Scattered Spider recent campaigns shows that the threat group seem to have migrated away from AS CHOOPA 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

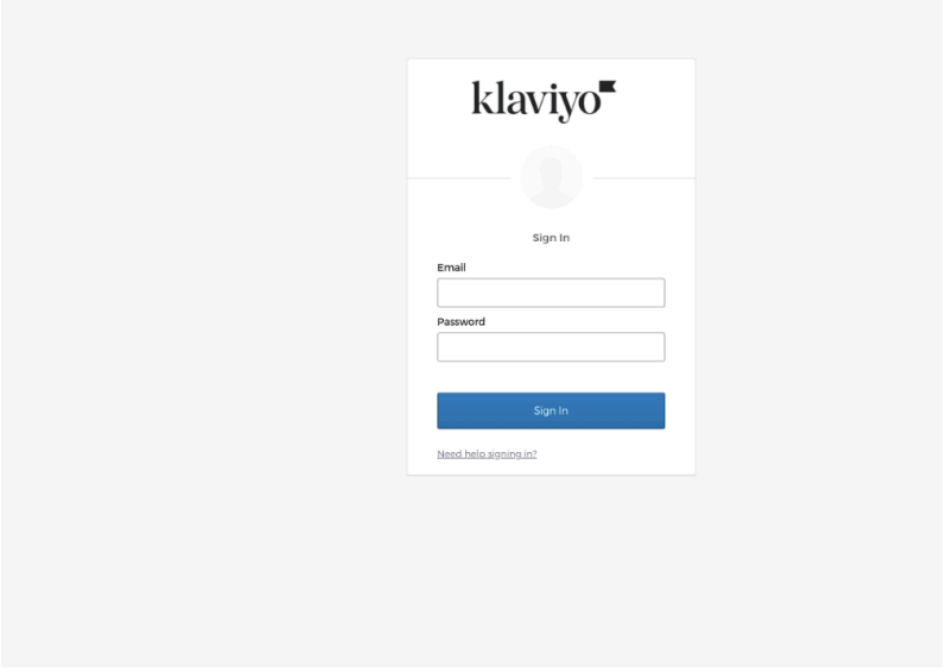
Klaviyo

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



klavlyo.com

162.33.177.163 Public Scan

Lookup | Go To | Rescan | Add Verdict | Report

URL: https://klavlyo.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 klavlyo.com.
TLS certificate: Issued by *R3* on April 15th 2024. Valid for: 3 months.

klavlyo.com scanned **21 times** on urlscan.io — Show Scans 21

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: Malicious for *klavlyo.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

Screenshot

Live screenshot | Full Image

Page Title

Sign In

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

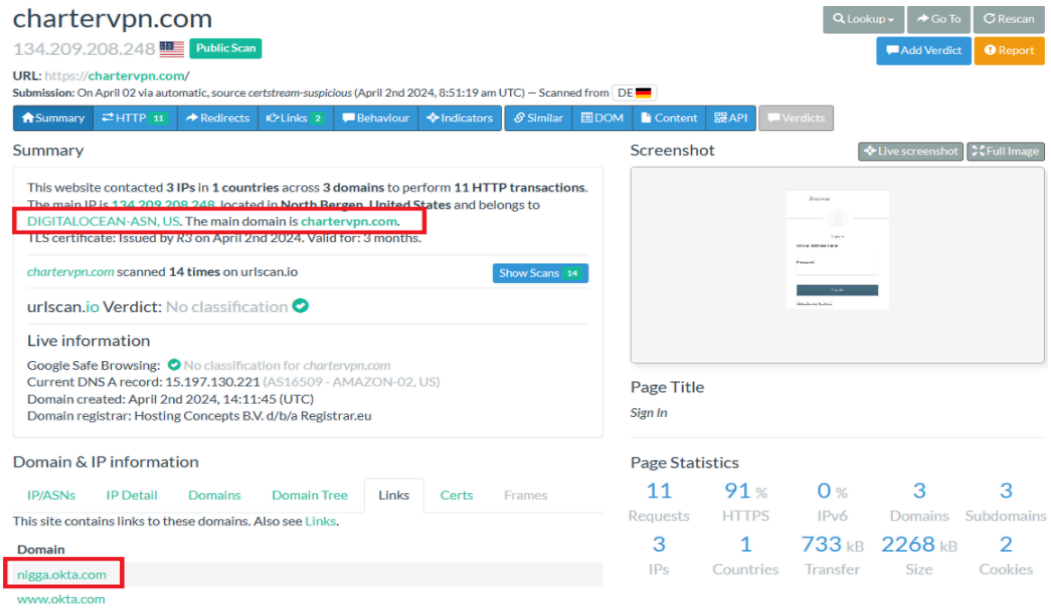
Page Statistics

Requests	HTTPS	IPv6	Domains	Subdomains
11	100 %	0 %	2	2

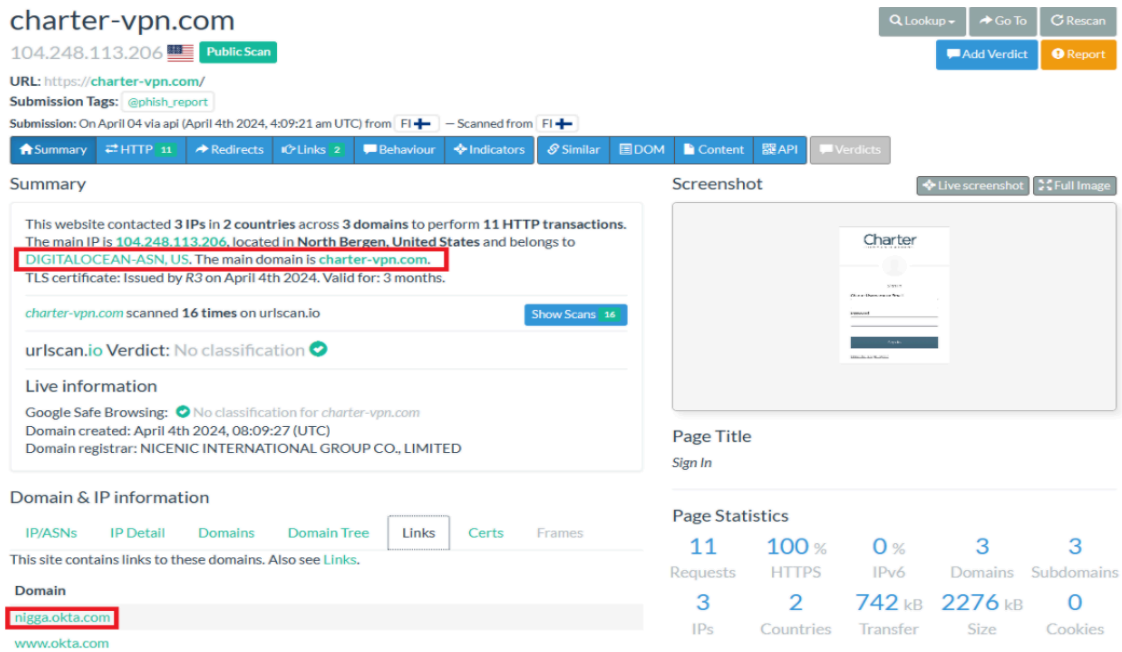
IPs	Countries	Transfer	Size	Cookies
2	1	735 kB	2270 kB	0

Charter Communications

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



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



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.