Lazarus APT: Techniques for Hunting Contagious Interview

validin.com/blog/inoculating_contagious_interview_with_validin/

January 16, 2025

By: Efstratios Lontzetidis

2025-01-16

general

Lazarus APT uses ClickFix social engineering to trick job seekers into executing malicious code, and Validin helps find related infrastructure and mitigate the threat.

Lazarus APT, a North Korean group, is using the ClickFix social engineering technique to trick job seekers into copying and pasting malicious code onto their devices during fake video job interviews ("Contagious Interview"). This blog post shows how to expand and pivot from threat intelligence using Validin to detect likely-related infrastructure and mitigate this threat.

Background

On December 28, 2024, a tweet by researcher @tayvano_ alerted the infosec community to a campaign using a talent recruitment theme to spread malware via ClickFix social engineering. The campaign was attributed to Lazarus APT due to similarities with Contagious Interview and domain registration patterns. This post describes how the initial alert led to a hunt for Lazarus APT ClickFix techniques using Validin to pivot from the initial indicators to identify more domains registered for the campaign.

Lazarus APT and their Latest Campaign

The Lazarus Group is a North Korean umbrella of multiple threat actor groups (i.e. Bluenoroff, Andariel, Kimsuky). Lazarus has been active since at least 2009 and is associated with the North Korean government's Reconnaissance General Bureau. They support the North Korean government through a combination of espionage, financial gain, and geopolitical disruption. Their financially motivated attacks usually target financial institutions, cryptocurrency firms, gambling platforms, and FinTech companies. Stolen funds from the APT's operations are used to fund North Korea's nuclear weapons and long-range missiles programs.

The Contagious Interview Campaign

One of the latest tracked campaigns of Lazarus, is the Contagious Interview, which started as early as December 2022 as described by PAN Unit 42, and it is about North Korean actors contacting software developers through job search platforms. They pose as a prospective employer, inviting them to participate in an online interview in which the actors attempt to convince the victims to download and install backdoor malware (BeaverTail, InvisibleFerret, CivetQ, etc).

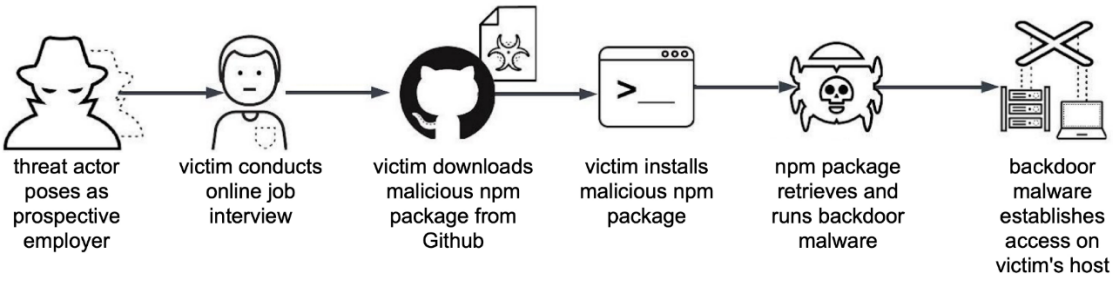


Figure 1. Simplified Chain of Events for a Variation of the Contagious Interview Campaign

The ClickFix Social Engineering Technique

One of the most hyped social engineering techniques in the last quarter of 2024, ultimately abused first by Lumma Stealer operators, was ClickFix. The ClickFix technique uses dialogue boxes containing fake error or reCAPTCHA messages to trick people into copying, pasting, and running malicious content on their own computer.

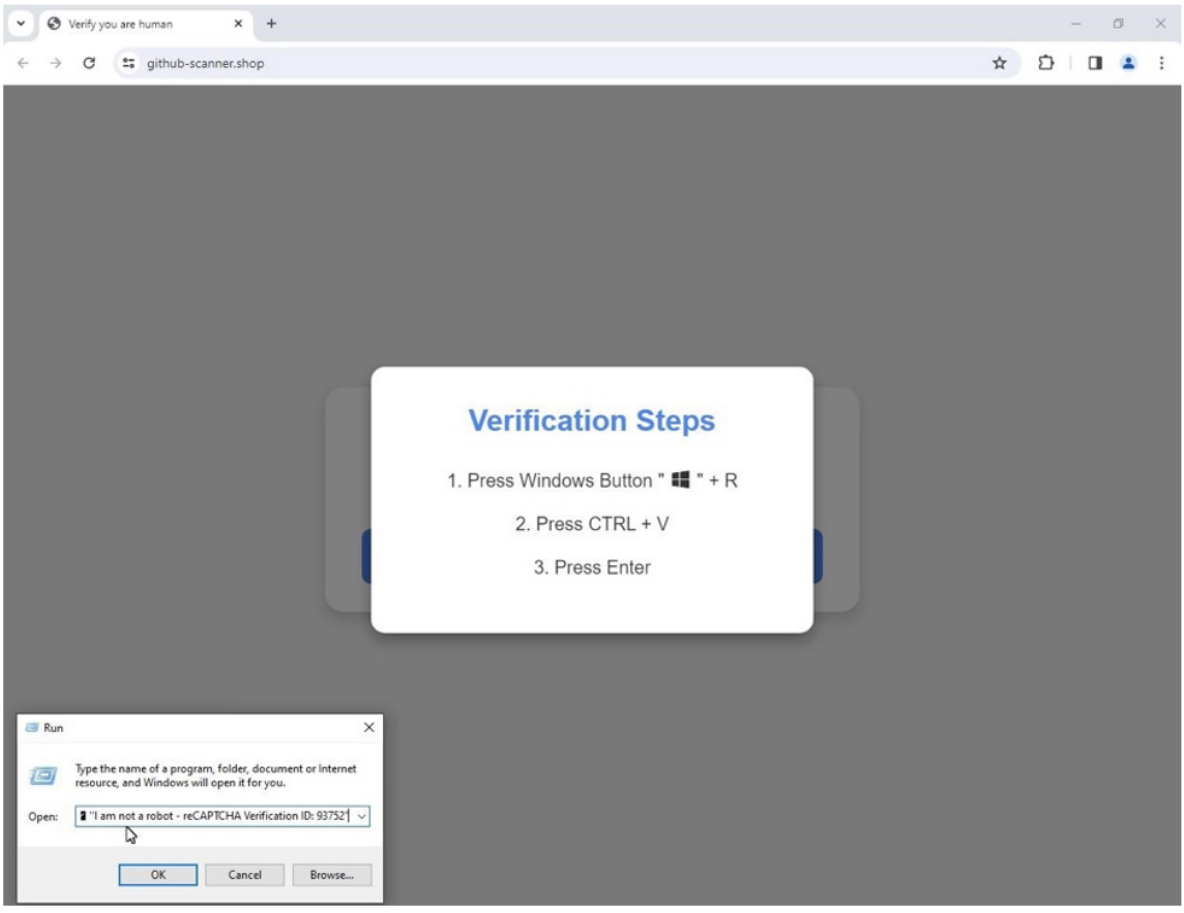


Figure 2. ClickFix style “verification steps” to execute PowerShell.

Lazarus APT’s Latest Campaign Encompassing ClickFix as part of Contagious Interview

The Lazarus group appears to have updated its social engineering tactics by incorporating ClickFix into its Contagious Interview campaign. This campaign targets job seekers with attractive pay ranges, often on platforms like LinkedIn, Telegram, and Discord. As reported first by the researcher @tayvano_, the initial contact often comes from a fake recruiter representing well-known companies, such as Kraken, MEXC, Gemini, and Meta, promoting attractive pay ranges on LinkedIn, Telegram, Discord, and other job posting sites. This approach entices victims to run malware on their devices.

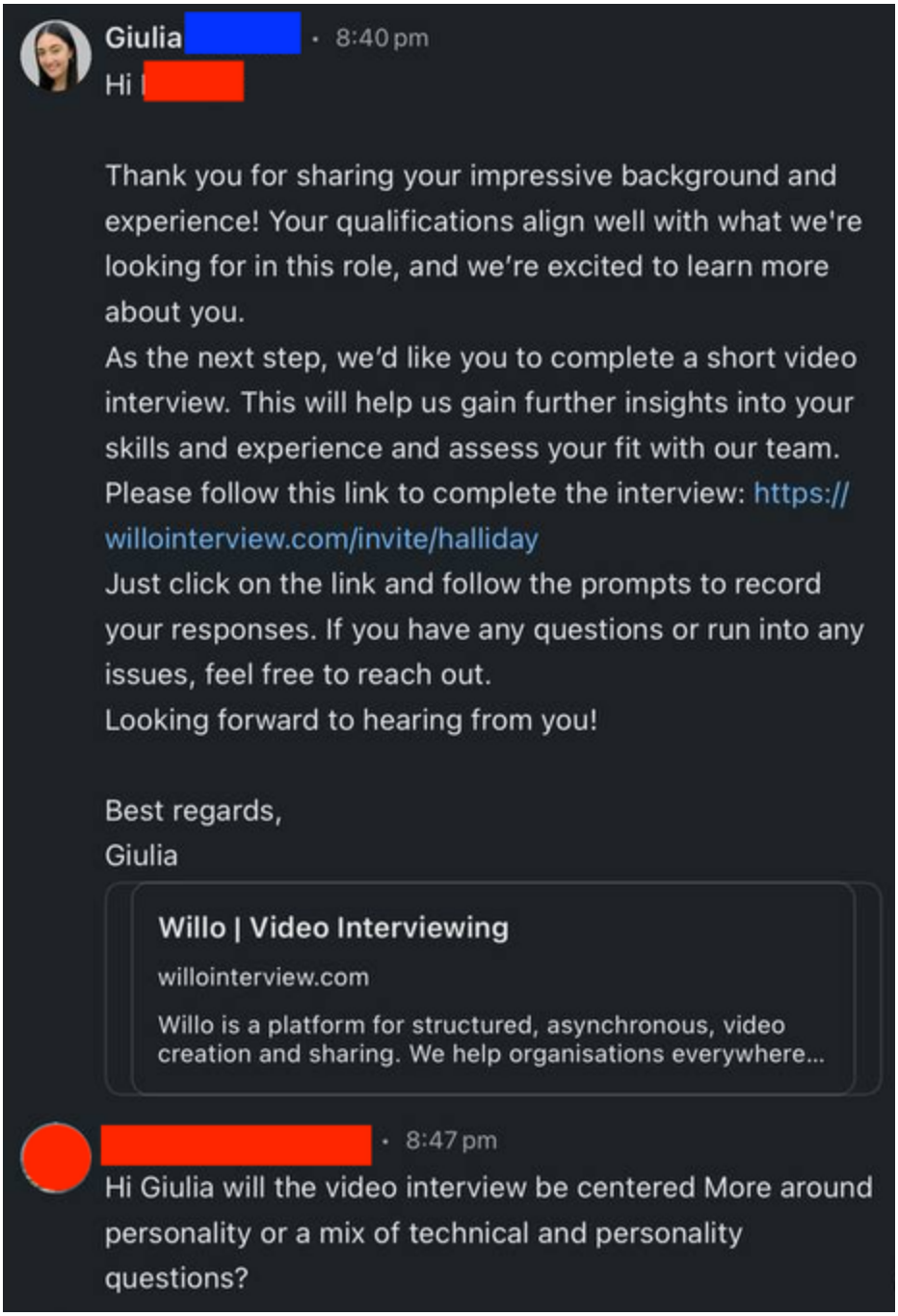


Figure 3. Sample Interaction with the Fake Recruiter

After exchanging some information, the threat actor eventually drops a link to a fake Willo website (Video Interviewing Screening Software) to continue the hiring process by answering some questions as part of the candidate's evaluation. Next, a long form of questions is presented to the candidate asking things relevant to the role.

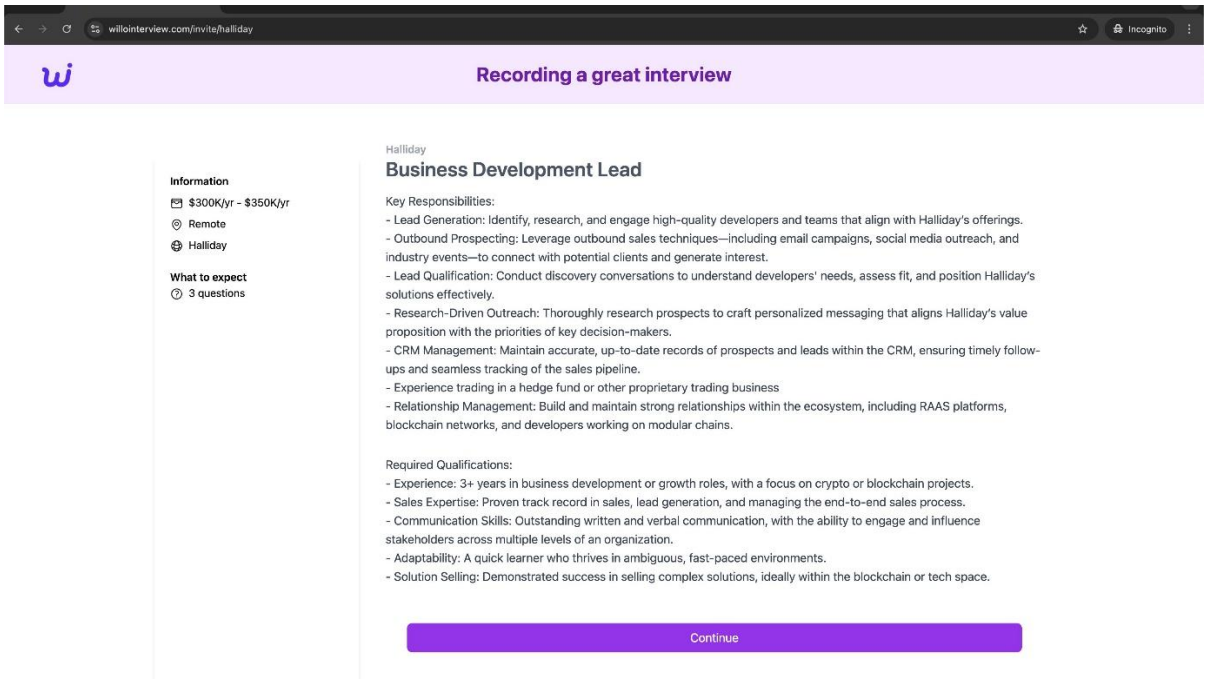


Figure 4. Sample Job Description

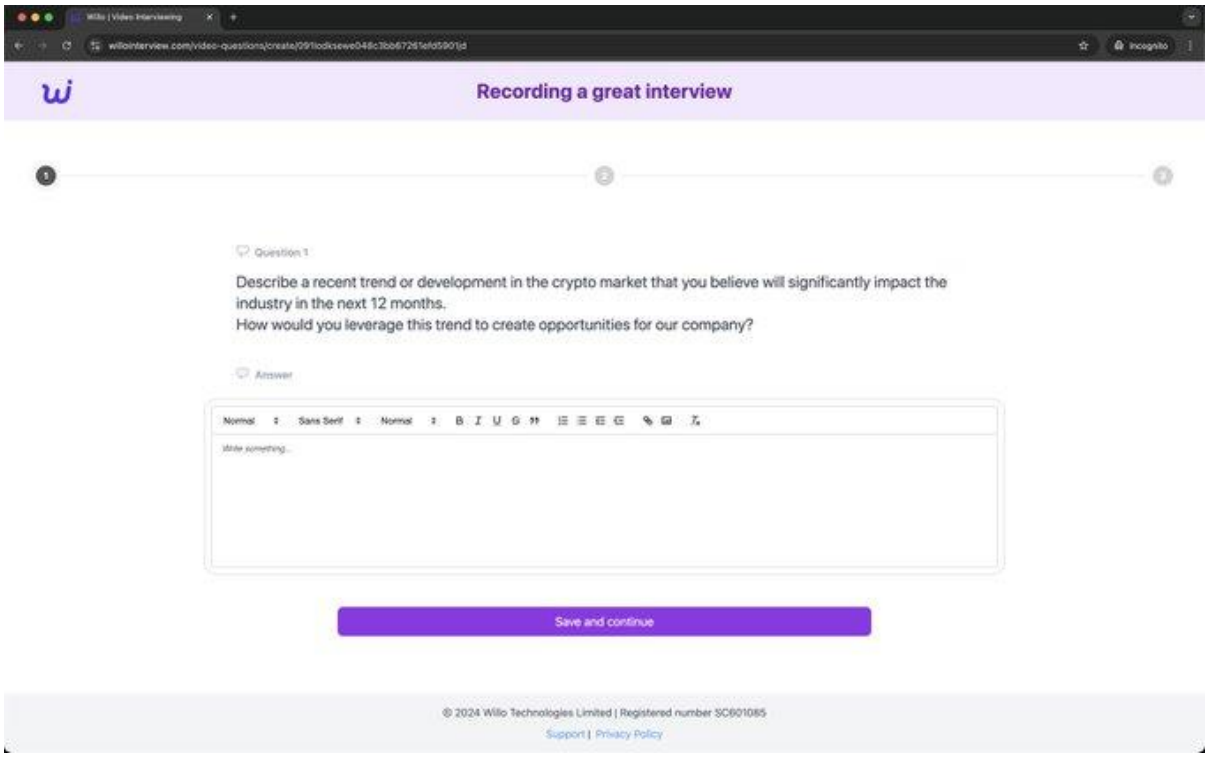


Figure 5. Sample Long Form Question

The last step is to record a video answer to the last question. By clicking the *Request Camera Access* button, a pop-up is displayed that guides the victim on how to enable access (the ClickFix technique) by attaching malicious code to be copied that installs malware on their device (payloads vary for Mac, Windows, and Linux devices).

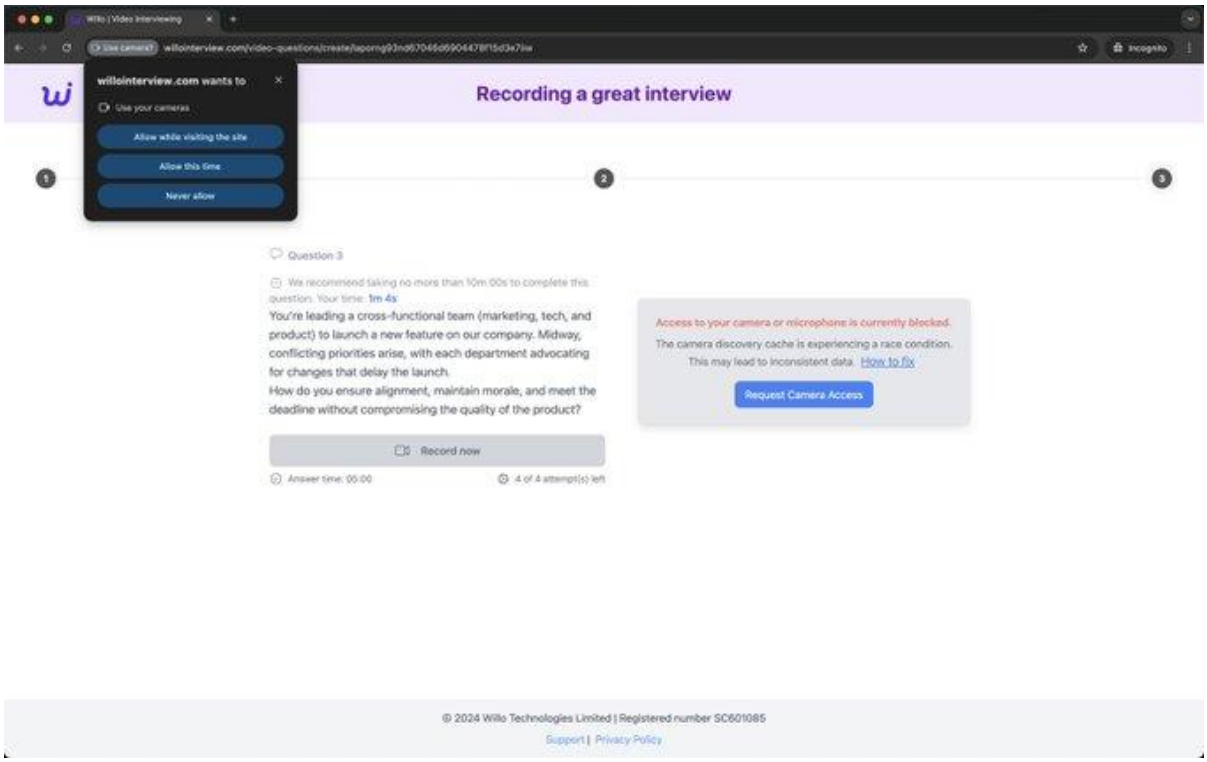


Figure 6. Requesting Access to Camera

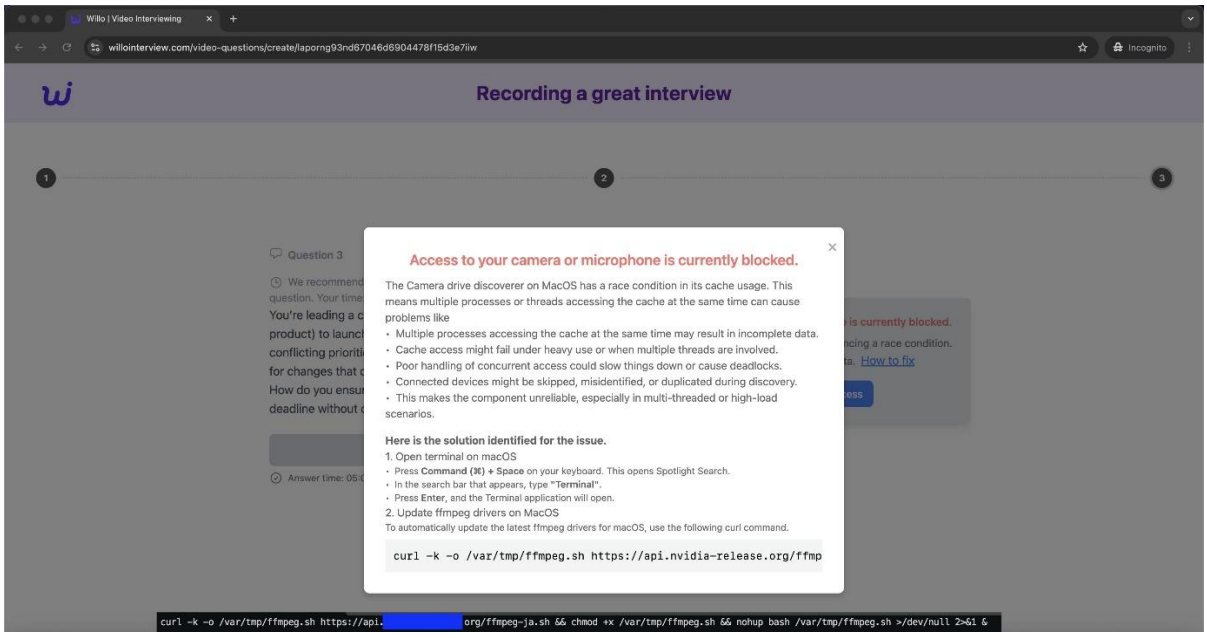


Figure 7. ClickFix Pop-up Displaying Malicious Code

Infrastructure Hunting

The objective in this report is to identify further Lazarus infrastructure that is used to deliver its payloads to potential victims. Let's create a project on Validin to collect our findings through the hunting process:

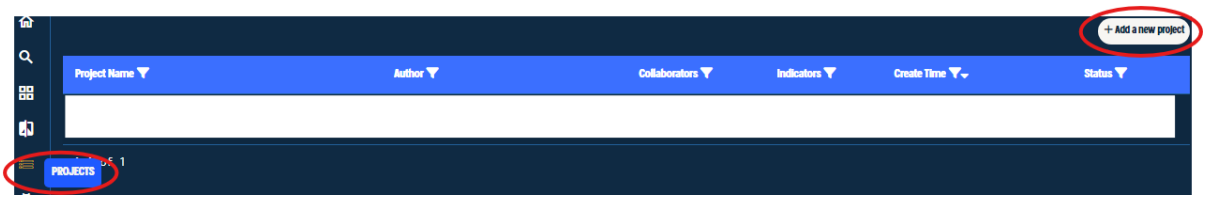


Figure 8. Project Creation Menu

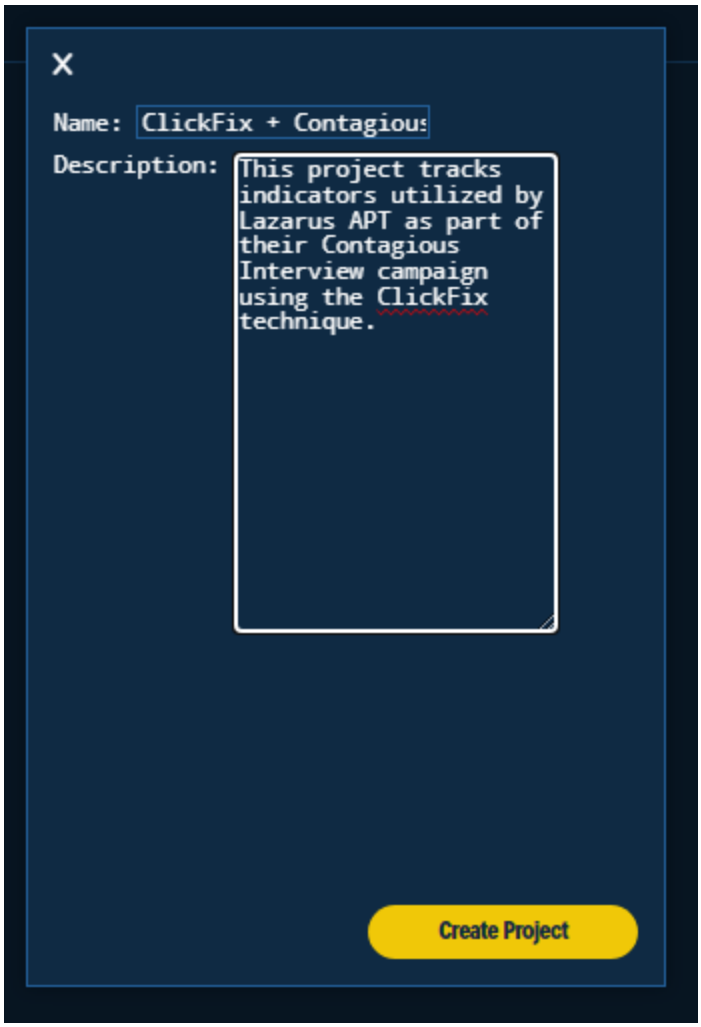


Figure 9. Project Details Menu

We'll populate it with our known indicators to be used as starting pivot points:

Figure 10. Adding Indicators to Project Menu

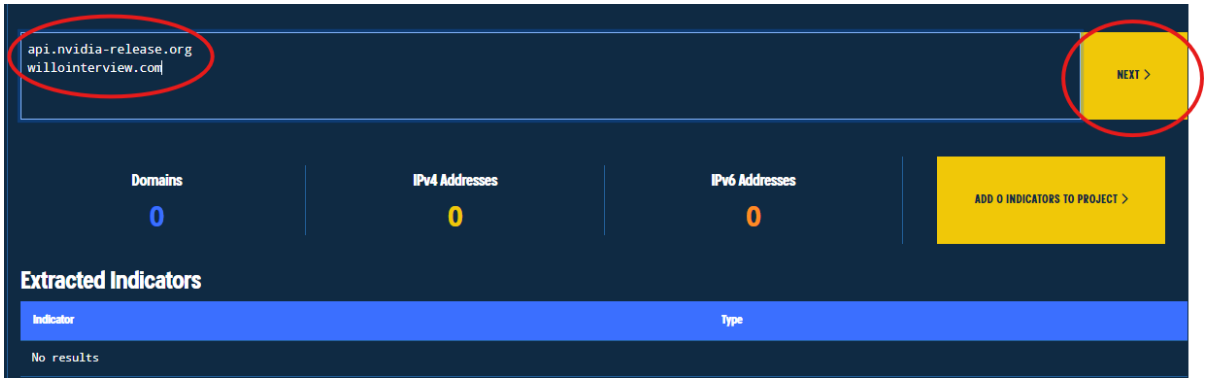


Figure 11. Adding First Indicators

Figure 12. Confirmation of Indicators Insertion

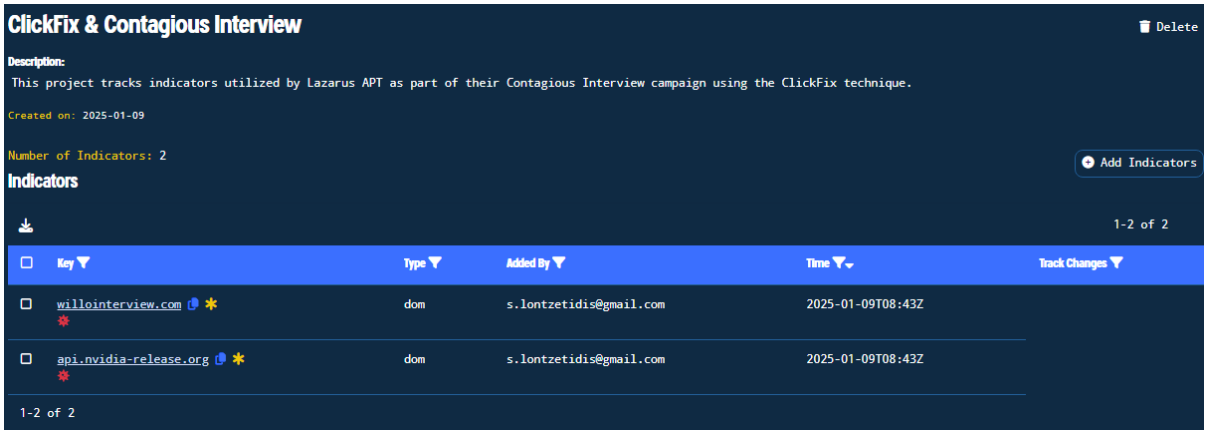


Figure 13. Final View of the Project with its Indicators

Now let's inspect the `willointerview[.]com` domain by clicking on it to see what we can extract from it to help us identify more domains serving ClickFix with this theme.

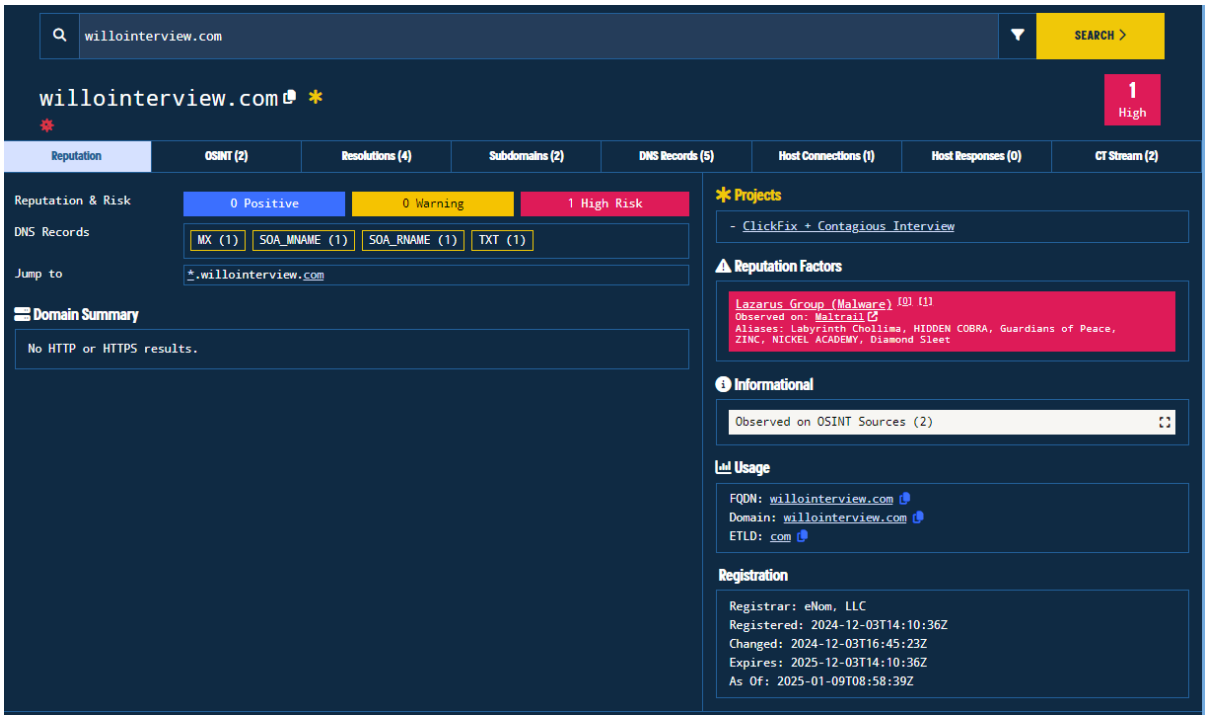


Figure 14. Overview Information of the `willointerview[.]com` Domain

From this screen (Reputation Tab), several information can be observed about this domain. For example, the Reputation Score and Factors (which flag this as associated with APT Lazarus), DNS records, FQDN, ETLD, Registration, etc. In each tab there is more detailed information. An important thing to notice is that each key/value field is a potential pivot point.

OSINT: The OSINT sources/lists where the indicator was referenced.

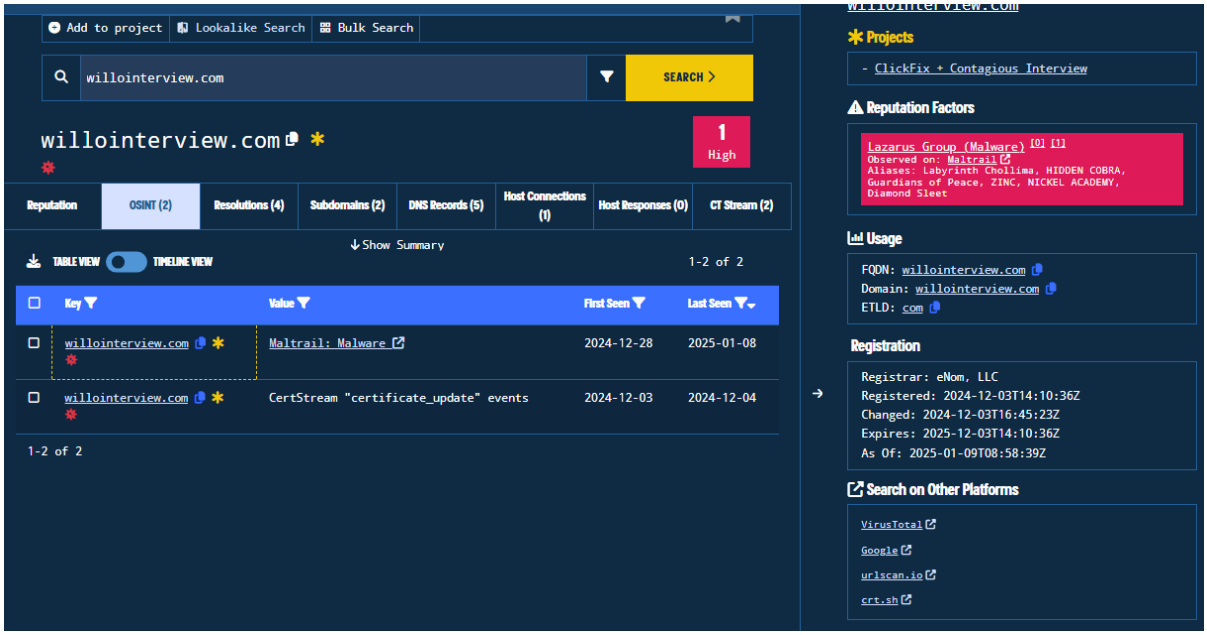


Figure 15. Osint Tab

Resolutions: Domain resolutions associated with the domain indicator. i.e. NS (Name Server), A (IPv4) resolutions. Here we can observe the IPv4 resolution which is `23.254.244[.]74`. Notice the information on the side panel that also includes information on the estimated pivot count (a really useful feature to determine if this attribute is commonly observed).

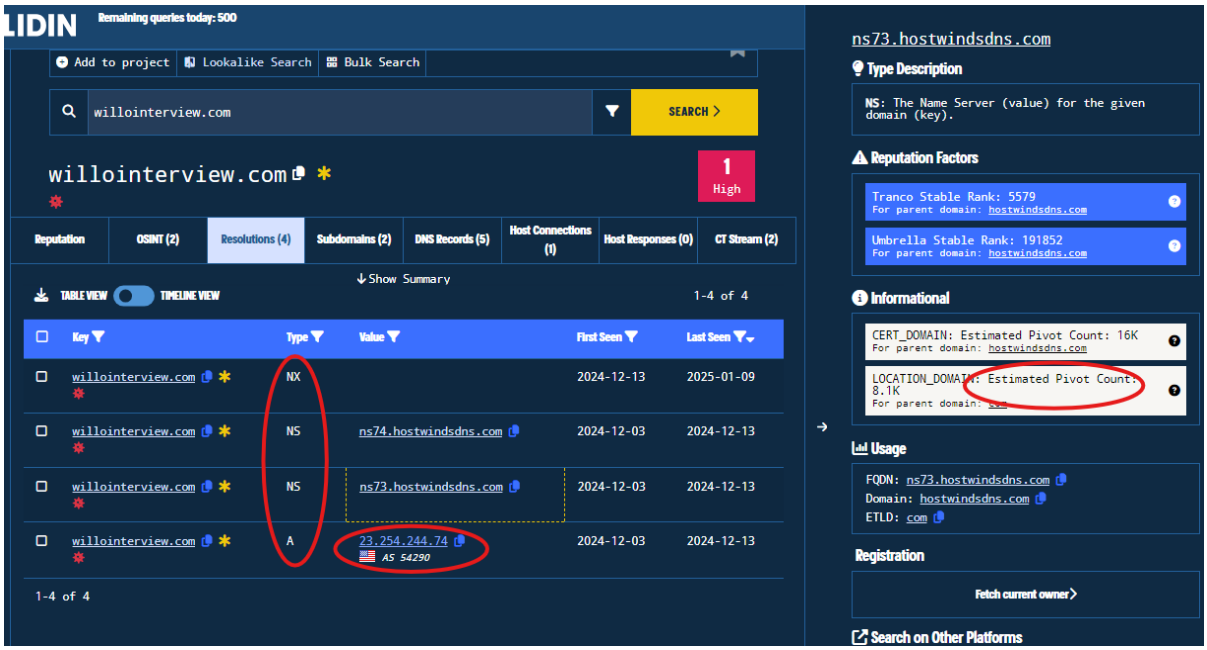


Figure 16. Resolutions Tab

Subdomains: The subdomains for the domain indicator.

Figure 17. Subdomain Tab

DNS Records: The DNS records for the associated domain indicator. Shows information like if the domain has MX (Mail eXchange), or other records like SPF that can be seen from the next figure (also a potential pivot point).

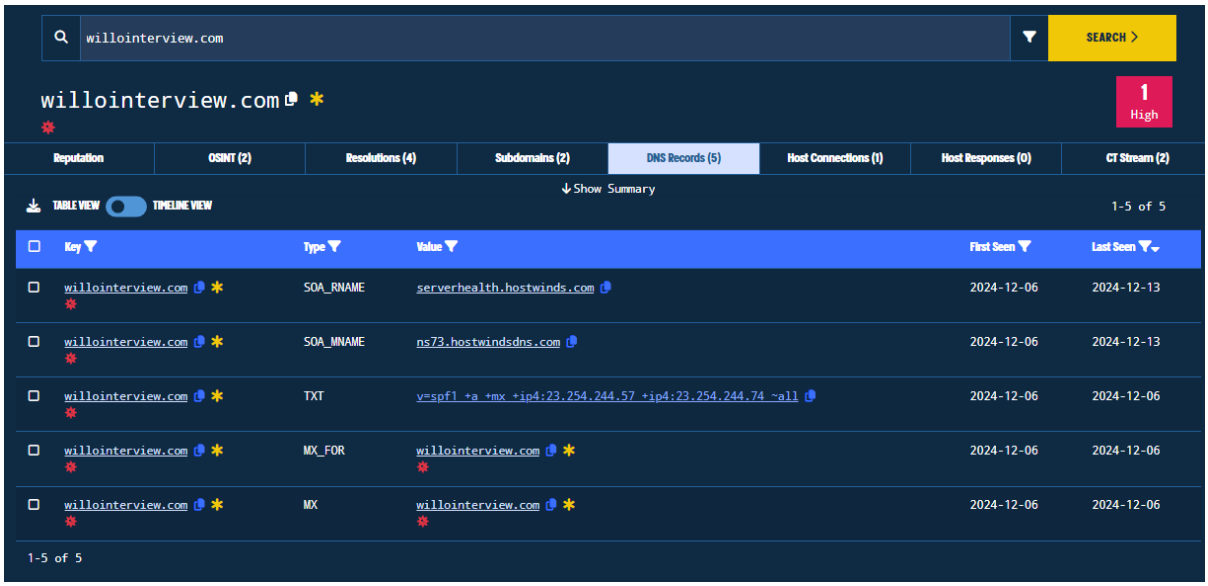


Figure 18. DNS Records Tab

Host Connections: Information regarding relationships between the investigated indicators. I.e. the following is the connection between Domain and IPv4.

Figure 19. Host Connections Tab

Host Responses: Information regarding HTTP Response Data.

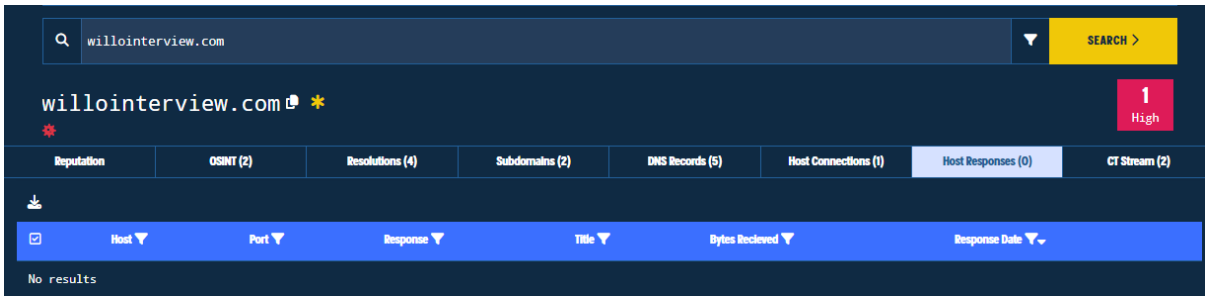


Figure 20. Host Responses Tab

CT Stream: Certificate Transparency information such as certificate fingerprints, common names and timestamps.

Figure 21. CT Stream Tab

Continuing with the hunt, by selecting the Resolutions tab and clicking on the IPv4 `23.254.244[.]74`, we pivot to the IP hosting the domain.

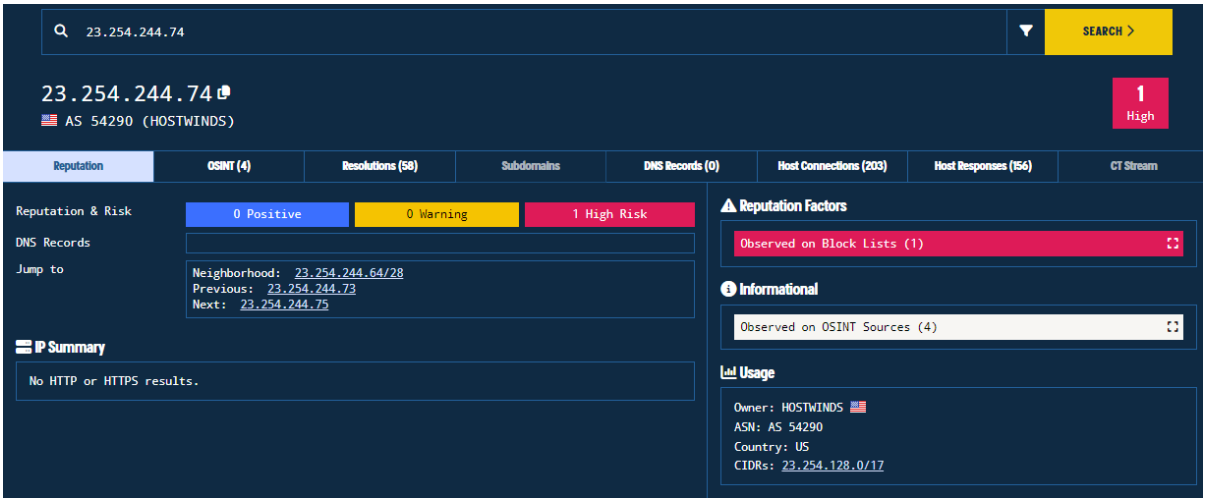


Figure 22. 23.254.244[.]73 Indicator Information

As we can see, this IP belongs to AS 54290 Hostwinds. Use of the Hostwinds ASN dedicated servers is a common tactic in Lazarus campaigns. Let's select Host Connections to see if there are any interesting and unique fingerprints.

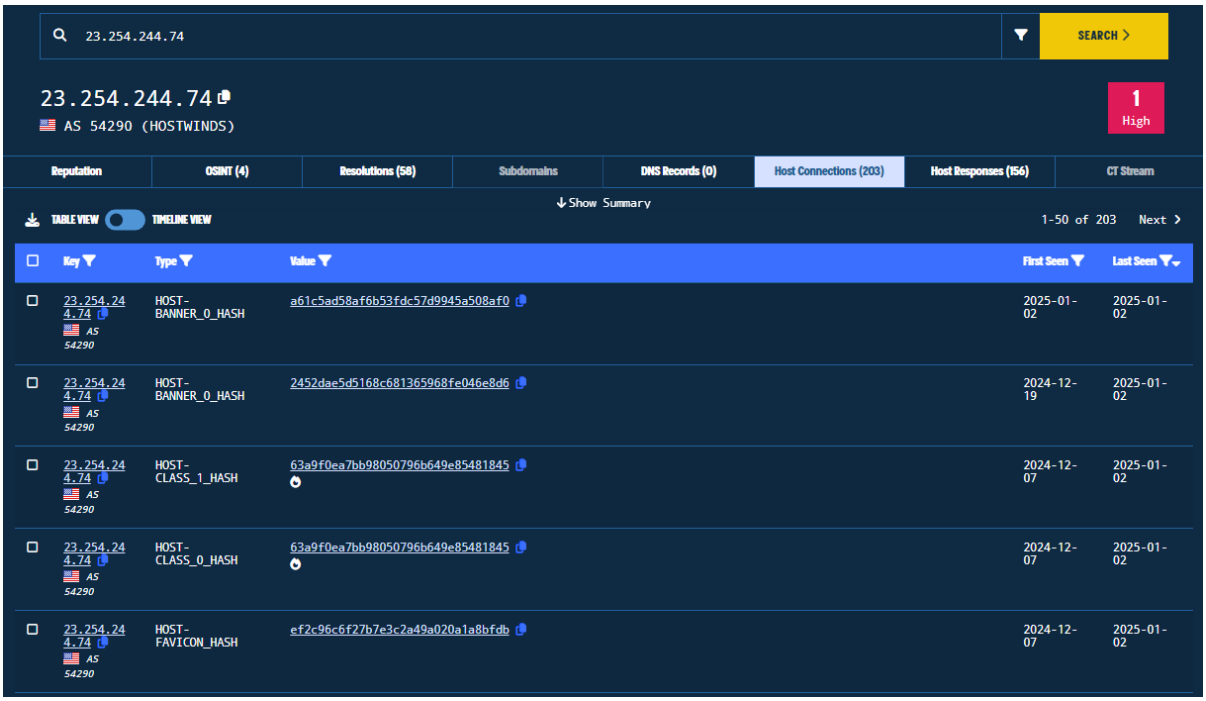


Figure 23. Host Connections Tab of the 22 23.254.244[.]73 Indicator

1st Method of Identifying Further Infrastructure: HTML Feature Pivoting

By scrolling a bit down, we can see a really unique type of host-meta header, present in the legitimate website for Willo.

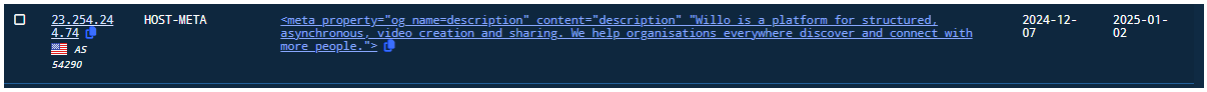


Figure 24. Willo HOST-META Header as an Interesting Pivot

By clicking on it to pivot and selecting the Host Connections tab, we observe additional domains with similar naming conventions and IPv4 addresses that share this exact host-meta header (136 total). This great pivot was first identified and reported by @500mk500.

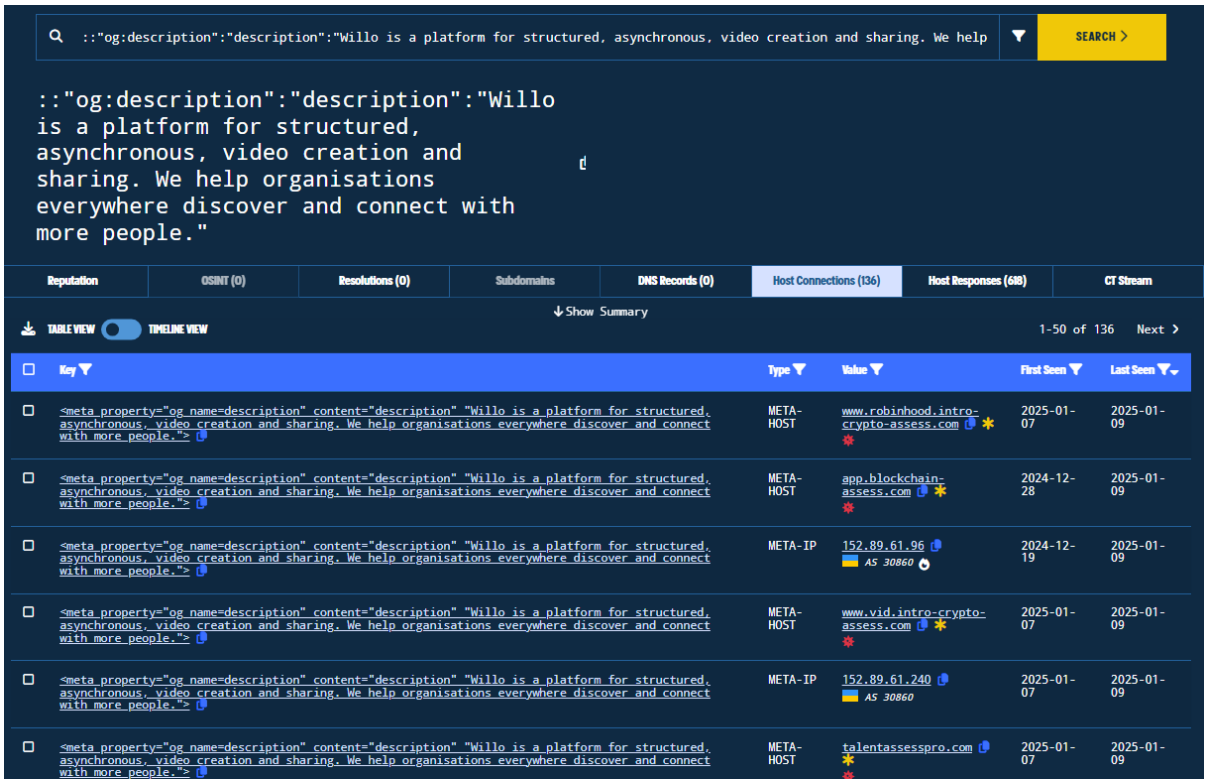


Figure 25. Host Connections Tab of the HOST-META Header

From there we can further filter the returned values to see only the domains.

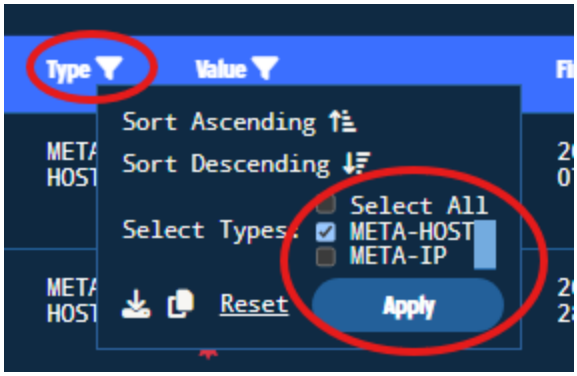


Figure 26. Type Filtering only for META-HOST

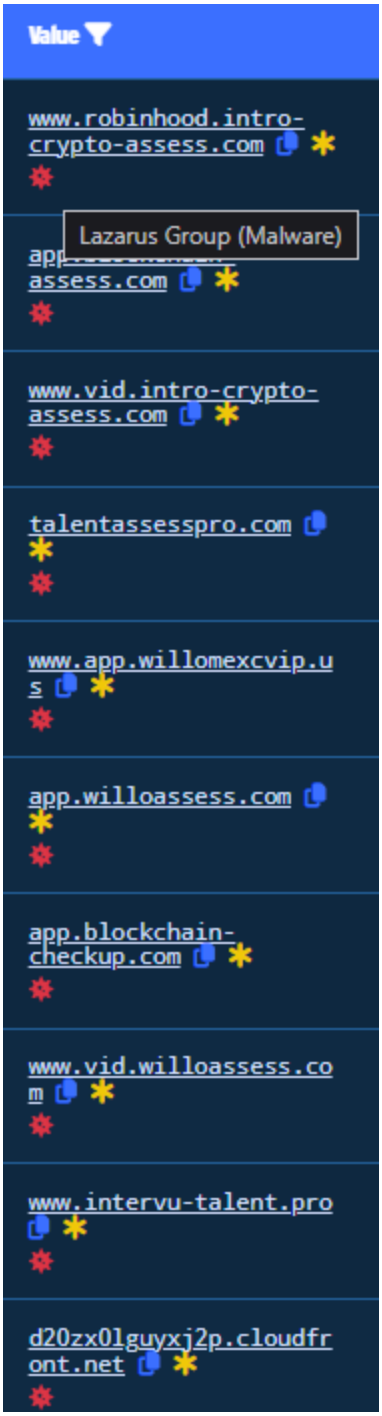


Figure 27. META-HOST Results

As we can see, there are similar domain registration patterns (already flagged as Lazarus related) containing also other keywords, such as *crypto, assess, **willo**, blockchain, interview, talent, hiring*, etc. Also, there are domains hosted on the Cloudfront CDN.

It is really important to notice here as a general principle that some pivots may contain false positives (i.e. in these results there are also legitimate domains of Willo that need to be filtered out from your project). Those are potentially related indicators and further verification is needed to be considered an Indicator of Compromise. For

example, this post from the researcher @banthisguy9349 suggests querying for this path on a suspected domain to confirm abuse: `/video-questions/create/531fbaedf67046d6904478f15d3e7142`

For example, for the following domain: `www.vid.willoassess[.]com`* *the following page was displayed by combining it with the aforementioned URI that confirmed it was part of the campaign:

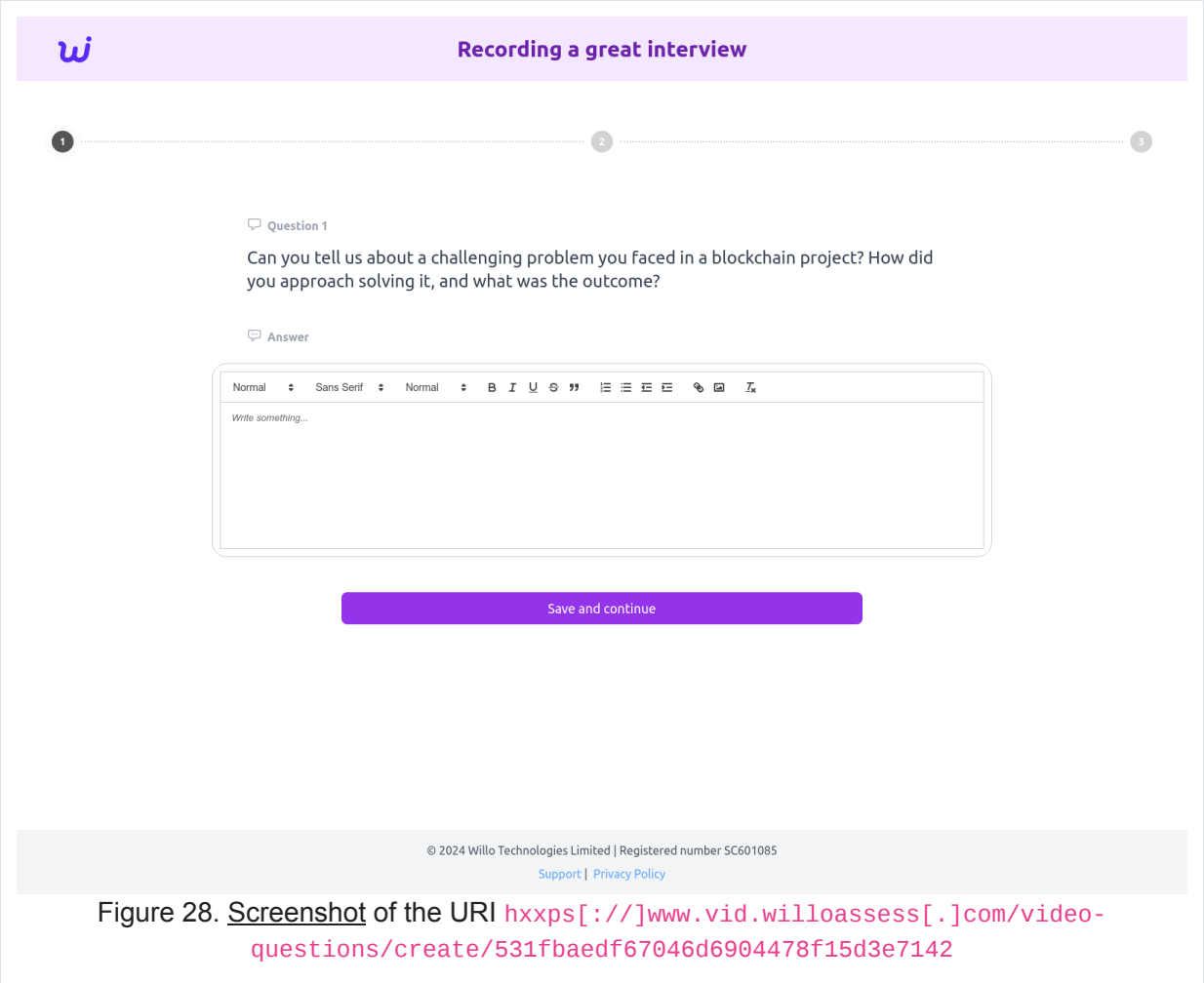


Figure 28. Screenshot of the URI `hxxps[://]www.vid.willoassess[.]com/video-questions/create/531fbaedf67046d6904478f15d3e7142`

Next, we can manually select the domains of interest (excluding false positives as mentioned), and add them to our project.

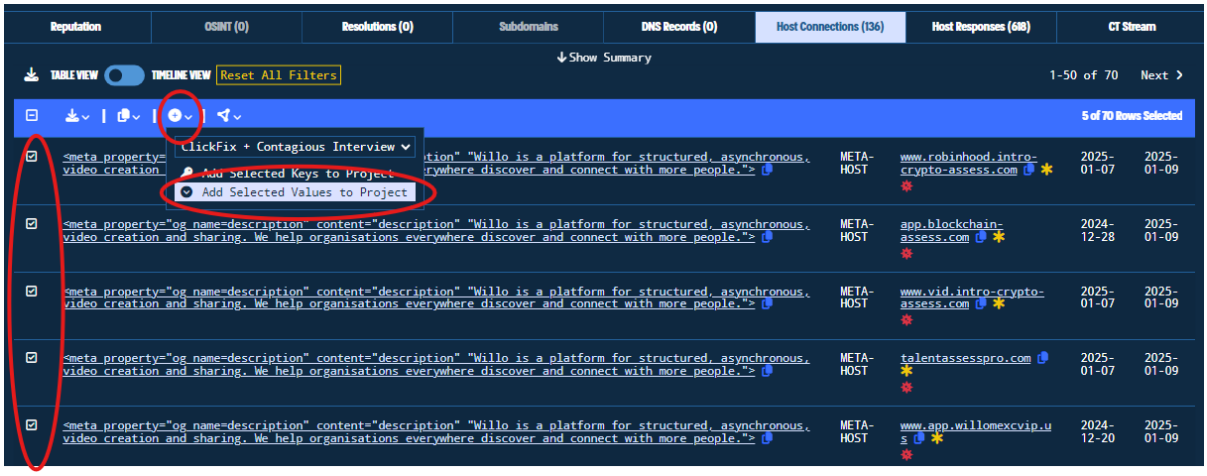


Figure 29. Adding the Domain Indicators to the Project Menu

Another really useful feature is the Timeline View, where we can observe the First & Last Seen timestamps of the domains containing this meta-host value. The following figure depicts the difference between Willo's legitimate domain and the malicious domains. It can also be observed that the malicious domains generated activity beginning no later than mid-December 2024.

Figure 30. Timeline View of the HOST-META Relationship with the Domains

Next, we can return to the Table View and filter again for META-IP, to observe other hosting patterns.

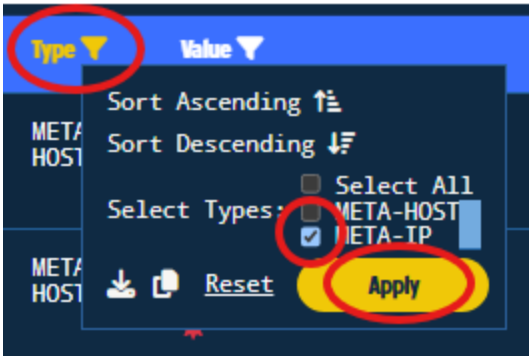


Figure 31. Type Filtering only for META-IP

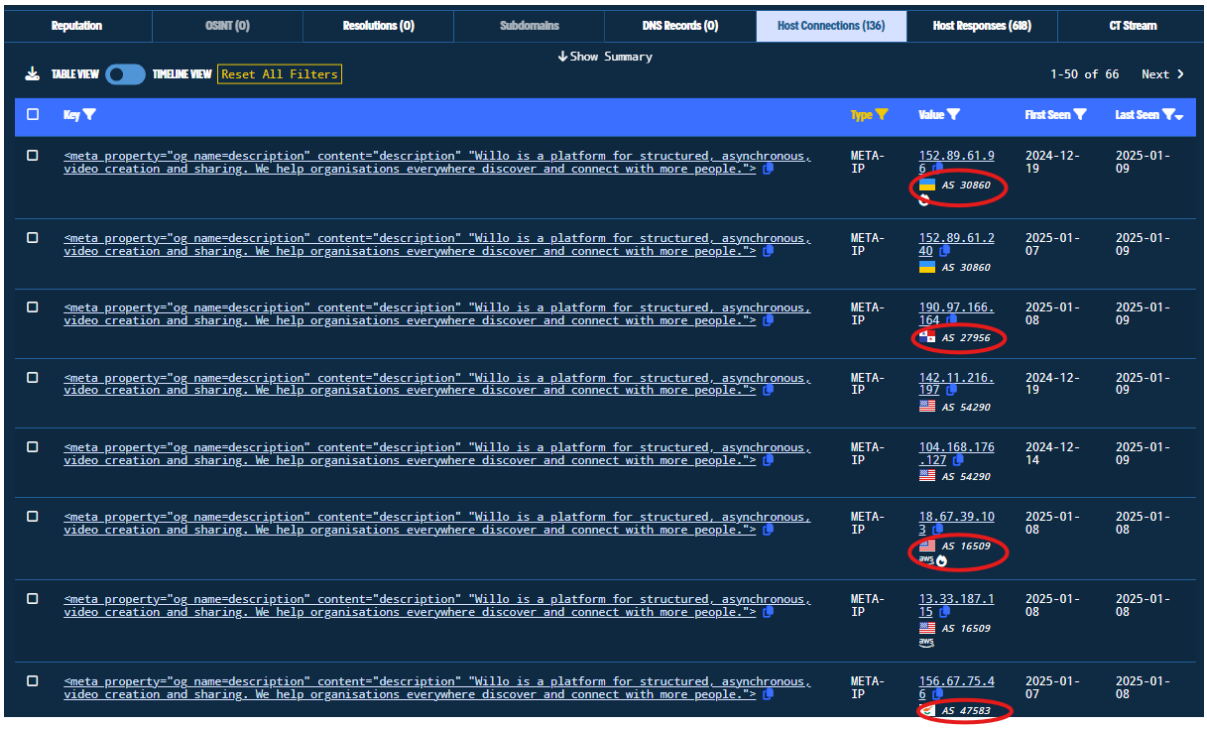


Figure 32. META-IP Results

Additional Autonomous Systems are represented, such as AS 30860, AS 27956, AS 16509, AS47583, and AS 54290. Those can provide insights into hosting preferences for Lazarus, or possibly different threat actor clusters. We can view these statistics by clicking on Show Summary:

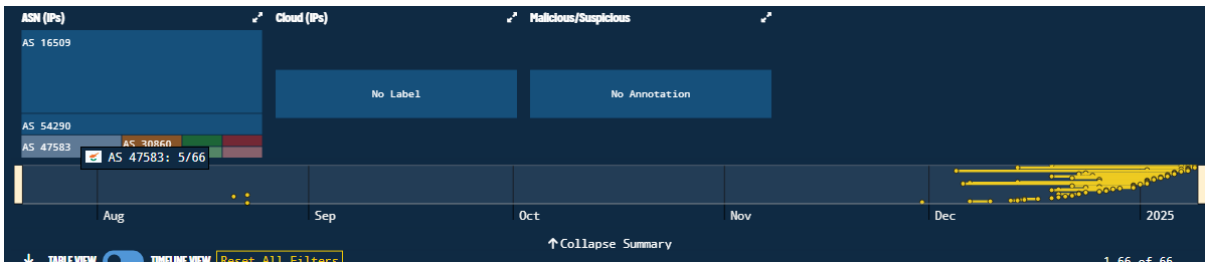


Figure 33. Summary of ASNs

2nd Method of Identifying Further Infrastructure: Bulk Search

Now that we have seen other IPv4 addresses hosting such malicious domains, we would like to search those IPv4 addresses to see if they host other domains with similar naming conventions that bypassed the security community's radars. We will manually select the IPv4 addresses of interest (excluding Amazon ASN and ASNs with high estimated pivots for resource efficiency), and add them to Bulk Search.

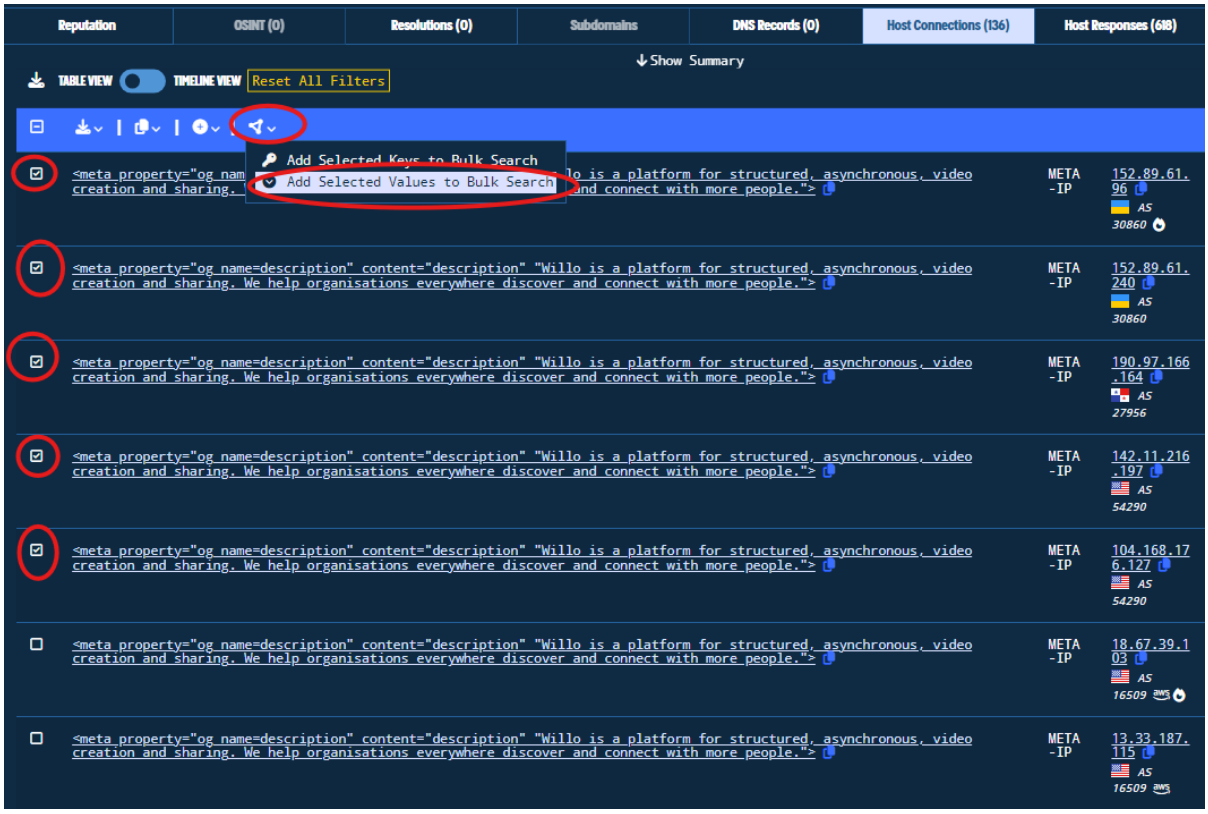


Figure 34. Selection of IPv4 Addresses and Insertion to Bulk Search

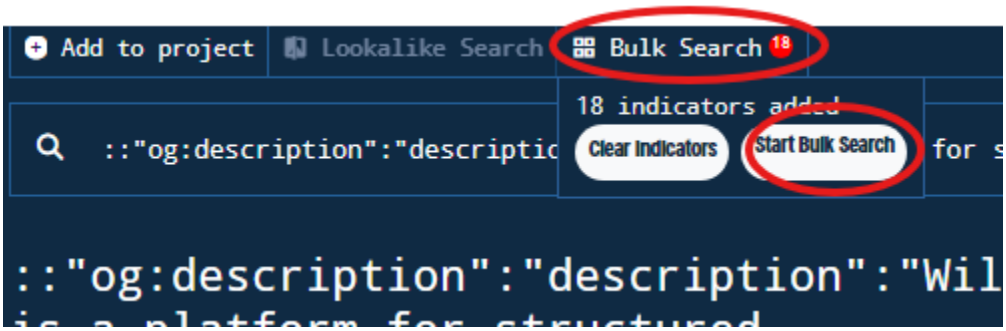


Figure 35. Adding indicators to Bulk Search

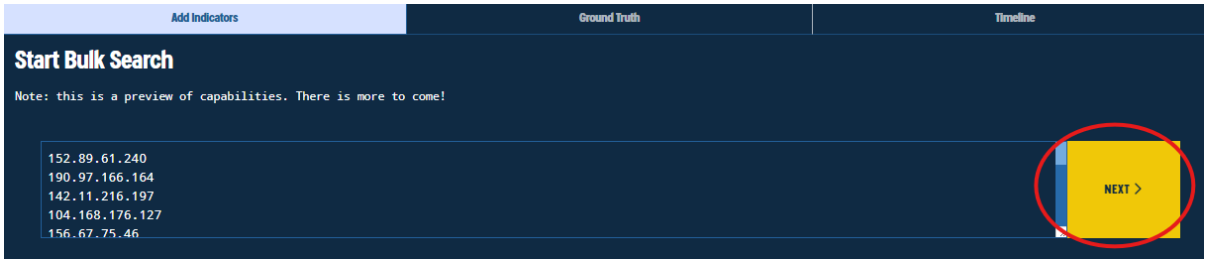


Figure 36. Submitting the Indicators to Bulk Search for initial enrichment

Now we will set the settings for the Bulk Search. We want to see only A records associations (IPv4 to DNS), and since we know the timeline of the activity pretty much, we will only consider timestamps of December.

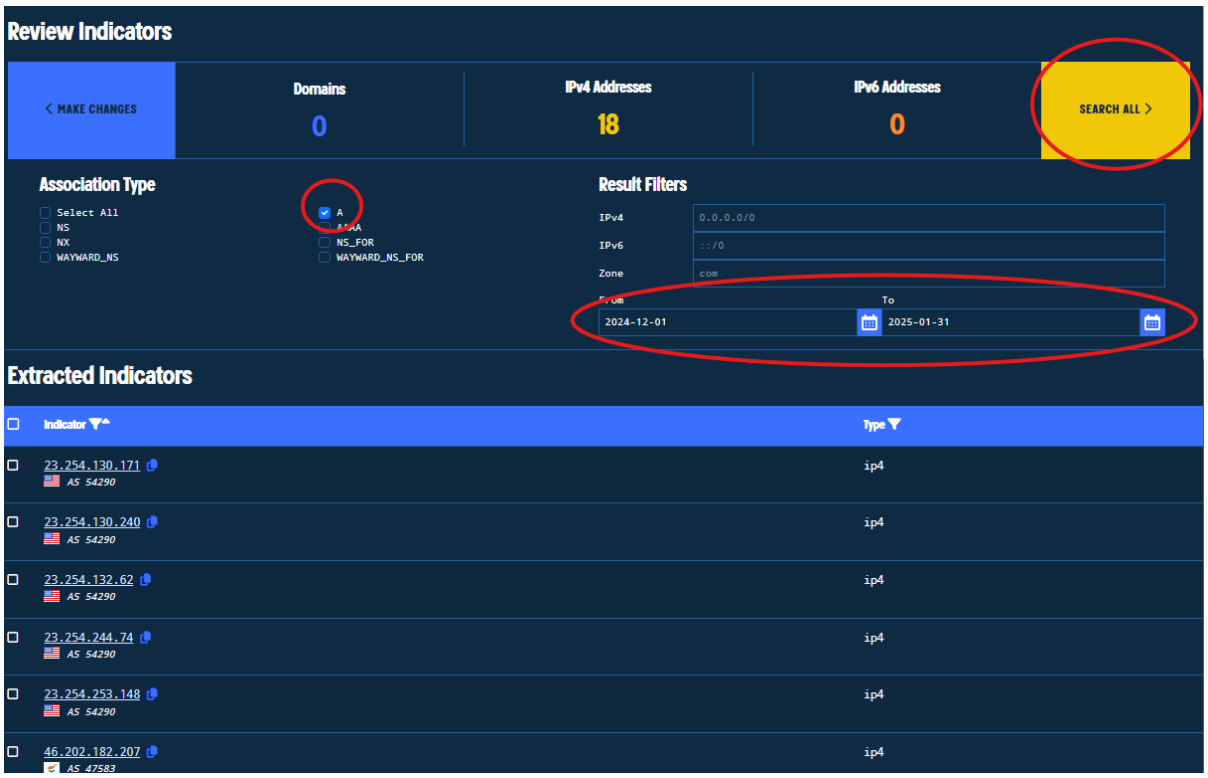


Figure 37. Setting Options for Bulk Searching

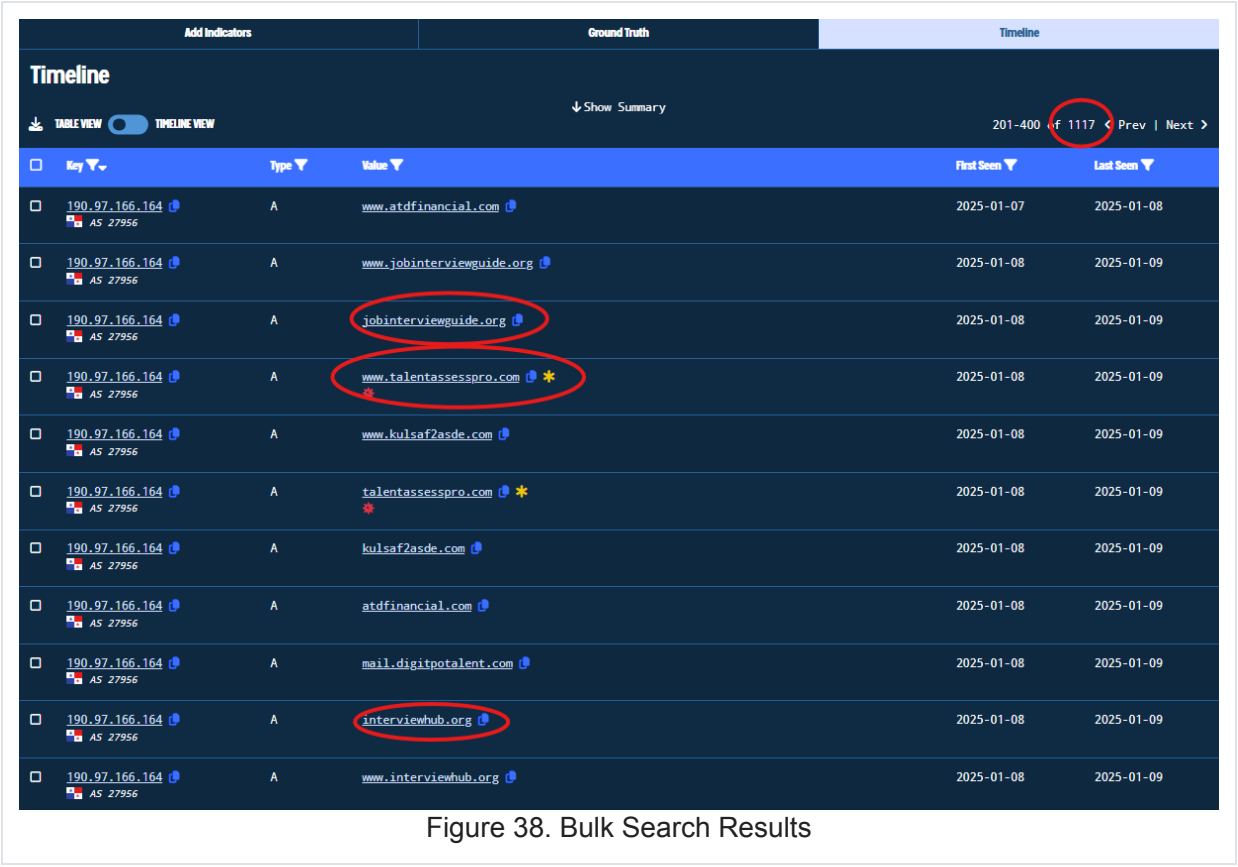


Figure 38. Bulk Search Results

In the results View we can see other domains associated with Lazarus (based on reputation) and some that also have the same naming convention that could indicate potential association. Of course, verification is necessary. We conclude with adding to our project the new findings from this search.

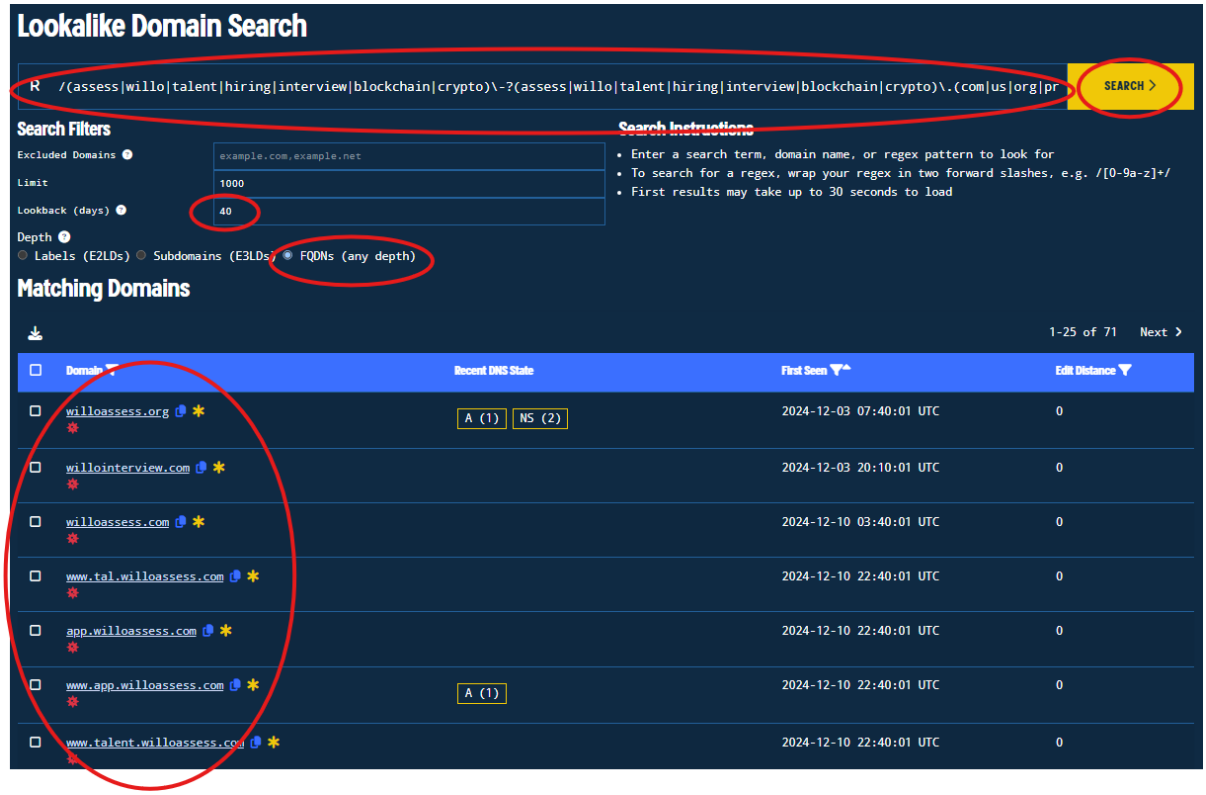
3rd Method of Identifying Further Infrastructure: Lookalike Domain Search

Another useful feature is the Lookalike Domain Search. From there we can use search terms, domain names or regex patterns to identify further domains of interest. From the previous batches of indicators collected with the previous two methods, we know some of the most common keywords Lazarus uses to register their domains for this campaign. Thus, we can combine them with multiple ways to further identify domains. Let's take for example the following regex:

```
/(assess|willo|wilo|talent|hiring|interview|blockchain|crypto|recruit|candidate|video)\-?(assess|willo|wilo|talent|hiring|interview|blockchain|crypto|recruit|candidate|video)\.(com|us|org|pro)/
```

Explanation of the regex: Some of the most relevant keywords regarding Willo, hiring and blockchain topics appended with or without dash, with the same pairs of keywords ending in a `.com`, `.us`, `.org`, `.pro` TLD (as commonly observed) - a good starting point.

Also, we refine the loopback to search only 40 days back since we know the campaign started in December 2024, and select the FQDNs option to search for any depth.



We can observe that we have results related to Lazarus! We can also dig deeper and investigate other candidates. Consider the following regexes:

- `/(willo|wilo|hiring|blockchain|crypto)\-?(assess|talent|hiring|interview)\.(com|us|org|pro)/` (better combined keywords)
- `/app\.(willo|wilo|hiring|blockchain|crypto)\-?(assess|talent|hiring|interview)\.[a-z]+/`(app subdomain + combined keywords + TLD agnostic)
- `/(willo|wilo|hiring|blockchain|crypto)\-?(video|candidate|talent|interview)\.[a-z]+/` (willo & blochain hiring themes + TLD agnostic)
- `/(video|candidate|talent|interview)\-?(willo|wilo|hiring|blockchain|crypto)\.[a-z]+/` (reversed order willo & blochain hiring themes + TLD agnostic)

We conclude by adding our newly identified indicators to our project.

Conclusion

Lazarus is a sophisticated group of threat actors, constantly refining their TTPs to achieve their objectives and support their country's agenda. It is up to us, security researchers to identify their behaviours and patterns and detect their infrastructure before it gets weaponized. In this blog we analyzed the new Lazarus campaign as part of Contagious Interview, utilizing the ClickFix social engineering technique. Through Validin's Search, Bulk Search and Lookalike Domain Search, we identified Lazarus' domain registration and hosting patterns. We shared further Indicators of Compromise along with the methodology on how to hunt malicious infrastructure.

Ready to level up your threat hunting, threat attribution, and incident response efforts? Validin's premium individual and enterprise solutions offer powerful tools, affordable pricing, and unparalleled insights to help your team work smarter and faster.

Contact us today to explore enterprise options and see how Validin can empower your threat intelligence team.

Connect with the author: Follow Efstratios on X.

Indicators

web[.]videoscreening[.]org
videoscreening[.]org
app[.]videoscreening[.]org
www[.]intervu-talent[.]pro
www[.]talentassesspro[.]com
www[.]app[.]videoforrecruitment[.]com
videoforrecruitment[.]com
app[.]videoforrecruitment[.]com
blockchain-assess[.]com
www[.]app[.]willotalents[.]org
willotalents[.]org
app[.]willotalents[.]org
app[.]willocandidate[.]com
webmail[.]complexassess[.]com
webdisk[.]complexassess[.]com
cpcontacts[.]complexassess[.]com
cpcalendars[.]complexassess[.]com
cpanel[.]complexassess[.]com
complexassess[.]com
autodiscover[.]complexassess[.]com
robinhood[.]vinterview[.]org
www[.]app[.]vinterview[.]org
app[.]vinterview[.]org
app[.]willotalentes[.]com
www[.]api[.]wtalents[.]us
api[.]wtalents[.]us
cpanel[.]wtalents[.]us
willoassessment[.]com
www[.]gemini-willoassessment[.]com[.]willoassessment[.]com
gemini-willoassessment[.]com[.]willoassessment[.]com
hiring[.]willoassessment[.]com
www[.]consensys[.]willoassessment[.]com
geminiskill[.]willoassessment[.]com
www[.]hiring[.]willoassessment[.]com
api[.]willoassessment[.]com
gemini[.]willoassessment[.]com
consensys[.]willoassessment[.]com
www[.]gemini[.]willoassessment[.]com
www[.]app[.]willotalent[.]xyz
app[.]willotalent[.]xyz
www[.]api[.]nvidia-release[.]us
api[.]nvidia-release[.]us
www[.]willorecruit[.]com
cpcontacts[.]willorecruit[.]com
cpcalendars[.]willorecruit[.]com
www[.]app[.]willorecruit[.]com
app[.]willorecruit[.]com
webmail[.]willorecruit[.]com
mail[.]willorecruit[.]com
cpanel[.]willorecruit[.]com
webdisk[.]willorecruit[.]com
willorecruit[.]com

www[.]willotalentes[.]com
www[.]app[.]willotalentes[.]com
willotalentes[.]com
willocandidates[.]com
www[.]fundcandidates[.]com
app[.]willohiring[.]com
www[.]willocandidate[.]com
www[.]app[.]willocandidate[.]com
willocandidate[.]com
www[.]api[.]nvidia-release[.]org
www[.]willotalent[.]us
www[.]app[.]willotalent[.]us
app[.]willotalent[.]us
willotalent[.]us
www[.]willotalent[.]pro
www[.]app[.]willotalent[.]pro
app[.]willotalent[.]pro
willotalent[.]pro
www[.]willointerview[.]com
www[.]willoassess[.]com
www[.]talent[.]willoassess[.]com
www[.]tal[.]willoassess[.]com
www[.]gemini[.]willoassess[.]com
gemini[.]willoassess[.]com
willoassess[.]com
www[.]willohiring[.]com
www[.]app[.]willohiring[.]com
www[.]gemini[.]willohiring[.]com
gemini[.]willohiring[.]com
www[.]meta[.]willohiring[.]com
meta[.]willohiring[.]com
willohiring[.]com
www[.]willohiringtalent[.]org
www[.]app[.]willohiringtalent[.]org
app[.]willohiringtalent[.]org
www[.]gemini[.]willohiringtalent[.]org
gemini[.]willohiringtalent[.]org
willohiringtalent[.]org
www[.]willoassess[.]org
www[.]willo-interview[.]us
www[.]talent[.]willo-interview[.]us
talent[.]willo-interview[.]us
www[.]app[.]willo-interview[.]us
app[.]willo-interview[.]us
willo-interview[.]us
www[.]intro-crypto-assess[.]com
cpcontacts[.]intro-crypto-assess[.]com
cpcalendars[.]intro-crypto-assess[.]com
webmail[.]intro-crypto-assess[.]com
mail[.]intro-crypto-assess[.]com
cpanel[.]intro-crypto-assess[.]com
webdisk[.]intro-crypto-assess[.]com

intro-crypto-assess[.]com
www[.]blockchain-assess[.]com
d20zx0lguyxj2p[.]cloudfront[.]net
d1yzmjg018adwf[.]cloudfront[.]net
d12rlkj8v5mwse[.]cloudfront[.]net
d3o9p0hkd7eul5[.]cloudfront[.]net
wilio-talent[.]net
willoassess[.]net
www[.]wtalents[.]us
www[.]app[.]wtalents[.]us
app[.]wtalents[.]us
mail[.]wtalents[.]us
wtalents[.]us
www[.]willomexcvip[.]us
www[.]app[.]willomexcvip[.]us
app[.]willomexcvip[.]us
mail[.]willomexcvip[.]us
www[.]werhiring[.]willomexcvip[.]us
werhiring[.]willomexcvip[.]us
willomexcvip[.]us
www[.]hiringtalent[.]pro
app[.]hiringtalent[.]pro
final[.]hiringtalent[.]pro
hiringtalent[.]pro
intervu-talent[.]pro
www[.]talentcompetency[.]com
talentcompetency[.]com
www[.]app[.]willoassessment[.]com
app[.]willoassessment[.]com
www[.]geminiskill[.]willoassessment[.]com
www[.]api[.]willoassessment[.]com
www[.]wilo-talent[.]com
app[.]wilo-talent[.]com
wilo-talent[.]com
www[.]complexassess[.]com
mail[.]complexassess[.]com
www[.]app[.]willoassess[.]com
app[.]willoassess[.]com
www[.]vid[.]willoassess[.]com
vid[.]willoassess[.]com
www[.]robinhood[.]intro-crypto-assess[.]com
www[.]vid[.]intro-crypto-assess[.]com
vid[.]intro-crypto-assess[.]com
www[.]app[.]blockchain-assess[.]com
app[.]blockchain-assess[.]com
www[.]vid[.]blockchain-assess[.]com
vid[.]blockchain-assess[.]com
fundcandidates[.]com
www[.]app[.]blockchain-checkup[.]com
app[.]blockchain-checkup[.]com
talentassesspro[.]com
www[.]willo-video[.]com

willo-video[.]com
www[.]robinhood[.]vinterview[.]org
vinterview[.]org
www[.]hiringinterview[.]org
www[.]app[.]hiringinterview[.]org
app[.]hiringinterview[.]org
hiringinterview[.]org
www[.]interviewnest[.]org
www[.]app[.]interviewnest[.]org
app[.]interviewnest[.]org
interviewnest[.]org
willoassess[.]org
www[.]app[.]videoscreening[.]org
www[.]web[.]videoscreening[.]org
willovideorec[.]com
willointerview[.]com
api[.]nvidia-release[.]org