

Zooming through BlueNoroff Indicators with Validin

 validin.com/blog/zooming_through_bluenoroff_pivots/

June 20, 2025



By: Kenneth Kinion

2025-06-20

general

Pivoting through recently-reported indicators to find BlueNoroff-associated domains

In a recent blog post ([Inside the BlueNoroff Web3 macOS Intrusion Analysis](#)), the Huntress research team detailed a targeted intrusion against a Web3 (cryptocurrency) organization that they attributed with high confidence to BlueNoroff. BlueNoroff, also known as [APT38](#), is a financially motivated subgroup of North Korea's Lazarus Group. This report highlights all stages of the attack chain including phishing lures, backdoors, and post-exploitation persistence intended to stealthily compromise victims in the Web3 space.

Investigating The Lure Domain

We'll investigate the domain `support[.]us05web-zoom[.]biz`, which hosted a malicious "Zoom extension" sent to the victim over Telegram after joining a staged Zoom meeting. We'll start by looking at that domain's DNS history in Validin.



Figure. DNS history for the lure domain shows resolution to 8.8.8.8, Google's well-known public DNS resolver.

Notably, Validin shows that this domain resolved to `8.8.8.8` for most of our history except for a couple of days in late May (May 25 and 26). This is interesting because `8.8.8.8` is a very well-known public DNS resolver run by Google. Pointing domain names to benign or private IP space is a tactic that has been used by cyber criminals for a long time to attempt to hinder infra discovery.

Since this attack appears to be highly targeted, it's entirely possible that the domain resolved to a malicious, attacker-controlled IP address very briefly, possibly for as little as a few minutes.

Since `8.8.8.8` is benign and NOT attacker-controlled, we won't be able to pivot on the host connections to the domain. However, there are still many options for discovering related infrastructure in Validin from this point.

Pivoting from 8.8.8.8

Using DNS to point malicious domain names to well-known IP addresses is itself a traceable behavior that can be tracked. Using Validin, we can pivot from 8.8.8.8 to find other domain names configured with similar behaviors.

At first glance, 8.8.8.8 doesn't appear to be easily pivotable because it has 10s of thousands of domain names pointing to it with DNS A records.

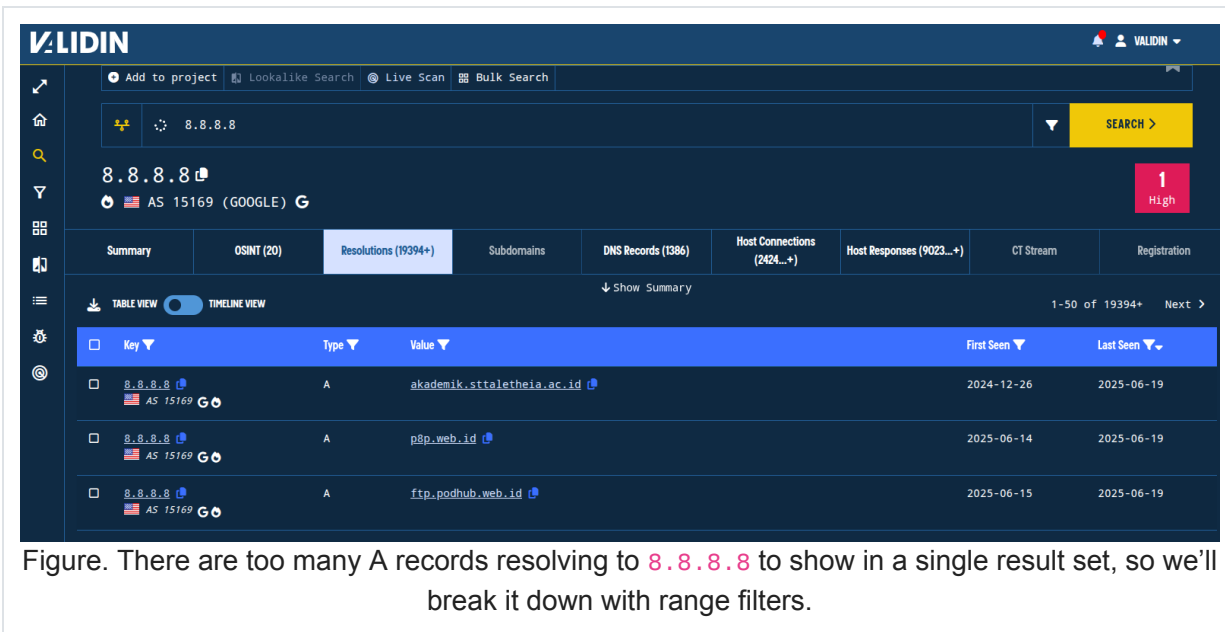


Figure. There are too many A records resolving to 8.8.8.8 to show in a single result set, so we'll break it down with range filters.

However, we can use Validin's range filter to break this down into smaller, workable chunks. We'll divide the search space in two ways:

- Time - we'll set defined start and end dates that are 1 day apart to find only resolutions that happened yesterday.
- TLD - we'll use a zone range filter to search the most likely TLDs for matches. We'll include .biz, .us, .com, and .space in our searches.

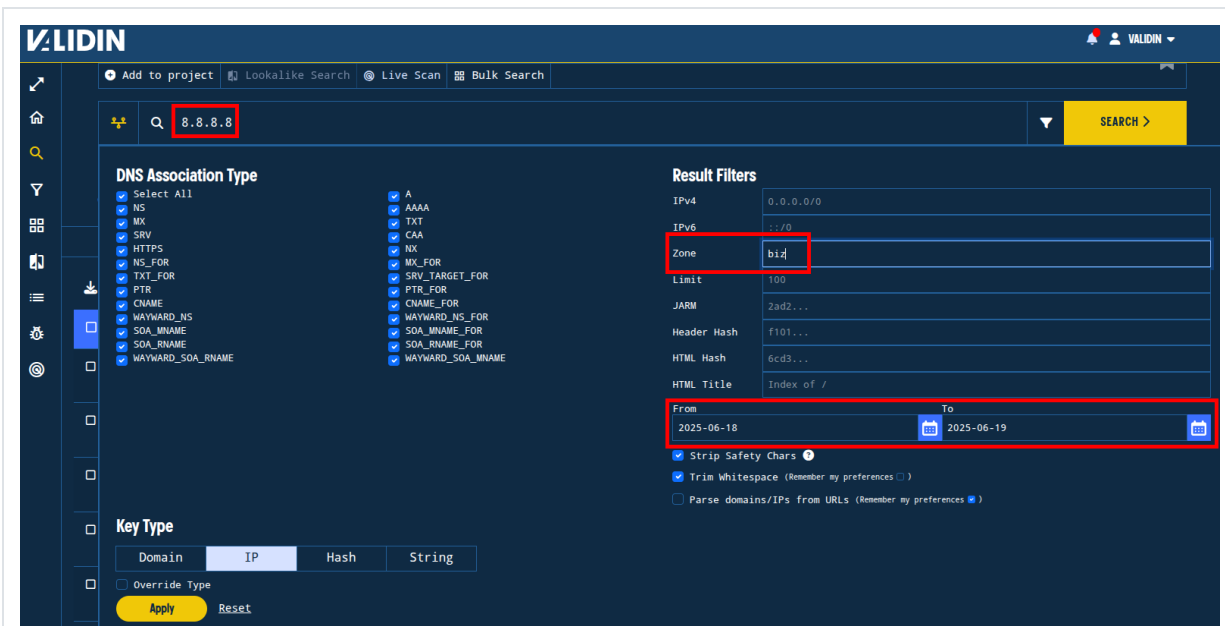


Figure. Setting zone and date range filters for the results to hone in on potentially related activity.

Applying this filtering technique to the **.biz** TLD, which is the TLD used to deliver the malicious “Zoom extension” to the victim, we are left with only 125 results. We can then apply table filters to search for keywords in this result set to identify potentially related domain names. For all of the TLDs we search, we’ll filter for “zoom”, “meet”, “web”, and “support” to look for domains that are similar to the original lure.

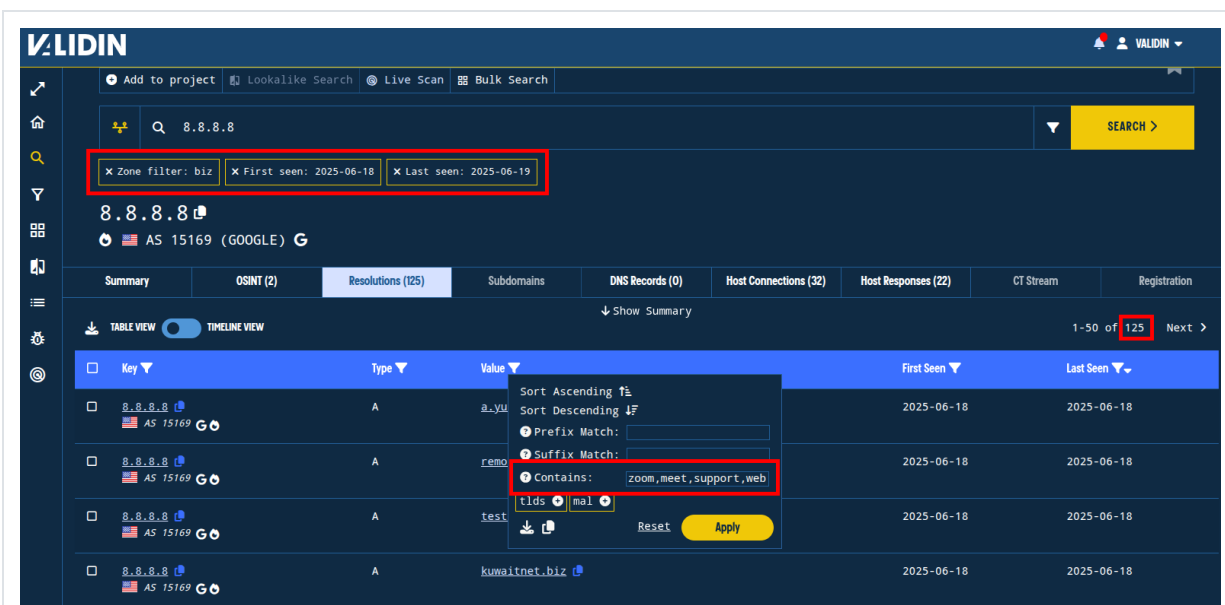


Figure. Applying table filters in Validin to look for keywords in the domain names of result sets.

In the case of **.biz**, we only find one net-new domain: **www[.]us05web-zoom[.]biz**, which is a sibling subdomain of the original lure. However, applying this process through all of our suspected TLDs, you’re able to quickly identify the following suspicious domain names among the results:

```
support[.]us05web-zoom[.]biz # The original lure domain
www[.]us05web-zoom[.]biz # Sibling domain of the original lure
zoom-sdk[.]com
hosting.us02web-zoom[.]com
api.us02web-zoom[.]com
support.us02web-zoom[.]com
www.us02web-zoom[.]com
test.ag-zoom[.]com
api-zoom[.]com
support-gmeet[.]com
www.us05web-zoom[.]space
support.us05web-zoom[.]space
officezoom[.]us
mediazoom[.]us
us05biz-zoom[.]us
us02www-zoom[.]us
web011zoom[.]us
extrazoom[.]us
us03www-zoom[.]us
zoom-sdk[.]us
```

I'll create a project called "BlueNoroff" and add all of these domains plus their subdomains, so we can track them as we pivot through the infrastructure and identify. Note that I didn't include likely false positives (popular domains with lengthy registration history) or domains that did not have similar naming patterns in the list above.

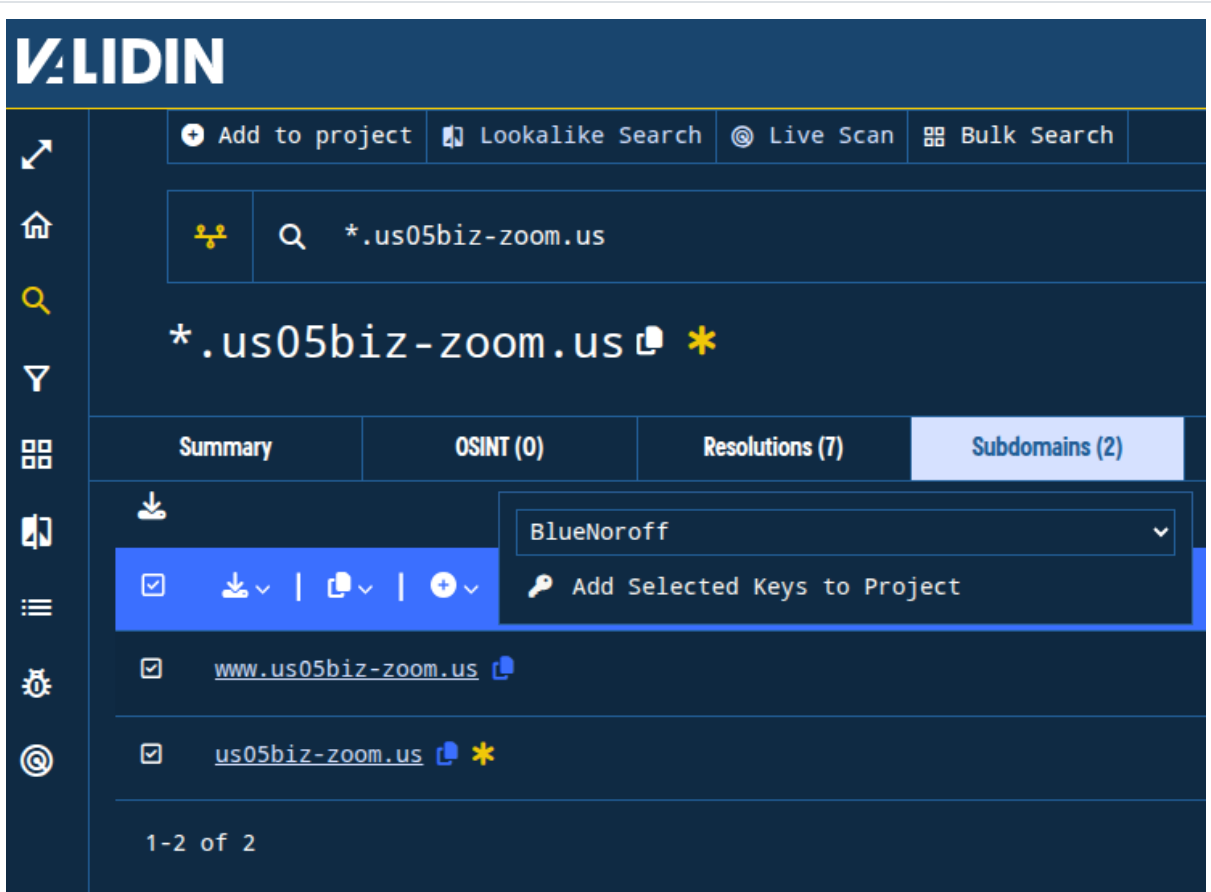
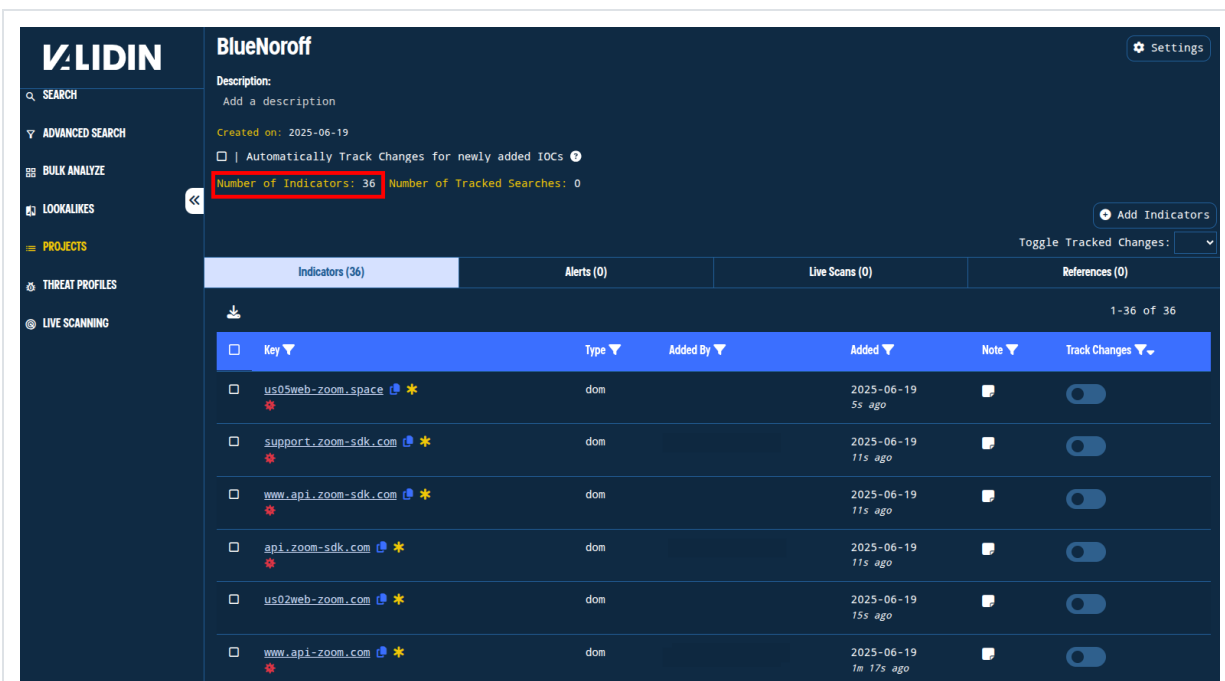


Figure. Adding subdomains for a suspected domain to a project. We repeated this process for the root domains discovered above.

After including subdomains, we have 36 total candidate domain names in our project.



DNS History Pivots

DNS History Pivots

With 36 indicators in the BlueNoroff project, we can revisit the original domain name, [support\[.\]us05web-zoom\[.\]biz](#), and pivot on other indicators directly tied to this domain (including the parent and sibling subdomains). We'll look for any indicators in those results that are already in our project from the previous pivots.

The sibling subdomain [www\[.\]us05web-zoom\[.\]biz](#) has interesting A record history: the IP address [23.254.247\[.\]53](#) has been associated with DPRK activity before, and Validin noted activity on the nearby IP [23.254.247\[.\]32](#) [on X in November 2024](#).

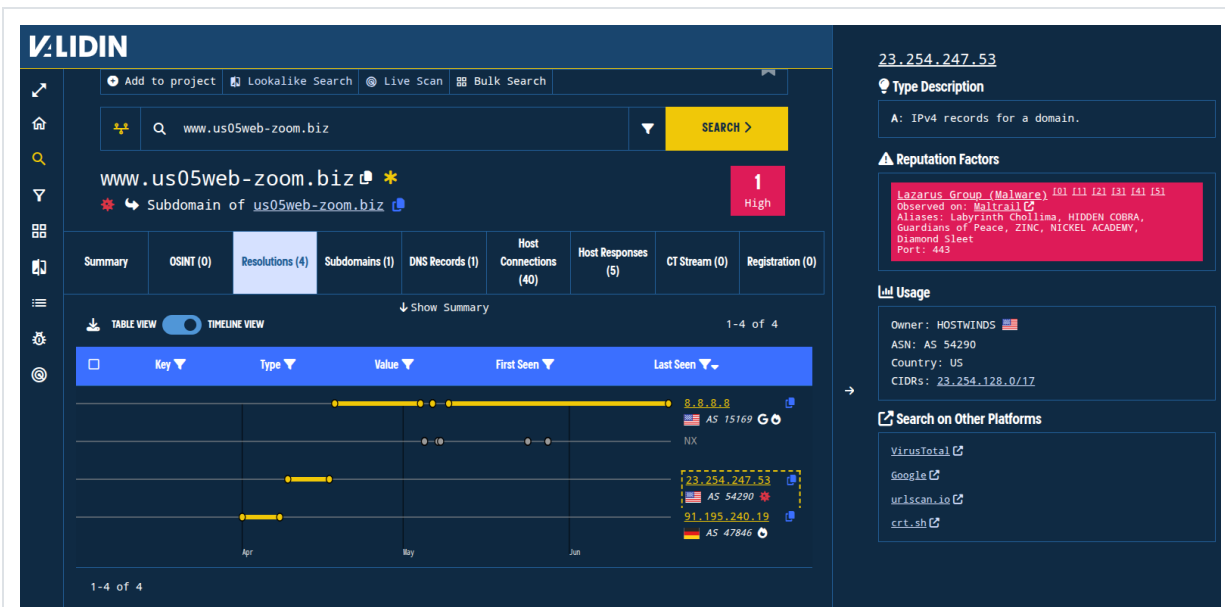


Figure. Historical DNS timeline for a BlueNoroff-associated domain name.

Pivoting on [23.254.247\[.\]53](#) yields many additional Zoom-themed domain names in recent DNS history, including many that we already found due to recently pointing to [8.8.8.8](#). Our timeline shows a surge in related activity beginning in November 2024 and continuing into June. This timing is most distinct when sorting by “First Seen,” descending.

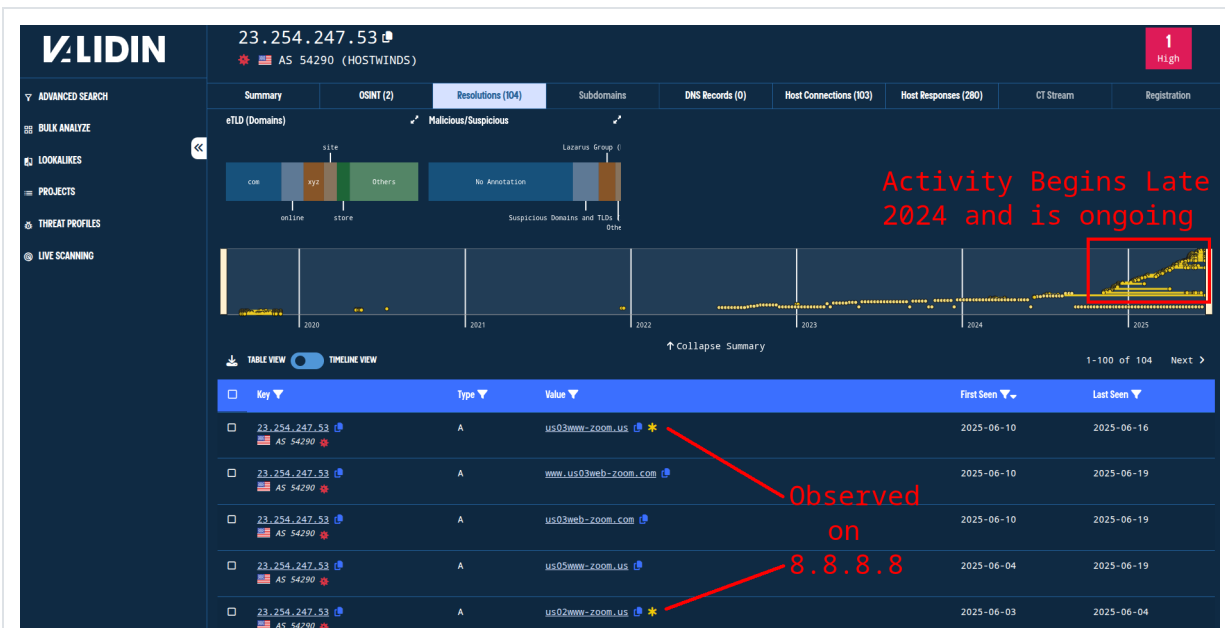


Figure. Observing connections to previous pivots and many additional Zoom and meeting themed domain names from an IP pivot.

Filtering out domains first seen before November 1, 2024, there are 70 candidate domain names. We'll add all of those domains and the IP to the BlueNoroff project, which nets 61 new domains. Of those, 53 are not yet reported as associated to DPRK threat actors by [Maltrail](#):

www[.]us03web-zoom[.]com
us03web-zoom[.]com
us05www-zoom[.]us
support[.]us06web-zoom[.]cc
www[.]us06web-zoom[.]cc
us05-zoom[.]uk
www[.]us07web-zoom[.]cc
support[.]us05web-zoom[.]ink
support[.]us05web-zoom[.]click
www[.]us05web-zoom[.]click
www[.]us05web-zoom[.]ink
support[.]us05web-zoom[.]forum
www[.]us05web-zoom[.]forum
www[.]us06web-zoom[.]xyz
www[.]us05web-zoom[.]uk
www[.]us05web-zoom[.]pro
www[.]us05web-zoom[.]cloud
www[.]us05web-zoom[.]xyz
www[.]us05web-zoom[.]site
www[.]newfromjune[.]site
www[.]us05web-zoom[.]store
www[.]venture-meeting[.]online
www[.]us05web-zoom[.]info
www[.]secure-meeting[.]cloud
www[.]secure-meeting[.]xyz
www[.]meeting-zone[.]team
www[.]online-conference[.]online
www[.]video-meeting[.]store
www[.]online-conference[.]store
www[.]meeting-hub[.]team
www[.]online-conference[.]pro
www[.]meet-client[.]xyz
www[.]online-conference[.]site
hostmaster[.]online-conference[.]site
www[.]online-conference[.]xyz
www[.]meetuphub[.]online
www[.]video-conference[.]cloud
www[.]video-conference[.]store
www[.]video-conference[.]pro
www[.]video-conference[.]site
nexologin[.]xyz
www[.]video-conference[.]xyz
www[.]team-meets[.]store
www[.]team-meets[.]cloud
www[.]team-meets[.]xyz
www[.]team-meets[.]site
www[.]room-meeting[.]online
www[.]team-meets[.]online
support[.]online-meets[.]store
7xvc[.]meetup-room[.]online
www[.]online-meets[.]store

Host Connection Pivots

Having identified an IP address that is likely controlled by the BlueNoroff threat actor, we can use Validin's host connections to discover additional fingerprints and connections that reveal additional candidate domain names and IP addresses.

Clicking on the "Host Connections" tab, we see 103 features and connections extracted from active host crawling by Validin over many months. We recently added a feature that makes it really easy to "peek" at connections (using the APIs) to see if they're worth pivoting. We'll use this to quickly look for HTTP, certificate, and host response features that appear likely to lead to more possible BlueNoroff infrastructure.

The screenshot shows the Validin web interface. The main panel displays a table of host connections for the IP 23.254.247.53. The table has columns for Key, Type, Value, First Seen, and Last Seen. The 'Host Connections' tab is selected, showing 103 items. A red dashed box highlights the 'HOST-CERT_CN' entry with the value 'hwc-hwp-7982830'. To the right, a sidebar shows the details for this pivot, including a 'Quick Pivots (inline API query)' section with a list of 3 records: 23.254.244.248, 23.254.247.32, and 23.254.247.53. A red arrow points from the highlighted entry in the table to the quick pivot sidebar.

Key	Type	Value	First Seen	Last Seen
23.254.247.53	HOST-CERT_ISSUER	/CN=hwc-hwp-7982830	2025-06-19	2025-06-19
23.254.247.53	HOST-CERT_CN	hwc-hwp-7982830	2025-06-19	2025-06-19
23.254.247.53	HOST-CERT_DOMAIN	hwc-hwp-7982830	2025-06-19	2025-06-19
23.254.247.53	HOST-CERT_FINGERPRINT_SHA256	af5ad8bada1cc7f81c20a261b448faecd4b2be0c11d32d0b7c0732b20020de1	2025-06-19	2025-06-19
23.254.247.53	HOST-CERT_FINGERPRINT	dfeb13cf56314f77f4ecacf65cf0d9edce08318	2025-06-19	2025-06-19
23.254.247.53	HOST-CERT_NOT_AFTER	2025-10-05T12:03:43Z	2025-06-19	2025-06-19

Figure. Clicking the "quick pivot" button makes an API request to pull up to 1000 related domains and IPs so you can quickly chase down pivoting leads without changing pages or opening new tabs.

Going down the list of connections, we note some highly relevant pivots:

- RDP certificate: The domain **hwc-hwp-7982830** in an RDP certificate (port 3389) connects to two other previously-reported DPRK-associated IP addresses: **23.254.244[.]248** and **23.254.247[.]32**
- HTTP Certificate: A certificate with the SHA1 fingerprint **38eaff53184ebca9046c2f10161c664ceb10d0c1** also connects to the same two previously-reported DPRK-associated IP addresses **23.254.244[.]248** and **23.254.247[.]32** and was returned with many other drop-box and conference-themed domains

VALIDIN

ADD to project Lookalike Search Live Scan Bulk Search

38eaff53184ebca9046c2f10161c664ceb10d0c1

38eaff53184ebca9046c2f10161c664ceb10d0c1

Summary OSINT (0) Resolutions (0) Subdomains DNS Records (0) Host Connections (26) Host Responses (378) CT Stream (0) Registration

TABLE VIEW TIMELINE VIEW

↓ Show Summary 1-26 of 26

Key	Type	Value	First Seen	Last Seen
38eaff53184ebca9046c2f10161c664ceb10d0c1	CERT_FINGERPRINT-HOST 2 responses	us03www-zoom.us	2025-06-12	2025-06-14
38eaff53184ebca9046c2f10161c664ceb10d0c1	CERT_FINGERPRINT-HOST 3 responses	www.us05web-zoom.lnk	2025-05-22	2025-06-19
38eaff53184ebca9046c2f10161c664ceb10d0c1	CERT_FINGERPRINT-HOST 3 responses	www.venture-meeting.online	2025-05-20	2025-06-17
38eaff53184ebca9046c2f10161c664ceb10d0c1	CERT_FINGERPRINT-HOST 3 responses	www.videotalks.xyz	2025-05-15	2025-06-12
38eaff53184ebca9046c2f10161c664ceb10d0c1	CERT_FINGERPRINT-HOST 4 responses	support.us05web-zoom.lnk	2025-05-15	2025-06-09
38eaff53184ebca9046c2f10161c664ceb10d0c1	CERT_FINGERPRINT-HOST 2 responses	www.businesstalks.site	2025-05-13	2025-06-10
38eaff53184ebca9046c2f10161c664ceb10d0c1	CERT_FINGERPRINT-HOST 3 responses	www.conference-go.online	2025-05-11	2025-06-08
38eaff53184ebca9046c2f10161c664ceb10d0c1	CERT_FINGERPRINT-HOST 3 responses	sitemaps.drop-box.store	2025-04-25	2025-06-06

Figure. Many hosts have returned the certificate for the domain `newfromjune[.]site` over the last several months.

Additional indicators from the certificate pivots:

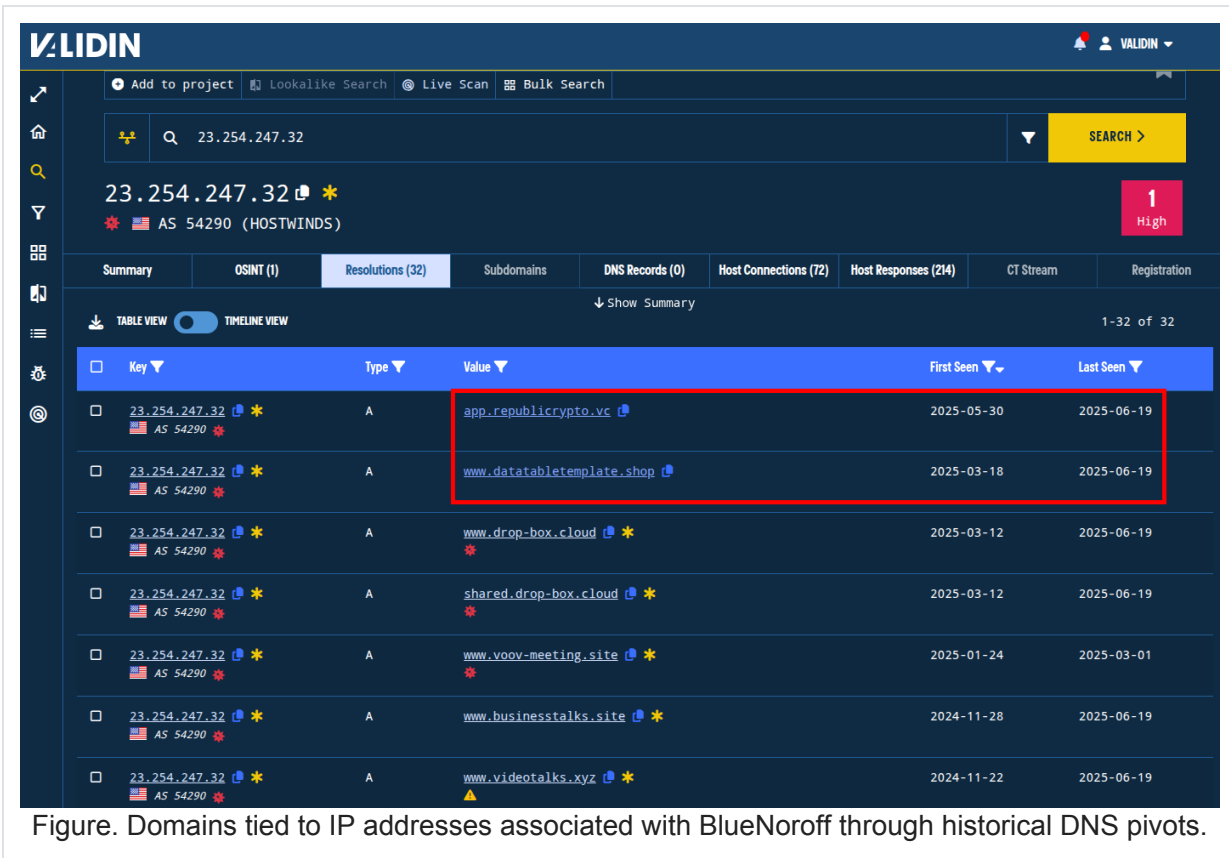
```
23[.]254[.]247[.]32
23[.]254[.]244[.]248
shared[.]drop-box[.]cloud
www[.]drop-box[.]cloud
backend[.]drop-box[.]store
api[.]drop-box[.]store
email[.]drop-box[.]store
admin[.]drop-box[.]store
demo[.]drop-box[.]store
www[.]demo[.]drop-box[.]store
app[.]drop-box[.]store
sitemaps[.]drop-box[.]store
dev[.]drop-box[.]store
www[.]drop-box[.]store
hostmaster[.]www[.]drop-box[.]store
www[.]businesstalks[.]site
em-oujuit78ytserve[.]com
em-oujuit78ytserve[.]net
www[.]videotalks[.]xyz
```

More DNS Pivots

Pivoting on the IP address `23.254.247[.]32`, which we connected through several host connection pivots and has been previously connected to DPRK threat activity, we find two additional domains:

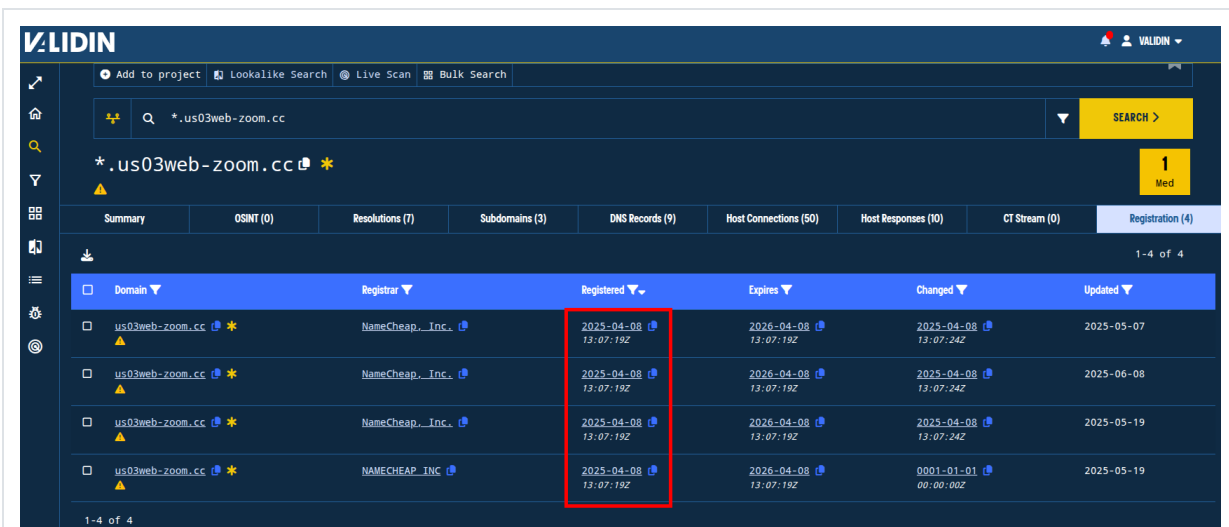
- `app.republiccrypto[.]vc`

- [www\[.\]datatabletemplate\[.\]shop](http://www[.]datatabletemplate[.]shop)

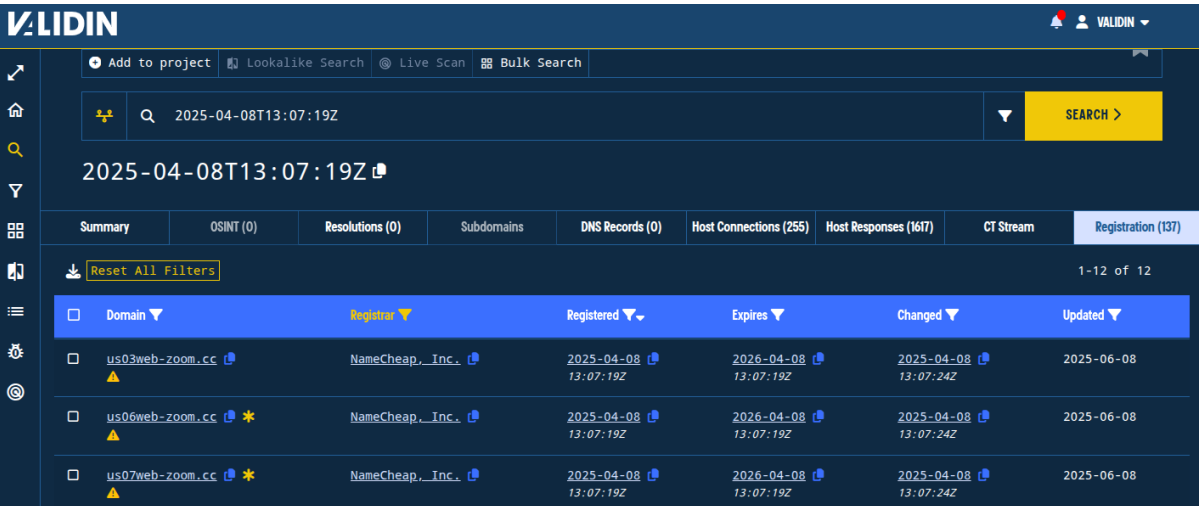


Registration Pivots

We can continue to pivot and discover domains related to this campaign through registration pivots. For example, we can use registration time pivots to discover additional domains that are very likely associated with this campaign.



Through registration pivots, we can find clusters of domains with similar naming conventions that are registered on the same registrar at the same time. This pivoting technique allows us to track domains registered in clusters and can find domains registered by the same individual or organization even without additional identifying information like name or email address.



The screenshot shows the Validin web interface. At the top, there's a search bar with the query '2025-04-08T13:07:19Z' and a 'SEARCH >' button. Below the search bar, there's a table with columns: Summary, OSINT (0), Resolutions (0), Subdomains, DNS Records (0), Host Connections (255), Host Responses (1617), CT Stream, and Registration (137). The 'Registration' tab is selected. The table shows three rows of domain data:

Domain	Registrar	Registered	Expires	Changed	Updated
us03web-zoom.cc	NameCheap, Inc.	2025-04-08 13:07:19Z	2026-04-08 13:07:19Z	2025-04-08 13:07:24Z	2025-06-08
us06web-zoom.cc	NameCheap, Inc.	2025-04-08 13:07:19Z	2026-04-08 13:07:19Z	2025-04-08 13:07:24Z	2025-06-08
us07web-zoom.cc	NameCheap, Inc.	2025-04-08 13:07:19Z	2026-04-08 13:07:19Z	2025-04-08 13:07:24Z	2025-06-08

Figure. Pivoting on WHOIS registration time in Validin reveals additional related domain names.

Conclusion

Through repeating the pivoting and validation process with the DNS, host connection, and registration pivots described above, we can find nearly 200 domains, with hundreds of subdomains, from the single starting domain that are likely related to the BlueNoroff “fake Zoom extension” campaign. Additionally, we’ve identified features that can be used to proactively track this threat. This capability provides advance notification for anyone concerned about this threat.

Ready to elevate your threat hunting, threat attribution, and incident response efforts? Whether you’re an individual analyst or part of a larger enterprise team, Validin offers solutions that meet your needs. Individual users can [create a free account and self-upgrade](#) to access more advanced features and data.

Part of a team? Contact us today to explore our enterprise options and discover how Validin can power your organizations with powerful tools and unparalleled data. Let Validin help you work smarter, faster, and more effectively in the fight against cyber threats.

Indicators

BlueNoroff-associated E2LDs:

us03web-zoom[.]cc
us06web-zoom[.]cc
us07web-zoom[.]cc
us-playground[.]vc
republiccrypto[.]vc
app-center[.]download
mzweb3[.]fund
video-conference[.]cloud
secure-meeting[.]cloud
us05web-zoom[.]cloud
online-meets[.]cloud
team-meets[.]cloud
deliverypost[.]cloud
drop-box[.]cloud
us05web-zoom[.]space
meetuphub[.]online
online-conference[.]online
venture-meeting[.]online
room-meeting[.]online
bizmeeting[.]online
meetup-room[.]online
conference-go[.]online
online-meets[.]online
team-meets[.]online
web-meet[.]online
bizmeet[.]online
meet-client[.]online
online-conference[.]store
video-conference[.]store
video-meeting[.]store
us05web-zoom[.]store
online-meets[.]store
team-meets[.]store
drop-box[.]store
online-conference[.]site
video-conference[.]site
newfromjune[.]site
us05web-zoom[.]site
businessstalks[.]site
online-meets[.]site
team-meets[.]site
downloadcenter[.]website
hanagroup[.]live
bizmeeting[.]org
bizmeet[.]org
us05web-zoom[.]click
us05web-zoom[.]link
re7[.]network
str8fire-team[.]network
us05-zoom[.]uk
us05web-zoom[.]uk
playgroundvc[.]capital

playgroundventures[.]capital
meeting-hub[.]team
mediaprime[.]team
meeting-zone[.]team
support-google[.]co[.]im
rxamia[.]com
xn--rxamia[.]com
synternetlab[.]com
capitalviabtc[.]com
twosigma-vc[.]com
doc-send[.]com
doc-bridge[.]com
em-oujuit78ytserve[.]com
zm-meeting[.]com
zoom-sdk[.]com
zmwebsdk[.]com
hartmanmcapital[.]com
vipocapital[.]com
picwe-team[.]com
us02web-zoom[.]com
us03web-zoom[.]com
api-zoom[.]com
jp-zoom[.]com
web01zoom[.]com
twosigmacap[.]com
dunamuventures[.]com
globiscapitals[.]com
calystiabusiness[.]com
fronterixbusiness[.]com
bizwebmeet[.]com
support-gmeet[.]com
zoom-support[.]com
daiwa-v[.]com
us05web-zoom[.]forum
support-google[.]co[.]in
mythicaigames[.]foundation
mythicalgames[.]foundation
superstatefund[.]co
globiscapital[.]co
bizmeeting[.]video
rwa-team[.]video
webzoom[.]video
hanagroup[.]video
webmeet[.]video
onlinemeet[.]video
openfort[.]video
us05web-zoom[.]info
web3fund[.]io
baiduweb[.]pro
online-conference[.]pro
video-conference[.]pro
us05web-zoom[.]pro

online-meets[.]pro
onlinemeet[.]pro
bizmeet[.]pro
communicationhub[.]vip
webmeet[.]vip
newfromjune[.]shop
datatabletemplate[.]shop
usweb01[.]us
usweb02[.]us
webus02[.]us
usweb005[.]us
ukweb05[.]us
webus05[.]us
ukweb06[.]us
ukweb07[.]us
webus07[.]us
ukweb08[.]us
usweb08[.]us
webus08[.]us
usweb09[.]us
webus09[.]us
us001web[.]us
uk03web[.]us
us004web[.]us
sg05web[.]us
hk05web[.]us
su05web[.]us
uk06web[.]us
uk07web[.]us
zoomhub[.]us
communicationhub[.]us
web3fund[.]us
webmeetoffice[.]us
support-google[.]us
zoom-tech[.]us
webmeetapi[.]us
zoom-sdk[.]us
zoomsdk[.]us
web001-zoom[.]us
usweb-zoom[.]us
ae-zoom[.]us
pre-zoom[.]us
cn-zoom[.]us
en-zoom[.]us
in-zoom[.]us
cr-zoom[.]us
er-zoom[.]us
as-zoom[.]us
business-zoom[.]us
support-zoom[.]us
bu-zoom[.]us
us02www-zoom[.]us

us03www-zoom[.]us
us05www-zoom[.]us
biz-zoom[.]us
us05biz-zoom[.]us
web001zoom[.]us
web011zoom[.]us
web031zoom[.]us
web041zoom[.]us
web071zoom[.]us
web091zoom[.]us
web02zoom[.]us
web06zoom[.]us
mediazoom[.]us
extrazoom[.]us
officezoom[.]us
sidezoom[.]us
interzoom[.]us
twosigmaventures[.]us
innerteams[.]us
techevent[.]us
support-google[.]ws
em-oujuit78ytserve[.]net
saisoncapital[.]net
webmeet[.]icu
aleslosev[.]workers[.]dev
us05web-zoom[.]biz
online-conference[.]xyz
video-conference[.]xyz
secure-meeting[.]xyz
room-meeting[.]xyz
boolnetwork[.]xyz
laserdigital[.]xyz
openfort-team[.]xyz
us05web-zoom[.]xyz
us06web-zoom[.]xyz
nexologin[.]xyz
videotalks[.]xyz
team-meets[.]xyz
team-meet[.]xyz
businessmeet[.]xyz
zoom-client[.]xyz
meet-client[.]xyz

IP Addresses that have been associated with BlueNoroff-associated domains within the last 6 months:

104.168.143[.]111
147.79.103[.]251
216.107.137[.]53
23.254.164[.]232
23.254.204[.]184
23.254.244[.]248
23.254.247[.]32
23.254.247[.]53
38.110.228[.]112
38.146.28[.]252
45.42.40[.]200
45.42.40[.]208
5.230.251[.]49
5.230.252[.]157
5.230.44[.]79
5.230.54[.]23
5.230.78[.]47

HTTP Feature Hashes that were useful pivots:

```
# banner_0_hash
083ca76e08cca8d8ebd337b836c9c8fb

# body SHA1 hash
23c501daff7991f82a93d94a4f14bd68fb5f61d9

# Certificate SHA1 hash
38eaff53184ebca9046c2f10161c664ceb10d0c1

# class_0_hash (HTML template fingerprint)
a945fc4a05f84c84ecb4ec7c24458e64

# header_hash
f200fb4fc2acba3276aa
```