

BRIGHTDATA FORENSIC ANALYSIS

EXECUTIVE SUMMARY

Night Lion Security was hired to investigate claims made by Qurium Media Foundation (“Qurium”), in a report titled “Qurium report analysis”, which claims the Bright Data network was used to carry out a Distributed Denial of Service (DDOS) attack against human rights organization Karapatan.org on July 2021. This audit is being carried out to specifically test the validity of those claims.

Scope

Night Lion Security has been contracted by Bright Data to perform an independent security and forensic review of the data and methods presented by Qurium. All Bright Data applications, systems, people, and processes are considered in-scope for this assessment.

Auditor’s Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Qurium report based on the criteria and technical accuracy of the report's assertions. Our examination and technical analysis were conducted in accordance with industry attestation standards.

Testing Overview

Night Lion’s methodology included testing the effectiveness of the security controls governing Bright Data’s application and online services.

All tests were designed to validate the Qurium report by re-creating the scenario presented in the report's technical analysis. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Opinion

Based on the information gathered and presented in this report, it is our conclusion that there is no evidence presented in either the Qurium report, or in any analysis and investigation performed by Night Lion’s forensic team, to support claims suggesting that any attacks carried out against Karapatan.org originated from Bright Data’s network.

Restricted Use

This report is intended solely for the information and use of Bright Data and its entities and should be distributed only under the direction and approval of Bright Data.

BRIGHTDATA FORENSIC ANALYSIS

REPORT ANALYSIS

Night Lion Security was hired to investigate claims made by Qurium Media Foundation, in a report titled “Qurium report analysis”, which claims the Bright Data network was used to carry out a Distributed Denial of Service (DDOS) attack against human rights organization Karapatan.org on July 2021. This section of the report contains our analysis of the information provided in Qurium’s report.

1. Digital Ocean IP Ownership

Night Lion confirmed with Digital Ocean that the seven IP addresses listed in the original Qurium report did not belong to Bright Data. The report was later updated with the following additional three IP addresses belonging to Bright Data.

- 207.148.113.149
- 128.199.74.148
- 216.128.146.195

These three IP addresses were identified by Qurium by querying against Censys.com for IPs with the TLS certificate containing the following sha256 fingerprint:

- 7f5d67fdd3ee7ebfd2a4cea8aaa35755bc1ee3101840f7d8679b7975c6102e3

However, Qurium’s report does not provide any evidence showing how or why this fingerprint, or any of the three IP addresses, are related to the DDOS attack.

2. DNS Resolutions Identifying BrightData

According to the Qurium report, Bright Data was identified as a contributor to the attack due to their DNS resolutions of Karapatan.org, which originated from Digital Ocean server addresses.

Testing Summary

During our assessment, Night Lion attempted to:

- Validate that no DNS leakage is occurring which would indicate that Bright Data had been submitting requests to resolve Karapatan.org.
- Conduct DNS resolutions through Bright Data network via HTTP requests and observed the requesting servers and details of each request.

Server Presence

Bright Data's network conducts DNS resolution on the server, only in regions where they have a server presence. In all other regions, DNS is conducted on the residential IP itself.

The Qurium report states the attack came from 5 main countries: Russia, Ukraine, Indonesia, Hong Kong, Vietnam and China, with the majority of activity originating from Russia. A review of Bright Data's server network finds only two active servers in China, and none in the other specified countries.

Due to the way Bright Data's services are configured, any DNS resolution observed from these countries during the attacks on Karapatan.org would have resolved to the residential IPs themselves, and not Digital Ocean. This is in direct contradiction to the Qurium report findings.

Server DNS Observation

The list of observed servers is provided below alongside their public ownership information. The list below represents the servers that forwarded the DNS queries from Bright Data's network to Night Lion's receiving server. Using this information, we do not believe it is possible to conclude the IP addresses sending the original DNS queries.

Night Lion was unable to identify Bright Data servers as the origin of the requests, nor did Night Lion identify evidence of source leakage.

Requesting Server

104.156.251.15
107.191.42.180
138.197.107.226
138.197.65.60
144.202.14.9
144.202.8.91
159.203.161.140
165.227.86.114
165.227.94.23
165.227.94.77
172.253.210.14, 172.253.210.69
172.253.210.73, 172.253.210.9
172.253.213.5
172.253.214.101, 172.253.214.109
172.253.8.1
172.253.9.3
173.194.168.195

Public Server Ownership

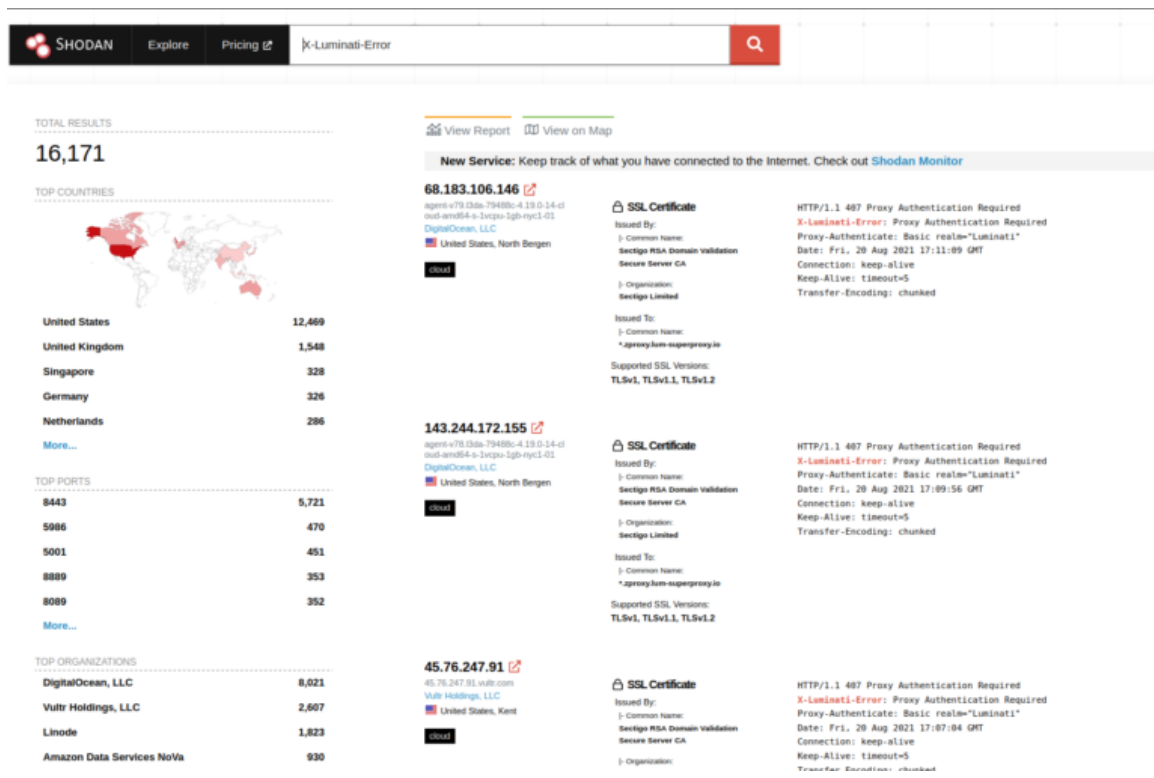
Vultr Holdings LLC (VHL-78)
Vultr Holdings LLC (VHL-78)
DigitalOcean LLC (DO-13)
DigitalOcean LLC (DO-13)
Vultr Holdings LLC (VHL-78)
Vultr Holdings LLC (VHL-78)
DigitalOcean LLC (DO-13)
DigitalOcean LLC (DO-13)
DigitalOcean LLC (DO-13)
DigitalOcean LLC (DO-13)
Google LLC (GOGL)
Google LLC (GOGL)
Google LLC (GOGL)
Google LLC (GOGL)
Google LLC (GOGL)
Google LLC (GOGL)
Google LLC (GOGL)

208.67.217.37	Cisco OpenDNS LLC (OPEND-2)
208.67.217.38	Cisco OpenDNS LLC (OPEND-2)
208.67.217.39	Cisco OpenDNS LLC (OPEND-2)
208.67.217.40	Cisco OpenDNS LLC (OPEND-2)
208.67.217.65 – 208.67.217.93	Cisco OpenDNS LLC (OPEND-2)
74.125.18.3	Google LLC (GOGL)

Server Configuration and Port Forwarding

The Qurium report appeared to attribute the IP addresses in its report to Bright Data because of a 407 response and X-Liminati-Error header displayed by Shodan.

These responses can occur when servers have a specific configuration that specifies ports to be forwarded Bright Data’s servers. This is specifically relevant because this response only occurs when testing these IPs using the HTTPs protocol.



The screenshot shows a Shodan search for 'X-Liminati-Error'. The search bar at the top contains the query and a search icon. Below the search bar, the total number of results is 16,171. The 'TOP COUNTRIES' section shows a world map with the United States having the highest count at 12,469. The 'TOP PORTS' section lists port 8443 as the most common. The 'TOP ORGANIZATIONS' section lists DigitalOcean, LLC as the most frequent. The main results area shows three entries for IP addresses 68.183.106.146, 143.244.172.155, and 45.76.247.91. Each entry includes a 'New Service' notification, a 'View Report' and 'View on Map' link, and detailed information about the service, including the organization (DigitalOcean, LLC), the certificate issuer (Setigo RSA Domain Validation Secure Server CA), and the supported SSL versions (TLSv1, TLSv1.1, TLSv1.2). The detailed information also shows an 'HTTP/1.1 407 Proxy Authentication Required' response with an 'X-Liminati-Error' header.

It should be noted that **Bright Data only uses the HTTP protocol to transmit data**, and not HTTPs. When the same tests are run on the standard HTTP port (80), the result is a different response “X-Subworks-Error”.

3. Connection Log Analysis

Night Lion reviewed the available connection logs provided by Bright Data to identify any attacks occurring from the BD network. Night Lion identified the resolutions and connections to Karapatan.org from the Bright Data network broken down by the provided log files below:

- Backjs Logs.xlsx
 - Logs for 2021-08-09 and 2021-08-10
- 104 total observed connections to Karapatan.org***
- 35.190.30.96.txt
 - Contains logs for the following dates:
 - 2021-08-01, 2021-08-02, 2021-08-04, 2021-08-06, 2021-08-07, 2021-08-10, 2021-08-11, 2021-08-12, 2021-08-13, 2021-08-17, 2021-08-18, 2021-08-19, 2021-08-20, 2021-08-21, 2021-08-22, 2021-08-23, 2021-08-24, 2021-08-25

43 total observed connections to Karapatan.org across these dates

- karapatan.org_logs.txt
 - Contains logs for the following dates:
 - 2021-08-06, 2021-08-08, 2021-08-10, 2021-08-12, 2021-08-13, 2021-08-14, 2021-08-15, 2021-08-16, 2021-08-17, 2021-08-18, 2021-08-19, 2021-08-20, 2021-08-21, 2021-08-23

Total Observed HTTP connections per day

- 209 on 08/06
- 2 on 08/08
- 8 on 08/10
- 73 on 08/12
- 4 on 08/13
- 110 on 08/14
- 22 on 08/15
- 53 on 08/16
- 45 on 08/17
- 107 on 08/18 (81 resolutions)
- 43 on 08/19 (39 resolutions)
- 1031 on 08/20 (37 resolutions)
- 10 on 08/21 (8 resolutions)
- 1 on 08/23 (1 resolution)

The number of connections and resolutions to Karapatan.org do not indicate that a DDOS attack originated from Bright Data's network.



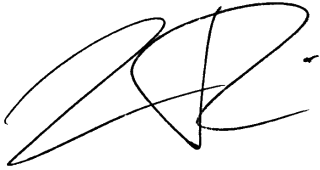
BRIGHTDATA FORENSIC ANALYSIS

THANK YOU

Thank you for using Night Lion Security. We truly value and appreciate your time, and hope that you will consider us a valuable security partner. If you have any questions, please do not ever hesitate to contact us.

Thank you again,

Sincerely,



Vinny Troia
CEO, Night Lion Security