



# Probing the DNS Depths of PHALT#BLYX

## Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Artifacts](#)

## Executive Report

Securonix recently published their analysis of stealthy campaign PHALT#BLYX, which targeted the European hospitality sector. They used click-fix social engineering, fake CAPTCHAs, and fake BSOD pages to trick users into downloading DCRat so the threat actors could take full remote access to infected systems and drop secondary payloads. The researchers cited 11 original IoCs in their [report](#) comprising one URL, seven domains, and three IP addresses.

After extracting an additional domain from the URL, we analyzed 12 IoCs in total—one URL, eight domains, and three IP addresses. Our investigation uncovered these findings:

- Three domains identified as IoCs were deemed likely to turn malicious 28–177 days before being reported as such
- 7,099 unique potential victim IP addresses communicated with two IP addresses identified as IoCs
- 21,638 email-connected domains, four of which turned out to be malicious
- Six additional IP addresses, five of which turned out to be malicious
- Six IP-connected domains, three of which turned out to be malicious
- Seven string-connected domains

## More on the booking[.]com Lure

According to Securonix, the PHALT#BLYX attack started with the threat actors sending phishing emails to mostly European users. The potential victims were tricked into accessing a fake booking[.]com CAPTCHA page. Those who fell for the ruse then saw a fake BSOD page while DCRat was silently dropped onto their systems.

We took a closer look at booking[.]com using [Jake AI](#) and discovered that while the domain was legitimate, cyber attackers could be typosquatting on its popularity. In fact, we learned how many of its look-alikes were registered in the past seven, 30, and 90 days, along with some examples.



Of course. Here is a summary of the findings organized by the different timeframes.

Timeframe	New Domains Found	Examples of Likely Typosquatting
Past 7 Days	1,725	booking-confirmation-id8186.com booking-guest4947-reservation.com quickverify90-booking.com
Past 30 Days	7,004	booking-com-payments-upd.vg recheck239-booking.com booking-secure-auth.com
Past 90 Days	10,000	confirmation89100-booking.com userverify61-booking.com booking-secure-verify.com

Jake AI result for the booking[.]com query “Discover domains containing “booking” in reference to booking.com for the past 7, 30, and 90 days.”

Our AI tool also clued us in to the various typosquatting methods that could have been used to mimic the site with examples as well.

Of course! Here is a summary table of the different typosquatting techniques we found in the search results.

Typosquatting Type	Description	Examples
Keyword Addition	Appending or prepending keywords to the brand name to create a sense of urgency, legitimacy, or relevance to a specific service.	confirmation89100-booking.com userverify61-booking.com trivago-hotel-booking.com
Top-Level Domain (TLD) Abuse	Using the exact brand name but with an unconventional or misleading TLD (e.g., .xyz, .store, .online) to trick users.	bookingstaking.xyz sunbooking.store jwmarriottbooking.online
Hyphenation	Inserting hyphens into the domain name to mimic a structured, official-looking URL or to capture mistyped entries.	booking-park.com global-village-booking.com intercontinental-hotels.com-hotel-booking.com
Country Code TLDs (ccTLDs)	Registering the brand name under various country-code domains to target specific regions or appear as a local, official entity.	booking-com.de (Germany) smtp.bookingcom.pl (Poland) lastminutebooking.co.uk (UK)



Jake AI query result for “What were there different typosquatting tactics used for the sample domains found?”

## Additional Information the URL IoC

A sole URL was also identified as an IoC and we dug up more information about it via Jake AI, too. We learned that the site has been associated with malware distribution since 17 December 2025, two days after its creation. The site it led to did not have content as well. Interestingly, the site name **2fa-bns** could have been designed to impersonate a legitimate service potentially for a 2FA phishing scam.

What can you tell me about <http://2fa-bns.com>

Used **whois** tool from WhoisXML API 234ms

Used **threat\_intelligence** tool from WhoisXML API 419ms

Used **categorization** tool from WhoisXML API 1.25s

Based on my analysis, the domain `2fa-bns.com` is **not legitimate and appears to be malicious**.

Here's a summary of what I found:

- **Malware Association:** My threat intelligence tool has flagged this domain for being associated with **malware**. The first sighting was on December 17, 2025, just two days after the domain was created.
- **Recent Creation:** The domain was registered on December 15, 2025, making it very new. This is a common characteristic of domains used for malicious campaigns.
- **No Website Content:** The website is not responsive and has no content, which is another significant red flag.

The name "2fa-bns" seems designed to impersonate a legitimate service, possibly for a two-factor authentication (2FA) phishing scam.

Given these findings, I strongly advise you to **avoid this website** and not enter any personal information.

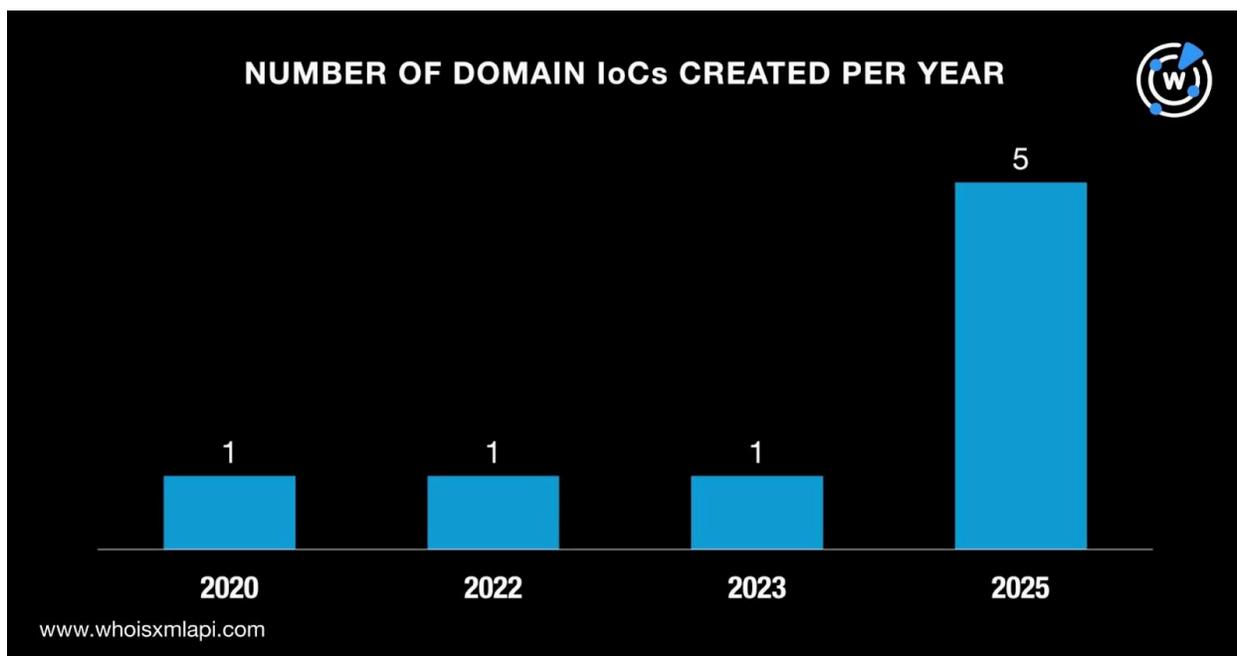


## New Findings for the Domain IoCs

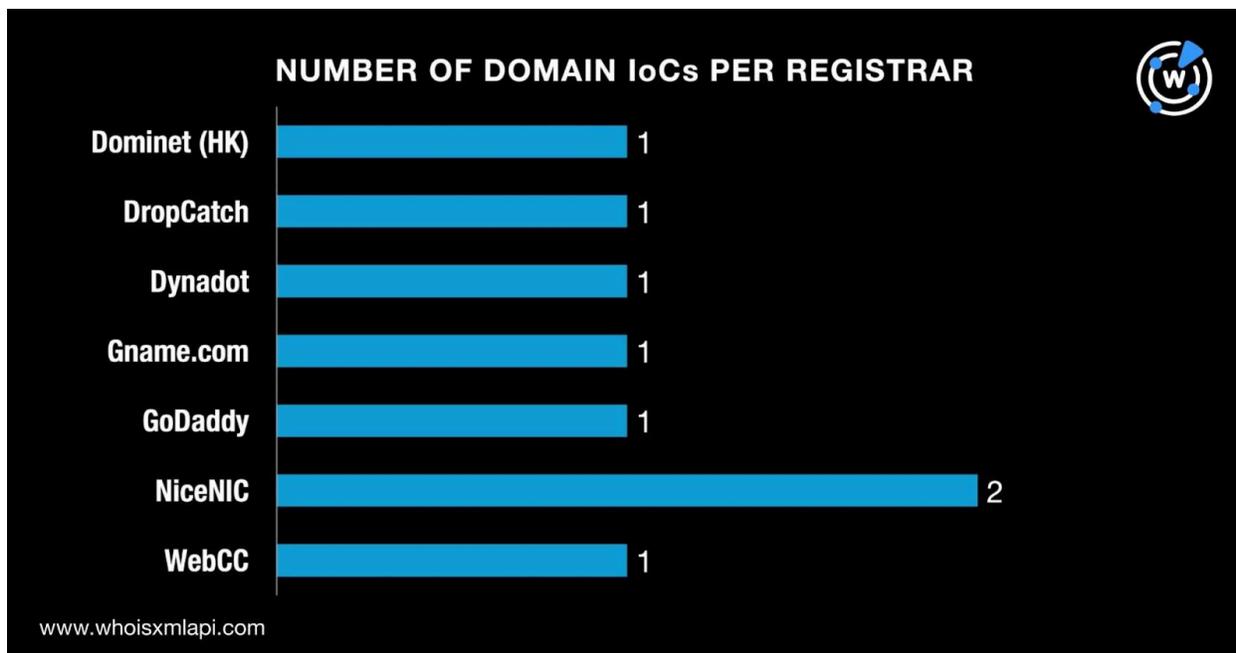
Our [First Watch Malicious Domains Data Feed](#) query results revealed that three domains identified as IoCs were registered with malicious intent. They were classified as malicious 28–177 days before the report’s publication on 6 January 2026.

Next, we queried the eight domains identified as IoCs on [WHOIS API](#) and discovered that:

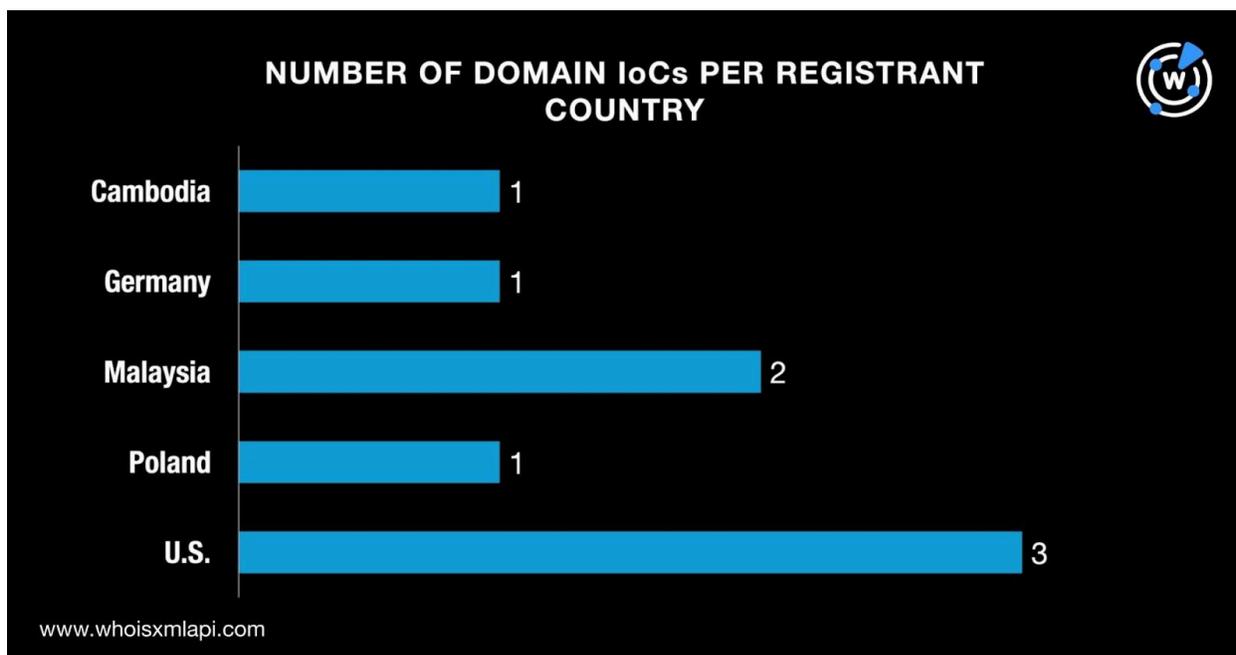
- They were created between 8 June 2022 and 15 December 2025.



- They were administered by six different registrars led by NiceNIC.



- They were registered in five different countries, with a majority in the U.S.



The differences in registrar and registrant country could be a misdirection tactic the threat actors employed to evade the prying eyes of law enforcement agencies as to their actual location, which, according to the researchers, was in Russia (i.e., not even on the list of registrant countries).



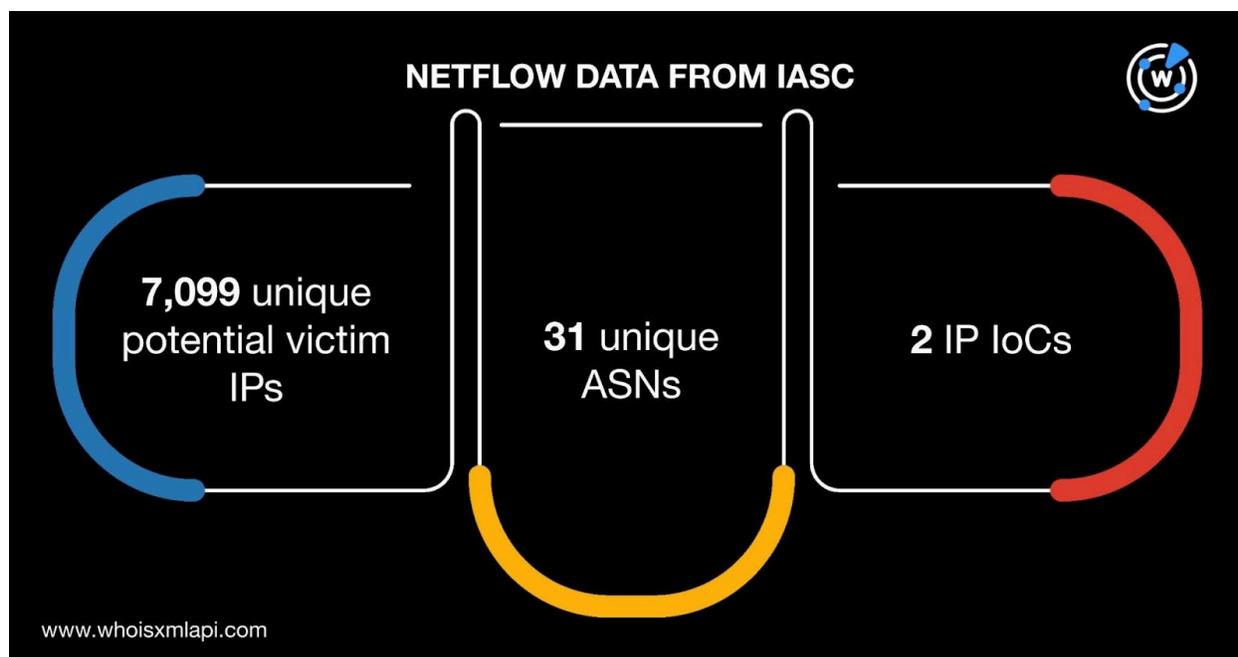
Finally, [DNS Chronicle API](#) queries for the eight domains identified as IoCs showed that seven recorded 523 historical domain-to-IP resolutions over time. The domain asj88[.]com's oldest resolution was recorded on 5 February 2017.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
asj88[.]com	186	02/05/17	01/09/26
wmk77[.]com	171	04/29/17	01/07/26
asj99[.]com	154	11/03/17	06/13/24

Given the discrepancies between the WHOIS creation dates (i.e., 2023, 2025, and 2022) and first domain-to-IP resolution dates (i.e., 2017) for the three domains above, we could infer that they may have been reregistered for the campaign's use. And while one of them stopped actively resolving to an IP address in 2024, two remain active to date.

## New Insights into the IP IoCs

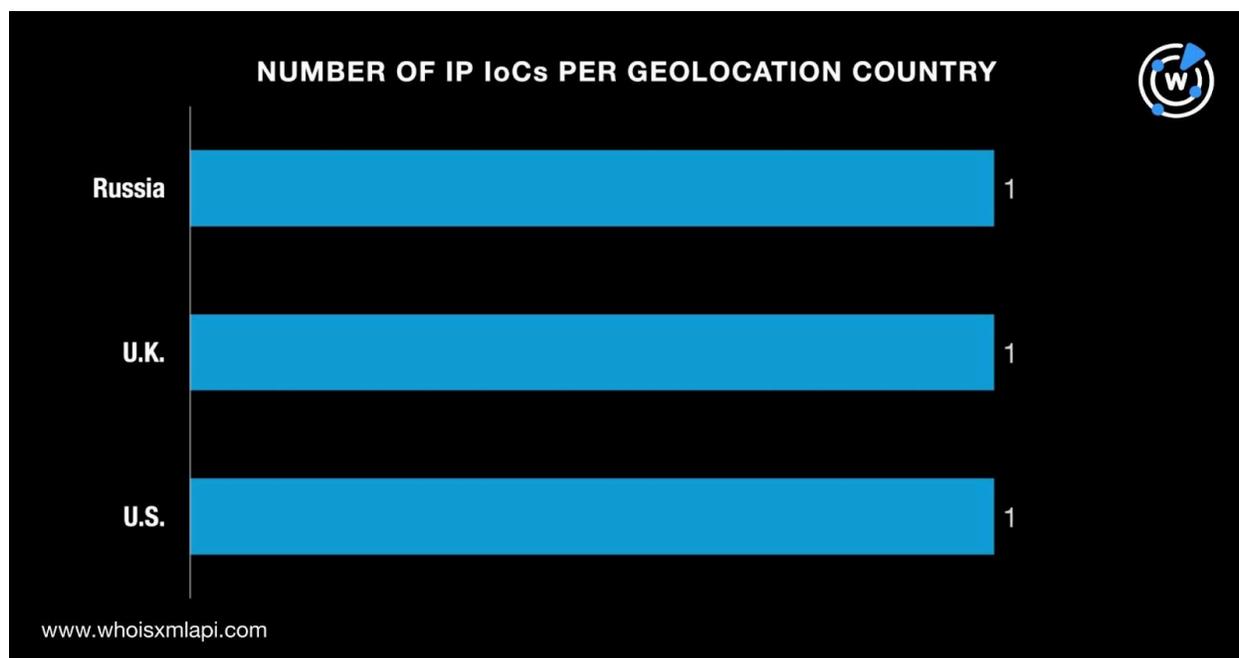
Sample network traffic data from the [IASC](#) revealed that 7,099 unique potential victim IP addresses under 31 distinct ASNs communicated with two IP addresses identified as IoCs between 9 September 2025 and 16 January 2026.



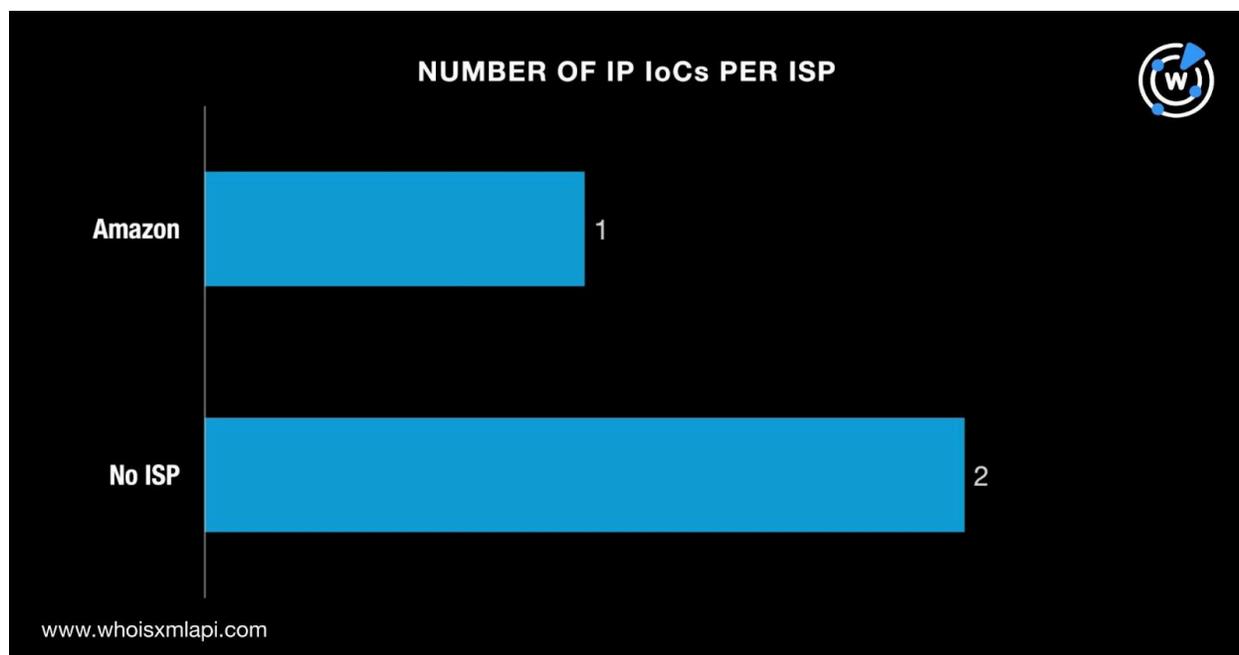


A [Bulk IP Geolocation Lookup](#) query for the three IP addresses identified as IoCs showed that:

- They were geolocated in three distinct countries. And this time, one of the nations was Russia—the attack’s origin. Note, too, that the U.S. was among both the IP geolocation and registrant countries.



- While two IP addresses did not have ISPs on record, one was administered by Amazon.



Our DNS Chronicle API query results for the three IP addresses identified as IoCs, meanwhile, revealed that two recorded 1,015 historical IP-to-domain resolutions over time. The IP address 194[.]169[.]163[.]140 recorded its first resolution on 23 January 2021.

## The Hunt for New Artifacts Begins

We kicked off our search for new artifacts by querying the eight domains identified as IoCs on [WHOIS History API](#). We discovered that six had 32 unique email addresses in their historical WHOIS records. Of these, 13 were public email addresses.

We then queried 13 email addresses on [Reverse WHOIS API](#) and found out that while none of them were present in current WHOIS records, all of them appeared in historical records. After excluding two email addresses that could belong to domainers, we uncovered 21,638 unique email-connected domains after those already identified as IoCs were filtered out.

[Threat Intelligence API](#) queries for the email-connected domains showed that four have already been weaponized for various attacks. An example is cp57[.]top, which was used to distribute malware from 9 March 2023 to 14 January 2026.

Next, we queried the eight domains identified as IoCs on [DNS Lookup API](#) and discovered that six resolved to six unique IP addresses not yet tagged as IoCs.

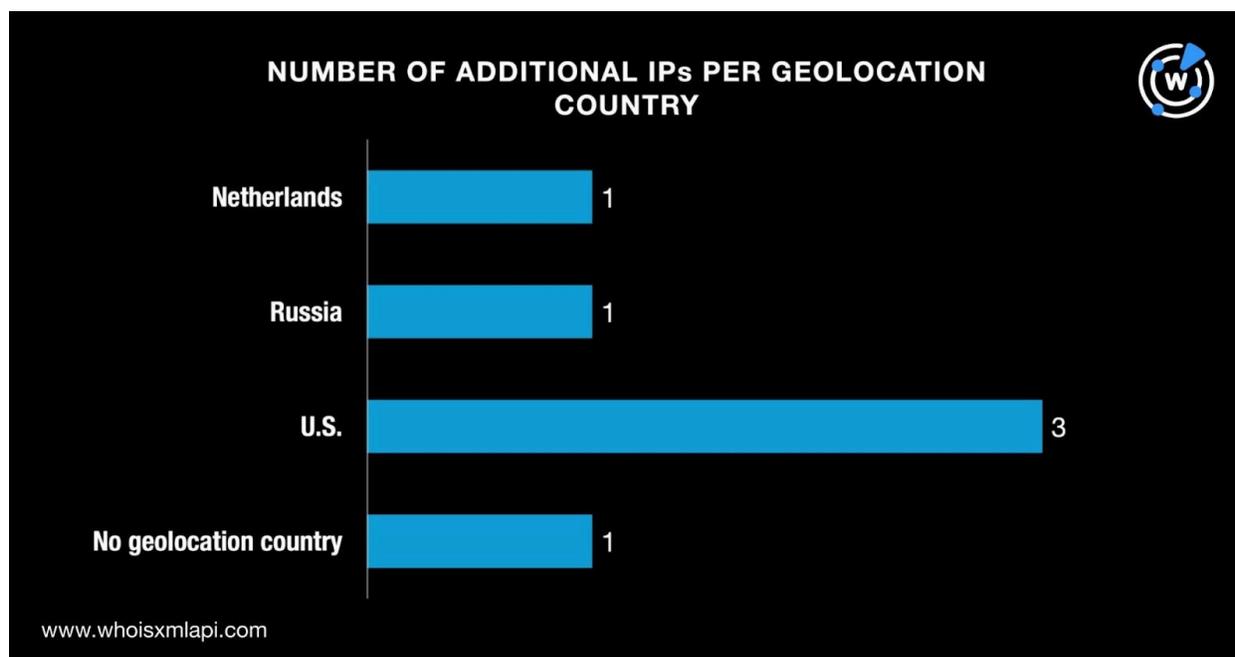


According to Threat Intelligence API, five of the additional IP addresses have already figured in various attacks.

ADDITIONAL IP	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
54[.]243[.]117[.]197	Phishing	08/07/25	01/16/26
	Malware distribution	08/07/25	01/16/26
	C&C	08/07/25	01/15/26
	Generic threat	08/07/25	01/14/26
	Spamming	09/17/25	12/02/25
158[.]94[.]210[.]43	Spamming	09/17/25	01/15/26
	Attack	09/18/25	01/15/26
	Malware distribution	11/18/25	01/14/26
	Phishing	11/25/25	12/30/25
104[.]21[.]20[.]46	Malware distribution	01/23/24	01/14/26

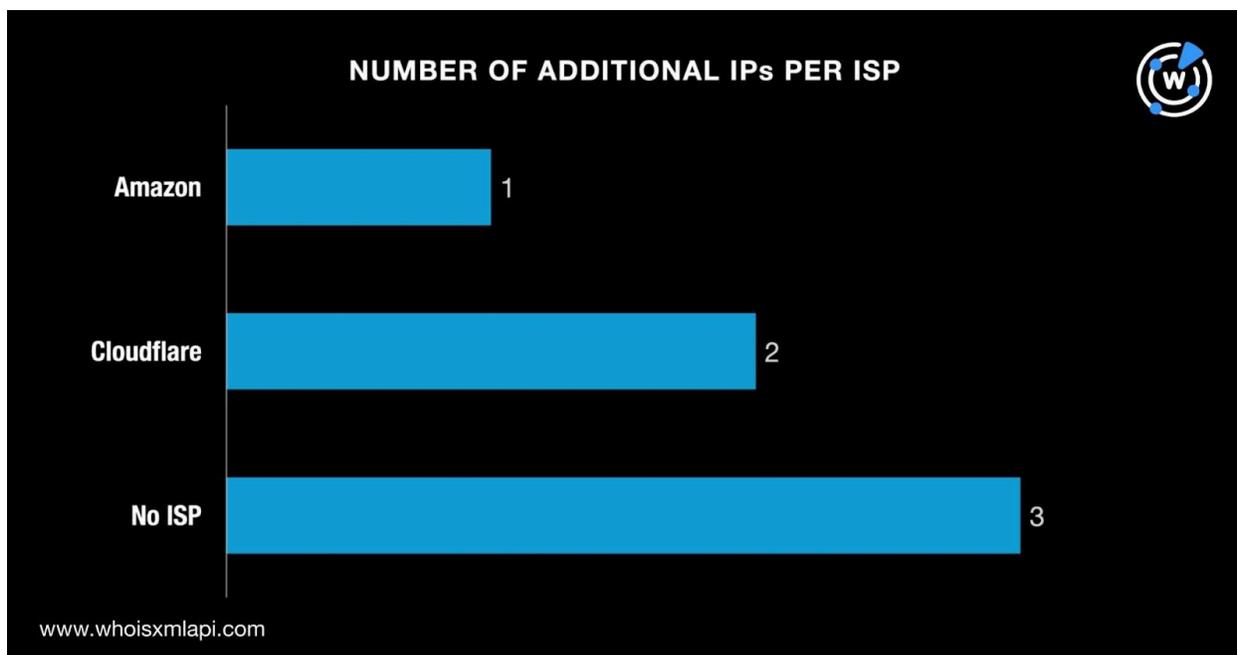
A Bulk IP Geolocation Lookup query for the six additional IP addresses revealed that:

- While one did not have a geolocation country on record, the remaining five originated from three different nations. Note that two of the countries were consistent with the geolocations of some of the IP addresses identified as IoCs.





- And while three did not have ISPs on record, the other three were administered by two ISPs. Note that Amazon was also among the list of ISPs for the loCs.



We now had nine IP addresses in all for the next step. We queried them on [Reverse IP API](#) and discovered that one could be a dedicated host. It hosted six unique IP-connected domains after those already identified as loCs and the email-connected domains were filtered out.

Based on the results of our Threat Intelligence API queries, three IP-connected domains have already been weaponized for various attacks. An example is `asj177[.]com`, which has been associated with malware distribution since 29 December 2025. Incidentally, this malicious domain looked very similar to three of the loCs—`asj77[.]com`, `asj88[.]com`, and `asj99[.]com`. The IP-connected domain `asj177[.]com` also shared the registrar, registrant country, domain status, and name server of the loC `asj77[.]com` according to Jake AI.



What other similarities apart from structure does asj177.com share with asj77.com, asj88.com, and asj99.com?

Used whois tool from WhoisXML API 6.74s

Used whois tool from WhoisXML API 7.80s

Used whois tool from WhoisXML API 6.67s

Used whois tool from WhoisXML API 7.19s

Of the four domains you listed, `asj177.com` and `asj77.com` share the most similarities beyond their naming structure. Here's a breakdown of what I found:

**Similarities between asj177.com and asj77.com:**

- **Registrar:** Both domains are registered with the same registrar, NICENIC INTERNATIONAL GROUP CO., LIMITED.
- **Registrant Location:** The registrant for both domains is located in Berlin, Germany.
- **Domain Status:** They share the same three domain statuses: `clientDeleteProhibited`, `clientTransferProhibited`, and `clientHold`. This combination often indicates the domains are not in use.
- **Nameservers:** Both use DNSPOD.COM nameservers, suggesting they are managed under the same DNS provider.

**How the other domains differ:**

- **asj88.com:** This domain is registered by a different entity, HugeDomains.com, through the registrar DropCatch.com 401 LLC. It uses different nameservers and is registered in the United States. This domain appears to be for sale.
- **asj99.com:** This domain is not currently registered.

In short, `asj177.com` and `asj77.com` appear to be owned or managed by the same entity, while the others are not.

If you have any more questions, feel free to ask

Next, we extracted eight unique text strings from the eight domains identified as loCs. Searches for these on [Domains & Subdomains Discovery](#) showed that five appeared at the start of seven unique string-connected domains not on the loC list and after the email- and IP-connected domains were filtered out. The strings were:



- asj77.
- asj88.
- asj99.
- low-house.
- wmk77.

—

Our in-depth analysis of the PHALT#BLYX campaign IoCs revealed that three domains identified as IoCs were deemed likely to turn malicious 28–177 days before being reported as such. In addition, 7,099 unique potential victim IP addresses communicated with two IP addresses identified as IoCs.

Meanwhile, we also unearthed 21,657 new artifacts comprising 21,638 email-connected domains, six additional IP addresses, six IP-connected domains, and seven string-connected domains. It is worth noting that, to date, 12 of them have already figured in various attacks.

***If you wish to learn more about the products used in this research, please don't hesitate to [contact us](#).***

***Disclaimer:*** We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as “threats” or “malicious” may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.



## Appendix: Sample Artifacts

### Sample Email-Connected Domains

- 001jie[.]com
- 001jm[.]top
- 007fox[.]com
- a-1drycleaners[.]com
- a-health-day[.]com
- a-zgdg[.]com
- b-chocolate[.]com
- b161[.]top
- b162[.]top
- c-black[.]cn
- c-fol[.]top
- c-ps[.]top
- d-event[.]com
- d-koncept[.]com
- d133[.]top
- e-compusoft[.]net
- e-nonymous[.]com
- e-panz[.]com
- f050[.]top
- f051[.]top
- f115[.]top
- g-cores[.]top
- g-dance[.]com
- g-email[.]top
- h0591[.]top
- h0724[.]top
- h122[.]top
- i-911[.]com
- i-gamer[.]top
- i-mad[.]top
- j-sun[.]com[.]cn
- j-test[.]top
- j073[.]top
- k-warehouse[.]com
- k0pu[.]net
- k1768[.]com
- l125[.]top
- l126[.]top
- l127[.]top
- m-cctv[.]com
- m021[.]top
- m035[.]top
- n039[.]top
- n071[.]top
- n088[.]top
- o-hr[.]top
- o-sky[.]top
- o185[.]top
- p-anna[.]com
- p-sb[.]com
- p014[.]top
- q-ti[.]com
- q10s[.]com
- q177[.]top
- r-carlylefans[.]com
- r-kirk[.]com
- r112[.]top
- s-linktravel[.]com
- s-xiaojiu[.]com
- s038[.]top
- t-cell-15[.]com
- t-elleboudoirphotography[.]com
- t0001[.]top
- u-poo[.]com
- u-reachworld[.]com
- u050[.]top
- v08v[.]top
- v09v[.]top
- v0u[.]top
- w-mtour[.]com
- w-nm[.]com
- w0407[.]com



- x-hua[.]com
- x-kicks[.]top
- x026[.]top
- y082[.]top
- y117[.]top
- y122[.]top
- z-boxfitness[.]com
- z053[.]top
- z060[.]top

### Sample Additional IP Addresses

- 104[.]21[.]20[.]46
- 127[.]0[.]0[.]127
- 158[.]94[.]210[.]43

### Sample IP-Connected Domains

- asj177[.]com
- connff77[.]com
- kssx77[.]com

### Sample String-Connected Domains

- asj77[.]tk
- asj88[.]cn
- asj99[.]top
- low-house[.]md
- wmk77[.]top