Cybersecurity Suspicious Web Threat Interactions

Prepare

Hypothesis:

I believe the Aws Cloudwatch logs contains IOCs that would indicate data exfiltration.

Objective:

Determine if suspicious web traffic is contained in the AWS Cloudwatch logs.
My investigation will be focusing on MITRE ATT&CK techniques:

- **T1530 -** Data from Cloud Storage
- **T1048** - Exfiltration Over Alternative Protocol

Data Source

- Cybersecurity: Suspicious Web Threat Interactions dataset

Relevant Fields

Fields	Description
bytes_in	Bytes received by the server.
bytes_out	Bytes sent from the server.
creation_time	Timestamp of when the record was created.
end_time	Timestamp of when the connection ended.
src_ip	Source IP address.
src_ip_country_code	Country code of the source IP.
protocol	Protocol used in the connection.
response_code	HTTP response code.
dst_port	Destination port on the server.
dst_ip	Destination IP address.

Tools & Queries

Splunk ES and SPL will be utilized to conduct this investigation.

Execute

Hunting Methodology

This threat hunt will be conducted on the premise that src_ip represents possible attacker IP address, bytes_in represents incoming data to the attacker IP, bytes_out represents sent data from the attacker IP.

Queries

Convert bytes to megabytes and sort from highest to lowest:

```
source="CloudWatch_Traffic_Web_Attack.csv" host="soc" index="eca_cloud_web_data"
sourcetype="csv"
| eval MB_to_attacker=round(bytes_in/1024/1024,2),
MB_from_attacker=round(bytes_out/1024/1024,2)
| stats avg(bytes_in), avg(bytes_out) by src_ip, protocol, dst_ip, dst_port, MB_to_attacker,
MB_from_attacker
| sort - avg(bytes_in)
```

Zero in on IP 155.91.45.242 and convert _time to AM/PM

```
source="CloudWatch_Traffic_Web_Attack.csv" host="soc" index="eca_cloud_web_data"
sourcetype="csv" src_ip="155.91.45.242"
| eval _time=strftime(_time,"%m/%d/%Y %I:%M:%S %p") ```Convert _time to AM/PM```
| eval MB_In=round(bytes_in/1024/1024,2), MB_Out=round(bytes_out/1024/1024,2)
```Convert bytes_in and bytes_out to Mb```
| table _time, src_ip, MB_In, MB_Out,
```

Zero in on IP 155.91.45.242 and convert _time to AM/PM

```
source="CloudWatch_Traffic_Web_Attack.csv" host="soc" index="eca_cloud_web_data"
sourcetype="csv" src_ip="165.225.240.79"
| eval _time=strftime(_time,"%m/%d/%Y %I:%M:%S %p") ```Convert _time to AM/PM```
| eval MB_In=round(bytes_in/1024/1024,2), MB_Out=round(bytes_out/1024/1024,2)
```Convert bytes_in and bytes_out to Mb```
| table _time, src_ip, MB_In, MB_Out,
```

Findings

- On 4/25/2024 and 4/26/2024 AWS Cloudwatch flagged some web traffic as suspicious.
- Port 443 was used to transfer data out of the victim server.
- IP address 155.91.45.242 has received large data transfers and has connected to the victim server many times.
- IP address 155.91.45.242 has large spikes in received bytes relative to output bytes.
- IP address 165.225.240.79 has large spikes in received bytes relative to output bytes.

Act

Analysis & Investigation

The findings appear to confirm the hypothesis.

Between 4/25 and 4/26 of 2024, IP Address 155.91.45.242 connected to the victim server 28 times starting at 7:30pm on 4/25 ending at 5:50am of 4/26. On 4/25 between 7:30pm and 9:40pm IP address 155.91.45.242 received about 4.5Mb of data roughly every 10 minutes. Resuming at 5:00am on 4/26, 155.91.45.242 began receiving larger amounts at about 17.5Mb up to 24Mb ending at 5:50am.
This would seem to indicate data exfiltration over an alternative protocol being that port 443 was accessed on the victim server an used by 155.91.45.242 to receive large amounts of data.

During the same time frame IP address 165.225.240.79 connected 18 times receiving close to 2Mb of data from each of 11 connections. This would seem to be a suspicious amount in comparison to the the amount of data sent by this IP address.

Theses incidents should be escalated to IR.

Know

Indicators of Compromise (IOCs)

- **IPs:** 155.91.45.242, 165.225.240.79
- **Ports:** Outbound 443 during 04/25–04/26/2024
- **Behavior:** Frequent sessions, large inbound bytes, periodic transfer cadence (~10 min)

Next Steps & Recommendations

Executive Summary (High-Level Next Steps)

1. **Escalate to Incident Response (IR):** Treat this as suspected data exfiltration.
2. **Preserve Evidence:** Logs, snapshots, and system images before containment.
3. **Follow IR Workflow:** Containment → Eradication → Recovery → Lessons Learned.

Priority Actions

P1 — Immediate (within hours):

- Block outbound traffic to 155.91.45.242 and 165.225.240.79 at firewall/security groups.

- Snapshot affected EC2/VM instances and preserve logs.
- Isolate suspected hosts from the network.

P2 — Short Term (within 48 hours):

- Collect host forensic artifacts (processes, sockets, cron jobs, memory).
- Export Splunk results and pivot on attacker IPs.
- Identify user accounts or API keys active on the host.

P3 — Mid Term (2–7 days):

- Root cause analysis: confirm initial access vector.
- Rotate credentials and API keys.
- Re-image compromised hosts if persistence is found.

P4 — Long Term (7+ days):

- Harden configurations and update detection rules.
- Conduct tabletop exercises and refine playbooks.

Forensic & Evidence Collection

- Preserve: CloudWatch, VPC Flow Logs, ELB/ALB, S3, and host logs.
- Capture: memory, disk snapshots, process lists, network connections, scheduled tasks.
- Document chain-of-custody with UTC timestamps.

Containment Steps

1. Add firewall deny rules for 155.91.45.242 and 165.225.240.79.
2. Block/throttle outbound HTTPS from affected hosts.
3. Rotate or disable exposed credentials.
4. Enable enhanced logging or packet capture on the subnet.

Knowledge sharing

This report will be shared with the team.