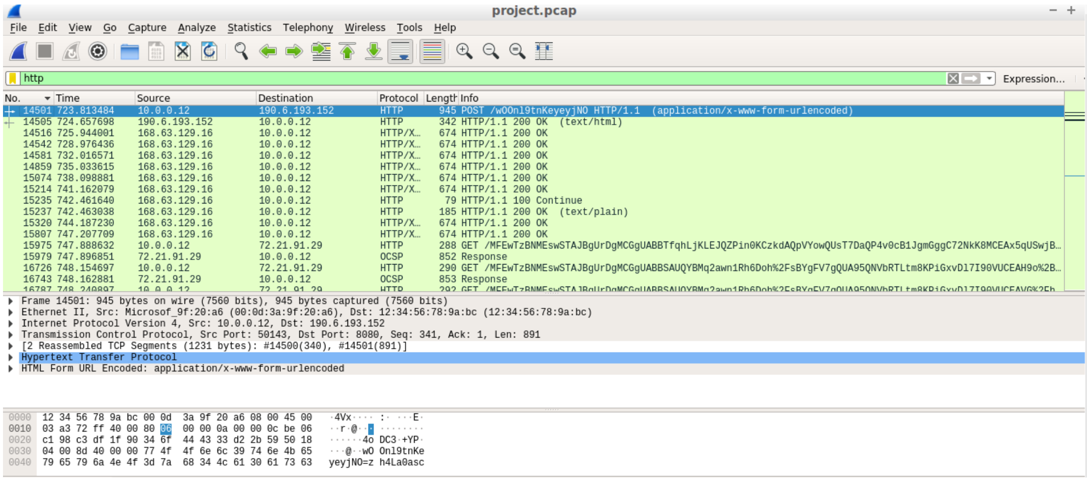
- alert of classtype policy-violation, which is of high priority.
- Downloaded malware named fnpufu.exe, the request made with an unusual user-agent.

The Source IP "216.154.220.53" shows no suspicious indication on VirusTotal. Further analysis include

- Download the payload fnpufu.exe and calculate the SHA256 using **sha256sum fnpufu.exe**
- Lookup the resulting file hash on VirusTotal.

2 Additional Indicators of compromise

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. Other ways to investigate the network packet capture is using wireshark. Looking at the HTTP packets only, the following entry was detected



project.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

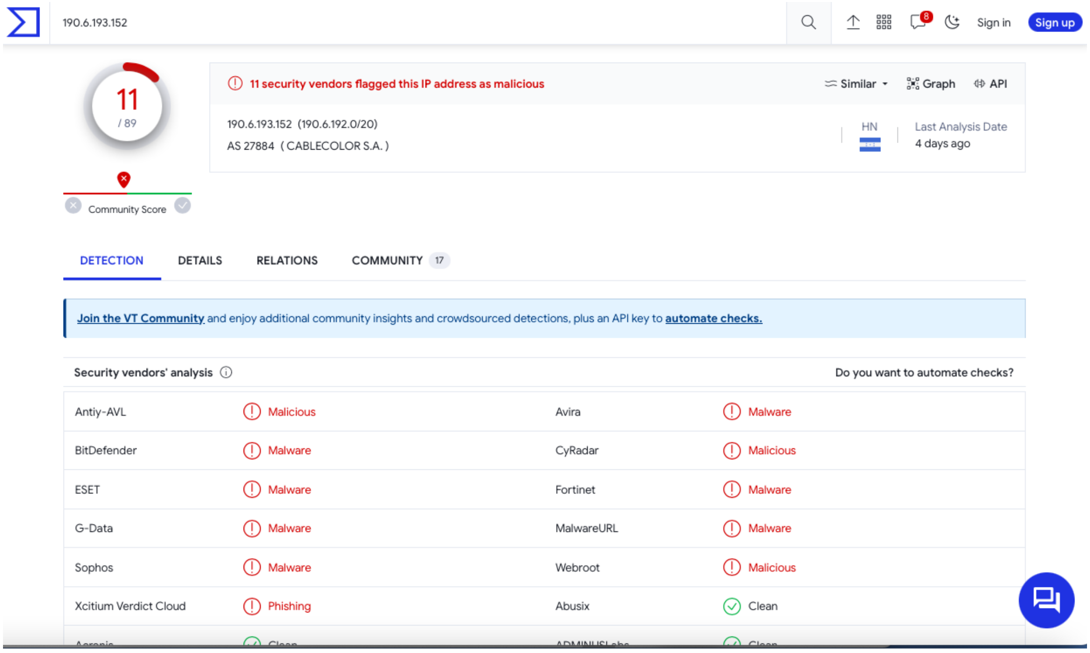
http

```
No.    Time       Source          Destination     Protocol Length Info
14501 723.813484  10.0.0.12       190.6.193.152   HTTP      945 POST /wOOnl9tnKeyeyjNO HTTP/1.1  (application/x-www-form-urlencoded)
14505 724.657698  190.6.193.152   10.0.0.12       HTTP      342 HTTP/1.1 200 OK  (text/html)
14516 725.944001  168.63.129.16   10.0.0.12       HTTP/X…   674 HTTP/1.1 200 OK
14542 728.976436  168.63.129.16   10.0.0.12       HTTP/X…   674 HTTP/1.1 200 OK
14581 732.016571  168.63.129.16   10.0.0.12       HTTP/X…   674 HTTP/1.1 200 OK
14859 735.033615  168.63.129.16   10.0.0.12       HTTP/X…   674 HTTP/1.1 200 OK
15074 738.098881  168.63.129.16   10.0.0.12       HTTP/X…   674 HTTP/1.1 200 OK
15214 741.162079  168.63.129.16   10.0.0.12       HTTP/X…   674 HTTP/1.1 200 OK
15235 742.461640  168.63.129.16   10.0.0.12       HTTP       79 HTTP/1.1 100 Continue
15237 742.463038  168.63.129.16   10.0.0.12       HTTP      185 HTTP/1.1 200 OK  (text/plain)
15320 744.187230  168.63.129.16   10.0.0.12       HTTP/X…   674 HTTP/1.1 200 OK
15807 747.207709  168.63.129.16   10.0.0.12       HTTP/X…   674 HTTP/1.1 200 OK
15975 747.888632  10.0.0.12       72.21.91.29     HTTP      288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEAx5qUSwjB…
15979 747.896851  72.21.91.29     10.0.0.12       OCSP      852 Response
16726 748.154697  10.0.0.12       72.21.91.29     HTTP      290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAH9o%2B…
16743 748.162881  72.21.91.29     10.0.0.12       OCSP      853 Response
16787 748.240897  10.0.0.12       72.21.91.29     HTTP      292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAVG%2Fh

▸ Frame 14501: 945 bytes on wire (7560 bits), 945 bytes captured (7560 bits)
▸ Ethernet II, Src: Microsof_9f:20:a6 (00:0d:3a:9f:20:a6), Dst: 12:34:56:78:9a:bc (12:34:56:78:9a:bc)
▸ Internet Protocol Version 4, Src: 10.0.0.12, Dst: 190.6.193.152
▸ Transmission Control Protocol, Src Port: 50143, Dst Port: 8080, Seq: 341, Ack: 1, Len: 891
▸ [2 Reassembled TCP Segments (1231 bytes): #14500(340), #14501(891)]
▸ Hypertext Transfer Protocol
▸ HTML Form URL Encoded: application/x-www-form-urlencoded

0000  12 34 56 78 9a bc 00 0d  3a 9f 20 a6 08 00 45 00   ·4Vx···· :· ···E·
0010  03 a3 72 ff 40 00 80 06  00 00 0a 00 00 0c be 06   ··r·@··· ········
0020  c1 98 c3 df 1f 90 34 6f  44 43 33 d2 2b 59 50 18   ······4o DC3·+YP·
0030  04 00 8d 40 00 00 77 4f  4f 6e 6c 39 74 6e 4b 65   ···@··wO Onl9tnKe
0040  79 65 79 6a 4e 4f 3d 7a  68 34 4c 61 30 61 73 63   yeyjNO=z h4La0asc
```

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,



190.6.193.152

11 security vendors flagged this IP address as malicious

190.6.193.152 (190.6.192.0/20)
AS 27884 (CABLECOLOR S.A.)

HN

Last Analysis Date
4 days ago

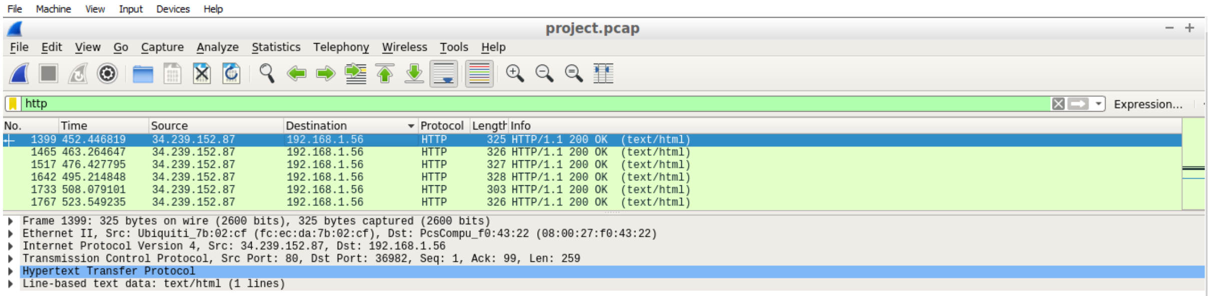
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	Avira	Malware
BitDefender	Malware	CyRadar	Malicious
ESET	Malware	Fortinet	Malware
G-Data	Malware	MalwareURL	Malware
Sophos	Malware	Webroot	Malicious
Xcitium Verdict Cloud	Phishing	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

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



File Machine View Input Devices Help
project.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1399	452.446819	34.239.152.87	192.168.1.56	HTTP	325	HTTP/1.1 200 OK (text/html)
1465	463.264647	34.239.152.87	192.168.1.56	HTTP	326	HTTP/1.1 200 OK (text/html)
1517	476.427795	34.239.152.87	192.168.1.56	HTTP	327	HTTP/1.1 200 OK (text/html)
1642	495.214848	34.239.152.87	192.168.1.56	HTTP	328	HTTP/1.1 200 OK (text/html)
1733	508.079101	34.239.152.87	192.168.1.56	HTTP	303	HTTP/1.1 200 OK (text/html)
1767	523.549235	34.239.152.87	192.168.1.56	HTTP	326	HTTP/1.1 200 OK (text/html)

```
▸ Frame 1399: 325 bytes on wire (2600 bits), 325 bytes captured (2600 bits)
▸ Ethernet II, Src: Ubiquiti_7b:02:cf (fc:ec:da:7b:02:cf), Dst: PcsCompu_f0:43:22 (08:00:27:f0:43:22)
▸ Internet Protocol Version 4, Src: 34.239.152.87, Dst: 192.168.1.56
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 36982, Seq: 1, Ack: 99, Len: 259
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (1 lines)
```