

Scattered Spider recent campaigns shows that the threat group seem to have migrated away from AS CHOOA and into **Digital Ocean** and **BLNWX ASN (AS399629)**

New Campaigns noticed as of late March to April indicates Scattered spider switched to another registrar - **registrar[.]eu**

Furthermore most Scattered Spider phishing pages contain an invisible list with a distinct URL in the HTML code eg:

Unset

```
<a href="hxxps://nigga.okta[.]com/help/login" data-se="help-link"
```

On the basis of previously reported scattered spider victimology we assess that below phishing domains are newly created by scattered spider threat group for ongoing campaign

For April month, following are the list of targeted organization

- Klaviyo
- Charter Communications
- T-Mobile

Klaviyo

Domain : hxxps://klavlyo[.]com

This website contacted 2 IPs in 1 country across 2 domains to perform 11 HTTP transactions. The main IP is 162.33.177[.]163, located in Chicago, United States and belongs to BLNWX, US. The main domain is klavlyo[.]com.

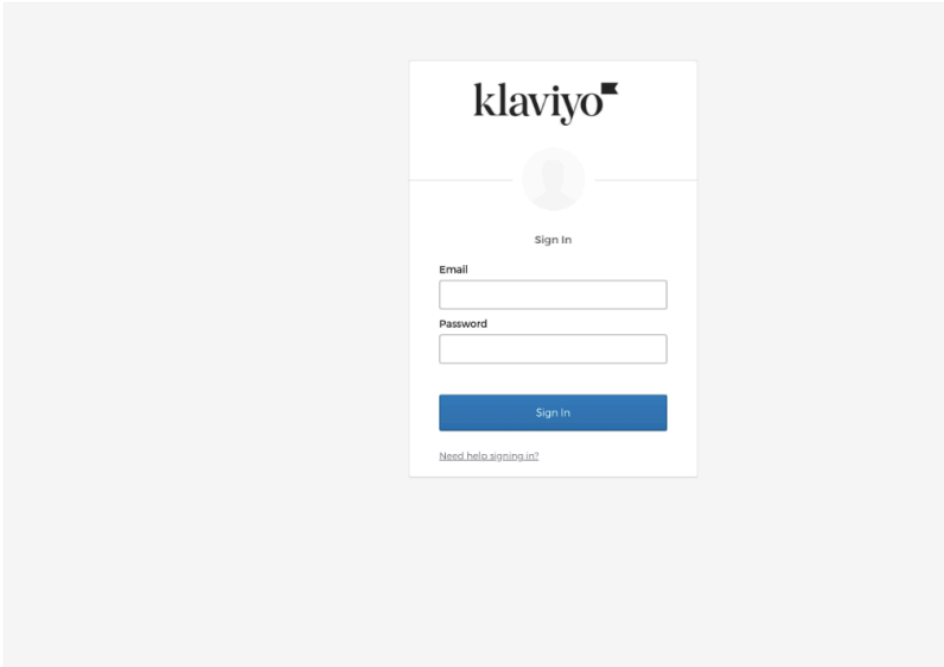
TLS certificate: Issued by R3 on April 15th 2024. Valid for: 3 months

Live information

Google Safe Browsing: Malicious for klavlyo[.]com

Domain created: April 15th 2024, 17:41:49 (UTC)

Domain registrar: Hosting Concepts B.V. d/b/a Registrar.eu



klaviyo.com

162.33.177.163 Public Scan

URL: <https://klaviyo.com/>

Submission Tags: @phish_report

Submission: On April 15 via api (April 15th 2024, 1:13:41 pm UTC) from FI+ — Scanned from FI+

[Summary](#) [HTTP 11](#) [Redirects](#) [Links 2](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary

This website contacted 2 IPs in 1 countries across 2 domains to perform 11 HTTP transactions. The main IP is 162.33.177.163, located in Chicago, United States and belongs to BLNWX, US. The main domain is klaviyo.com. TLS certificate: Issued by R3 on April 15th 2024. Valid for: 3 months.

klaviyo.com scanned 21 times on urlscan.io

Show Scans 21

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: Malicious for klaviyo.com
Current DNS A record: 15.197.130.221 (AS16509 - AMAZON-02, US)
Domain created: April 15th 2024, 17:41:49 (UTC)
Domain registrar: Hosting Concepts B.V. d/b/a Registrar.eu

Domain & IP information

[IP/ASNs](#) [IP Detail](#) [Domains](#) [Domain Tree](#) [Links](#) [Certs](#) [Frames](#)

This site contains links to these domains. Also see [Links](#).

Domain

nigga.okta.com

www.okta.com

[Lookup](#) [Go To](#) [Rescan](#)

[Add Verdict](#) [Report](#)

Screenshot

[Live screenshot](#) [Full Image](#)



Page Title

Sign In

Page Statistics

11	100 %	0 %	2	2
Requests	HTTPS	IPv6	Domains	Subdomains
2	1	735 kB	2270 kB	0
IPs	Countries	Transfer	Size	Cookies

Charter Communications

Domain : hxxps://chartervpn[.]com
Domain Created : April 2nd 2024

chartervpn.com

134.209.208.248 Public Scan

URL: <https://chartervpn.com/>

Submission: On April 02 via automatic, source certstream-suspicious (April 2nd 2024, 8:51:19 am UTC) — Scanned from

Summary

HTTP 11

Redirects

Links 2

Behaviour

Indicators

Similar

DOM

Content

API

Verdicts

Summary

This website contacted 3 IPs in 1 countries across 3 domains to perform 11 HTTP transactions. The main IP is 134.209.208.248 located in North Bergen, United States and belongs to DIGITALOCEAN-ASN, US. The main domain is chartervpn.com.

TLS certificate: Issued by R3 on April 2nd 2024. Valid for: 3 months.

chartervpn.com scanned 14 times on urlscan.io Show Scans 14

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for chartervpn.com

Current DNS A record: 15.197.130.221 (AS16509 - AMAZON-02, US)

Domain created: April 2nd 2024, 14:11:45 (UTC)

Domain registrar: Hosting Concepts B.V. d/b/a Registrar.eu

Domain & IP information

IP/ASNs

IP Detail

Domains

Domain Tree

Links

Certs

Frames

This site contains links to these domains. Also see [Links](#).

Domain

nigga.okta.com

www.okta.com

Lookup

Go To

Rescan

Add Verdict

Report

Screenshot

Live screenshot

Full Image

Page Title

Sign In

Page Statistics

11	91 %	0 %	3	3
Requests	HTTPS	IPv6	Domains	Subdomains
3	1	733 kB	2268 kB	2
IPs	Countries	Transfer	Size	Cookies

Domain : hxxps://charter-vpn[.]com
Domain Created : April 4th 2024
Domain registrar: Nicenic International Group Co. Ltd

charter-vpn.com

104.248.113.206 Public Scan

URL: <https://charter-vpn.com/>

Submission Tags: @phish_report

Submission: On April 04 via api (April 4th 2024, 4:09:21 am UTC) from — Scanned from

Summary

HTTP 11

Redirects

Links 2

Behaviour

Indicators

Similar

DOM

Content

API

Verdicts

Summary

This website contacted 3 IPs in 2 countries across 3 domains to perform 11 HTTP transactions. The main IP is 104.248.113.206 located in North Bergen, United States and belongs to DIGITALOCEAN-ASN, US. The main domain is charter-vpn.com.

TLS certificate: Issued by R3 on April 4th 2024. Valid for: 3 months.

charter-vpn.com scanned 16 times on urlscan.io Show Scans 16

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for charter-vpn.com

Domain created: April 4th 2024, 08:09:27 (UTC)

Domain registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED

Domain & IP information

IP/ASNs

IP Detail

Domains

Domain Tree

Links

Certs

Frames

This site contains links to these domains. Also see [Links](#).

Domain

nigga.okta.com

www.okta.com

Lookup

Go To

Rescan

Add Verdict

Report

Screenshot

Live screenshot

Full Image

Page Title

Sign In

Page Statistics

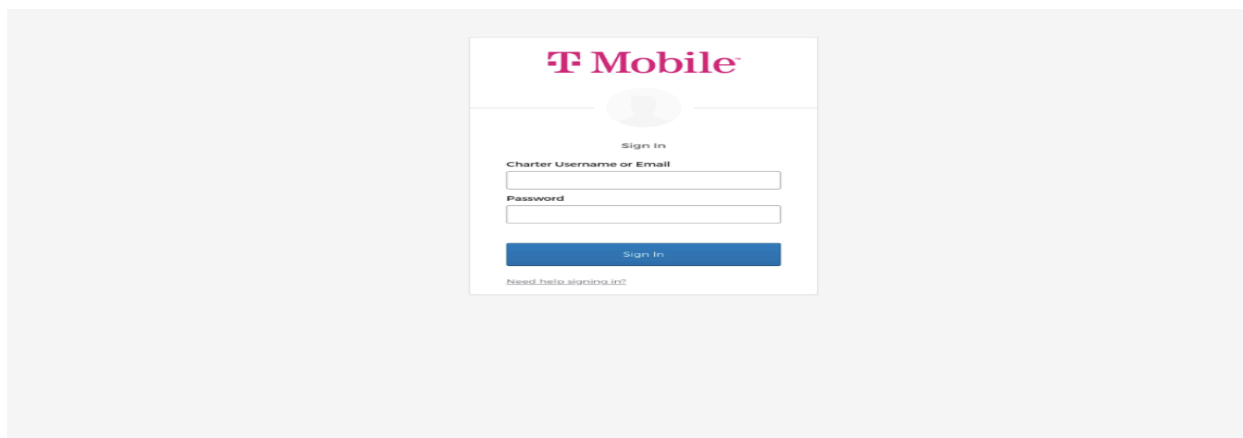
11	100 %	0 %	3	3
Requests	HTTPS	IPv6	Domains	Subdomains
3	2	742 kB	2276 kB	0
IPs	Countries	Transfer	Size	Cookies

T-Mobile

hxxps://104.248.113[.]206/

This website contacted 3 IPs in 1 countries across 1 domains to perform 11 HTTP transactions. The main IP is 104.248.113[.]206, located in North Bergen, United States and belongs to DIGITALOCEAN-ASN, US.

The main domain is 104.248.113[.]206.
TLS certificate: Issued by R3 on April 4th 2024.
Valid for: 3 months.



104.248.113.206

104.248.113.206 **Malicious Activity!** Public Scan

URL: <https://104.248.113.206/>
Submission: On April 04 via manual (April 4th 2024, 10:31:54 am UTC) from — Scanned from

Summary

HTTP

Redirects

Links

Behaviour

Indicators

Similar

DOM

Content

API

Verdicts

Summary

This website contacted 3 IPs in 1 countries across 1 domains to perform 11 HTTP transactions. The main IP is 104.248.113.206, located in North Bergen, United States and belongs to DIGITALOCEAN-ASN, US. The main domain is 104.248.113.206. TLS certificate: Issued by R3 on April 4th 2024. Valid for: 3 months.

104.248.113.206 scanned 4 times on urlscan.io Show Scans

urlscan.io Verdict: **Potentially Malicious**

Targeting these brands: Telekom (Telecommunication)

Live information

Google Safe Browsing: No classification for 104.248.113.206 (AS14061 - DIGITALOCEAN-ASN, US)

Screenshot

Live screenshot

Full image

Page Title

Sign In

Page Statistics

11 Requests

73 % HTTPS

0 % IPv6

1 Domains

2 Subdomains

3 IPs

1 Countries

661 kB Transfer

2196 kB Size

0 Cookies

Domain & IP information

IP/ASNs

IP Detail

Domains

Domain Tree

Links

Certs

Frames

This site contains links to these domains. Also see Links.

Domain

nigga.okta.com

www.okta.com