Challenge: [NerisBot Lab]

Platform: CyberDefenders

Category: Threat Hunting

Difficulty: Easy

Tools Used: Splunk

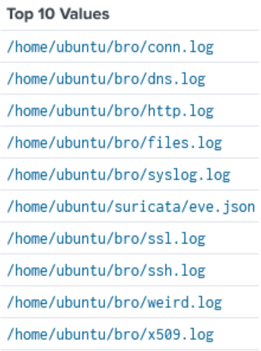
Summary: This challenge involved using Splunk to perform threat hunting. I found this challenge to be relatively difficulty, I don't necessarily agree with the difficulty rating of easy, I honestly think it should be changed to medium, if not hard. However, given the hints and a lot of research, this room does teach you a lot, especially about Zeek logs and Suricata alerts.

Scenario: Unusual network activity has been detected within a university environment, indicating potential malicious intent. These anomalies, observed six hours ago, suggest the presence of command and control (C2) communications and other harmful behaviors within the network.

Your team has been tasked with analyzing recent network traffic logs to investigate the scope and impact of these activities. The investigation aims to identify command and control servers and uncover malicious interactions.

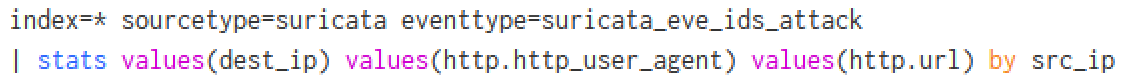
During the investigation of network traffic, unusual patterns of activity were observed in Suricata logs, suggesting potential unauthorized access. One external IP address initiated access attempts and was later seen downloading a suspicious executable file. This activity strongly indicates the origin of the attack.
What is the IP address from which the initial unauthorized access originated?

Based on the source field, this Splunk instance seems to have ingested zeek logs:



```
Top 10 Values
/home/ubuntu/bro/conn.log
/home/ubuntu/bro/dns.log
/home/ubuntu/bro/http.log
/home/ubuntu/bro/files.log
/home/ubuntu/bro/syslog.log
/home/ubuntu/suricata/eve.json
/home/ubuntu/bro/ssl.log
/home/ubuntu/bro/ssh.log
/home/ubuntu/bro/weird.log
/home/ubuntu/bro/x509.log
```

After some trial and error, I ended up using the hints to help me out. Within the hint is an SPL query:

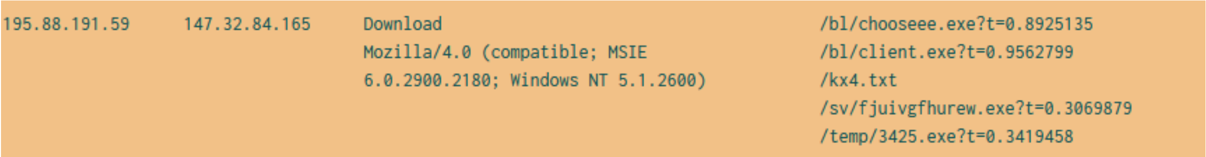


```
index=* sourcetype=suricata eventtype=suricata_eve_ids_attack
| stats values(dest_ip) values(http.http_user_agent) values(http.url) by src_ip
```

This query looks for Suricata IDS attack alerts. It then groups results by src_ip, for each source IP it lists:

- All unique dest_ip values
- All unique http.http_user_agent strings
- All unique http.uri values

After looking through the results, I came across 147.32.84.165 which made a series of suspicious requests to 195.88.191.59:



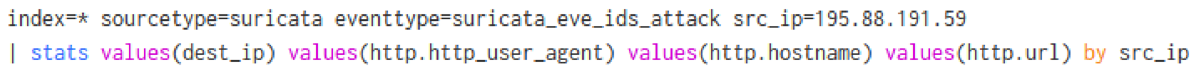
195.88.191.59	147.32.84.165	Download Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)	/bl/chooseee.exe?t=0.8925135 /bl/client.exe?t=0.9562799 /kx4.txt /sv/fjuivgfhurew.exe?t=0.3069879 /temp/3425.exe?t=0.3419458

Not only are there suspicious requests being made, one of the user-agents is “Download”, which is atypical for a user-agent string.

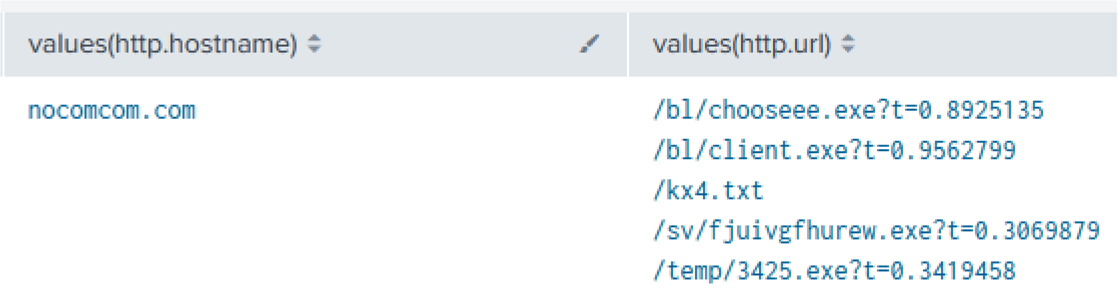
Answer: 195.88.191.59

Investigating the attacker’s domain helps identify the infrastructure used for the attack, assess its connections to other threats, and take measures to mitigate future attacks. What is the domain name of the attacker server?

In order to find the domain name associated with the suspicious activity observed in question one, we can add the http.hostname field to the original query and filter for the specific source IP:

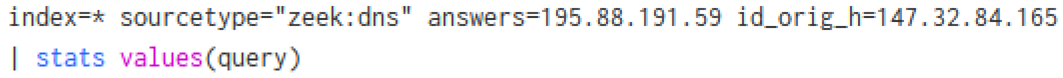


```
index=* sourcetype=suricata eventtype=suricata_eve_ids_attack src_ip=195.88.191.59
| stats values(dest_ip) values(http.http_user_agent) values(http.hostname) values(http.url) by src_ip
```

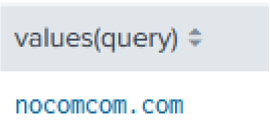


values(http.hostname)	values(http.url)
nocomcom.com	/bl/chooseee.exe?t=0.8925135 /bl/client.exe?t=0.9562799 /kx4.txt /sv/fjuivgfhurew.exe?t=0.3069879 /temp/3425.exe?t=0.3419458

Alternatively, you can look at the DNS queries made by 147.32.84.165:



```
index=* sourcetype="zeek:dns" answers=195.88.191.59 id_orig_h=147.32.84.165
| stats values(query)
```



values(query)
nocomcom.com

As you can see, both queries are able to find the domain associated with 195.88.191.59. The second query that uses the DNS logs looks for DNS responses where the returned IP was 195.88.191.59 (i.e., the query returned the attackers IP) and the source of the query was 147.32.84.165.

Answer: nocomcom.com

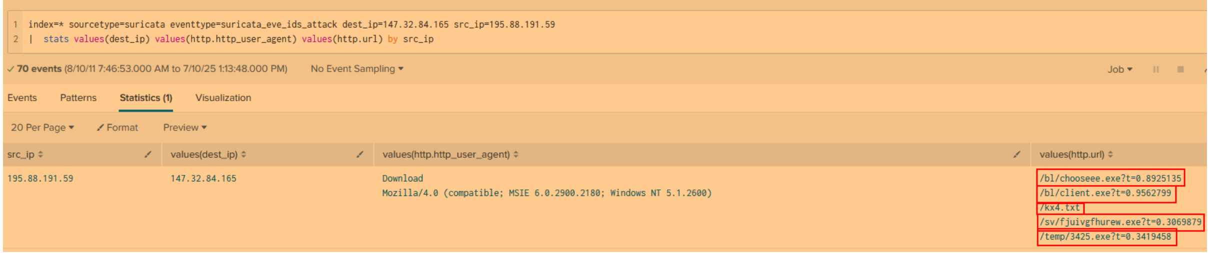
Knowing the IP address of the targeted system helps focus remediation efforts and assess the extent of the compromise. What is the IP address of the system that was targeted in this breach?

In question one, you can see that the destination IP of the host that downloaded the suspicious executable files was 147.32.84.165. Meaning that 147.32.84.165 downloaded the files from the attacker's domain which resolves to 195.88.191.59.

Answer: 147.32.84.165

Identify all the unique files downloaded to the compromised host. How many of these files could potentially be malicious?

Recall in question one we were able to see the requests made to the malicious domain. If you run this query again, you can see that the host downloaded 5 files, 4 being executables and one being a text file.



```
index=* sourcetype=suricata eventtype=suricata_eve_ids_attack dest_ip=147.32.84.165 src_ip=195.88.191.59
|  stats values(dest_ip) values(http.http_user_agent) values(http.url) by src_ip
```

✓ 70 events (8/10/11 7:46:53.000 AM to 7/10/25 1:13:48.000 PM) No Event Sampling ▾

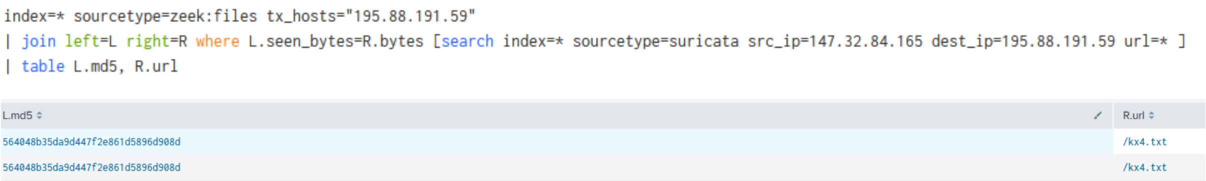
src_ip	values(dest_ip)	values(http.http_user_agent)	values(http.url)
195.88.191.59	147.32.84.165	Download Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)	/bl/chooseee.exe?t=0.8925135 /bl/client.exe?t=0.9562799 /kx4.txt /sv/fjuivgfhurew.exe?t=0.3069879 /temp/3425.exe?t=0.3419458

The file names are seemingly random, except for client.exe and chooseee.exe, although from this alone you should be relatively suspicious. Unfortunately, given the file names, we cannot determine the behaviour of these executables.

Answer: 5

What is the SHA256 hash of the malicious file disguised as a .txt file?

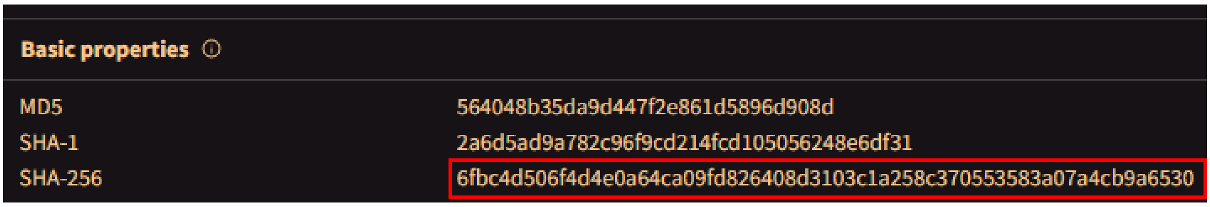
I honestly looked around for ages, and I just couldn't find the right log source. I started off checking the zeek:files source, but all the filename fields were blank. I ended up using the hints which gave this super long query:



```
index=* sourcetype=zeek:files tx_hosts="195.88.191.59"
| join left=L right=R where L.seen_bytes=R.bytes [search index=* sourcetype=suricata src_ip=147.32.84.165 dest_ip=195.88.191.59 url=* ]
| table L.md5, R.url
```

L.md5	R.url
564048b35da9d447f2e861d5896d908d	/kx4.txt
564048b35da9d447f2e861d5896d908d	/kx4.txt

If you chuck this MD5 hash into VirusTotal, you can find the SHA256 hash in the Details tab:



Basic properties

MD5	564048b35da9d447f2e861d5896d908d
SHA-1	2a6d5ad9a782c96f9cd214fcd105056248e6df31
SHA-256	6fbc4d506f4d4e0a64ca09fd826408d3103c1a258c370553583a07a4cb9a6530

Answer: 6fbc4d506f4d4e0a64ca09fd826408d3103c1a258c370553583a07a4cb9a6530