WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

# Massive Photo ZIP Campaign Targets Booking.com Partner and Other Hotels across Japan and Europe

Threat Report

## Table of Contents

# Executive Report

Microsoft Threat Intelligence recently uncovered an active multistage intrusion campaign targeting organizations in the hospitality and hotel industry in Europe and Asia, particularly Japan, since April 2026.

The unknown threat actors used photo-themed ZIP archives that users were tricked into downloading. These archives contained fake image shortcut files that, when launched, started an attack chain that relied on an obfuscated PowerShell script, a Node.js-based implant, dual registry persistence, and C&C communications over nonstandard ports. In addition, the campaign's postcompromise activities included C&C beaconing, forced shutdowns, and a compilation of PE payloads. While its ultimate objective remained unclear, the researchers believed the fact that obfuscation and persistence were ensured could indicate they were preparing the infected devices for more follow-on activities.

The threat actors also misused legitimate services like Calendly's email notification infrastructure and Google's URL redirect functionality to deliver phishing emails with multilingual lures and subject lines. These emails attempted to bypass conventional authentication checks through authentication laundering.

The researchers identified 78 network IoCs comprising 73 domains and five IP addresses in their report. After filtering out a domain owned by a legitimate entity aided by the WhoisXML API MCP Server, we were left with 77 IoCs for further analysis.

Our own investigation of the threat led to these discoveries:

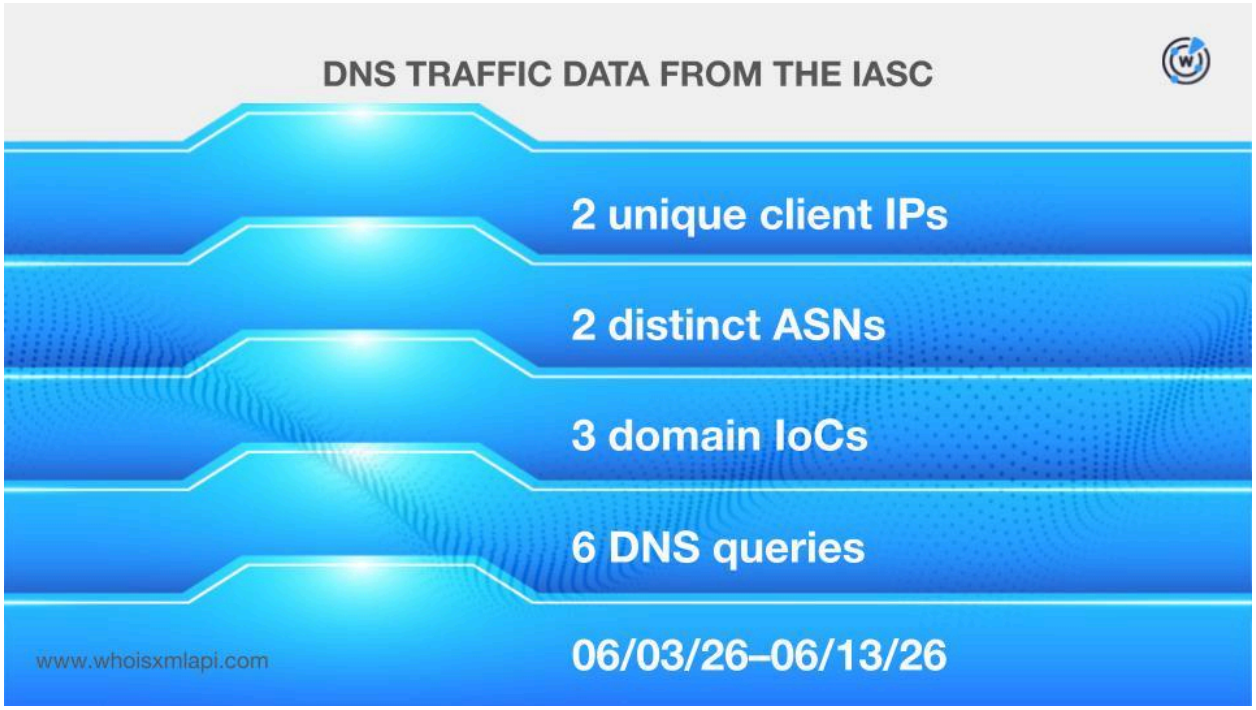
- Two unique client IP addresses that communicated with three domain IoCs
- Five domain IoCs that appeared in four typosquatting groups
- One domain IoC that was likely registered with malicious intent
- 2,357 distinct IP addresses potentially belonging to victims that communicated with five IP IoCs
- 2,840 email-connected domains, 26 confirmed malicious
- 123 additional IP addresses, all confirmed malicious
- 144 IP-connected domains
- 95 string-connected domains

## Photo ZIP Campaign Domain IoCs Dissected

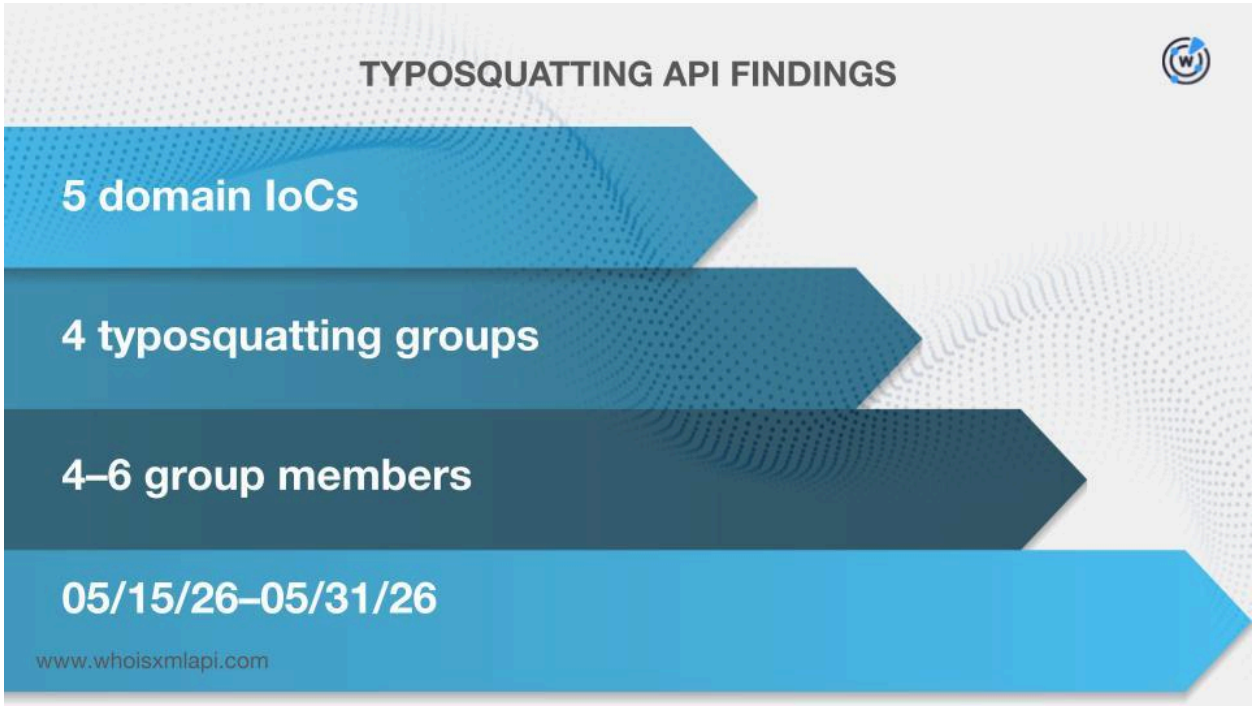
We began our DNS deep dive by looking more closely at the 72 domain IoCs.

First, we learned from sample network traffic data from the IASC that two unique client IP addresses under two distinct ASNs communicated with three of the domain

IoCs—photo-26653[.]cfd, photo-26656[.]cfd, and photo-27857[.]cfd—via six DNS queries recorded between 3 and 13 June 2026.




Next, we learned that five domain IoCs appeared in four typosquatting groups based on the results of our Typosquatting API queries.



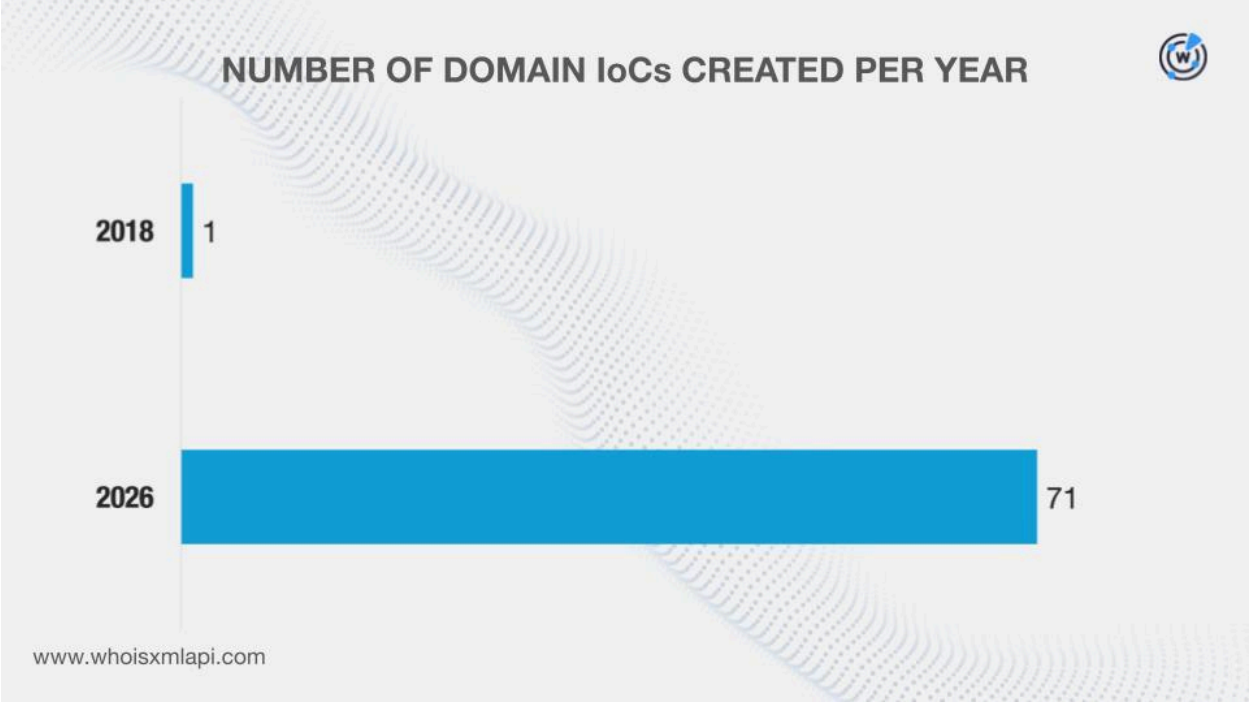

Take a look at more details below.

| DOMAIN IoC | GROUP NUMBER ID | GROUP MEMBER NUMBER | GROUP MEMBERS OTHER THAN THE IoCs | CREATION DATE |
|---|---|---|---|---|
| photo-132454[.]cfd created on 05/28/26 | 5601 | 5 | photo-432454[.]cfd<br>photo-532454[.]cfd<br>photo-332454[.]cfd<br>photo-232454[.]cfd | 05/28/26<br>05/28/26<br>05/28/26<br>05/28/26 |
| photo-21473[.]xyz created on 05/15/26 | 5333 | 4 | photo-41473[.]xyz<br>photo-51473[.]xyz<br>photo-31473[.]xyz | 05/15/26<br>05/15/26<br>05/15/26 |
| photo-26654[.]cfd and photo-26254[.]cfd created on 05/31/26 | 3103 | 4 | photo-26554[.]cfd<br>photo-26154[.]cfd | 05/31/26<br>05/31/26 |
| photo-8632454[.]cfd created on 05/27/26 | 4487 | 6 | photo-3632454[.]cfd<br>photo-1632454[.]cfd<br>photo-4632454[.]cfd<br>photo-7632454[.]cfd<br>photo-6632454[.]cfd | 05/27/26<br>05/27/26<br>05/27/26<br>05/27/26<br>05/27/26 |

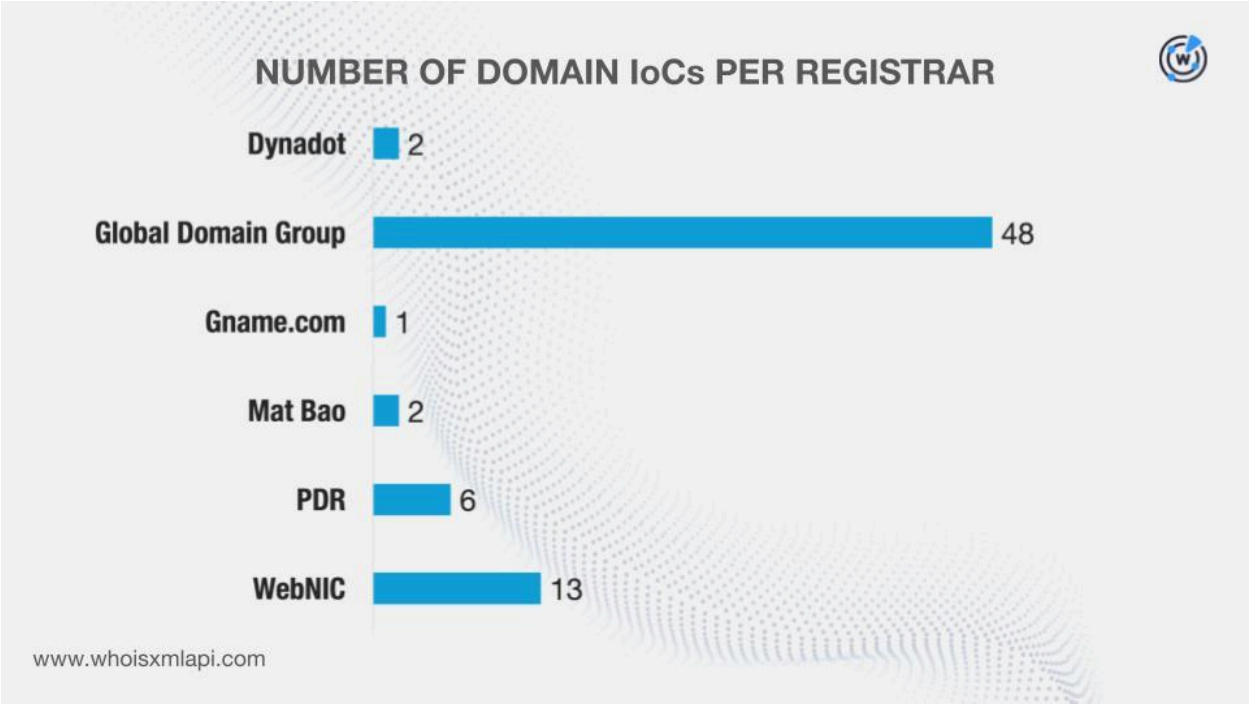
The First Watch Malicious Domains Data Feed also provided interesting findings. We discovered that the domain IoC—zloapobikahy23[.]bond—created on 20 February 2026 was likely registered with malicious intent. It was dubbed as such 125 days prior to when it was declared an IoC on 25 June 2026.

We then queried the domain IoCs on WHOIS API and discovered that:

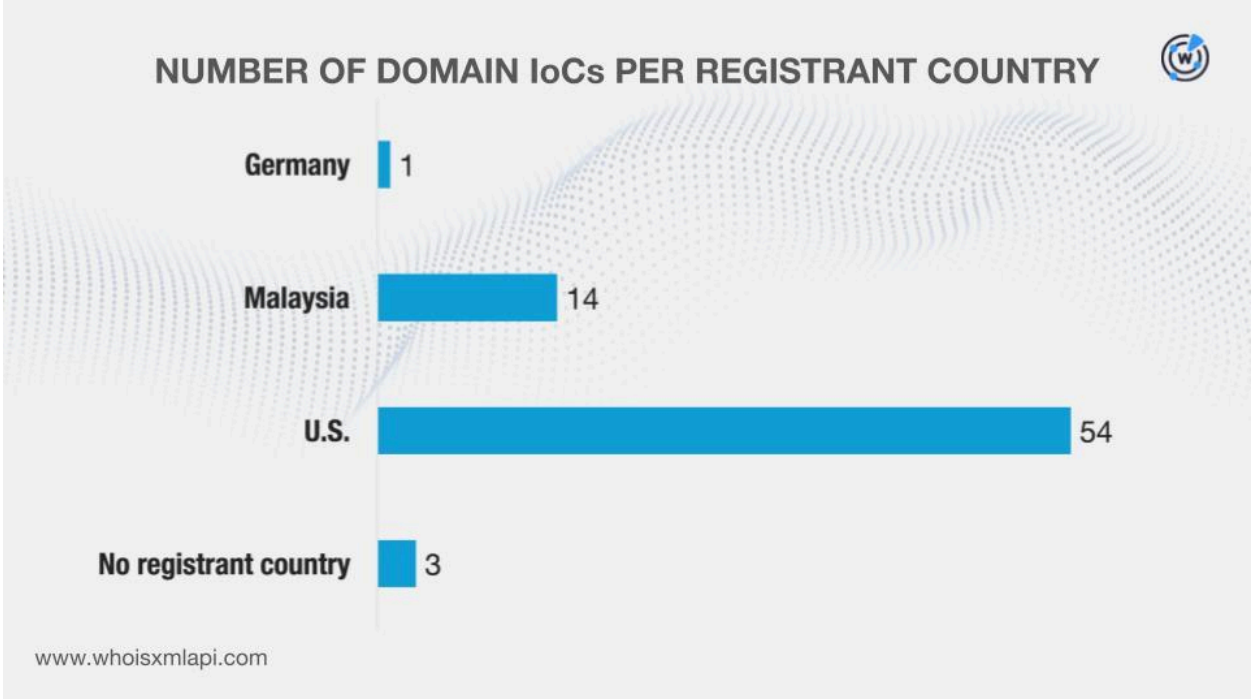
- While a vast majority—71 to be exact—were relatively newly registered, one was notably aged.




- They were administered by six registrars.




- While three domain IoCs did not have registrant countries on record, the remaining 69 were registered in three countries.



Finally, we queried the domain IoCs on DNS Chronicle API and found out that all 72 recorded 981 historical domain-to-IP resolutions over time. Here are more details for five examples.

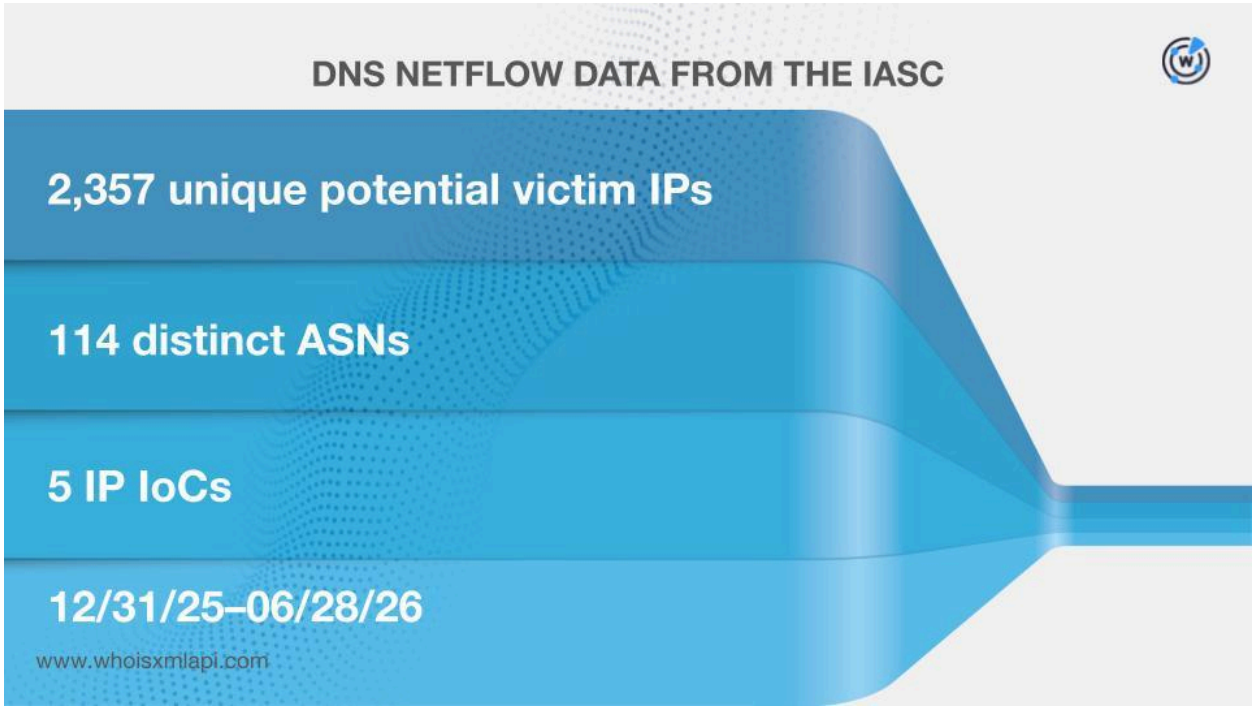
| DOMAIN IoC | NUMBER OF DOMAIN-TO-IP RESOLUTIONS | DATES SEEN |
|---|---|---|
| heliosup[.]info | 142 | 02/28/20–05/14/26 |
| haobbao[.]com | 115 | 06/25/18–05/19/26 |
| lestresot[.]info | 16 | 04/02/26–05/25/26 |
| visaphoto-secure[.]info | 16 | 04/16/26–05/26/26 |
| photo-box[.]info | 13 | 02/06/17–05/28/26 |

While 71 domain IoCs were registered in 2026 as mentioned earlier, only 69 started posting domain-to-IP resolutions this year. That could indicate that the registrations of two of the relatively new domain IoCs lapsed and they were recently reregistered.

## Photo ZIP Campaign IP IoCs Investigated

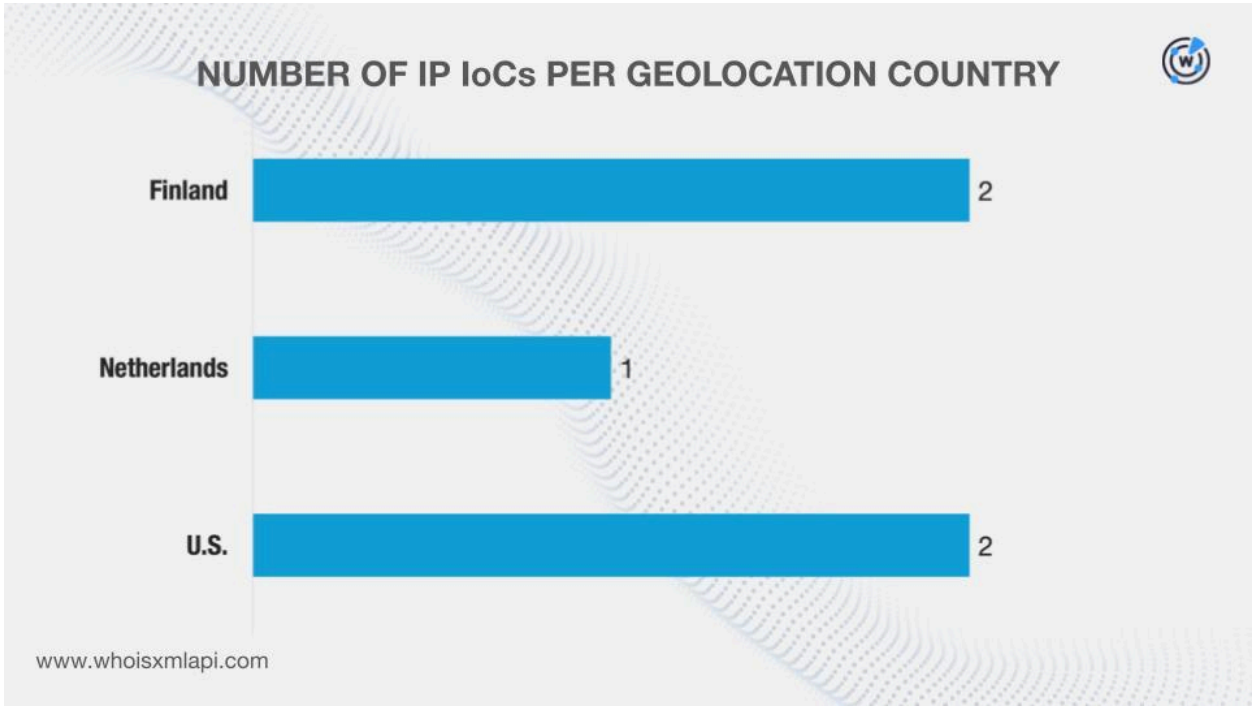
Now, on to the five IP IoCs.

First, sample network traffic data from the IASC showed that 2,357 unique IP addresses potentially owned by victims under 114 distinct ASNs communicated with the five IP IoCs between 31 December 2025 and 28 June 2026.

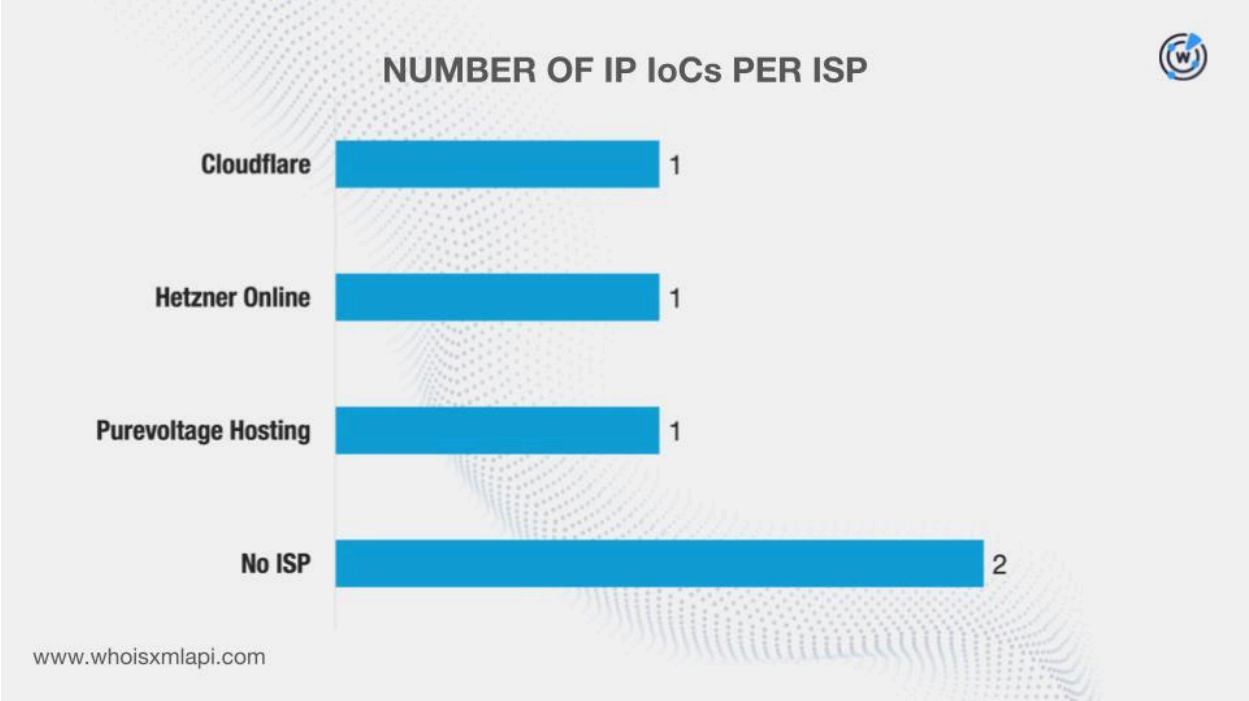



Next, we queried the IP IoCs on [Bulk IP Geolocation Lookup] and learned that:

- They were geolocated in three countries, one of which—the U.S.—was also named a registrant country.



- While two did not have ISPs on record, the remaining three were administered by three ISPs.




Finally, our DNS Chronicle API query results for the IP IoCs revealed that only three recorded historical IP-to-domain resolutions over time— 1,101 to be exact. The IP IoC 172[.]67[.]161[.]215, for instance, posted 1,000 resolutions from 26 May to 27 November 2020.

## Photo ZIP Campaign New Artifacts Collated

After learning more about the network IoCs, we jumped off them to uncover new possibly connected artifacts.

First, we queried the domain IoCs on WHOIS History API and learned that 23 had 75 email addresses in their historical records. Upon closer examination, we determined that 12 were public email addresses.

We then queried the public email addresses on Reverse WHOIS API and discovered that four could belong to domainers, hence their exclusion from further analysis. The remaining eight public email addresses, meanwhile, led to the discovery of 2,840 unique email-connected domains after those already dubbed as IoCs.

Next, we queried the email-connected domains on Threat Intelligence API and found out that 26 have already been weaponized for various threats. Here are more details for five examples.

| MALICIOUS EMAIL-CONNECTED DOMAIN | ASSOCIATED THREAT | DATES SEEN |
|---|---|---|
| admbooked[.]pro | Malware distribution | 05/06/26–06/26/26 |
| bjsdaklska283saik[.]com | Malware distribution | 06/04/26–06/27/26 |
| erifakd391lsja[.]com | Malware distribution | 05/06/26–06/26/26 |
| guestphotohot[.]pro | Malware distribution | 05/06/26–06/26/26 |
| haddjskak827sja[.]com | Malware distribution | 06/05/26–06/27/26 |

Note the similarity in first date seen—6 May 2026—for three of the examples above. This could be indicative of having been used for the same campaign. And there may be more malicious connected domains with the same first seen date.

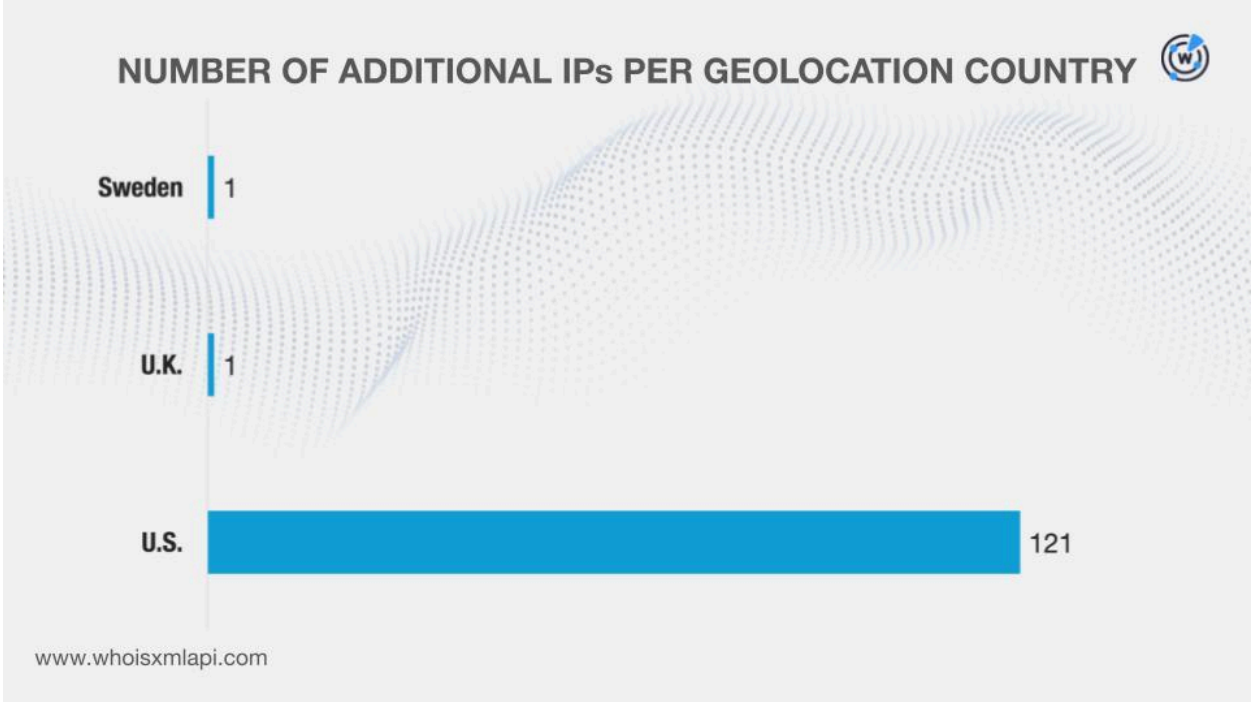
We then queried the domain IoCs on DNS Lookup API and uncovered 123 unique additional IP addresses.

After querying the additional IP addresses on Threat Intelligence API, we learned that they have all figured in various malicious campaigns. Take a look at more information for five examples below.

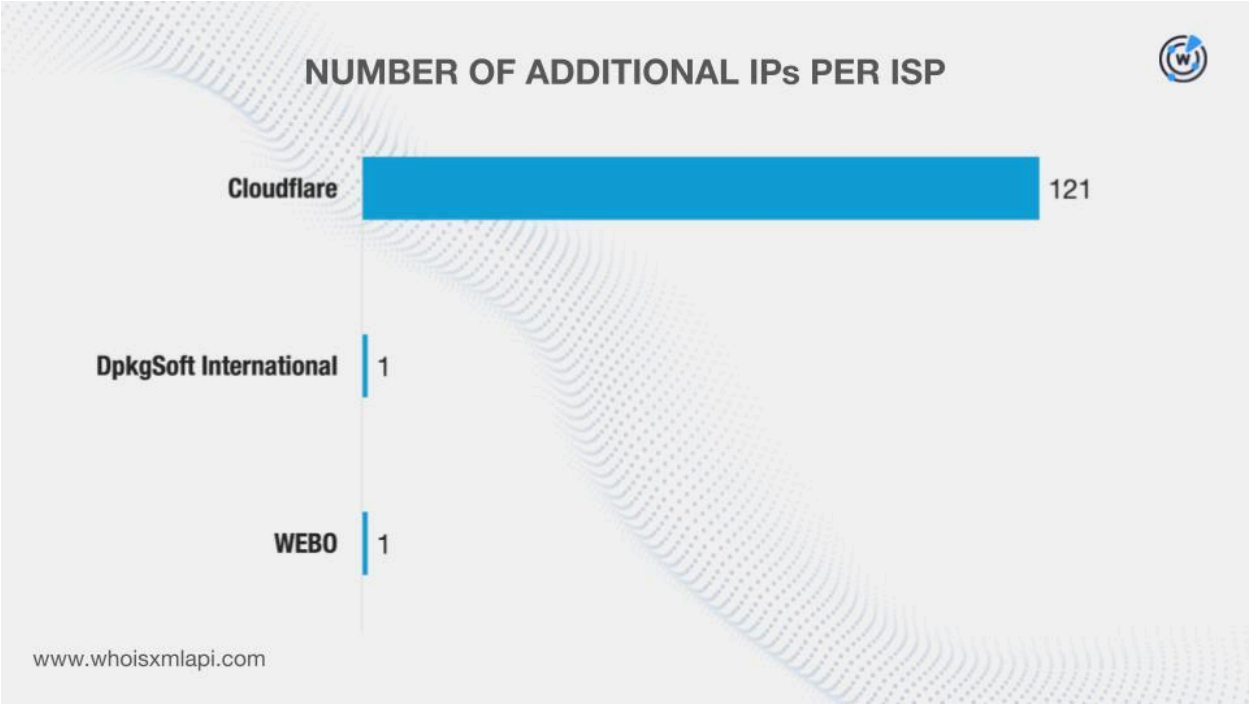
| MALICIOUS ADDITIONAL IP ADDRESS | ASSOCIATED THREAT | DATES SEEN |
|---|---|---|
| 104[.]21[.]0[.]190 | Malware distribution | 10/27/24–06/26/26 |
| 172[.]65[.]211[.]209 | Phishing | 06/13/26–06/13/26 |
| 185[.]107[.]74[.]11 | Attack<br>Spam campaign | 05/22/26–06/27/26<br>05/15/26–06/27/26 |
| 77[.]91[.]97[.]85 | Spam campaign<br>Attack<br>Malware distribution | 08/01/23–06/27/26<br>05/22/26–06/27/26<br>06/04/26–06/26/26 |
| 104[.]21[.]10[.]142 | Phishing<br>Malware distribution | 04/08/23–06/28/26<br>10/27/24–06/18/26 |

Next, we queried the additional IP addresses on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in three countries, only one of which—the U.S.—was shared by the IP IoCs.




- They were administered by three ISPs, only one of which—Cloudflare—was shared by the IP IoCs.




Now, we had 128 IP addresses in all—five IoCs and 123 additional ones—for this part of our analysis. We queried them on Reverse IP API and discovered that only four could be dedicated hosts. Together, they hosted 144 unique IP-connected domains after those already named as IoCs and the email-connected domains were filtered out.

Next, we zoomed in on the domain IoCs and extracted 72 unique text strings. We searched for domains other than those already listed as IoCs and email- and IP-connected via Domains & Subdomains Discovery using the **Domains only** and **Starts with** parameters. We uncovered connections for these strings:

- dancamp.
- deeprace.
- fairyspells.
- finallyrain.
- heliosup.
- joincroud.
- ministrew.
- photo-21473.
- photo-box.
- photo-dekor.
- prejointl.
- recallnine.
- snapkeep.

All in all, we found 95 unique string-connected domains after those tagged as IoCs and the email- and IP-connected domains were filtered out.

Note that the string-connected domains only serve to reflect the overall popularity of the strings extracted from the IoCs. As such, determining their legitimacy may require further investigation.

## Final Word

Our DNS infrastructure investigation of the massive photo ZIP campaign revealed that two unique client IP addresses communicated with three domain IoCs while 2,357 distinct IP addresses potentially owned by victims communicated with five IP IoCs, both according to our analysis of sample network traffic data from the IASC.

In addition, we learned that five domain IoCs appeared in four typosquatting groups while one domain IoC was likely registered with malicious intent.

Our IoC list expansion, meanwhile, turned up 3,202 new artifacts comprising 2,840 email-connected domains, 123 additional IP addresses, 144 IP-connected domains, and 95 string-connected domains. It is also worth noting that, to date, 149 of these artifacts have already been confirmed malicious.

***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

- 01011001[.]com
- 020jhsy[.]com
- 020xiegui[.]com
- a2kg70kg[.]com
- aabb99[.]cn
- abcmultimedia[.]net
- b-fund2014[.]com
- babespenthouse[.]com
- baby17go[.]cn
- c3255[.]cn
- c3dsm[.]com
- c4573[.]cn
- d5r1vnn[.]cn
- d97m[.]cn
- dafengtrade[.]com
- e-kai[.]cn
- e-zhizhu[.]com
- e9nd1f54[.]cn
- f3tgocu[.]cn
- f9nf[.]cn
- fa814888[.]cn
- g121314[.]com
- gangqinjianpu[.]cn
- ganxif[.]com
- h0797[.]com
- h196[.]net
- h20camollc[.]com
- i-dvr[.]cn
- i-muco[.]com[.]cn
- i1419[.]cn
- jamymall[.]cn
- jassecurity[.]com
- javierarmaolea[.]com
- kaarh[.]com
- kaixuanyushi[.]com
- kamigatastyle[.]jp
- l7knibv[.]cn
- laishijing-baijiu[.]com[.]cn
- lanaot[.]com
- m-honma[.]com
- maevaidosa[.]com
- magentoproduct[.]com
- n0yaj8n[.]cn
- n1488[.]cn
- nailb888[.]com
- oasgk[.]com
- office198[.]com
- ofjzzs[.]com
- p2p-print[.]cn
- p676[.]cn
- pa135[.]cn
- qdbujuyige[.]com
- qddysjc[.]com
- qdhtsy[.]com
- r2sbot[.]com
- r6187[.]cn
- raiwit[.]com
- s6312[.]cn
- sadilinikad[.]com
- saibeiyang[.]com
- taadawx[.]com
- tailijing[.]com
- taiokedu[.]com
- u0572[.]cn
- u087wep[.]cn
- u118[.]cn
- v-delite[.]cn
- v2312[.]cn
- v7111[.]cn
- w-script[.]com
- w7528[.]cn
- waihuirensheng[.]com
- xa-18[.]cn
- xagfdq[.]cn

- xarthg[.]com
- y1958[.]cn
- y3357[.]cn
- y4katgsi7[.]cn
- z-fz[.]cn
- zai-zai[.]cn
- zaoju360[.]com

## Sample Additional IP Addresses

- 104[.]21[.]0[.]190
- 104[.]21[.]10[.]142
- 104[.]21[.]15[.]104
- 172[.]65[.]211[.]209
- 172[.]67[.]128[.]54
- 172[.]67[.]130[.]11
- 185[.]107[.]74[.]11
- 77[.]91[.]97[.]85

## Sample IP-Connected Domains

- 1243n[.]com
- 1xique[.]app
- 200101[.]vip
- a9vz3[.]shop
- aichubao[.]com
- alli[.]xn--q9jyb4c
- b4pes[.]com
- bbm-1[.]shop
- bbm-3[.]shop
- cdnlyweb[.]com
- cfzjy[.]com
- chinarantai[.]com
- dfghjjihvb[.]shop
- drqj5[.]buzz
- dymtr[.]com
- exp[.]gname[.]net
- ff506[.]com
- fyptq[.]cn
- g0kj1op13[.]shop
- g0kj1op27[.]shop
- g0kj1op34[.]shop
- haodaibao[.]com
- hchqn[.]app
- ig23[.]vip
- ig28[.]vip
- ig32[.]vip
- jiefuhgzdzn[.]com
- jintel[.]com[.]cn
- jshsk[.]com
- kaikai3368[.]vip
- kefu810[.]xyz
- kefu815[.]com
- lijun918[.]vip
- lixisy[.]com
- lmje96[.]vip
- mengqiqi11[.]vip
- mfcrsp10[.]buzz
- mtsyxtaz[.]com
- no-on[.]net
- notjnup[.]shop
- nzu31[.]shop
- p8kz5[.]com
- pehchanindia[.]com
- pinying-sougou[.]com
- qa853[.]com
- qiongbi123[.]vip
- qq110924[.]vip
- reviewdocky[.]com
- rhinstitutionalbf[.]icu
- rhtutionalnew[.]top
- saoh354[.]cc
- sdfangxiaoer[.]com
- sdy1990[.]vip
- thjjszp[.]com
- toniandguy-opticians[.]co[.]uk
- toniandguy-opticians[.]com

- v5354[.]com
- w-5226[.]co
- wanye168[.]vip
- whataeecn[.]icu
- xam338[.]top
- xfhs009[.]com
- xga1433[.]top
- y2584[.]com
- y2610[.]com
- y974811y[.]vip
- z54231677[.]vip
- zhou2020[.]vip
- zrgefami1n[.]com

## Sample String-Connected Domains

- dancamp[.]co
- dancamp[.]com
- dancamp[.]de
- deeprace[.]cfd
- deeprace[.]cl
- deeprace[.]com
- fairyspells[.]co[.]uk
- fairyspells[.]com
- fairyspells[.]studio
- finallyrain[.]com
- finallyrain[.]org[.]bb
- heliosup[.]com
- heliosup[.]ph
- heliosup[.]vg
- joincroud[.]org
- ministrew[.]ph
- photo-21473[.]co[.]bb
- photo-box[.]app
- photo-box[.]at
- photo-box[.]be
- photo-dekor[.]ru
- prejointl[.]ph
- recallnine[.]com
- recallnine[.]stream
- snapkeep[.]ai
- snapkeep[.]app
- snapkeep[.]cn