

Tyler Ebra
CSEC 2003
October 29, 2024
Incident Report

The UDP protocol reveals that the device on IP address 192.51.100.15 has sent multiple DNS requests to the IP of 203.0.113.2 on port 53.

This is based on the result of the network analysis, which shows that the ICMP echo reply returned the error message UDP port 53 unreachable.

The port noted in the error message is used for DNS as it is port 53.

The most likely issue is that the DNS server is down or that the IP address 192.51.100.15 is being blocked.

The incident began happening at 1:24 all the way until 1:28..

The issue became apparent when customers put in complaints as they could not reach the company website.

The network traffic was analyzed and documented using Wireshark.

The network traffic analysis showed that port 53 is the port that is causing the customers to repeatedly fail when trying to connect to the DNS server. The logs indicate that real users are not able to connect to the server due to a high number of SYN requests being sent.

A potential explanation can be a DoS attack that is sending SYN requests to overwhelm the server.

The logs indicate a massive amount of SYN requests being sent to the server from the same IP address.

The most likely explanation is that it is a SYN flood attack.

A SYN flood attack is when a malicious actor sends a large amount of SYN packets they are trying to overload the server and cause it to crash. This works by sending one request that gets acknowledged and then it sends many more SYN until no one else is able to use the server as it is moved all resources to dealing with the overwhelming number of SYN requests.

Packet Capture Using Wireshark

The IP address 184.97.44.177 is from Best Buy's website. My VM was listening on port 80. I captured multiple packets using Wireshark and was able to observe the connection attempts and successful connection of the device using the IP address of 10.0.2.5.

The first screenshot is the log of the first successful connection attempt and the second screenshot is the log of the successful disconnection of the website. In both screenshots the completed SYN ACK and FIN ACK requests are highlighted.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	184.97.44.177	TCP	74	38242 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1676456588 TSecr=0 WS=128
2	0.000043	184.97.44.177	10.0.2.15	TCP	60	80 → 38242 [ACK] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1676456588 TSecr=0 WS=128
3	0.000089	184.97.44.177	10.0.2.15	TCP	60	80 → 38242 [ACK] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1676456588 TSecr=0 WS=128
4	0.000895	10.0.2.15	184.97.44.177	TCP	54	38242 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
5	0.001030	10.0.2.15	184.97.44.177	HTTP	389	GET / HTTP/1.1
6	0.001380	184.97.44.177	10.0.2.15	TCP	60	80 → 38248 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7	0.001381	184.97.44.177	10.0.2.15	TCP	60	80 → 38242 [ACK] Seq=1 Ack=336 Win=65535 Len=0
8	0.001392	10.0.2.15	184.97.44.177	TCP	54	38248 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
9	0.174955	184.97.44.177	10.0.2.15	HTTP	229	HTTP/1.1 301 Moved Permanently
10	0.174973	10.0.2.15	184.97.44.177	TCP	54	38242 → 80 [ACK] Seq=336 Ack=376 Win=31945 Len=0
11	4.238151	10.0.2.15	192.229.211.108	TCP	74	58762 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1927238018 TSecr=0 WS=128
12	4.250596	192.229.211.108	10.0.2.15	TCP	60	80 → 58762 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
13	4.250606	10.0.2.15	192.229.211.108	TCP	54	58762 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
14	4.250711	10.0.2.15	192.229.211.108	OCSP	470	Request
15	4.250877	192.229.211.108	10.0.2.15	TCP	60	80 → 58762 [ACK] Seq=1 Ack=417 Win=65535 Len=0
16	4.268427	192.229.211.108	10.0.2.15	OCSP	791	Response
17	4.268436	10.0.2.15	192.229.211.108	TCP	54	58762 → 80 [ACK] Seq=417 Ack=738 Win=31691 Len=0
18	4.281300	10.0.2.15	192.229.211.108	OCSP	470	Request
19	4.281543	192.229.211.108	10.0.2.15	TCP	60	80 → 58762 [ACK] Seq=738 Ack=833 Win=65535 Len=0
20	4.303313	192.229.211.108	10.0.2.15	OCSP	791	Response
21	4.303495	10.0.2.15	192.229.211.108	OCSP	470	Request
22	4.305676	192.229.211.108	10.0.2.15	TCP	60	80 → 58762 [ACK] Seq=1475 Ack=1249 Win=65535 Len=0
23	4.330297	192.229.211.108	10.0.2.15	OCSP	791	Response
24	4.354554	10.0.2.15	192.229.211.108	TCP	74	58774 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1927238135 TSecr=0 WS=128
25	4.364593	192.229.211.108	10.0.2.15	TCP	60	80 → 58774 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
26	4.364604	10.0.2.15	192.229.211.108	TCP	54	58774 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
27	4.370260	10.0.2.15	192.229.211.108	TCP	54	58762 → 80 [ACK] Seq=1249 Ack=2212 Win=31691 Len=0
28	4.906090	10.0.2.15	142.250.9.94	TCP	74	57852 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1629722870 TSecr=0 WS=128
29	4.906129	10.0.2.15	142.250.9.94	TCP	74	57858 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1629722870 TSecr=0 WS=128
30	4.924644	142.250.9.94	10.0.2.15	TCP	60	80 → 57858 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
31	4.924661	10.0.2.15	142.250.9.94	TCP	54	57858 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
32	4.924762	10.0.2.15	142.250.9.94	OCSP	472	Request
33	4.924995	142.250.9.94	10.0.2.15	TCP	60	80 → 57858 [ACK] Seq=1 Ack=419 Win=65535 Len=0
34	4.933527	142.250.9.94	10.0.2.15	TCP	60	80 → 57852 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
35	4.933541	10.0.2.15	142.250.9.94	TCP	54	57852 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
36	4.933692	10.0.2.15	142.250.9.94	OCSP	472	Request
37	4.933876	142.250.9.94	10.0.2.15	TCP	60	80 → 57852 [ACK] Seq=1 Ack=419 Win=65535 Len=0
38	4.993670	142.250.9.94	10.0.2.15	OCSP	1158	Response
39	4.993678	10.0.2.15	142.250.9.94	TCP	54	57852 → 80 [ACK] Seq=419 Ack=1105 Win=31016 Len=0
40	5.106605	142.250.9.94	10.0.2.15	OCSP	1158	Response
41	5.106684	10.0.2.15	142.250.9.94	TCP	54	57858 → 80 [ACK] Seq=419 Ack=1105 Win=31016 Len=0
42	5.122694	10.0.2.15	192.229.211.108	OCSP	470	Request
43	5.122978	192.229.211.108	10.0.2.15	TCP	60	80 → 58762 [ACK] Seq=2212 Ack=1665 Win=65535 Len=0
44	5.135858	192.229.211.108	10.0.2.15	OCSP	791	Response
45	5.135870	10.0.2.15	192.229.211.108	TCP	54	58762 → 80 [ACK] Seq=1665 Ack=2949 Win=31691 Len=0
46	5.365196	10.0.2.15	192.229.211.108	OCSP	470	Request
47	5.365513	192.229.211.108	10.0.2.15	TCP	60	80 → 58762 [ACK] Seq=2949 Ack=2081 Win=65535 Len=0
48	5.375913	192.229.211.108	10.0.2.15	OCSP	791	Response

No.	Time	Source	Destination	Protocol	Length	Info
...	15.61...	99.84.25...	10.0.2.15	TCP	60	80 → 60524 [ACK] Seq=1 Ack=427 Win=65535 Len=0
...	15.63...	99.84.25...	10.0.2.15	OC...	9...	Response
...	15.63...	10.0.2.15	99.84.25...	TCP	54	60524 → 80 [ACK] Seq=427 Ack=944 Win=31177 Len=0
...	15.76...	10.0.2.15	142.250.9.94	TCP	54	33122 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32120 Len=0
...	15.76...	142.250.9.94	10.0.2.15	TCP	60	80 → 33122 [ACK] Seq=1 Ack=2 Win=65535 Len=0
...	15.78...	142.250.9.94	10.0.2.15	TCP	60	80 → 33122 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
...	15.78...	10.0.2.15	142.250.9.94	TCP	54	33122 → 80 [ACK] Seq=2 Ack=2 Win=32120 Len=0
...	16.15...	10.0.2.15	99.84.25...	OC...	4...	Request
...	16.15...	99.84.25...	10.0.2.15	TCP	60	80 → 60524 [ACK] Seq=944 Ack=852 Win=65535 Len=0
...	16.19...	99.84.25...	10.0.2.15	OC...	9...	Response
...	16.19...	10.0.2.15	99.84.25...	TCP	54	60524 → 80 [ACK] Seq=852 Ack=1887 Win=31177 Len=0
...	16.19...	10.0.2.15	99.84.25...	OC...	4...	Request
...	16.19...	99.84.25...	10.0.2.15	TCP	60	80 → 60524 [ACK] Seq=1887 Ack=1277 Win=65535 Len=0
...	16.23...	10.0.2.15	99.84.25...	TCP	74	50964 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=...
...	16.23...	10.0.2.15	99.84.25...	TCP	74	50970 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=...
...	16.23...	99.84.25...	10.0.2.15	OC...	9...	Response
...	16.23...	10.0.2.15	99.84.25...	OC...	4...	Request