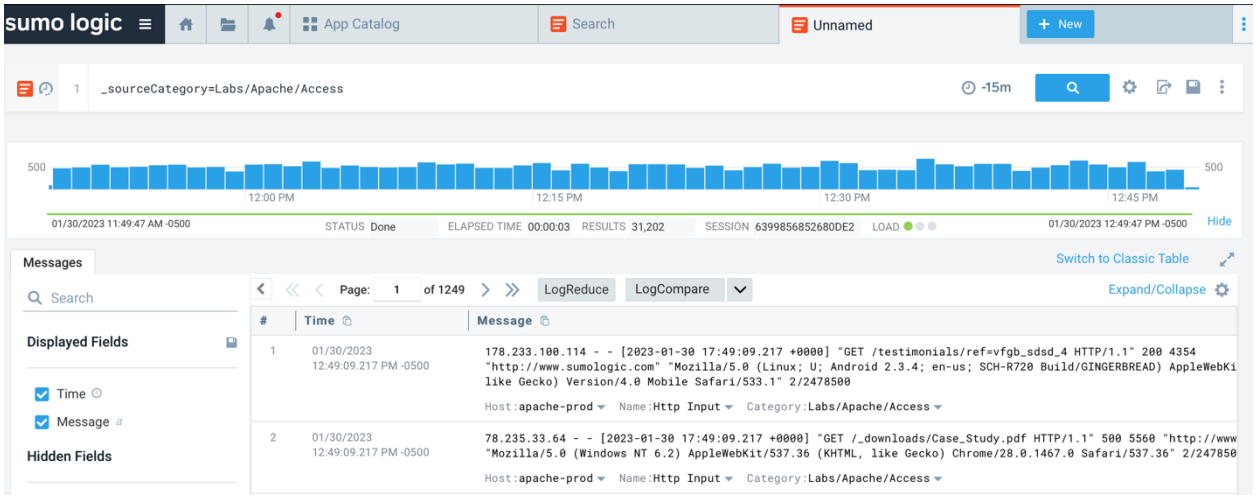
WEB APPLICATION ATTACK ASSIGNMENT

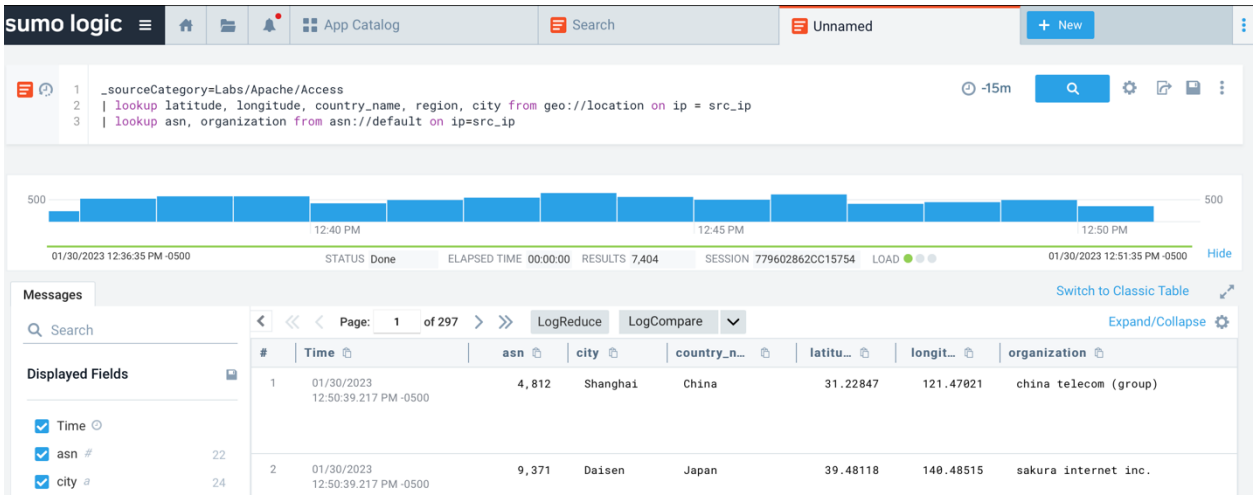
Screenshots from the lab

Reviewing logs

_sourceCategory=Labs/Apache/Access

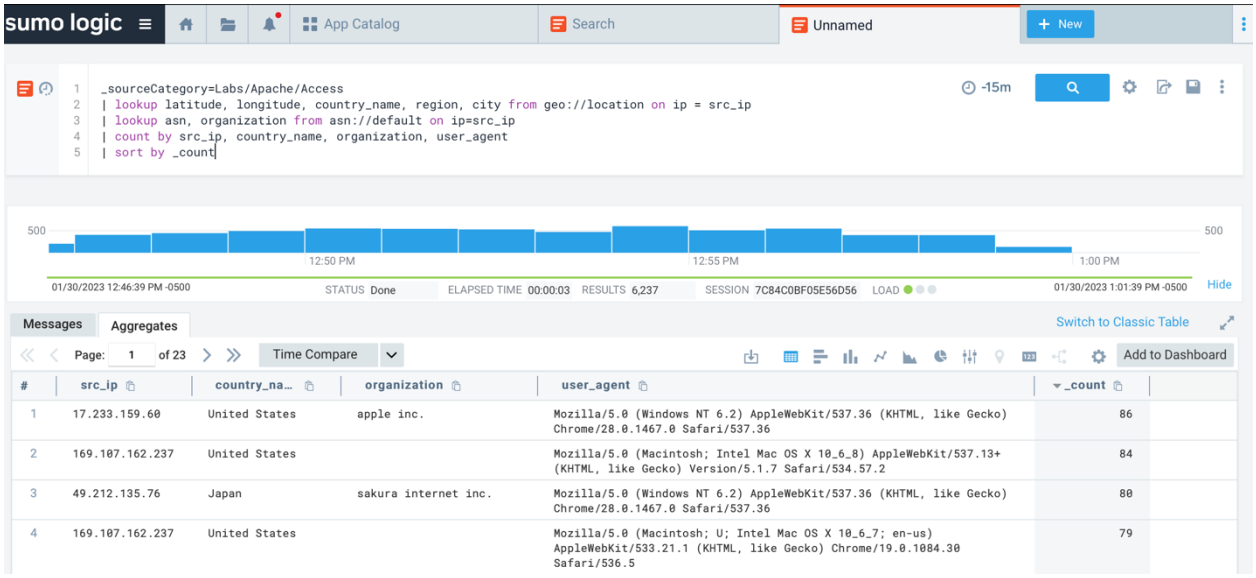


_sourceCategory=Labs/Apache/Access
| lookup latitude, longitude, country_name, region, city from geo://location on ip = src_ip
| lookup asn, organization from asn://default on ip=src_ip



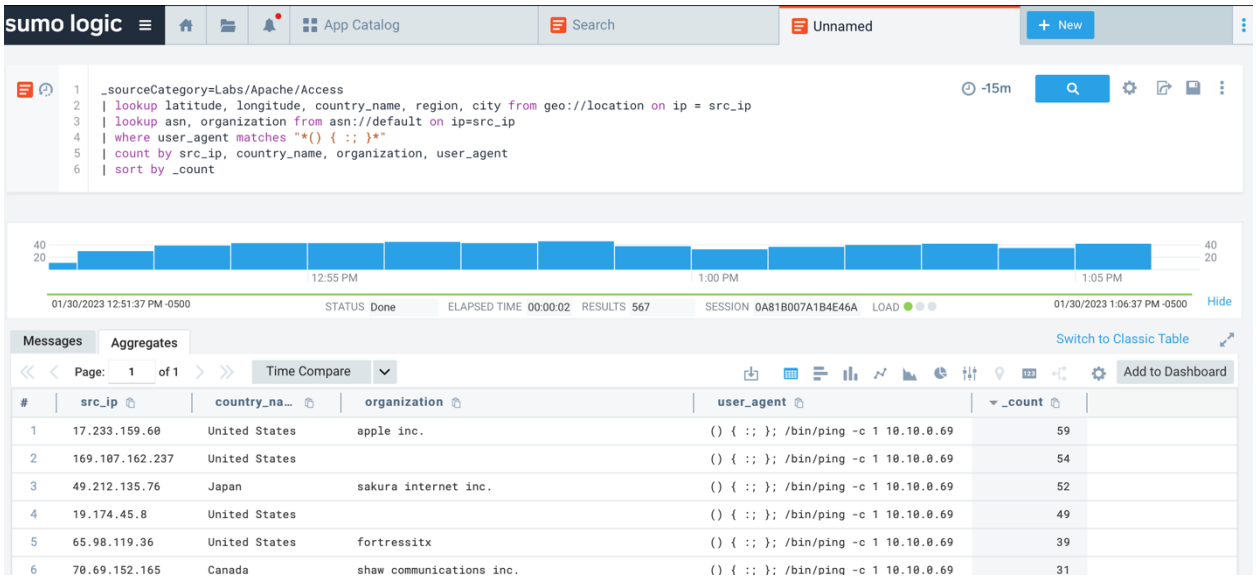
Malicious User String Agent

```
_sourceCategory=Labs/Apache/Access
| lookup latitude, longitude, country_name, region, city from geo://location on ip = src_ip
| lookup asn, organization from asn://default on ip=src_ip
| count by src_ip, country_name, organization, user_agent
| sort by _count
```



#	src_ip	country_na…	organization	user_agent	_count
1	17.233.159.60	United States	apple inc.	Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1467.0 Safari/537.36	86
2	169.107.162.237	United States		Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/537.13+ (KHTML, like Gecko) Version/5.1.7 Safari/534.57.2	84
3	49.212.135.76	Japan	sakura internet inc.	Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1467.0 Safari/537.36	80
4	169.107.162.237	United States		Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_7; en-us) AppleWebKit/533.21.1 (KHTML, like Gecko) Chrome/19.0.1084.30 Safari/536.5	79

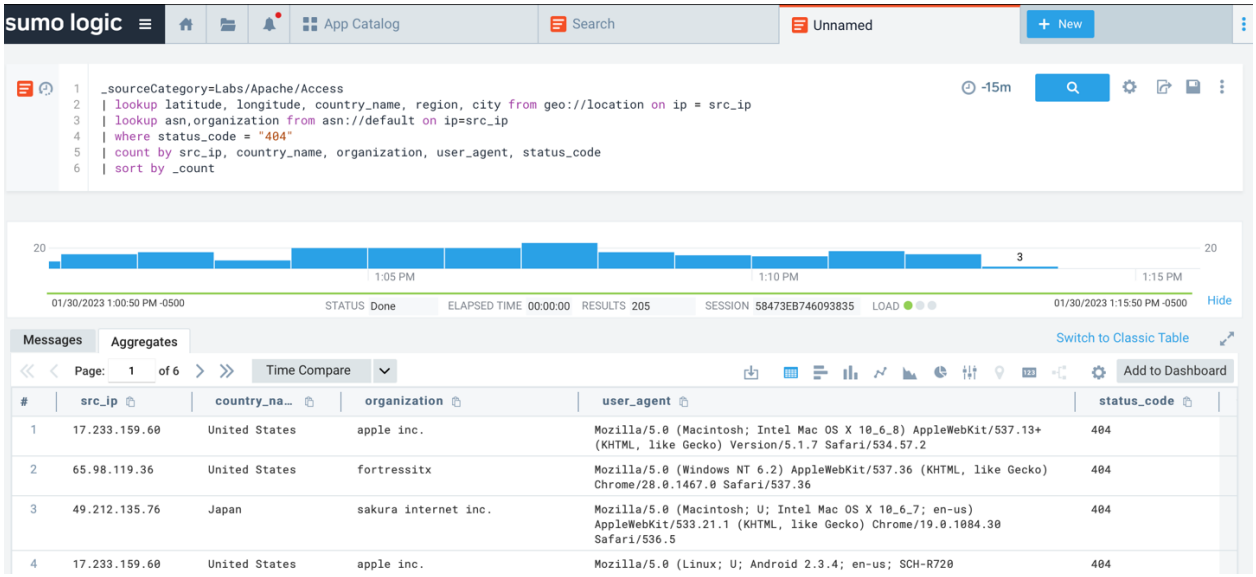
```
_sourceCategory=Labs/Apache/Access
| lookup latitude, longitude, country_name, region, city from geo://location on ip = src_ip
| lookup asn, organization from asn://default on ip=src_ip
| where user_agent matches "*() { :; }*"
| count by src_ip, country_name, organization, user_agent
| sort by _count
```



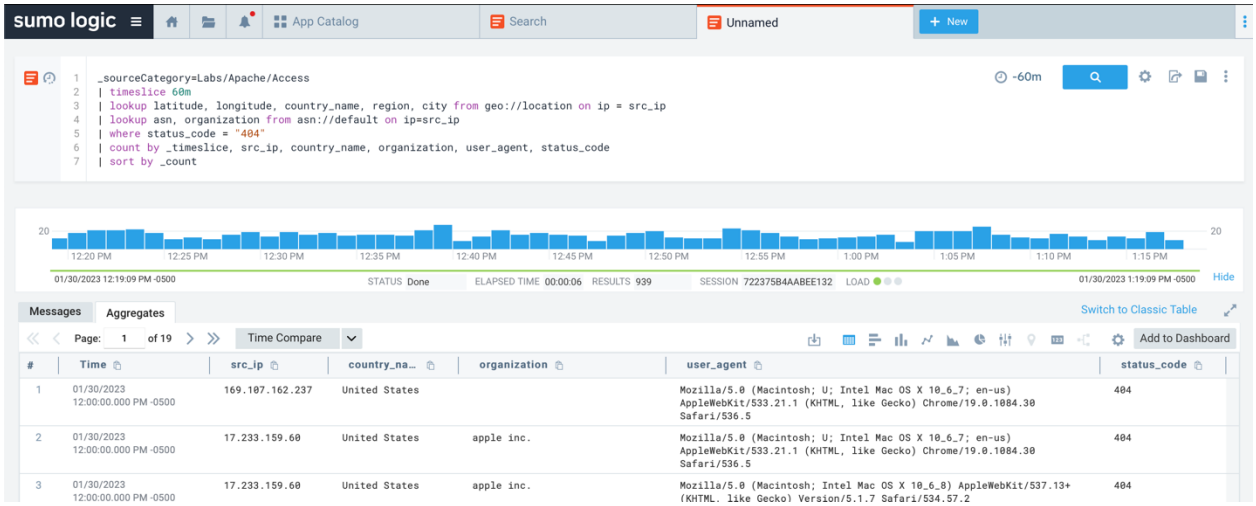
#	src_ip	country_na…	organization	user_agent	_count
1	17.233.159.60	United States	apple inc.	() { :; }; /bin/ping -c 1 10.10.0.69	59
2	169.107.162.237	United States		() { :; }; /bin/ping -c 1 10.10.0.69	54
3	49.212.135.76	Japan	sakura internet inc.	() { :; }; /bin/ping -c 1 10.10.0.69	52
4	19.174.45.8	United States		() { :; }; /bin/ping -c 1 10.10.0.69	49
5	65.98.119.36	United States	fortressitx	() { :; }; /bin/ping -c 1 10.10.0.69	39
6	70.69.152.165	Canada	shaw communications inc.	() { :; }; /bin/ping -c 1 10.10.0.69	31

Brute Force Discovery

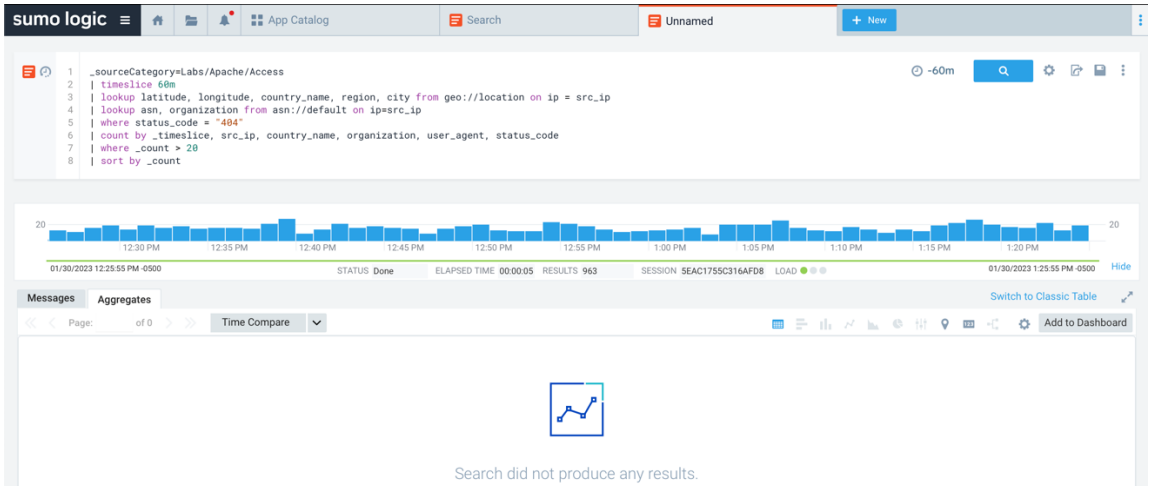
```
_sourceCategory=Labs/Apache/Access
| lookup latitude, longitude, country_name, region, city from geo://location on ip = src_ip
| lookup asn,organization from asn://default on ip=src_ip
| where status_code = "404"
| count by src_ip, country_name, organization, user_agent, status_code
| sort by _count
```




```
_sourceCategory=Labs/Apache/Access
| timeslice 60m
| lookup latitude, longitude, country_name, region, city from geo://location on ip = src_ip
| lookup asn, organization from asn://default on ip=src_ip
| where status_code = "404"
| count by _timeslice, src_ip, country_name, organization, user_agent, status_code
| sort by _count
```

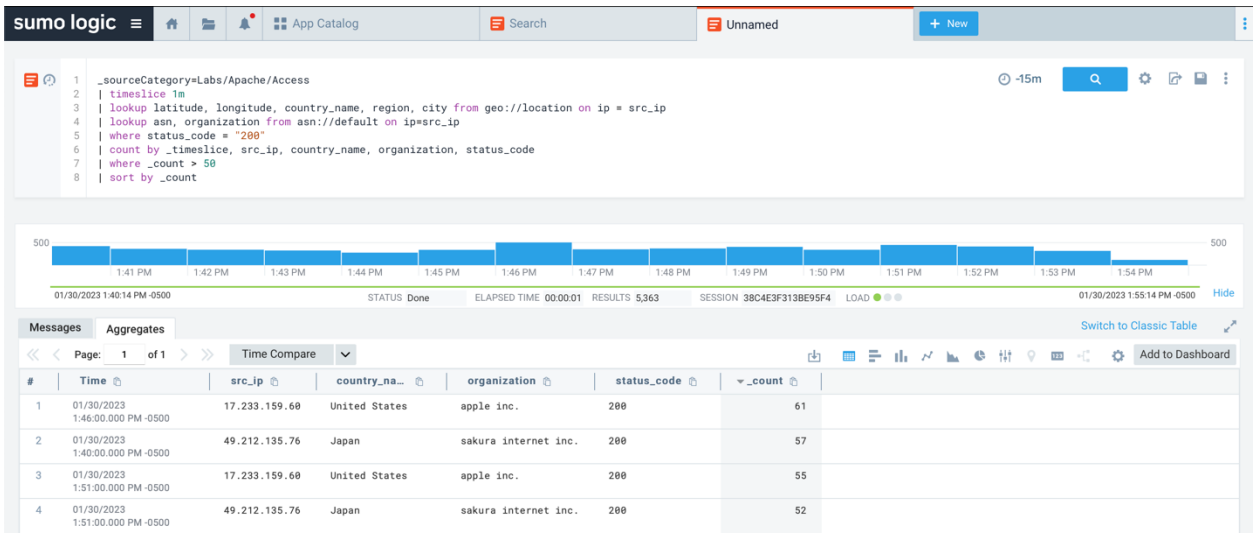


```
_sourceCategory=Labs/Apache/Access
| timeslice 60m
| lookup latitude, longitude, country_name, region, city from geo://location on ip = src_ip
| lookup asn, organization from asn://default on ip=src_ip
| where status_code = "404"
| count by _timeslice, src_ip, country_name, organization, user_agent, status_code
| where _count > 20
| sort by _count
```



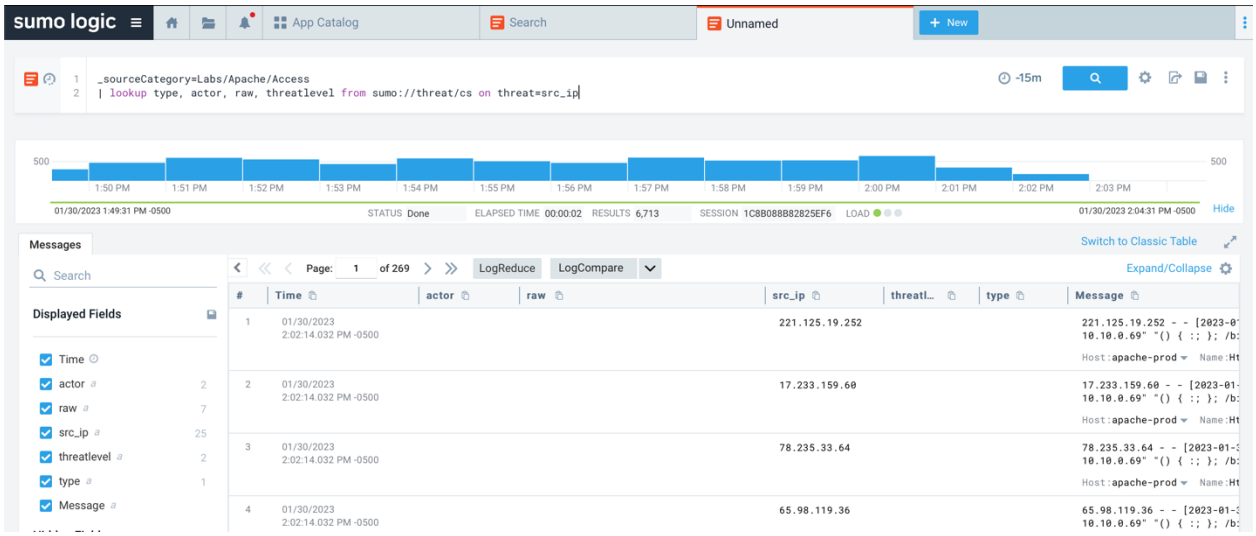
Crawling Detection

```
_sourceCategory=Labs/Apache/Access
| timeslice 1m
| lookup latitude, longitude, country_name, region, city from geo://location on ip = src_ip
| lookup asn, organization from asn://default on ip=src_ip
| where status_code = "200"
| count by _timeslice, src_ip, country_name, organization, status_code
| where _count > 50
| sort by _count
```

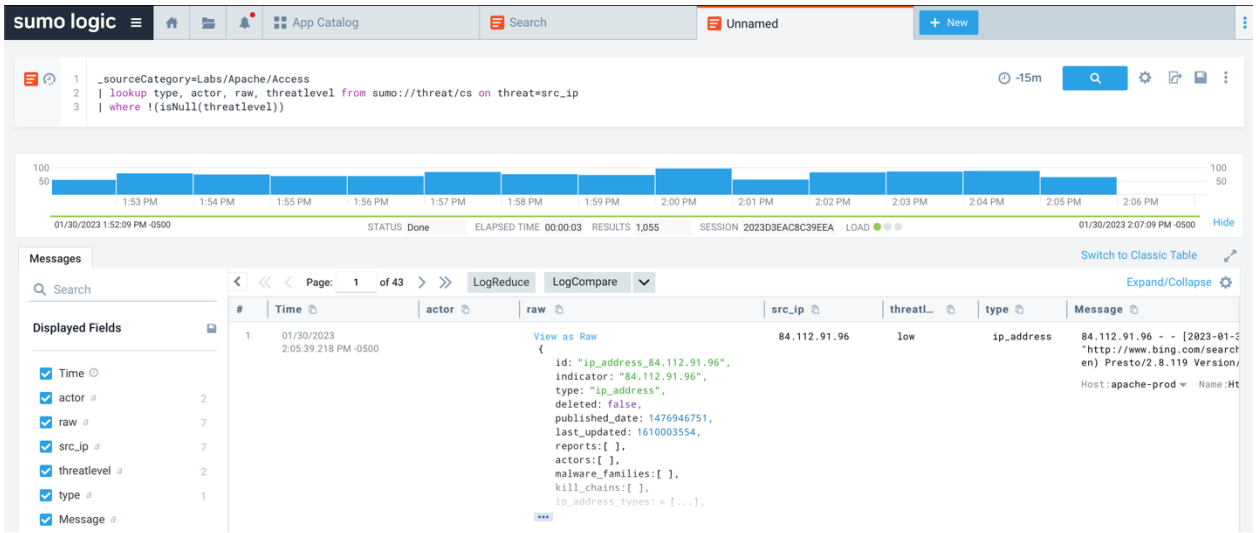


Threat Intelligence

_sourceCategory=Labs/Apache/Access
| lookup type, actor, raw, threatlevel from sumo://threat/cs on threat=src_ip



_sourceCategory=Labs/Apache/Access
| lookup type, actor, raw, threatlevel from sumo://threat/cs on threat=src_ip
| where !(isNull(threatlevel))



EXERCISE

Scenario 1: Malicious User String Agents

1. Threat Simulation

To investigate malicious user string attacks, it is very important that I create customized alerts that would send notifications as soon as a condition is triggered, or malicious user string agents are detected. As soon as an alert is triggered, I will analyze all logs captured on sumo logic prior to and after the alert to identify targeted resources or systems, and the activities of the attacker. By using the "time compare" button on sumo logic, I will be able to compare logs captured at a given time against a previous one to identify patterns and gather intelligence. I will use the Access and Authentication monitoring dashboard and add a customized panel that will monitor user agents. I will work with other security teams to deploy an incident response plan to remediate any potential threat to the organization. The criticality to be assigned to an alert would depend on the purpose of the user agent. A user string agent which is designed to bypass security systems would be assigned priority 1 (highest) whilst an agent for gathering information would be assigned priority 2. A post-incident report would be generated, and the threat intel would be updated.

2. Business Impacts

A detection can impact the business in a positive and negative way. An early detection can help prevent the attacker from exploiting the business or reduce the impacts. However, detecting a completed attack can affect business operations. A compromised server can halt business operations for hours (if not days). Short-term risks include lawsuits, lost revenue when the business could not operate, data breaches, and extortion through ransomware attacks. Long-term risks could be a loss of the company's reputation and the collapse of the business.

3. Incident Remediation

To remediate the incident requires real-time monitoring of all log data to detect malicious string user agents in real-time, regularly install all security patches and block user agents that belong to a suspicious bot.

Brute Force Discovery

1. Threat Simulation

As a SOC analyst, to be able to respond to a brute-force alert would require that I study and analyze the log files within a given timeframe from and before the alert. To effectively review the logs, I will divide the logs into time slices, and create an outlier to detect all IP addresses with high 4** error status codes within a time slice. This will reduce my log data and help me focus on the relevant ones. the access and authentication monitoring dashboard would be used to monitor failed logins and attempted resource access. after log analysis, IP addresses with malicious activities will be blocked, and other security measures will be implemented. A report will be created to document the event and update the threat intelligence of the company to build signatures to prevent future threats. Due to the impact of brute force attacks, an alert indicating a suspicious brute force attack will be considered as a "Critical Impact" alert.

2. Business Impact

A brute force attack will impact business processes and compromise systems. It can shut down business operations for several hours or days. Detecting brute force attacks will protect the company from such instances. Short-term risks to the company are system hijacking, disruption of business processes, huge financial loss, and stealing of sensitive data. Long-term risks are ruining of business reputation, legal actions and data protection compliance issues, and the collapse of the company.

3. Incident remediation

Real-time monitoring will be conducted to monitor the logs to create alerts in real-time. Limit login attempts to systems, enforce multi-factor authentication, and educate employees on safety practices.

Crawling Detection

1. Threat Simulation

As a SOC analyst, investigating crawling detection requires that I define an outlier or the condition for triggering the alert. By defining the outlier, I will be able to detect any deviation from the standard or the normal. By specifying an outlier, I will be able to easily review my logs by using a line graph on sumo logic. After that, I will review all logs with the 200-status code within a 60-minute timeframe before the alert and possibly all the logs that were captured after that. I will build a customized monitoring dashboard that would be composed of different panels created from search queries meant to detect web crawlers. Web crawling does not present a high-security risk to business processes and as a result, the criticality level would be medium (Priority 3 of 5). A report will be written on the alert and a threat signature will be created to update threat intel.

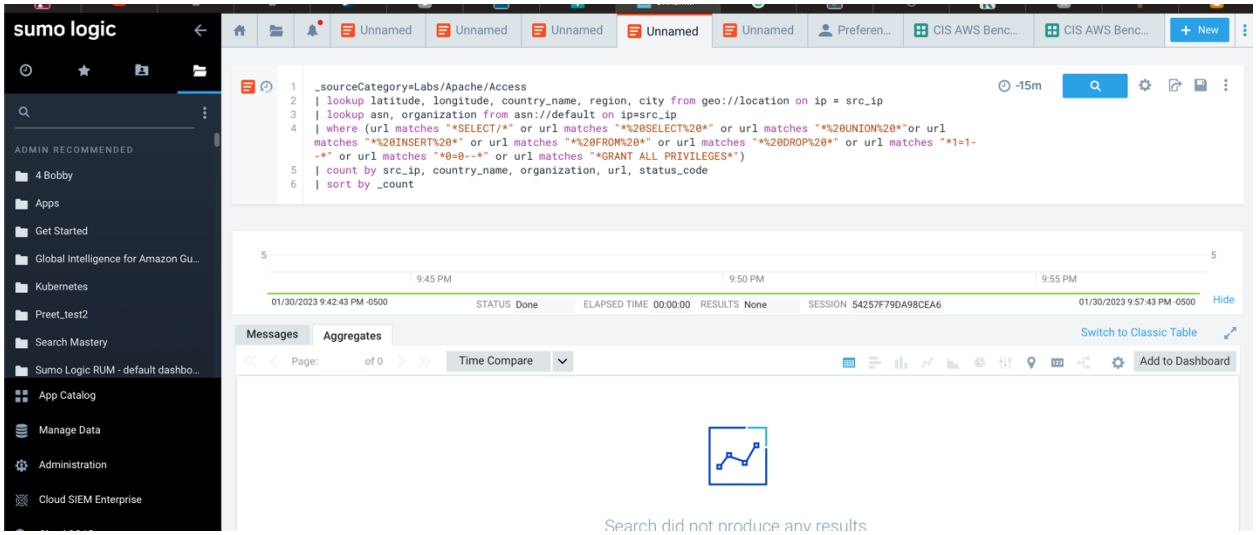
2. Business impacts

Detecting malicious web crawlers and putting in place measures to limit or block their activities will protect the business from data breaches and unauthorized access to resources. Web crawlers can be used to learn more about a particular server to detect vulnerabilities to initiate an attack. Detecting them will help to prevent such possible attacks. Short-term risks associated with crawlers could be exposure of sensitive company information. If detected malicious crawlers are not resolved, they could lead to long-term risks such as legal company issues, huge financial loss from security breaches, and the destruction of consumer trust.

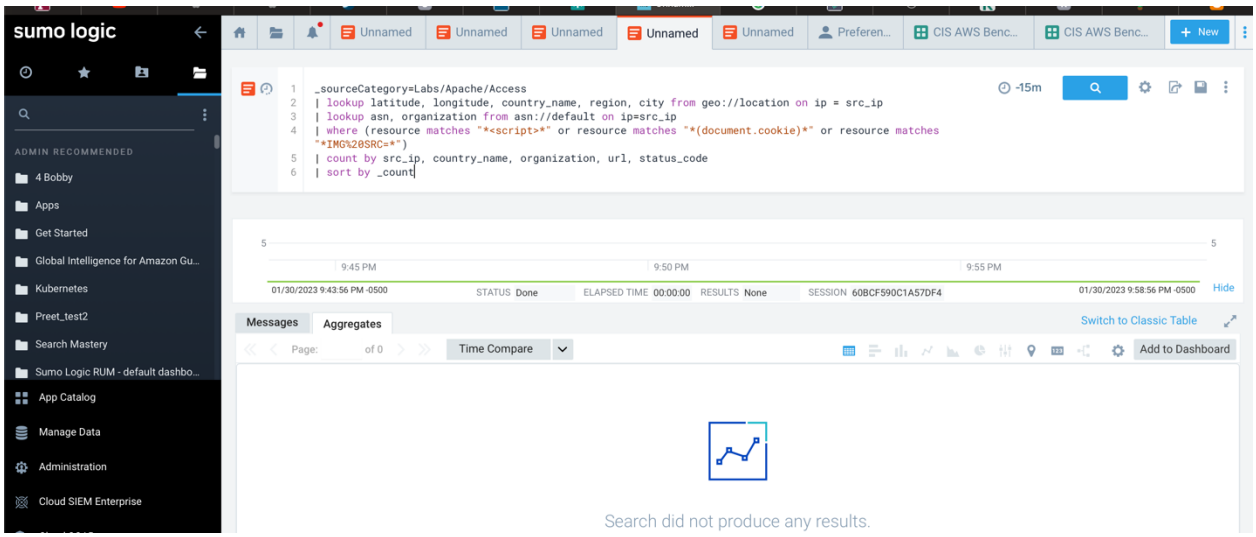
3. Incident Remediation

To remediate the exploitation of web crawlers, there is a need to employ third-party systems to automatically block all malicious bots. Other measures include real-time monitoring of system logs on sumo logic and using advanced encryption to save all sensitive data.

SQL Injections



Cross-site scripting



References

Red Points (n.d). How should your business deal with spoofing attacks? Retrieved January 30, 2023 from https://www.redpoints.com/blog/spoofing-attacks/

Ekran (2021, December 21). Protect User Credentials and Manage Access Rights to Prevent Brute Force Attacks. Retrieved January 29, 2023 from https://www.ekransystem.com/en/blog/brute-force-attacks

Bandos, T. (2022, December 28). The Five Steps of Incident Response. Retrieved January 23, 2023 from https://digitalguardian.com/blog/five-steps-incident-response.

Kaspersky (n.d). What is Spoofing – Definition and Explanation. Retrieved January 30, 2023 from https://www.kaspersky.com/resource-center/definitions/spoofing.

Manners, D. (2012, February 21). The User Agent Field: Analyzing and Detecting the Abnormal or Malicious in your Organization. Retrieved January 29, 2023 from https://sansorg.egnyte.com/dl/pGWQkGIq5N

Raz, I (2018). User-Agent based attacks are a low-key risk that shouldn't be overlooked. Retrieved January 29, 2023 from https://betanews.com/2017/03/22/user-agent-based-attacks-are-a-low-key-risk-that-shouldnt-be-overlooked/