WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A DNS Investigation of Shadow-Earth-053

Threat Report

Table of Contents

Executive Report

Shadow-Earth-053, a recently identified set of China-aligned campaigns, targeted government entities and critical infrastructure across South, East, and Southeast Asia and a NATO member state.

The group behind the attack exploited N-day vulnerabilities in Internet-facing Microsoft Exchange and IIS servers then deployed GODZILLA to maintain persistent access and stage ShadowPad implants via DLL sideloading of legitimate signed executables.

Trend Micro's in-depth analysis of the threat identified 26 network IoCs comprising subdomains, domains, and IP addresses.

We extracted domains from the subdomain IoCs, which left us with 10 domain IoCs for our own investigation. According to the WhoisXML API MCP Server, none of the domains were legitimate and all were currently active. We thus ended up with 31 IoCs for further study comprising 16 subdomains, 10 domains, and five IP addresses.

Our DNS deep dive into Shadow-Earth-053 led to these discoveries:

- 865 unique client IP addresses that communicated with three of the domain IoCs
- Two domain IoCs that were likely registered with malicious intent
- 10 distinct IP addresses potentially owned by victims that communicated with three of the IP IoCs
- 835 email-connected domains
- Nine additional IP addresses, seven of which were confirmed malicious
- Nine IP-connected domains, one of which was confirmed malicious
- 749 string-connected domains, six of which were confirmed malicious

Shadow-Earth-053 Subdomain IoCs in the Spotlight

We began our investigation by taking a closer look at the 16 subdomain IoCs.

The WhoisXML API MCP Server revealed that they were part of a cohesive, purpose-built threat actor infrastructure and not a random collection of suspicious domains. They, in fact, shared overlapping tradecraft and together described a complete kill chain—a rogue DNS resolution led to router compromise to traffic interception to credential harvesting to persistence. The table below shows specific details for each subdomain.

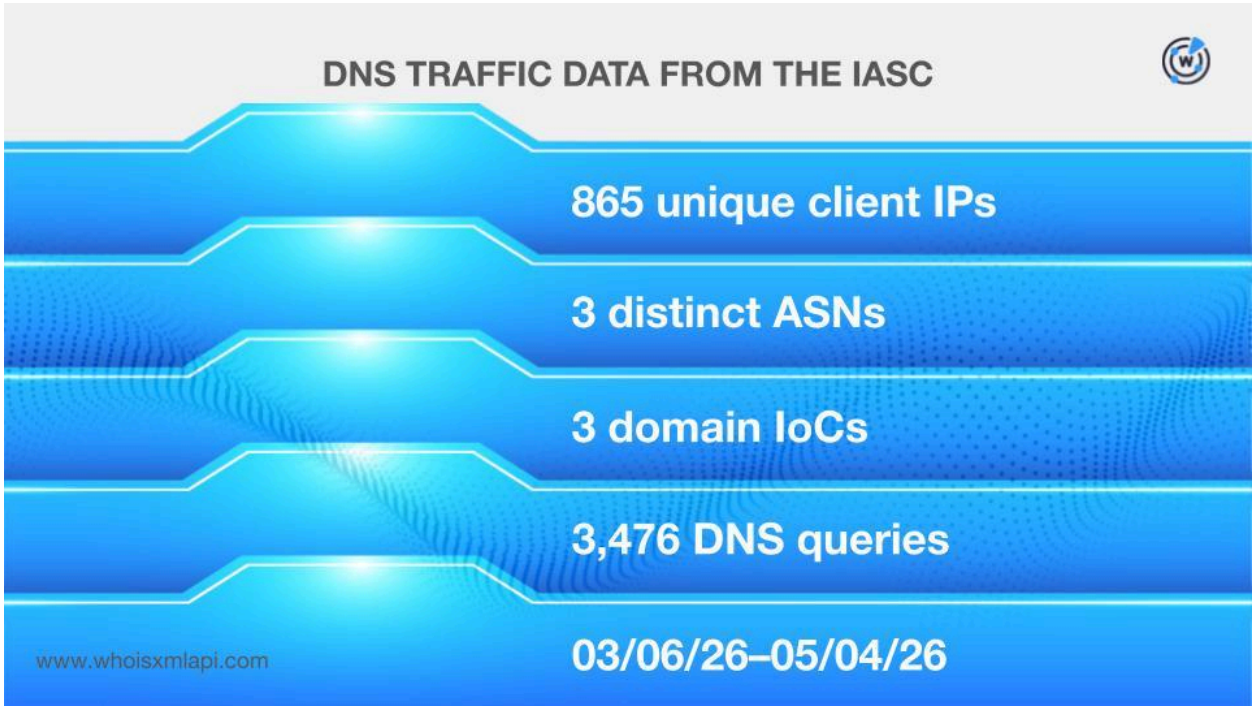
SUBDOMAIN IoC	WXA MCP SERVER FINDING
cert[.]kaspersky[.]icu	Likely targets industrial and security professionals; impersonates Kaspersky with a real CERT that uses kaspersky[.]com
erp[.]kaspersky[.]icu	Can serve fake login pages for Kaspersky's enterprise portal; acts as a credential theft vector
news[.]kaspersky[.]icu	Can distribute fake Kaspersky threat reports or malware disguised as software updates
ns1[.]kaspersky[.]icu	NS record allows full DNS control under a fake Kaspersky zone; is a hallmark of APT28's FrostArmada TTPs
ns2[.]kaspersky[.]icu	The previous NS paired with this form a complete operator-controlled DNS zone under the Kaspersky brand; has an identical risk profile to the previous NS; also mirrors APT28's FrostArmada NS infrastructure pattern
update[.]kaspersky[.]icu	Is dangerous in that it can serve trojanized software update packages; mirrors Evasive Panda's DNS poisoning TTP that hijacked legitimate software updater domains to deliver MgBot malware
ns1[.]group-ib[.]icu	Impersonates cybersecurity firm Group-IB to lower victims' guard; mirrors APT28's infra pattern
ns2[.]group-ib[.]icu	This paired with the previous NS strongly indicates an operator-controlled DNS zone; has an identical threat profile to the previous NS
check[.]office365-update[.]com	Follows a classic Microsoft 365 credential harvesting pattern; used in campaigns targeting financial execs and government employees; consistent with APT28's FrostArmada domains
check[.]dnsmaps[.]com	DNS-adjacent naming designed to evade detection in network logs; is a pretext for malicious DNS resolver activity
dns[.]dnserver[.]life	Can be configured as a malicious DNS resolver similar to APT28's FrostArmada VPS nodes; the nonstandard TLD used for DNS infra is suspicious
nslookup[.]dnserver[.]life	Named after the standard DNS tool nslookup as a social engineering and evasion tactic since network

	logs will show nslookup[.]dnserver[.]life, which appears routine but is not; is consistent with APT operator tradecraft
router[.]dnserver[.]life	Directly mirrors APT28's FrostArmada TTPs connected to a SOHO router compromise and redirection to attacker-controlled servers; is consistent with a C&C or configuration endpoint for hijacked router DNS settings
ww12[.]dnserver[.]life	wwN subdomain patterns are used by domain parking services and CDN redirectors; on an already-suspicious parent domain, this likely functions as a traffic relay or redirect node for phishing or AitM operations
dns[.]dnsmap[.]icu	The strong combination of DNS infrastructure mimicry and the .icu TLD is strongly indicative of malicious intent; likely a rogue resolver or an AitM node
time[.]microsofttrends[.]com	time subdomains are commonly used for C&C beaconing periodic check-ins disguised as NTP or telemetry traffic; combined with microsofttrends[.]com, this is a high-confidence malicious domain that likely serves as C&C infrastructure or AitM endpoint; consistent with nation-state actor tradecraft

Shadow-Earth-053 Domains IoCs Dissected

Next, we dug deeper into the 10 domain IoCs.

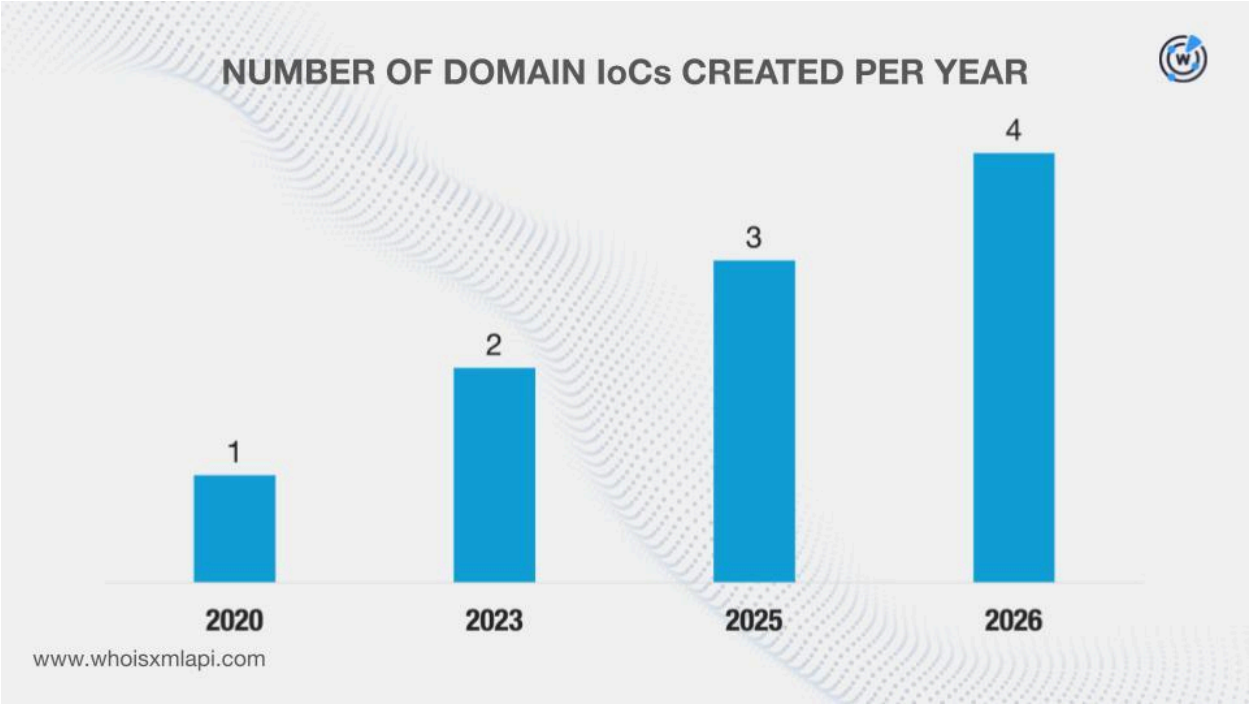
Sample network traffic data from the IASC revealed that 865 unique client IP addresses under three distinct ASNs communicated with three of the domain IoCs via 3,476 DNS queries made between 6 March and 4 May 2026.



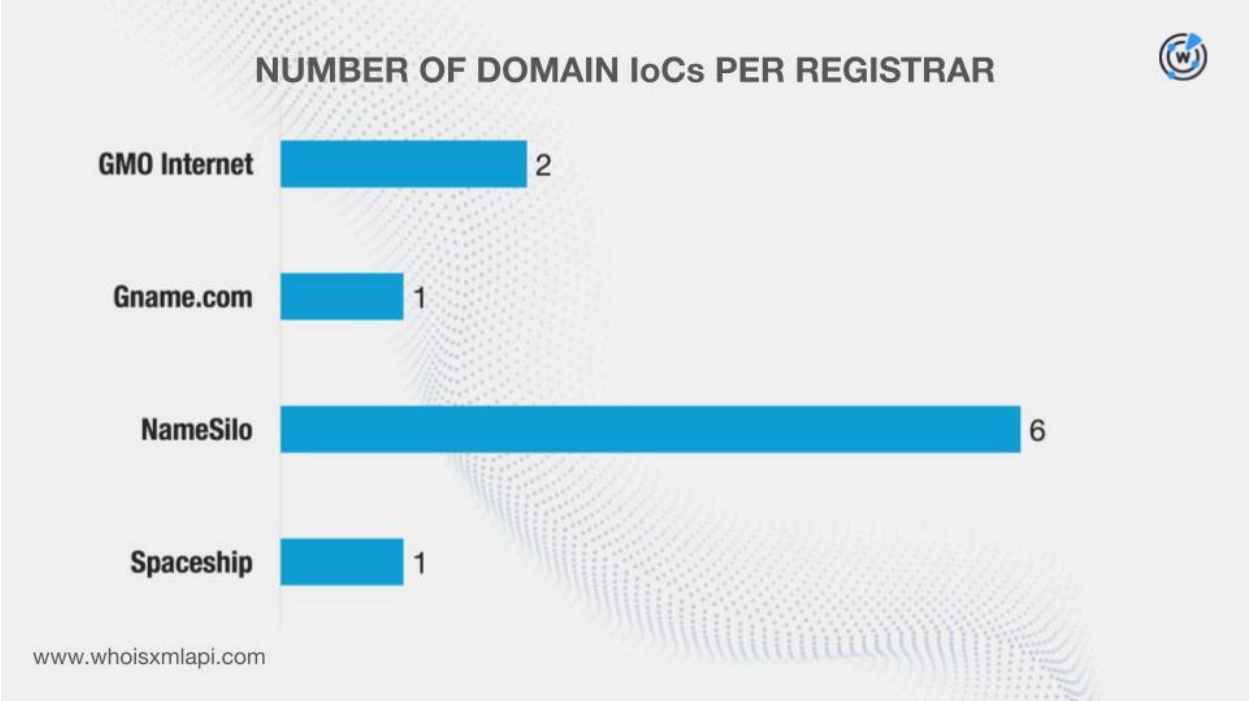
In addition, we discovered that two domain IoCs—zimbra-beta[.]info and office365-update[.]com—were recorded on the First Watch Malicious Domains Data Feed. They were likely registered with malicious intent 727 and 161 days, respectively, before they were tagged as IoCs on 30 April 2026.

Next, we queried the domain IoCs on WHOIS API and found out that:

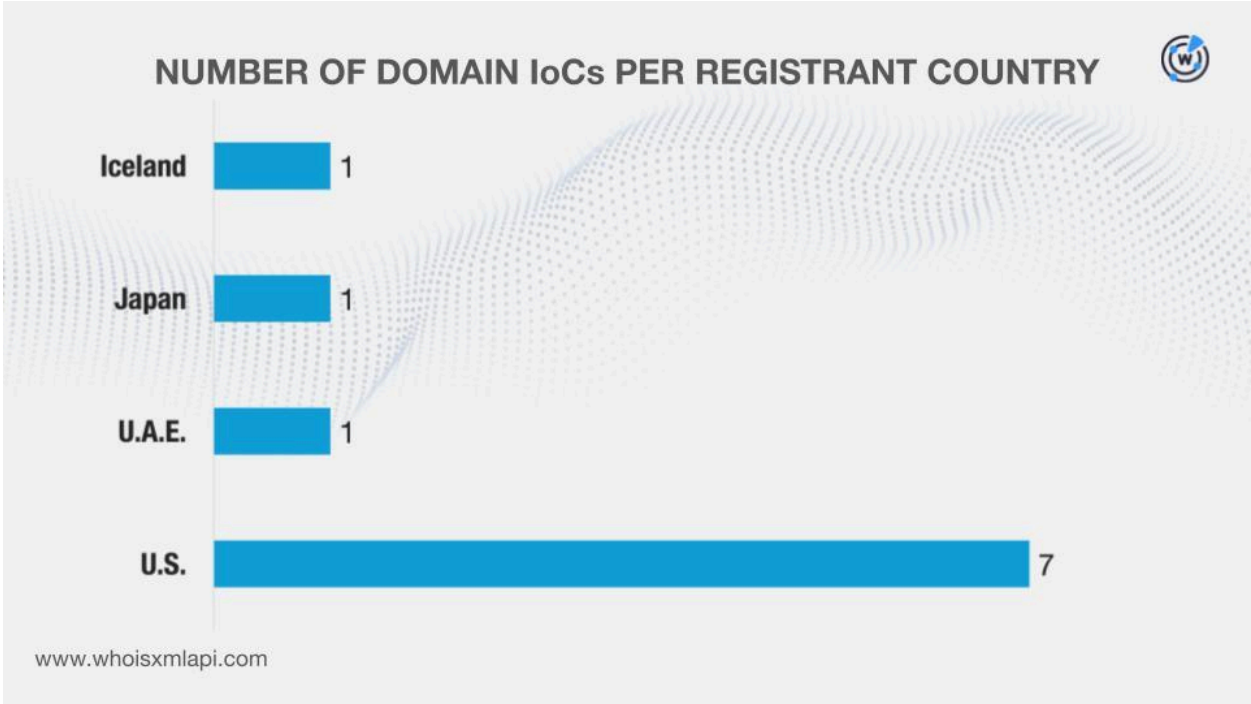
- They were created between 12 March 2020 and 9 April 2026, hinting that the attackers did not have a preference with regard to domain age.



- They were administered by four different registrars.



- They were registered in four different countries.



We then queried the domain IoCs on DNS Chronicle API and discovered that nine recorded 1,297 historical domain-to-IP resolutions over time. Here are more details for five examples.

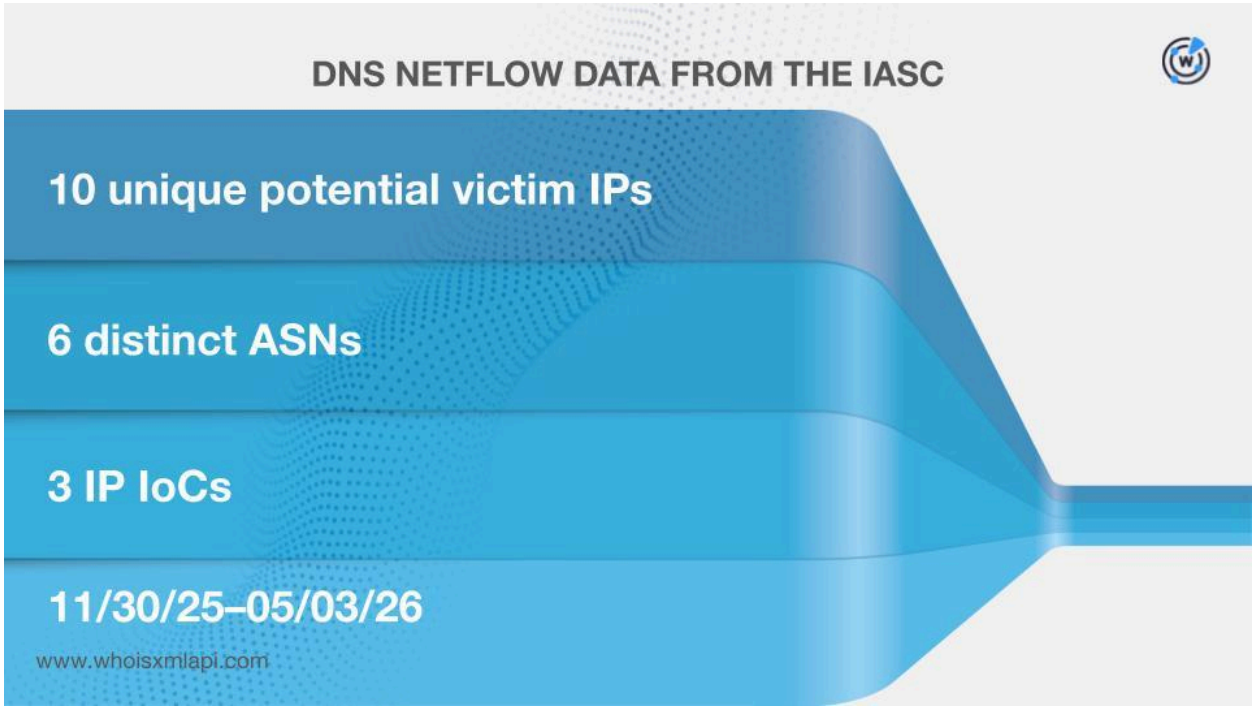
DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
microsofttrends[.]com	726	02/06/17–05/03/26
office365-update[.]com	194	02/06/17–05/03/26
dnserver[.]life	193	08/17/23–08/15/25
kaspersky[.]icu	64	12/01/18–05/06/23
zimbra-beta[.]info	64	05/15/24–04/14/26

To date, seven domain IoCs continued to resolve to IP addresses this year. These were dnsmaps[.]com, group-ib[.]icu, microsi0ft[.]com, microsofttrends[.]com, office365-update[.]com, zimbra-beta[.]info, and zimbra[.]life.

Shadow-Earth-053 IP IoCs Investigated

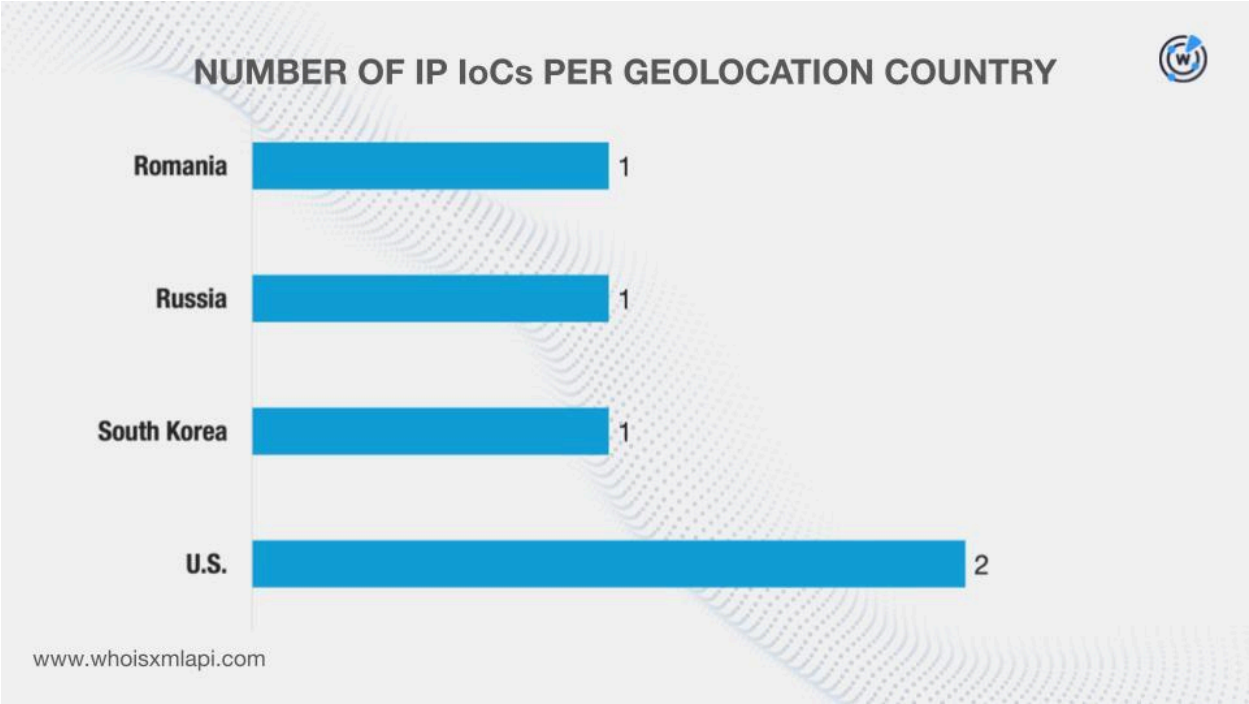
Here, we further investigated the five IP IoCs.

First, sample network traffic data from the IASC showed that 10 unique IP addresses potentially owned by victims under six distinct ASNs communicated with three of the IP IoCs between 30 November 2025 and 3 May 2026.

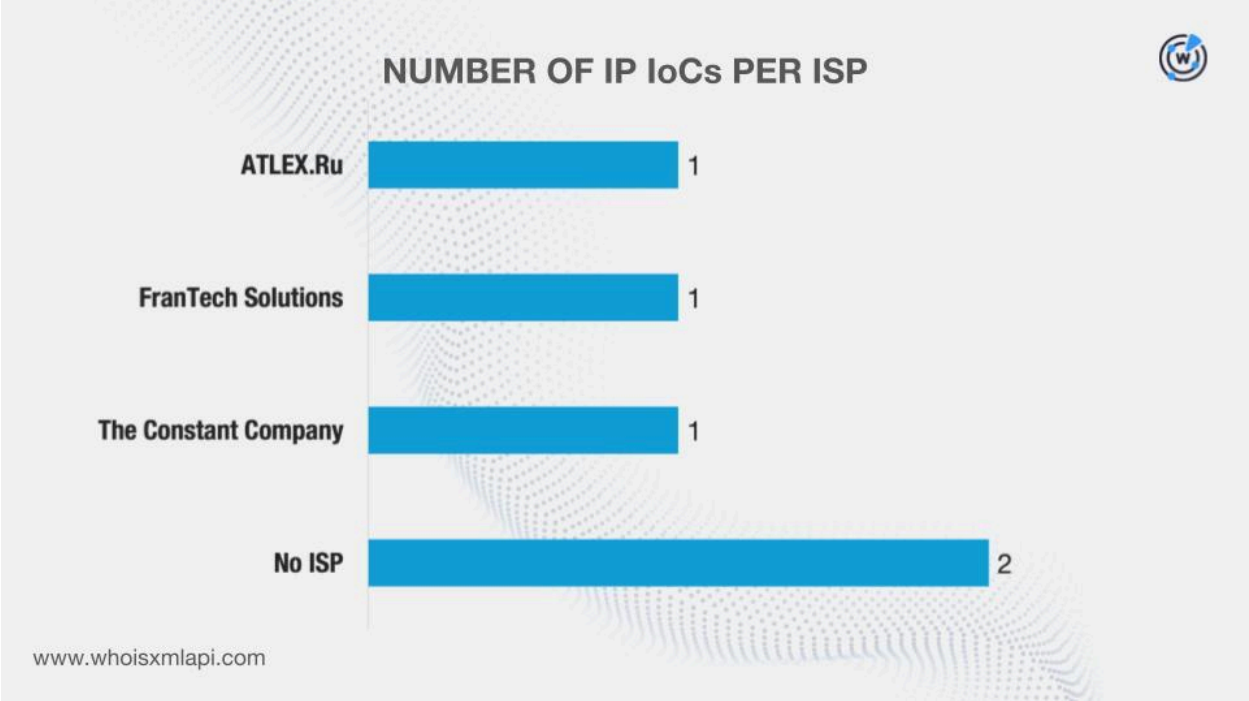


We then queried the IP IoCs on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in four different countries, only one of which—the U.S.—was also on the registrant country list.



- While two of them did not have ISPs on record, the remaining three were administered by a different ISP each.



Next, we queried the IP IoCs on DNS Chronicle API and found out that four posted 839 historical IP-to-domain resolutions over time. The IP address 194[.]38[.]11[.]3, for instance, recorded 757 resolutions between 6 February 2021 and 4 May 2026.

To date, three of the IP IoCs continued to resolve to domains this year.

New Shadow-Earth-053 Artifacts Exposed

In this section, we hunted down new artifacts that could be connected to Shadow-Earth-053.

We began by querying the 10 domain IoCs on WHOIS History API and discovered that eight had 32 email addresses in their historical WHOIS records. Closer scrutiny revealed that five were public email addresses.

We then queried the public email addresses on Reverse WHOIS API and found out that they were used to register 835 unique email-connected domains after the domain IoCs were filtered out.

Next, we queried the domain IoCs on DNS Lookup API, which led to the discovery of nine unique additional IP addresses.

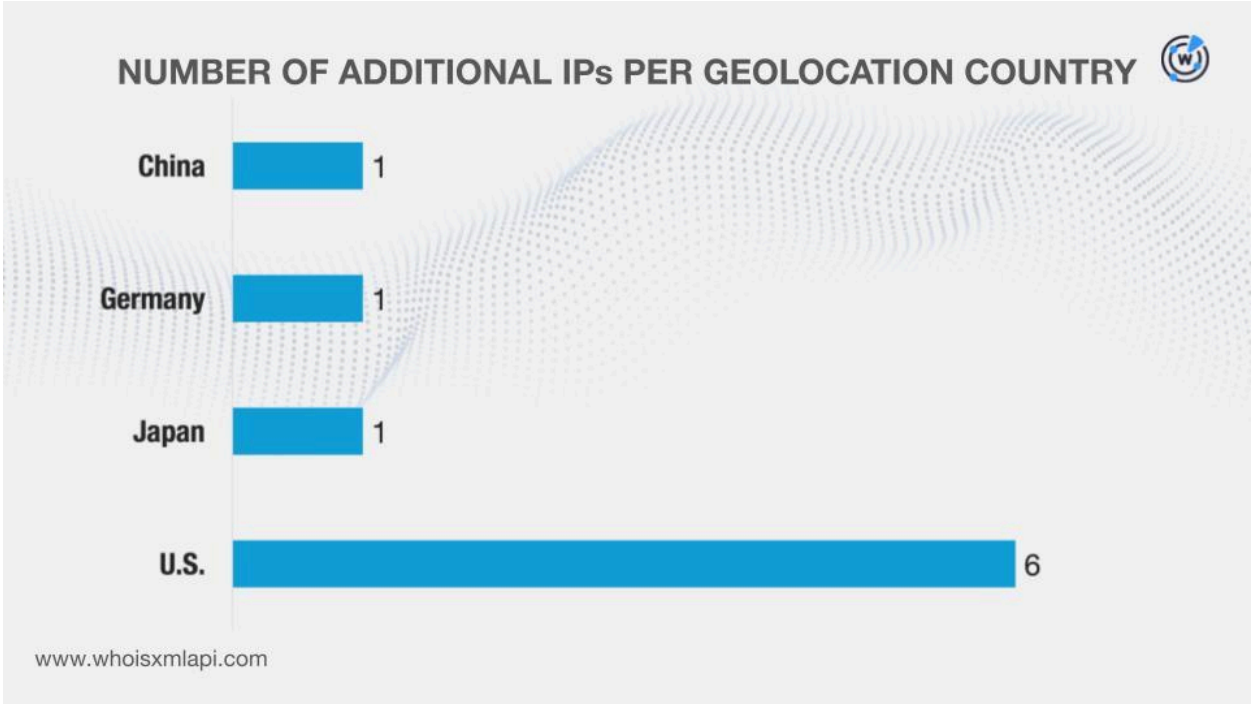
Threat Intelligence API queries for the additional IP addresses revealed that seven have already been weaponized for various attacks. Take a look at more details for five examples below.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
91[.]195[.]240[.]123	Phishing Malware distribution Generic threat Spam campaign	05/04/23–05/04/26 03/29/23–05/03/26 04/11/23–04/26/26 07/01/23–04/16/26
207[.]246[.]78[.]75	Malware distribution Phishing Generic threat	08/25/25–05/03/26 08/18/25–05/03/26 07/24/25–04/10/26
104[.]21[.]8[.]206	Malware distribution Phishing	11/22/24–05/03/26 03/28/23–04/10/26
160[.]16[.]200[.]77	Malware distribution Phishing	10/19/24–05/03/26 04/01/25–04/20/26

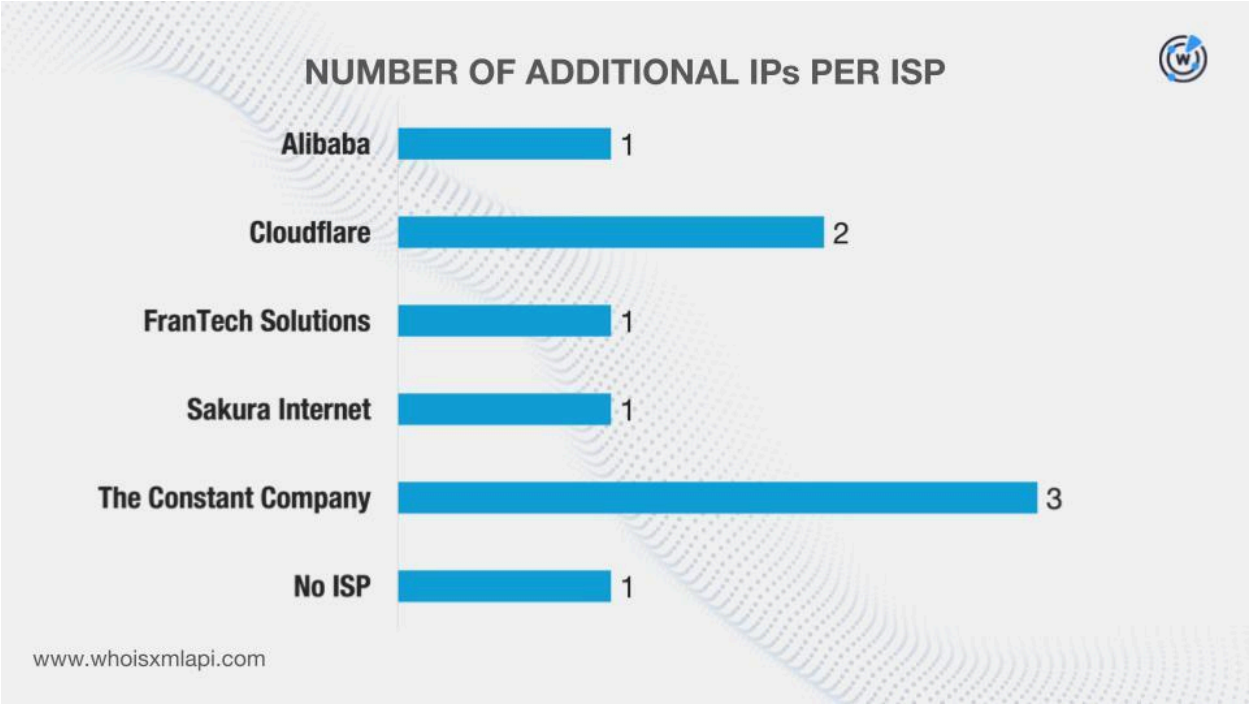
45[.]77[.]75[.]133	Malware distribution Phishing Generic threat	08/25/25–05/03/26 08/18/25–05/03/26 07/24/25–04/10/26

We then sought more information about the additional IP addresses using Bulk IP Geolocation Lookup. We discovered that:

- They were geolocated in four different countries, only one of which—the U.S.—was named an IoC geolocation country.



- While one did not have an ISP on record, the remaining eight were administered by five different ISPs. It is worth noting that two ISPs—FranTech Solutions and The Constant Company—were also part of the IoCs' ISP list.



After that, we now had 14 IP addresses—five IP IoCs and nine additional ones—for further analysis. Reverse IP API queries for them showed that five could be dedicated hosts. Together, they hosted nine unique IP-connected domains after the domain IoCs and the email-connected domains were filtered out.

Threat Intelligence API queries for the IP-connected domains revealed that one—check[.]office365-update[.]com—already figured in malware distribution between 11 December 2025 and 3 May 2026.

Next, we extracted 10 unique text strings from the domain IoCs. We then used Domains & Subdomains Discovery to uncover domains that started with the strings we identified. We uncovered 749 unique string-connected domains after the domain IoCs and the email- and IP-connected domains were filtered out. They started with these strings:

- dnserver.
- dnsmap.
- dnsmaps.
- group-ib.
- kaspersky.
- office365-update.
- zimbra.

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, especially those that contained the names of legitimate companies like Group-IB and Kaspersky, may require further investigation.

Threat Intelligence API queries for the string-connected domains revealed that six have already been weaponized for various malicious campaigns. Here are three examples.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
kaspersky[.]host	Malware distribution	03/09/23–05/03/26
office365-update[.]co	Malware distribution	03/09/23–05/03/26
zimbra[.]page	Malware distribution	02/22/25–05/03/26

Final Thoughts

Our DNS deep dive into the inner workings of Shadow-Earth-053 revealed that 865 unique client IP addresses communicated with three of the domain IoCs. We also learned that two of the domain IoCs were likely registered with malicious intent. In addition, we determined that 10 unique IP addresses that could belong to victims communicated with three of the IP IoCs.

We also discovered 1,602 new artifacts comprising 835 email-connected domains, nine additional IP addresses, nine IP-connected domains, and 749 string-connected domains. Note, too, that 14 of these artifacts have already figured in various threat campaigns.

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

- 06depo[.]com
- 1mapy[.]cz
- 24dientes[.]com
- abbotmain[.]com
- abicflorida[.]com
- aboubakar-fofana[.]com
- badevlad[.]com
- barbodegasd[.]com
- barceloformentor[.]com
- cabmaddux[.]com
- cafehidalgofullerton[.]com
- caffeconcertomodena[.]com
- d0hnuts[.]com
- dabwaha[.]com
- danblacksound[.]com
- earthsorganicskincare[.]com
- eatnewcastlegateshead[.]com
- ebxloakal[.]com
- fa-carling[.]com
- fahrenheitsbooks[.]com
- fairmapscolorado[.]com
- gamesforweirdpeople[.]com
- gazagirlsbook[.]com
- geekroar[.]com
- haloheadphones[.]com
- hcnn[.]net
- healingmalorie[.]com
- ichromecastsetup[.]com
- idellseitel[.]com
- idreamoflinux[.]com
- jackietrent[.]com
- jacob-jensen[.]com
- jadelianature[.]com
- karicasady[.]com
- kashar[.]net
- katalinakicks[.]com
- la-tyrolienne[.]com
- lacienegafarmersmarket[.]com
- lakesimcoearms[.]com
- macsdrivein[.]net
- madhostel[.]com
- madplatternashville[.]com
- nanospireinc[.]com
- narrowsburghoneybeefest[.]com
- nastiacloutierignatiev[.]com
- obrienforseattle[.]com
- offthebeatentrackmovie[.]com
- offthebus[.]net
- pacedev[.]net
- paloaltochilicookoff[.]com
- panevinoesandaniele[.]net
- quemadura[.]net
- questforconsciousness[.]com
- quicklockapp[.]com
- raidcall-emsone[.]com
- raphaelsite[.]com
- reasonweekly[.]com
- sacemaquarterly[.]com
- sactownunion[.]com
- salescontrol[.]cz
- t-locator[.]cz
- tailspinshow[.]com
- talentedmrfox[.]com
- u-sophia[.]com
- u8watch[.]net
- ubs-ch2[.]com
- vanshowcase[.]com
- varidecicognani[.]com
- veggiewala[.]com
- washersettlementclaim[.]com
- watanili[.]com
- weatherlook[.]net
- xlogs[.]net
- xtrainvegas[.]com

- y-find[.]com
- yeatsday[.]com
- yehforgames[.]com
- zacktravel[.]com
- zadostovyjadreni[.]cz
- zexemplar[.]com

Sample Additional IP Addresses

- 104[.]21[.]8[.]206
- 160[.]16[.]200[.]77
- 172[.]67[.]130[.]161
- 198[.]98[.]52[.]206
- 207[.]246[.]78[.]75

Sample IP-Connected Domains

- ablemoongodland[.]mooo[.]com
- canadainsider[.]live
- danielhoffman[.]org
- nslookup[.]onedriver[.]live
- one[.]googledriver[.]group
- www[.]ablemoongodland[.]mooo[.]com

Sample String-Connected Domains

- dnserver[.]at
- dnserver[.]audnedaln[.]no
- dnserver[.]be
- dnsmap[.]app
- dnsmap[.]cf
- dnsmap[.]ch
- group-ib[.]ae
- group-ib[.]agency
- group-ib[.]arab
- kaspersky[.]abc[.]br
- kaspersky[.]academy
- kaspersky[.]ae
- office365-update[.]be
- office365-update[.]co
- office365-update[.]net
- zimbra[.]ae
- zimbra[.]ai
- zimbra[.]al