SIEM Log Analysis Report

Inicident: Website Outage – ByteBistro.com (Public web server – IP: 203.0.113.55)
Analyst: Sami Assi
Analyst Workstation: workstation26 – 10.0.0.26
Date: October 31, 2025
Tools used: Splunk SIEM, tcpdump/Wireshark, Suricata, Web Server Logs, Kernel Logs

1. Objective

The purpose of this analysis is to examine the logs collected during the service outage of ByteBistro.com on October 31, 2025, to identify the root cause, assess the scope of impact, and determine the indicators of compromise or attack patterns observed across network, system, and application logs.

DNS Resolution Logs:

The following DNS query logs show that normal DNs resolutions occurred for the company website before the service disruption. This confirms that name resolution was functioning correctly, and the outage was NOT cause by DNS issues.

09:44:05.003 workstation26 (10.0.0.26) dns: query[0x1a2b] A? www.bytebistro.com from 10.0.0.26 (workstation26) to 8.8.8.8:53
09:44:05.006 dns.google dns: response[0x1a2b] A 203.0.113.55 to 10.0.0.26 (workstation26):53

Analysis: The DNS server at 8.8.8.8 successfully resolved the hostname www.bytebistro.com to IP address 203.0.0113.55 (workstation 26). This indicates the workstation was able to reach external DNS infrastructure normally. The problem therefore occurred after DNS resolution – likely during the TCP connection phase.

HTTP Request Confirmation Logs:

The following HTTP access logs show that 2 internal workstations within the organisation was able to make a HTTP request & connection just before the service outage. Confirming that at 9:44 am, http connections with the organisational web server were functioning properly.

09:44:06.200 httpd[2345]: access_log: 10.0.0.26 (workstation26) - - [31/Oct/2025:09:44:06 +0000] "GET / HTTP/1.1" 200 14432 "-" "Mozilla/5.0 (Windows)"
09:44:10.500 httpd[2345]: access_log: 10.0.0.27 (workstation27) - - [31/Oct/2025:09:44:10 +0000] "GET /about HTTP/1.1" 200 8520 "-" "Mozilla/5.0 (Windows)"

Analysis: HTTP access logs from 09:44 a.m. show successful connections from internal workstations 10.0.026 and 10.0027. Each log entry includes a valid HTTP status code 200 (OK), confirming that the web server was functioning normally immediately prior to the incident.

Kernel Logs:

09:46:00.150 kernel[web-prod-01.bytebistro.com] : TCP: Possible SYN flooding on port 80. Check SNMP counters.
09:46:00.200 kernel[web-prod-01.bytebistro.com] : tcp_listen_port_release: backlog limit reached for port 80
09:46:00.203 kernel[web-prod-01.bytebistro.com] : nf_conntrack: table full, dropping packet.

Analysis: The kernel logs collected from the web server (web-prod-01.bytebistro.com) indicate that the host's TCP/IP stack was under severe stress from excess inbound connection attempts on port 80. The log entry "Possible SYN flooding on port 80" confirms that the Linux kernel detected an abnormal rate of half-open TCP connections.

Further log entries show the TCP backlog queue reached its limit and the connection tracking table becoming full, forcing the system to drop packets. This further confirms our initial analysis that the attack was a SYN flood attack.

Kernel Logs (Socket Status Logs):

3 spoofed IP addresses

09:46:00.205 ss[web-prod-01.bytebistro.com] : SYN-RECV 10240 0 0.0.0.0:80 **198.51.100.200**:51021
09:46:00.206 ss[web-prod-01.bytebistro.com] : SYN-RECV 10235 0 0.0.0.0:80 **203.0.113.45**:40001
09:46:00.207 ss[web-prod-01.bytebistro.com] : SYN-RECV 10230 0 0.0.0.0:80 **198.51.100.71**:60012

Analysis: The following socket status logs were collected from the web server (web-prod-01.bytebistro.com). These socket status entries show multiple connections to port 80 on the web server that are stuck in the SYN-RECV (SYN received) state. This indicates that the server has received a TCP SYN packet from a client and sent back a SYN-ACK, but has **not received the final ACK** required to complete the three way handshake.

This high count of connections in SYN-RECV state shows evidence of this incident being a **SYN flood attack**, where **attackers repeatedly send SYN packets without completing the handshake**. Each half-open connection consumes a slot in the server TCP backlog queue, overwhelming the system and preventing legitimate users from establishing new connections and therefore accessing the web domain.

The following source IP's are most likely **spoofed** and used by the attacker for this SYN attack: **198.51.100.200**, **203.0.113.45**, **198.51.100.71**

Apache Access Logs:

09:46:01.100 httpd[2345]: access_log: 192.0.2.22 (monitor) - - [31/Oct/2025:09:46:01 +0000] "GET /favicon.ico HTTP/1.1" 503 178 "-" "monitor/1.0"
09:46:01.250 httpd[2345]: access_log: 192.0.2.33 (bot) - - [31/Oct/2025:09:46:01 +0000] "GET / HTTP/1.1" 502 512 "-" "Mozilla/5.0 (bot)"

Analysis: The above Apache access logs record incoming HTTP requests made to the web server. The first log shows a request from 192.0.2.22. The server responded with a 503 – Service Unavailable, which indicates that the server was temporarily unable to handle the request. Likely due to being overwhelmed at the time of the SYN flood attack.

The second log show another request from 192.0.2.33 (bot) attempting to access the root of the website, but receiving a 502 – Bad Gateway error, suggesting communication issues.

These two errors (**error 502 & error 503**) suggest the web server is working at a degraded performance, preventing it from serving normal website content.

Suricata (IDS) Alert & SIEM Logs:

09:46:02.200 suricata: ALERT [1:1000001:0] "SYN flood detected" src_net=203.0.113.0/24 dst=203.0.113.55 pps=24600 distinct_src=1520

09:46:02.500 splunk: correlation:alert id=INC-4532 severity=critical msg="Correlated event: HIGH SYN RATE -> www.bytebistro.com (203.0.113.55) per kernel + web 5xx + IDS"
09:46:03.000 itsm: ticket INC-4532 created Priority=P1 Assigned=NetworkOps msg="Auto-created by SOC: High SYN flood"

Analysis: The following entries originate from the organization's security monitoring and alerting systems. The first alert was generated by Suricata IDS, which detected a SYN flood attack targeting the public web server (203.0.11.55).

The IDS identified a traffic rate of approximately 24,600 packets per second indicated by pps= 24600. With 1520 distinct source IP's within the subnet 203.0.113.0/24, indicating that the attacker was using IP spoofing to disguise the true origin of the attack.

It is important to note that the IDS alert was triggered approximately two minutes after the last successful HTTP logs at 09:44. Following this, the SIEM platform (Splunk) automatically produced a single critical correlation alert. Confirming that the flood was actively impacting the web server's availability.

Finally in the last log the organization's incident management system (ITSM) automatically created a critical (p1) incident ticket for immediate action for the Network Operations team for immediate investigation and mitigation.

Post-Mitigation System SIEM Logs

09:47:00.200 kernel[web-prod-01.bytebistro.com] : net.ipv4.tcp_syncookies=1 (enabled)

09:47:05.500 httpd[2345]: access_log: 198.51.100.50 (healthcheck) - - [31/Oct/2025:09:47:05 +0000] "GET / HTTP/1.1" 200 14432 "-" "HealthCheck/1.0"

09:47:06.000 splunk: event msg="INC-4532 updated: mitigations applied; monitoring continues"

09:48:00.000 itsm: INC-4532 resolved resolution="Syncookies & upstream filtering; post-incident review arranged"

Analysis: At 09:47:00, the **system (kernel) log** confirmed that TCP SYN cookies were enabled on the Linux web server, indicating that DoS mitigation had been activated.

Five seconds later, the **web server access log** recorded an HTTP 200 OK response from an automated health check, confirming that the website has recovered.

The **SIEM correlation log** (Splunk) at 09:47:06 documented the incident update, noting that mitigations were applied, and monitoring would continue.

Finally, the **ITSM incident log** at 09:48:00 confirmed that the incident was resolved and post-incident review was scheduled.

Snippet_oct31_0948.pcap – Wireshark/tcpdump Capture:

Oct 31 09:48:30.000 splunk: event msg="Wireshark/tcpdump capture uploaded: snippet_oct31_0948.pcap (size 2.1MB); parsed with Suricata; 5,120 SYN packets identified and correlated with kernel and web logs"

- A packet capture file (snippet_oct31_0948.pcap) was collected during the incident and analysed
- This SIEM log documents the upload of a packet capture (.pcap) to the SIEM for analysis.

- The capture was parsed with Suricata, which identified 5,120 TCP SYN packets, confirming a SYN flood attack.
- Spoofed destination IP address identified earlier (**203.0.113.55**) was also observed in the packet capture

Conclusion:

The SIEM correlated the spoofed destination IP address (**203.0.113.55**), previously identified in earlier IDS and kernel logs, with the same addressed observed in the packet capture (snippet_oct31_0948.pcap). This correlation confirms that the SYN flood traffic captured at 09:48 was part of the same ongoing attack that concluded with and coincided with and contributed to the web server outage. The combined analysis of IDS, kernel logs, and packet captures demonstrates a clear link between the attack traffic and the service disruption.