

REVIEW SIEM DATA AND CORRELATE ACTIVITIES TO THE CYBER KILL CHAIN

Jordan Patterson
2024

Review the data for Sep 2023 - May 2024 in Sumologic SIEM based on the country assigned to you (Finland). Identify and correlate activities to the cyber kill chain for the source ips. Analyze the top 20 events by count as per the country assigned to make your inference.

In this report I will investigate and answer the following questions. Please see the report on the following pages to see how I achieved my answers.

1. what is the source of the attack?

- The source(s) of the attack are Hetzner Online GmbH and Aeza International LTD, both organizations are cloud/server hosting services.

2. what are they attacking?

- They are attacking servers hosted by DigitalOcean LLC which is also a cloud/hosting platform.

3. Why is the target being attacked?

- The target seems to be getting attacked as part of an SSH Brute force attack.

4. What can you identify about the infrastructure used to attack, who does it belong to?

- The infrastructure used to attack is comprised of cloud/server hosting services. The attackers rented servers and then launched their attack from there. In some cases, some IP's were identified as hosting Minecraft servers so the attackers are using these servers for multiple purposes.

5. What TTPs do you observe?

- The main TTP that was observed was the SSH Brute Force attack which would fall under the Credential Access Tactic TTP.

Country Assigned to me: Finland

I started my research by adjusting my date range to September 1 2023 – May 31 2024 and began querying SumoLogic using the following query:

`_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland"`

The screenshot shows the SumoLogic search interface. At the top, the query `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland"` is entered. The date range is set from 2023-09-01 12:00:00 AM to 2024-05-31 11:59:59 PM. The search status is "Processing" with 2,180 results. The results table has columns: #, Time, city, country_code, country_name, latitude, longitude, src_ip, state, and Message. Two results are shown, both originating from Helsinki, Finland. The first result is an "rtsp" event, and the second is an "ssh" event. Both events show a source IP of 84.231.193.228 and a destination IP of 134.209.159.70.

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2024-05-31 8:14:43.133 PM -0400	Helsinki	FI	Finland	60.165	24.935	84.231.193.228	Uusima	<pre>{ "timestamp": "2024-06-01T00:14:43.133Z", "flow_id": 6638728861618, "in_iface": "rtsp", "event_type": "rtsp", "src_ip": "84.231.193.228", "src_port": 48630, "dest_ip": "134.209.159.70", "dest_port": 22, "proto": "TCP", "seq": 1, "len": 1 }</pre>
2	2024-05-31 8:13:30.346 PM -0400	Helsinki	FI	Finland	60.165	24.935	84.231.193.228	Uusima	<pre>{ "timestamp": "2024-06-01T00:13:30.346Z", "flow_id": 6638728861618, "in_iface": "ssh", "event_type": "ssh", "src_ip": "84.231.193.228", "src_port": 48630, "dest_ip": "134.209.159.70", "dest_port": 22, "proto": "TCP", "seq": 1, "len": 1 }</pre>

This query allowed me to narrow down the results to alerts that originate from my assigned country, Finland.

I then went ahead and used the query:

`_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | top 20 src_ip by count`

This query then showed me the top 20 source IP's from Finland which were the most common/reoccurring. I found that the most reoccurring source IP was 135.181.237.60 with 1,128 events originating from this IP. In fact, the top 3 source IP's all began with 135.181. This information has helped me narrow down the IP range that the attacker is using.

Messages			Aggregates		
<< < 1 of 1 > >>			Time Compare ▼		
#	src_ip	_count			
1	135.181.237.60	1,128			
2	135.181.126.172	746			
3	135.181.126.164	561			
4	35.228.169.211	542			
5	77.91.78.115	484			
6	135.181.51.116	410			
7	65.108.239.145	401			
8	65.108.17.222	381			
9	95.216.68.161	335			
10	65.108.18.28	334			
11	65.108.234.37	306			
12	80.85.241.213	304			
13	77.91.70.64	301			
14	77.91.70.251	300			
15	95.216.197.30	280			
16	135.181.108.61	256			
17	65.21.70.50	248			
18	65.109.132.76	240			
19	65.108.87.234	230			
20	95.216.92.65	198			

I then took the top source IP and searched for it in Shodan. Shodan revealed that the hostname of the machine is **d14.joinserver.xyz** and that it belongs to an organization called **Hetzner Online GmbH**.

135.181.237.60 Regular View Raw Data

General Information

Hostnames	d14.joinserver.xyz
Domains	JOINSERVER.XYZ
Country	Germany
City	Gunzenhausen
Organization	Hetzner Online GmbH
ISP	Hetzner Online GmbH
ASN	AS24940

I then turned to VirusTotal and one again found that this IP is registered under **Hetzner Online GmbH**. In addition, VirusTotal using MalwareURL's analysis has identified this IP as Malware.

135.181.237.60 Sign in Sign up

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#). [Accept terms of use](#)

1 / 93

Community Score

1/93 security vendor flagged this IP address as malicious

Reanalyze Similar Graph API

135.181.237.60 (135.181.0.0/16)
AS 24940 (Hetzner Online GmbH)

FI Last Analysis Date 25 days ago

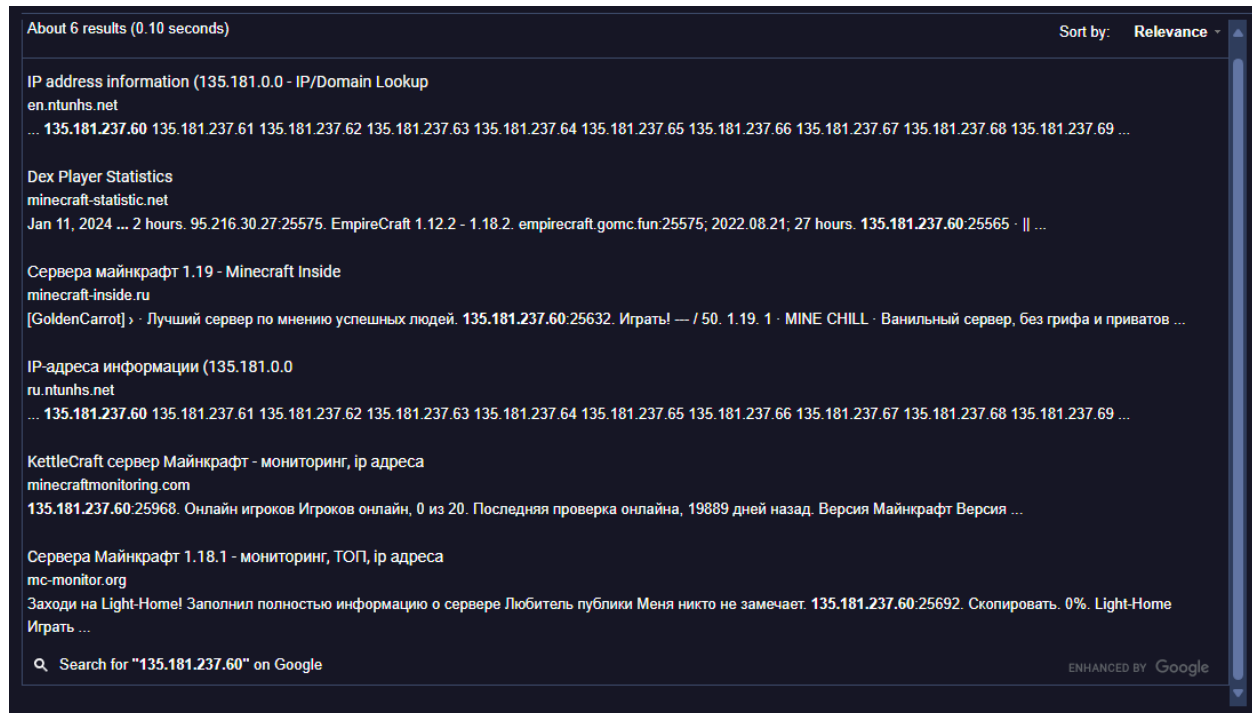
DETECTION DETAILS RELATIONS COMMUNITY

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ Do you want to automate checks?

MalwareURL	ⓘ Malware	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean

Virus Total also gives use some google results. These results suggest that this IP may be a Finnish/German/Russian Minecraft Server, at least on the surface.



With the information that we've found so far in mind, I went ahead and ran the other top source IP's beginning with the same 2 octets (134.181), and they all give the same or similar results. Minecraft servers that are hosted by **Hetzner Online GmbH** and flagged by VirusTotal and MalwareURL as potential Malware.

135.181.126.172

Regular ViewRaw Data

General Information

Hostnames

n3joinserver.xyz

Domains

JOINSERVER.XYZ

Country

Germany

City

Gunzenhausen

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

Operating System

Linux

135.181.126.172

Sign inSign up

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

Accept terms of use

1

/ 93

Community Score

1/93 security vendor flagged this IP address as malicious

ReanalyzeSimilarGraphAPI

135.181.126.172 (135.181.0.0/16)

FI

Last Analysis Date

AS 24940 (Hetzner Online GmbH)

15 days ago

DETECTIONDETAILSRELATIONSCOMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic Properties

Network

135.181.0.0/16

Autonomous System Number

24940

Autonomous System Label

Hetzner Online GmbH

Regional Internet Registry

RIPE NCC

Country

FI

Continent










EU



I did some basic reconnaissance to get an idea of who/what Hetzner Online GmbH is and it seems that they are a company that provides various server hosting services.

HETZNER Dedicated Cloud Web & Managed Colocation Storage Services

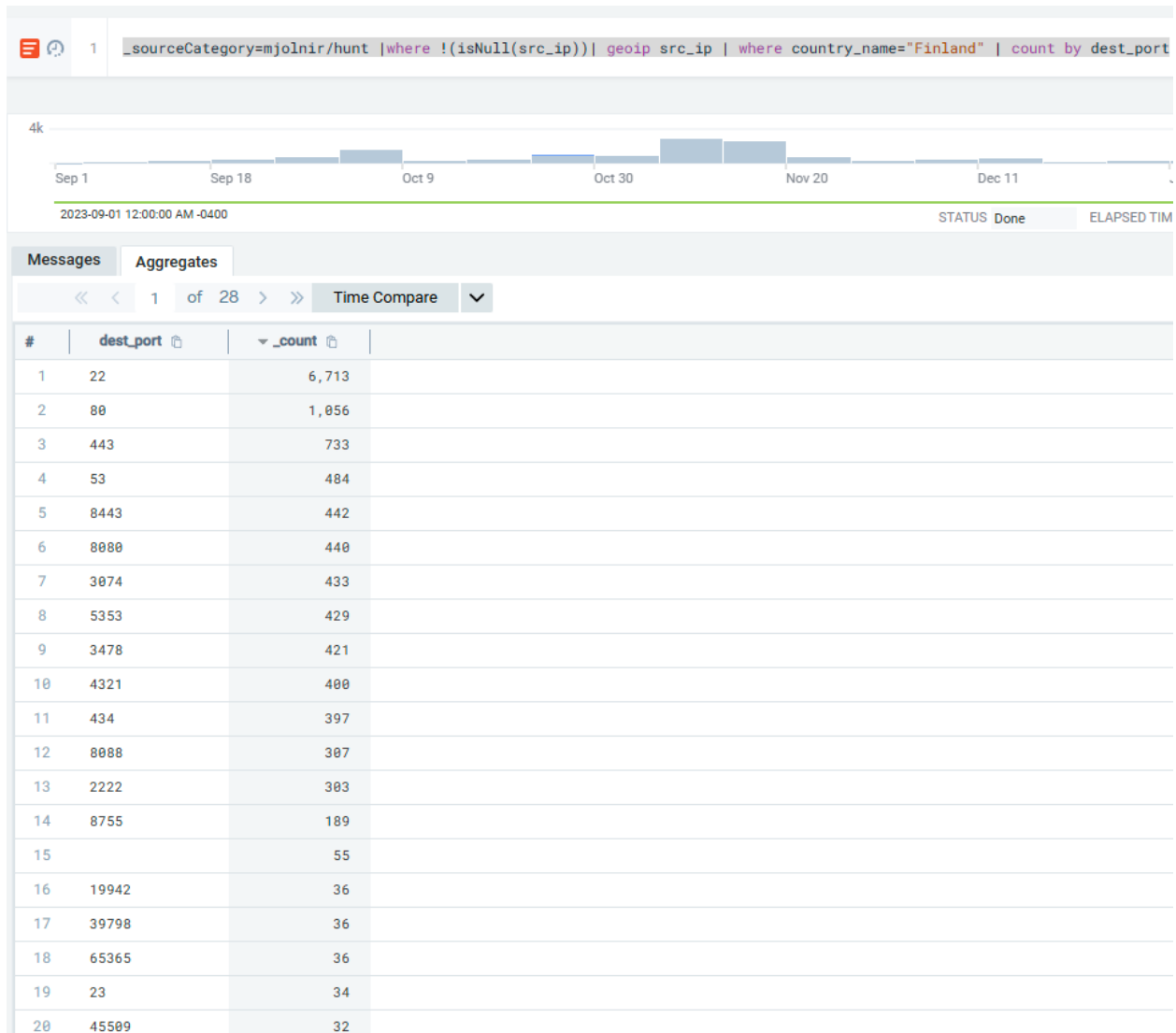
PRODUCT OVERVIEW

 <p>SERVER AUCTION</p> <p>Prices drop & excitement mounts. Place bids in our Server Auction!</p> <p>Starting at € 32.13</p> <p>Overview</p>	 <p>DEDICATED SERVER</p> <p>Dedicated root servers to meet any need. Top performance with an excellent connection.</p> <p>Starting at € 54.74</p> <p>Overview</p>	 <p>CLOUD</p> <p>A little money gets you lots of cloud. Flexible cloud servers with high-end hardware.</p> <p>Starting at € 4.51</p> <p>Overview</p>
 <p>MANAGED SERVERS</p> <p>Stress-free server connection. We'll take care of the technical stuff.</p> <p>Starting at € 40.46</p> <p>Overview</p>	 <p>WEB HOSTING</p> <p>The quick and cheap way to your own homepage. Prices for beginners and businesses.</p> <p>Starting at € 2.09</p> <p>Overview</p>	 <p>STORAGE SHARE</p> <p>Easily store and share files. Access your data at any time and from any place with Storage Share.</p> <p>Starting at € 5.11</p> <p>Overview</p>
 <p>STORAGE BOXES</p> <p>Access your storage from everywhere and at any time via PC, smartphone, and tablet.</p>	 <p>COLOCATION</p> <p>State-of-the-art infrastructure for your project. A range of colocation racks to choose from.</p>	 <p>CUSTOM SOLUTIONS</p> <p>Because your business isn't one size fits all. Get the tailored setup and hardware you need.</p>

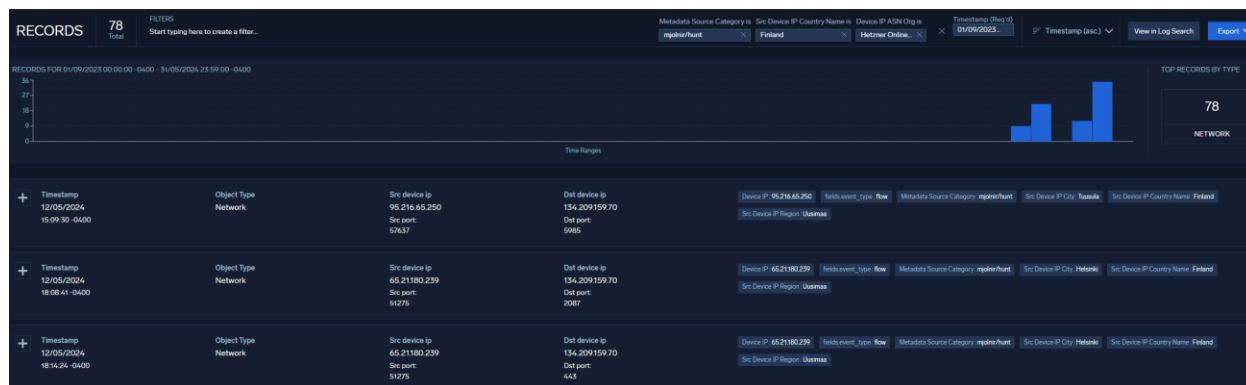
I returned to SumoLogic and ran the following query to find out which ports were being attacked/accessed from Finland the most often.

`_sourceCategory=mjolnir/hunt | where !(isNull(src_ip)) | geoip src_ip | where country_name="Finland" | count by dest_port`

Port 22 (SSH) and port 80 (HTTP) were by far the most commonly accessed ports followed by ports 443 (HTTPS) and 53 (DNS). This suggests to me that the attackers are possibly attempting an SSH Brute Force Attack. This type of attack falls under the Weaponization and Delivery Stages of the Cyber Killchain.



To further corroborate and investigate my initial findings, I turned to the SumoLogic SIEM to look for any possible alerts from Finland, during our specified date range, originating from Hetzner Online GmbH and where the source category is mjolnir/hunt. A total of 78 records were found.



Now that I have an idea of where the attacks are coming from, what they're trying to attack, and how, I will now repeat the steps noted above and formally analyse the top 20 IP addresses and answer these questions (see page 1 for answers):

1. what is the source of the attack?
2. what are they attacking?
3. Why is the target being attacked?
4. What can you identify about the infrastructure used to attack, who does it belong to?
5. What TTPs do you observe?

135.181.237.60

Hostname: d14.joinserver.xyz

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 5985

Destination Port: 80

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnr/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "135.181.237.60"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-11-15 3:50:31.256 PM -0500	Helsinki	FI	Finland	60.165	24.935	135.181.237.60	Uusimaa	<pre> { timestamp: "2023-11-15T20:50:31.256419-0000", flow_id: 230799425954878, src_ip: "135.181.237.60", dest_ip: "134.209.159.70", src_port: 5985, dest_port: 80, proto: "TCP", flow: { ... }, top: { ... } } </pre>

135.181.237.60

Regular ViewRaw Data

OpenMapTiles SatelliteMapTilerOpenStreetMap contributors

General Information

Hostnames

d14joinserver.xyz

Domains

JOINSERVER.XYZ

Country

Germany

City

Gunzenhausen

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

Open Ports

229999

// 22 / TCP

129231561 | 2024-06-06T20:29:48.583042

OpenSSH 9.2p1 Debian 2+deb12u1

SSH-2.0-openssh_9.2p1_Debian-2+deb12u1
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQGCsmhxgSDlVQ1Qc3gd70LwHp4EwqnlIyaP7ASV5ahbY2tHIhoueVdG+uXcnnPXSvVgwnA/gwUzVwKbapnDPfNAQIAP+ZjrhYu7YoXYSmCUhMTBoJAS4eAfft1pT+1GjehdER2wXr55+QFhQZQWVFLHbQCdVbCnWfHChsoa2hloyF7K4h2L1eOTKm/ewIgvxvqrXEBomzdih5TtpS34EhUZYncd3JDKwdsXFRQNd8aHMuZGSv6wA1jr1LehAph400g0exdup77Y90qD6rc3Zy2KjmmX4e21YK1TA/BZpphy2H33PX91CSwT/wOC6tI23+ayShkrtC0jCD9evkteHQCsy3Xovr0URRhtcWlAykh9r26nFxyv5wK2/actQH4m6Zk7ipCEf2CDGVCQmUsprfPkcZF080HUS08uL15jFZ2B6qK5FULqRxEaUGYAq9331aW89nrUeLlw/y1v4v1BUuBLgXQXTenF/bdyxprJ77EY54oG1muJTOXWJ=

Fingerprint: ae:ad:54:c0:c7:1e:36:6c:b6:44:61:87:31:de:c6:aa

Kex Algorithms:
sntrup761x25519-sha512@openssh.com
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group14-sha256

135.181.237.60

Sign inSign up

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

Accept terms of use

1/93

Community Score

1/93 security vendor flagged this IP address as malicious

ReanalyzeSimilarGraphAPI

135.181.237.60 (135.181.0.0/16)

FI

Last Analysis Date

AS 24940 (Hetzner Online GmbH)

25 days ago

DETECTIONDETAILSRELATIONSCOMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

MalwareURL	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

135.181.126.172

Hostname: n3.joinserver.xyz

Operating System: Linux

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 17728

Destination Port: 5353

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjoinlr/hunt |where !isNull(src_ip)| geoip src_ip | where country_name="Finland" | where src_ip = "135.181.126.172"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-11-15 8:15:53.583 PM -0500	Heinola	FI	Finland	60.165	24.935	135.181.126.172	Uusimaa	<div>View as Raw</div> <pre>{ timestamp: "2023-11-16T01:15:53.583162+0000", flow_id: 841970023985285, in_iface: "eth0", event_type: "flow", src_ip: "135.181.126.172", src_port: 17728, dest_ip: "134.209.159.70", dest_port: 5353, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 1, bytes_to_server: 56, bytes_to_client: 54, start: "2023-11-16T01:11:03.772293+0000", end: "2023-11-16T01:11:03.772340+0000", age: 0, state: "closed", reason: "timeout", alerted: false }, tcp: { ... } }</pre> <div>Host: ubuntu-s-1vcpu-2gb-intel-b1r1-81 Name: /var/log/auriscata/evs.json Category: mjoinlr/hunt Index: sumologic_default</div>

135.181.126.172

Regular View

Raw Data

General Information

Hostnames

n3.joinserver.xyz

Domains

JOINSERVER.XYZ

Country

Germany

City

Gunzenhausen

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

Operating System

Linux

1

/ 93

Community Score

1/93 security vendor flagged this IP address as malicious

Reanalyze

Similar

Graph

API

135.181.126.172 (135.181.0.0/16)

AS 24940 (Hetzner Online GmbH)

FI

Last Analysis Date

15 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

MalwareURL	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AlLabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy AV	Clean

135.181.126.164

Hostname: d18.joinserver.xyz

Operating System: Linux

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 46217

Destination Port: 3074

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "135.181.126.164"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-11-09 1:29:43.220 PM -0500	Helsinki	FI	Finland	60.165	24.935	135.181.126.164	Uusima	<pre> { timestamp: "2023-11-09T18:29:43.220771-0000", flow_id: 2172013536295818, in_iface: "eth0", event_type: "flow", src_ip: "135.181.126.164", src_port: 46217, dest_ip: "134.209.159.70", dest_port: 3074, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 1, bytes_to_server: 56, bytes_to_client: 54, start: "2023-11-09T18:24:44.609162-0000", end: "2023-11-09T18:24:44.609196-0000", age: 0, state: "closed", reason: "timeout", alerted: false }, tcp: { ... } } </pre>

General Information

Hostnames

cd18.joinserver.xyz

Domains

JOINSERVER.XYZ

Country

Germany

City

Gunzenhausen

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

Operating System

Linux

1

/ 93

Community Score

1/93 security vendor flagged this IP address as malicious

Reanalyze Similar Graph API

135.181.126.164 (135.181.0.0/16)

AS 24940 (Hetzner Online GmbH)

FI

Last Analysis Date
6 months ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

MalwareURL	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

35.228.169.211

Hostname: 211.169.228.35.bc.googleusercontent.com

Source Organization: Google

Destination Organization: Digital Ocean LLC

Source Port: 48950

Destination Port: 22 (SSH)

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "35.228.169.211"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2024-01-17 12:47:16.339 AM -0500	Lappeenranta	FI	Finland	61.8334	28.21171	35.228.169.211	Etelä-karjala	<div>View as Raw</div> <pre>{ timestamp: "2024-01-17T05:47:16.339851-0500", flow_id: "180508699000783", interface: "eth0", event_type: "flow", src_ip: "35.228.169.211", src_port: 48950, dest_ip: "134.209.159.70", dest_port: 22, proto: "TCP", app_proto: "ssh", flow: { ... }, tcp: { ... } }</pre>

35.228.169.211

Regular View > Raw Data

Vejansaari Uirinsaari

// TAGS: cloud

General Information

Hostnames

211.169.228.35.bc.googleusercontent.com

Domains

GOOGLEUSERCONTENT.COM

Cloud Provider

Google

Cloud Region

europa-north1

Country

Finland

City

Lappeenranta

Organization

Google LLC

ISP

Google LLC

ASN

AS396982

4

/ 93

Community Score

Community Score

Community Score

Community Score

4/93 security vendors flagged this IP address as malicious

Reanalyze

Similar

Graph

API

35.228.169.211 (35.228.0.0/16)

FI

Last Analysis Date

AS 396982 (GOOGLE-CLOUD-PLATFORM)

5 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 12+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	BitDefender	Phishing
CyRadat	Malicious	G-Dat	Phishing
AlphaSOC	Suspicious	ArcSight Threat Intelligence	Suspicious

77.91.78.115

Hostname: test.aeza.network

Source Organization: Aeza International LTD

Destination Organization: Digital Ocean LLC

Operating System : Debian

Source Port: 40828

Destination Port: 22 (SSH)

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "77.91.78.115"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2024-01-06 14:48:00.278 PM -0500		FI	Finland	64	26	77.91.78.115		<div>View as Row</div> <pre> { timestamp: "2024-01-06T18:48:00.278400-0000", flow_id: 211240503271516, in_iface: "eth0", event_type: "flow", src_ip: "77.91.78.115", src_port: 40828, dest_ip: "134.209.159.70", dest_port: 22, proto: "TCP", app_proto: "ssh", flow: { pkts_server: 12, pkts_client: 12, bytes_server: 2050, bytes_client: 2389, start: "2024-01-06T18:44:49.606428-0000", end: "2024-01-06T18:44:51.257494-0000", age: 2, state: "closed", reason: "timeout", alerted: false }, tcp: { ... } } </pre>

77.91.78.115

Regular View

Raw Data

General Information

Hostnames

testaeza.network

Domains

AEZA.NETWORK

Country

Sweden

City

Stockholm

Organization

Aeza International LTD

ISP

AEZA INTERNATIONAL LTD

ASN

AS210644

Operating System

Debian

8 / 93

Community Score

8/93 security vendors flagged this IP address as malicious

Reanalyze

Similar

Graph

API

77.91.78.115 (77.91.78.0/24)

FI

Last Analysis Date

AS 210644 (Aeza International Ltd)

5 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 6

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	BitDefender	Phishing
Criminal IP	Malicious	CyRadar	Malicious
G-Dat	Phishing	GreenSnow	Malicious
Lionic	Malicious	SOCradar	Malicious
AlphaSOC	Suspicious	ArcSight Threat Intelligence	Suspicious

135.181.51.116

Hostname: DE-HETZNER-19931109

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 37148

Destination Port: 2222

Destination IP: 64.226.119.125

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "135.181.51.116"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-10-31 12:23:50.317 AM -0400	Helsinki	FI	Finland	60.165	24.935	135.181.51.116	Uusimaa	<div>View as Raw</div> <pre>{ timestamp: "2023-10-31T04:23:50.317660-0000", flow_id: 182349923731512, in_iface: "eth0", event_type: "Flow", src_ip: "135.181.51.116", src_port: 37148, dest_ip: "64.226.119.125", dest_port: 2222, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 0, bytes_to_server: 56, bytes_to_client: 0, start: "2023-10-31T04:19:22.594488-0000", end: "2023-10-31T04:19:22.594488-0000", age: 0, state: "new", reason: "timeout", alerted: true }, tcp: { ... } }</pre>

Shodan: No results

2
/ 93

Community Score

2/93 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

135.181.51.116 (135.181.0.0/16)

FI

Last Analysis Date
6 months ago

AS 24940 (Hetzner Online GmbH)

DETECTION

DETAILS

RELATIONS

COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

Antiy-AVL ⓘ Malicious

MalwareURL ⓘ Malware

65.108.239.145

Hostname: dertix-is-fucking-scam.fuckmedaddy.cc, static.65.108.239.145.clients.your-server.de

(I apologize for the profanities; I unfortunately do not get to choose the hostnames)

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 49135

Destination Port: 23

Destination IP: 64.226.119.125

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !isNull(src_ip)| geoip src_ip | where country_name="Finland" | where src_ip = "65.108.239.145"`

Sumologic event viewer showing a log entry for the IP 65.108.239.145. The event is a TCP connection attempt from the source IP to the destination IP 64.226.119.125 on port 23. The event is categorized as 'mjolnir/hunt'.

```
{
  "timestamp": "2024-05-31T10:23:26.50934-0000",
  "flow_id": "183701564753300",
  "ip_iface": "eth0",
  "event_type": "tcp",
  "src_ip": "65.108.239.145",
  "src_port": 49135,
  "dest_ip": "64.226.119.125",
  "dest_port": 23,
  "proto": "TCP",
  "flow": {
    "pkt_txserver": 1,
    "pkt_rcvclient": 1,
    "bytes_txserver": 54,
    "bytes_rcvclient": 54,
    "start": "2024-05-31T10:23:26.50934-0000",
    "end": "2024-05-31T10:23:26.50934-0000",
    "app": 0,
    "state": "closed",
    "reason": "normal",
    "aborted": false
  },
  "tcp": {
  }
}
```

65.108.239.145

Regular View > Raw Data

Ingels Kvärnen Pitkäsari Käärmesaari Ulko-Hattu

General Information

Hostnames	dertix-is-fucking-scam.fuckmedaddy.cc static.65.108.239.145.clients.your-server.de
Domains	FUCKMEDADDY.CC YOUR-SERVER.DE
Country	Finland
City	Helsinki
Organization	Hetzner Online GmbH
ISP	Hetzner Online GmbH
ASN	AS24940

2

/ 93

Community Score

2/93 security vendors flagged this IP address as malicious

Reanalyze

Similar

Graph

API

65.108.239.145 (65.108.0.0/15)

FI

Last Analysis Date

AS 24940 (Hetzner Online GmbH)

15 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

CRDF	Malicious	CyRadar	Malicious
AlphaSOC	Suspicious	Criminal IP	Suspicious

65.108.17.222

Hostname: static.222.17.108.65.clients.your-server.de

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 65454

Destination Port: 34087

Destination IP: 64.226.119.125

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "65.108.17.222"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-10-07 9:02:42.145 PM +000	Helsinki	FI	Finland	60.165	24.935	65.108.17.222	Uusimaa	<div>View as Raw</div> <pre>{ timestamp: "2023-10-08T01:02:42.145711+0000", flow_id: 657774219232265, src_iface: "eth0p", event_type: "flow", src_ip: "65.108.17.222", src_port: 65454, dest_ip: "64.226.119.125", dest_port: 34087, proto: "TCP", flow: { ... }, tcp: { ... } }</pre> <div>Host: ubuntu-s-1vcpu-2gb-intel-frs1-01 • Home: /var/log/auricasta/evs.json • Category: mjolnir/hunt • Index: sumologic_default •</div>

65.108.17.222

Regular View

Raw Data

Ingels

Kvärlan

Pitkäsaari

Käärmesaari

Ulko-Hattu

General Information

Hostnames

static.222.17108.65.clients.your-server.de

Domains

YOUR-SERVER.DE

Country

Finland

City

Helsinki

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

Operating System

Ubuntu

6

/ 93

Community Score

6/93 security vendors flagged this IP address as malicious

Reanalyze

Similar

Graph

API

65.108.17.222 (65.108.0.0/15)

FI

Last Analysis Date

AS 24940 (Hetzner Online GmbH)

7 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

AlphaSOC	Malware	Antiy-AVL	Malicious
BitDefender	Malware	CyRadat	Malware
G-Data	Malware	Sophos	Malware
Abusix	Clean	Arcabit	Clean

95.216.68.161

Hostname: static.161.68.216.95.clients.your-server.de

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 41349

Destination Port: 8080

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "95.216.68.161"`

2023-11-08 6:43:47.518 AM +0000	Tuusula	FI	Finland	68.42842	25.81132	95.216.68.161	Uusimaa	<div>View as Raw</div> <div><pre>{ timestamp: "2023-11-08T11:43:47.518367+0000", flow_id: "141056229428816", src_ip: "95.216.68.161", event_type: "flow", src_port: 41349, dest_ip: "134.209.159.79", dest_port: 8080, proto: "TCP", flow: { ... }, top: { ... } }</pre></div>
Host: ubuntu-8-1cpu-2gb-intel-8i1-8i1 - Home /var/log/syslogcat/evs.json - Category: mjolnir/hunt - Index: sumologic_default								

95.216.68.161

Regular View

> Raw Data

General Information

Hostnames

static.161.68.216.95.clients.your-server.de

Domains

YOUR-SERVER.DE

Country

Finland

City

Helsinki

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

2/93

Community Score

2/93 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

95.216.68.161 (95.216.0.0/15)

FI

Last Analysis Date 2 months ago

AS 24940 (Hetzner Online GmbH)

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

GreenSnow

Malicious

MalwareURL

Malware

65.108.18.28

Hostname: n32.joinserver.xyz

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 20877

Destination Port: 8443

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "65.108.18.28"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-11-06 9:21:59.119 AM -0500	Helsinki	FI	Finland	60.165	24.935	65.108.18.28	Uusimaa	<div>View as Raw</div> <pre>{ timestamp: "2023-11-06T14:21:59.119331+0000", flow_id: 71469258101283, src_iface: "eth0", event_type: "Flow", src_ip: "65.108.18.28", src_port: 20877, dest_ip: "134.209.159.70", dest_port: 8443, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 1, bytes_to_server: 56, bytes_to_client: 54, start: "2023-11-06T14:17:14.533537+0000", end: "2023-11-06T14:17:14.533558+0000", age: 0, state: "closed", reason: "timeout", alerted: false }, tcp: { ... } }</pre>

65.108.18.28

Regular ViewRaw Data

// TAGS: videogame

General Information

Hostnames

n32.joinserver.xyz

Domains

JOINSERVER.XYZ

Country

Germany

City

Gunzenhausen

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

Operating System

Linux

0
/ 93

Community Score

No security vendor flagged this IP address as malicious

Reanalyze Similar Graph API

65.108.18.28 (65.108.0.0/15)

FI

Last Analysis Date
19 days ago

AS 24940 (Hetzner Online GmbH)

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

0xSI_f33d	? Unrated	Abusix	? Unrated
Acronis	? Unrated	ADMINUSLabs	? Unrated

65.108.234.37

Hostname: gamely.pro , d7.gamely.pro

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 17171

Destination Port: 154

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "65.108.234.37"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-11-15 8:28:35.174 AM -0500	Helsinki	FI	Finland	60.165	24.935	65.108.234.37	Uusima	<div>View as Raw</div> <pre>{ timestamp: "2023-11-15T13:28:35.174873+0000", flow_id: 866482915771811, ip_iface: "eth0", event_type: "flow", src_ip: "65.108.234.37", src_port: 17171, dest_ip: "134.209.159.70", dest_port: 154, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 1, bytes_to_server: 56, bytes_to_client: 54, start: "2023-11-15T13:23:50.525731+0000", end: "2023-11-15T13:23:50.525773+0000", age: 0, state: "closed", reason: "timeout", alerted: false }, tcp: { ... } }</pre> <div>Host ubuntu-s-1vcpu-2gb-intel-b1r1-01 - Home /var/log/sumicata/evs.json - Category: mjolnir/hunt - Index: sumologic_default -</div>

65.108.234.37

Regular View

Raw Data

// TAGS: database

General Information

Hostnames

gamely.pro
d7gamely.pro

Domains

GAMELY.PRO

Country

Finland

City

Helsinki

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

1
/ 93

Community Score

1/93 security vendor flagged this IP address as malicious

Reanalyze

Similar

Graph

API

65.108.234.37 (65.108.0.0/15)

FI

Last Analysis Date

AS 24940 (Hetzner Online GmbH)

2 months ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

MalwareURL

Malware

Abusix

Clean

80.85.241.213

Hostname: olitary-observation.aeza.network, stats.vk-portal.net, vk.cc, vk.com, vk.design, vk.link, vk.me, vk.ru, vkontakte.com, vkontakte.ru

Source Organization: Aeza International LTD

Destination Organization: Digital Ocean LLC

Source Port: 28486

Destination Port: 22

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "80.85.241.213"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-11-16 9:40:09.000 PM -0500		FI	Finland	64	26	80.85.241.213		<div>View as Raw</div> <pre>{ timestamp: "2023-11-16T22:40:09.050966-0000", flow_id: 127228705570000, in_iface: "eth0", event_type: "flow", src_ip: "80.85.241.213", src_port: 28486, dest_ip: "134.209.159.70", dest_port: 22, proto: "TCP", app_proto: "ssh", flow: { pkts_totserver: 14, pkts_totclient: 12, bytes_totserver: 2183, bytes_totclient: 2557, start: "2023-11-16T22:36:56.400562-0000", end: "2023-11-16T22:36:57.909031-0000", age: 1, state: "closed", reason: "timeout", alerted: false }, tcp: { ... } }</pre>

80.85.241.213

Kurkio

Regular View

Raw Data

Brobacka

Högnäs

Nepperi

General Information

solitary-observation.aeza.network

stats.vk-portal.net

vk.cc

vk.com

vk.design

vk.link

vk.me

vk.ru

vkontakte.com

vkontakte.ru

Domains

AEZA.NETWORK

VK-PORTAL.NET

VK.CC

VK.COM

VK.DESIGN

VK.LINK

VK.ME

VK.RU

VKONTAKTE.COM

VKONTAKTE.RU

Country

Finland

City

Helsinki

Organization

Aeza International LTD

ISP

AEZA INTERNATIONAL LTD

ASN

AS210644

5/93

Community Score

5/93 security vendors flagged this IP address as malicious

80.85.241.213 (80.85.241.0/24)
AS 210644 (Aeza International Ltd)

FI
Last Analysis Date
1 month ago

ReanalyzeSimilarGraphAPI

DETECTIONDETAILSRELATIONSCOMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysisDo you want to automate checks?

Antiy-AVL	Malicious	BitDefender	Phishing
CyRadar	Malicious	G-Data	Phishing
SOCRadar	Malicious	Abusix	Clean

77.91.70.64

Hostname: brave-judge.aeza.network

Source Organization: Aeza International LTD

Destination Organization: Digital Ocean LLC

Source Port: 43882

Destination Port: 22

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: _sourceCategory=mjolo1nr/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "77.91.70.64"

12023-12-237:29:42.655 PM+0000FIFinland642677.91.70.64

View as Row

```
{
  timestamp: "2023-12-24T00:29:42.655282+0000",
  flow_id: 483531621142133,
  in_iface: "eth0",
  event_type: "flow",
  src_ip: "77.91.70.64",
  src_port: 43882,
  dest_ip: "134.209.159.70",
  dest_port: 22,
  proto: "TCP",
  app_proto: "ssh",
  flow: {
    pkts_to_server: 12,
    pkts_to_client: 12,
    bytes_to_server: 2030,
    bytes_to_client: 2589,
    start: "2023-12-24T00:25:40.003701+0000",
    end: "2023-12-24T00:25:41.634235+0000",
    age: 1,
    state: "closed",
    reason: "timeout",
    alerted: false
  },
  tcp: { ... }
}
```

Host: ubuntu-s-1vcpu-2gb-intel-blr1-01 | Name: /var/log/dockerdata/ev... | Category: mjolo1nr/hunt | Index: sumlogic_default

77.91.70.64



General Information

Hostnames	brave-judge.aeza.network
Domains	AEZA.NETWORK
Country	Finland
City	Helsinki
Organization	Aeza International LTD
ISP	AEZA INTERNATIONAL LTD
ASN	AS210644



Community Score

7/93 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

77.91.70.64 (77.91.70.0/24)

AS 210644 (Aeza International Ltd)



Last Analysis Date
1 month ago

DETECTION DETAILS RELATIONS COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	BitDefender	Phishing
Criminal IP	Malicious	CyRadar	Malicious
G-Data	Phishing	GreenSnow	Malicious
SOCradar	Malicious	AlphaSOC	Suspicious

77.91.70.251

Hostname: gullible-hand.aeza.network

Source Organization: Aeza International LTD

Destination Organization: Digital Ocean LLC

Source Port: 41258

Destination Port: 22

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "77.91.70.251"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-12-27 12:46:22.278 PM -0500		FI	Finland	64	26	77.91.70.251		<div>View as Raw</div> <pre>{ timestamp: "2023-12-27T17:46:22.278963-0000", flow_id: 2055132793762419, en_iface: "eth0", event_type: "flow", src_ip: "77.91.70.251", src_port: 41258, dest_ip: "134.209.159.70", dest_port: 22, proto: "TCP", app_proto: "ssh", flow: { flow: { pkts_to_server: 14, pkts_to_client: 12, bytes_to_server: 2182, bytes_to_client: 2589, start: "2023-12-27T17:41:21.268403-0000", end: "2023-12-27T17:41:23.607137-0000", age: 2, state: "closed", reason: "timeout", alerted: false } }, tcp: { } }</pre>

Host: ubuntu-s-2vcpu-2gb-intel-blr1-01 - Name: /var/log/suricata/eve.json - Category: mjolnir/hunt - Index: sumologic_default -

77.91.70.251

Regular View

> Raw Data

Ekerö

Fågelön

Kungshatt

General Information

Hostnames

gullible-hand.aeza.network

Domains

AEZA.NETWORK

Country

Sweden

City

Stockholm

Organization

Aeza International LTD

ISP

AEZA INTERNATIONAL LTD

ASN

AS210644

7/93

Community Score

7/93 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

77.91.70.251 (77.91.70.0/24)

FI

Last Analysis Date 1 month ago

AS 210644 (Aeza International Ltd)

DETECTION

DETAILS

RELATIONS

COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

Antiy-AVL	Malicious	BitDefender	Phishing
Criminal IP	Malicious	CyRadar	Malicious
G-Data	Phishing	IPsum	Malicious
SOCradar	Malicious	AlphaSOC	Suspicious

95.216.197.30

Hostname: static.30.197.216.95.clients.your-server.de

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 50718

Destination Port: 22

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "95.216.197.30"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-10-08 7:08:52.114 PM +000	Tuusula	FI	Finland	68.42642	25.81132	95.216.197.30	Uusimaa	<div><div>View as Raw</div><div><pre>{ timestamp: "2023-10-08T23:08:52.114207-0000", flow_id: 1861416099132730, is_iface: "eth0", event_type: "flow", src_ip: "95.216.197.30", src_port: 50718, dest_ip: "134.209.159.70", dest_port: 22, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 0, bytes_to_server: 58, bytes_to_client: 0, start: "2023-10-08T23:03:58.275770-0000", end: "2023-10-08T23:03:58.275770-0000", age: 0, state: "new", reason: "timeout", alerted: true }, tcp: { ... } }</pre></div></div>

Host ubuntu-s-1vcpu-2gb-intel-b1r1-01 - Name: /var/log/auriscata/evs.json - Category: mjolnir/hunt - Index: sumologic_default -

95.216.197.30

Regular View

Raw Data

Ingels

Kvärlan

Pitkasaari

Käärmesaari

Uiko-Hattu

General Information

Hostnames static.30.197.216.95.clients.your-server.de

Domains YOUR-SERVER.DE

Country Finland

City Helsinki

Organization Hetzner Online GmbH

ISP Hetzner Online GmbH

ASN AS24940



Community Score

6/93 security vendors flagged this IP address as malicious

Reanalyze

Similar

Graph

API

95.216.197.30 (95.216.0.0/15)

AS 24940 (Hetzner Online GmbH)

FI

Last Analysis Date
6 months ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

Activity related to MIRAI - according to source Cluster25 - 8 months ago
This IPV4 is used by MIRAI

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	Cluster25	Malicious
Criminal IP	Malicious	CyRadat	Malicious
MalwareURL	Malware	VIPRE	Malware
AlphaSOC	Suspicious	Abusix	Clean

135.181.108.61

Hostname: static.61.108.181.135.clients.your-server.de

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 33042

Destination Port: 22

Destination IP: 64.226.119.125

Sumologic query to see events caused by this IP: `_sourceCategory=mjolinir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "135.181.108.61"`

1	2023-12-19 10:50:21.408 PM @500	Helsinki	FI	Finland	60.165	24.935	135.181.198.61	Duisiana	View as Raw
									<pre>{ timestamp: "2023-12-14T03:50:21.408991+0000", flow_id: 2103707697698910, interface: "eth0", event_type: "flow", src_ip: "135.181.198.61", src_port: 33043, dest_ip: "64.226.119.125", dest_port: 22, proto: "TCP", app_proto: "ssh", flow: { pkts_to_server: 11, pkts_to_client: 10, bytes_to_server: 1890, bytes_to_client: 2497, start: "2023-12-14T03:45:51.080190+0000", end: "2023-12-14T03:45:51.253414+0000", age: 0, state: "closed", reason: "timeout", alerted: false }, tcp: {} (...)} }</pre>

135.181.108.61

Regular View

Raw Data

Ingels

Kvärlan

Pitkäsaari

Käärmeasaari

Uisko-Hattu

General Information

Hostnames

static.61.108.181.135.clients.your-server.de

Domains

YOUR-SERVER.DE

Country

Finland

City

Helsinki

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

1
/ 93

Community Score

1/93 security vendor flagged this IP address as malicious

Reanalyze Similar Graph API

135.181.108.61 (135.181.0.0/16)
AS 24940 (Hetzner Online GmbH)

FI
Last Analysis Date
6 months ago

DETECTIONDETAILSRELATIONSCOMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘDo you want to automate checks?

MalwareURL	ⓘ Malware	Abusix	✔ Clean
Acronis	✔ Clean	ADMINUSLabs	✔ Clean

65.21.70.50

Hostname: z6.joinserver.xyz

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 40773

Destination Port: 988

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "65.21.70.50"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-11-17 8:29:21.331 AM 0500	Heilsinki	FI	Finland	60.165	24.935	65.21.70.50	Uusima	<div>View as Raw</div> <pre>{ timestamp: "2023-11-17T13:29:21.331811+0000", flow_id: "1878088991622281", in_iface: "eth0", event_type: "flow", src_ip: "65.21.70.50", src_port: 40773, dest_ip: "134.209.159.70", dest_port: 988, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 1, bytes_to_server: 66, bytes_to_client: 64, start: "2023-11-17T13:24:34.209033+0000", end: "2023-11-17T13:24:34.209075+0000", age: 0, state: "closed", reason: "timeout", alerted: false }, tcp: { ... } }</pre>

Host: ubuntu-8-1vcpu-2gb-intel-blr1-01 | Name: /var/log/suricata/eve.json | Category: mjolnir/hunt | Index: sumologic.default

65.21.70.50 Regular View Raw Data

General Information

Hostnames	z6.joinserver.xyz
Domains	JOINSERVER.XYZ
Country	Germany
City	Gunzenhausen
Organization	Hetzner Online GmbH
ISP	Hetzner Online GmbH
ASN	AS24940
Operating System	Linux

0 / 93
Community Score

No security vendor flagged this IP address as malicious

65.21.70.50 (65.21.0.0/16)
AS 24940 (Hetzner Online GmbH)

FI Last Analysis Date a moment ago

Reanalyze Similar Graph API

DETECTION DETAILS RELATIONS COMMUNITY

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
--------	---------	---------	---------

65.109.132.76

Hostname: CLOUD-HEL1

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 36297

Destination Port: 22

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "65.109.132.76"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-10-09 8:05:38.504 AM +0400	Helsinki	FI	Finland	60.165	24.935	65.109.132.76	Uusimaa	<div>View as Raw</div> <pre>{ timestamp: "2023-10-09T12:05:38.504009+0000", flow_id: 58973852900506, in_iface: "eth0", event_type: "flow", src_ip: "65.109.132.76", src_port: 34297, dest_ip: "134.209.159.70", dest_port: 22, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 0, bytes_to_server: 56, bytes_to_client: 0, start: "2023-10-09T12:01:17.695450+0000", end: "2023-10-09T12:01:17.695450+0000", age: 0, state: "new", reason: "timeout", alerted: true }, tcp: { ... } }</pre> <div>Host: ubuntu-s-1cpu-2gb-intel-b1r1-01 Name: /var/log/suricata/eve.json Category: mjoinlr/hunt Index: sumologic_default</div>

6

/93

Community Score

6/93 security vendors flagged this IP address as malicious

Reanalyze

Similar

Graph

API

65.109.132.76 (65.108.0.0/15)

AS 24940 (Hetzner Online GmbH)

FI

Last Analysis Date
6 months ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 2

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

65.108.87.234

Hostname: static.234.87.108.65.clients.your-server.de

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 4813

Destination Port: 8088

Destination IP: 64.226.119.125

Sumologic query to see events caused by this IP: `_sourceCategory=mjoinlr/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "65.108.87.234"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-10-11 3:09:10.007 AM +0400	Helsinki	FI	Finland	60.165	24.935	65.188.87.234	Uusimaa	<div>View as Raw</div> <pre>{ timestamp: "2023-10-11T07:09:10.007740+0000", flow_id: 2151829232629351, in_iface: "eth0", event_type: "flow", src_ip: "65.108.87.234", src_port: 4813, dest_ip: "64.226.119.125", dest_port: 8088, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 0, bytes_to_server: 56, bytes_to_client: 0, start: "2023-10-11T07:05:23.694503+0000", end: "2023-10-11T07:05:23.694503+0000", age: 0, state: "new", reason: "timeout", alerted: true }, tcp: { ... } }</pre> <div>Host: ubuntu-s-1cpu-2gb-intel-fr1-01 Name: /var/log/suricata/eve.json Category: mjoinlr/hunt Index: sumologic_default</div>

65.108.87.234

Regular View

Raw Data

General Information

Hostnames

static.234.87108.65.clients.your-server.de

Domains

YOUR-SERVER.DE

Country

Finland

City

Helsinki

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

6 / 93

Community Score

6/93 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

65.108.87.234 (65.108.0.0/15)

FI

Last Analysis Date 2 months ago

AS 24940 (Hetzner Online GmbH)

DETECTION

DETAILS

RELATIONS

COMMUNITY 2

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	Cluster25	Malicious
CRDF	Malicious	CyRadar	Malicious
MalwareURL	Malware	VIPRE	Malware

95.216.92.65

Hostname: m16.joinserver.xyz

Source Organization: Hetzner Online GmbH

Destination Organization: Digital Ocean LLC

Source Port: 28026

Destination Port: 443

Destination IP: 134.209.159.70

Sumologic query to see events caused by this IP: `_sourceCategory=mjolnir/hunt |where !(isNull(src_ip))| geoip src_ip | where country_name="Finland" | where src_ip = "95.216.92.65"`

#	Time	city	country_code	country_name	latitude	longitude	src_ip	state	Message
1	2023-11-06 9:11:48.433 AM +0500	Tuusula	FI	Finland	66.42642	25.81132	95.216.92.65	Uusima	<pre> View as Raw { timestamp: "2023-11-06T14:11:48.433995+0000", flow_id: 2105238131264728, in_iface: "eth0", event_type: "flow", src_ip: "95.216.92.65", src_port: 28028, dest_ip: "134.209.159.70", dest_port: 443, proto: "TCP", flow: { pkts_to_server: 1, pkts_to_client: 1, bytes_to_server: 56, bytes_to_client: 54, start: "2023-11-06T14:06:52.316278+0000", end: "2023-11-06T14:06:52.316325+0000", age: 6, state: "closed", reason: "timeout", alerted: false }, tcp: { ... } } </pre>

95.216.92.65

Regular View Raw Data

IngelsKvärjanPitkäsaariKäärmesaariUlko-Hattu

General Information

Hostnames

m16joinsrvr.xyz

Domains

JOINSERVER.XYZ

Country

Finland

City

Helsinki

Organization

Hetzner Online GmbH

ISP

Hetzner Online GmbH

ASN

AS24940

Operating System

Debian

0

/ 93

Community Score

No security vendor flagged this IP address as malicious

Reanalyze

Similar

Graph

API

95.216.92.65 (95.216.0.0/15)

FI

Last Analysis Date

1 year ago

AS 24940 (Hetzner Online GmbH)

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	Clean	ADMINUSLabs	Clean
AlienVault	Clean	alphaMountain.ai	Clean