DNS Spotlight: The Silver Fox in the Henhouse

Table of Contents

Executive Report

Wearing a disguise has often worked when it comes to infiltrating well-protected targets. So long as threat actors stay in character, they could succeed with their ruse. And that is how Chinese APT group SilverFox managed to trick victims into thinking they were Russian. The actors used Cyrillic characters in their SEO poisoning campaign lures that deployed ValleyRAT.

Silver Fox abused Microsoft Teams to target Chinese organizations. They used ValleyRAT to conduct state-sponsored espionage for sensitive intelligence and engage in financial fraud and theft to fund their operations.

ReliaQuest originally identified 41 IoCs comprising six domains, 17 subdomains, and 18 IP addresses after analyzing the cyber attack in great depth. We investigated the Silver Fox infrastructure further and unearthed these discoveries:

- 2,357 unique client IP addresses communicated with one domain identified as an IoC
- Four domains identified as IoCs were bulk-registered with 3–4 look-alikes each
- Seven domains identified as IoCs were deemed likely to turn malicious 239–339 days before they were dubbed as such
- One potential victim IP address communicated with one domain identified as an IoC
- 45,949 email-connected domains, 51 of which turned out to be malicious
- Seven additional IP addresses, all of which turned out to be malicious
- 20 IP-connected domains
- 30 string-connected domains, one of which turned out to be malicious

A Closer Look at the Subdomains Identified as ValleyRAT IoCs

We started out by looking more closely at the 17 subdomains identified as IoCs using Jake AI. We learned that while none of them were inherently malicious, 16 were either uncategorized or inactive. We also found out that 15 of them, specifically those that started with the text string **teams.**, shared the same IP address.

Domain Information

The root domain, `xclyd.com`, was registered on **May 14, 2015**, making it one of the older domains in this group. Its registration is valid until May 14, 2026. Consistent with the majority of the other domains, the registrar is **Gname.com Pte. Ltd.**, and the owner's information is redacted for privacy.

DNS, Geolocation, and Security

The technical details are a perfect match. The subdomain `teams.xclyd.com` points directly to the IP address **103.112.99.135**. This server is located in **Hong Kong** and is part of the AROSS-AS network. My security scan found **no malicious activity**, and the website is currently **Uncategorized**.

The Big Picture

This is now the **fifteenth** domain that we have confirmed is part of this network, all pointing to the same server. The evidence of a single, coordinated operation is undeniable.

Here is the complete and updated list of all fifteen domains:

- `teams.xclyd.com`
- `teams.telegramzwxz.com`
- `teams.telegramtgxz.com`
- `teams.telegramgwxz.com`
- `teams.plsgongmu.com`
- `teams.kkkgenieyesl.cn` (Registrant: 李华炳)
- `teams.kensun4a.com`
- `teams.jqsnzp.com`
- `teams.hardepc.com`
- `teams.geroman.com`
- `teams.fjzwb.com`
- `teams.fin-tastikantioch.com`
- `teams.cpeakem.com`
- `teams.chetanagarbatti.com`
- `teams.baoyingkeji.com`

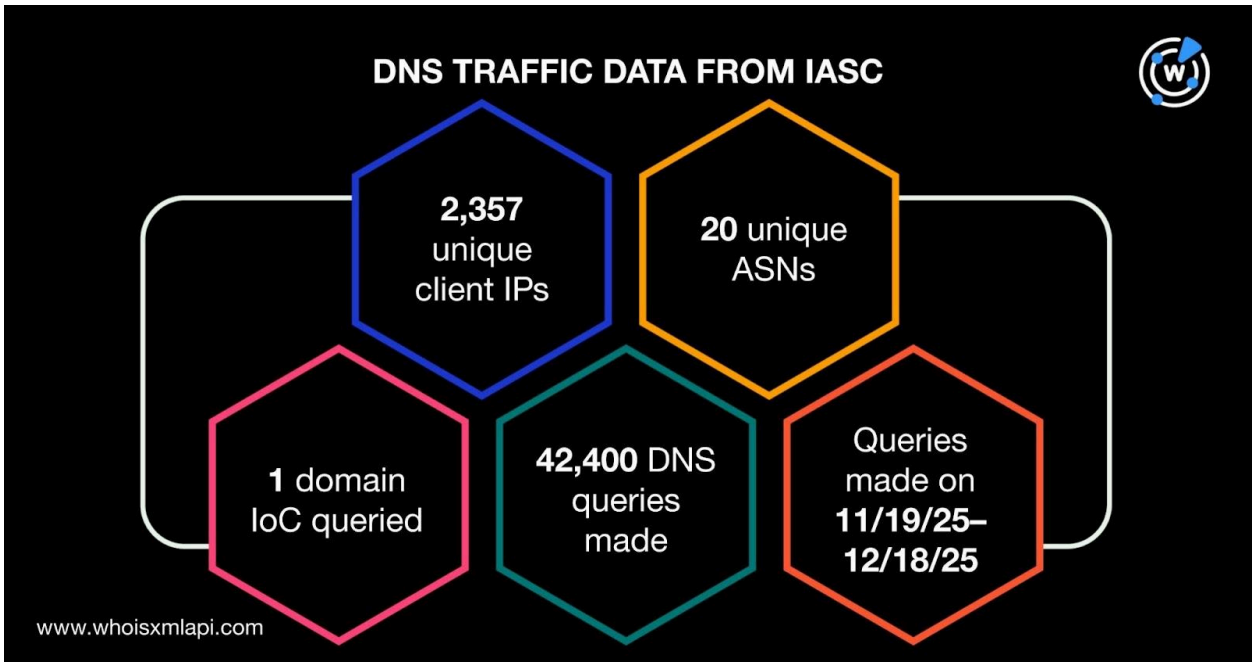
All fifteen domains share the same operational DNA: they resolve to the same IP address in Hong Kong, use the "teams" subdomain, and are uncategorized and non-malicious. The public registration of `teams.kkkgenieyesl.cn` to "李华炳" remains the most significant clue to the identity of the person or entity behind this extensive and intriguing network.

*Jake AI result showing the similarity among the 15 subdomains that started with the string **teams.***

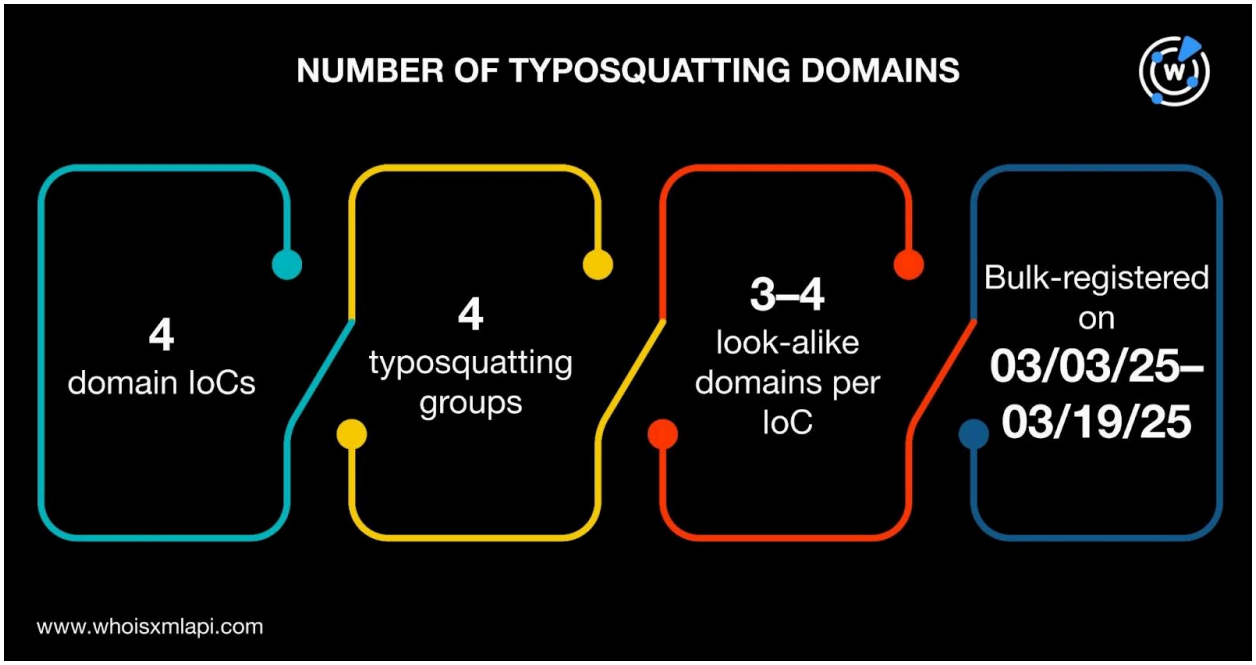
A More In-Depth Look at the Domains Identified as ValleyRAT IoCs

ReliaQuest originally identified six domains and 17 subdomains as IoCs as mentioned earlier. We extracted 17 unique domains from the 17 subdomains. Adding those to the six domains and ensuring none of them were duplicates brought the total number of unique domains to 23. We then checked if any of the 23 domains were owned by legitimate entities using the WhoisXML API MCP Server and took out three, which brought our final total number of domains for further analysis down to 20.

Sample network traffic data from the IASC revealed that 2,357 unique client IP addresses under 20 distinct ASNs communicated with one domain identified as an IoC via 42,400 DNS queries made between 19 November and 18 December 2025.



Data from the Typosquatting Data Feed, meanwhile, showed that four domains identified as IoCs were bulk-registered with 3–4 look-alikes each between 3 and 19 March 2025. A total of four typosquatting groups were found.

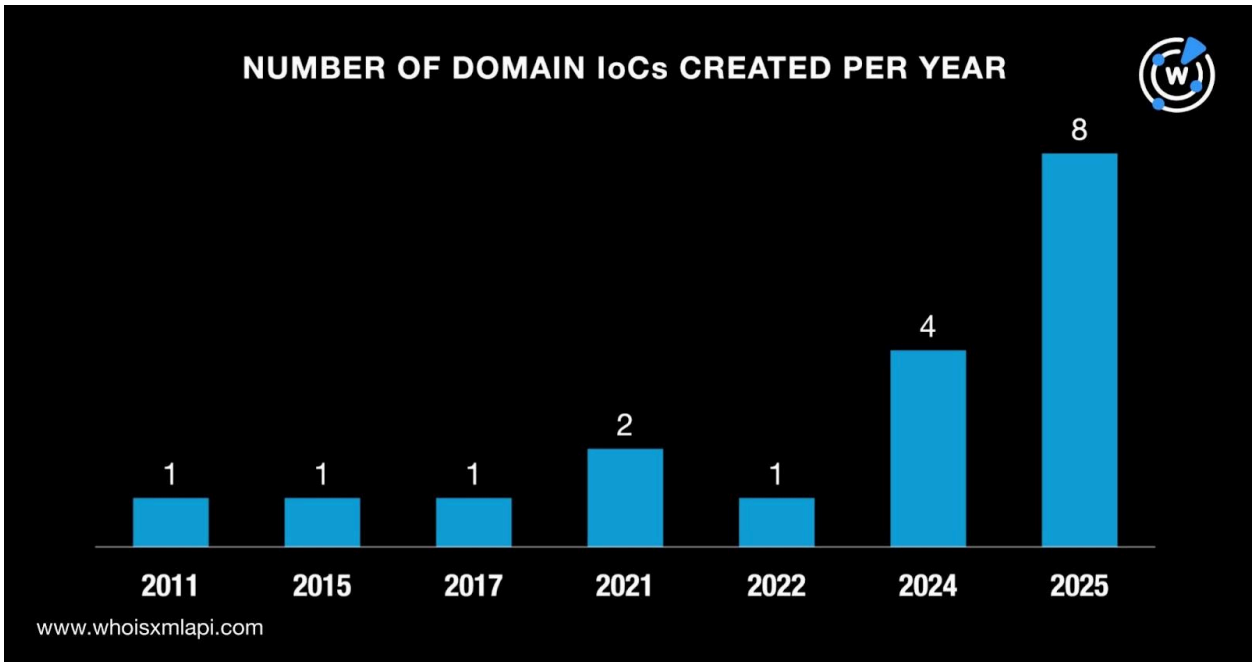


The results of our First Watch Malicious Domains Data Feed queries also revealed that seven domains identified as IoCs were deemed likely to turn malicious 239–339 before they were reported as such on 4 December 2025.

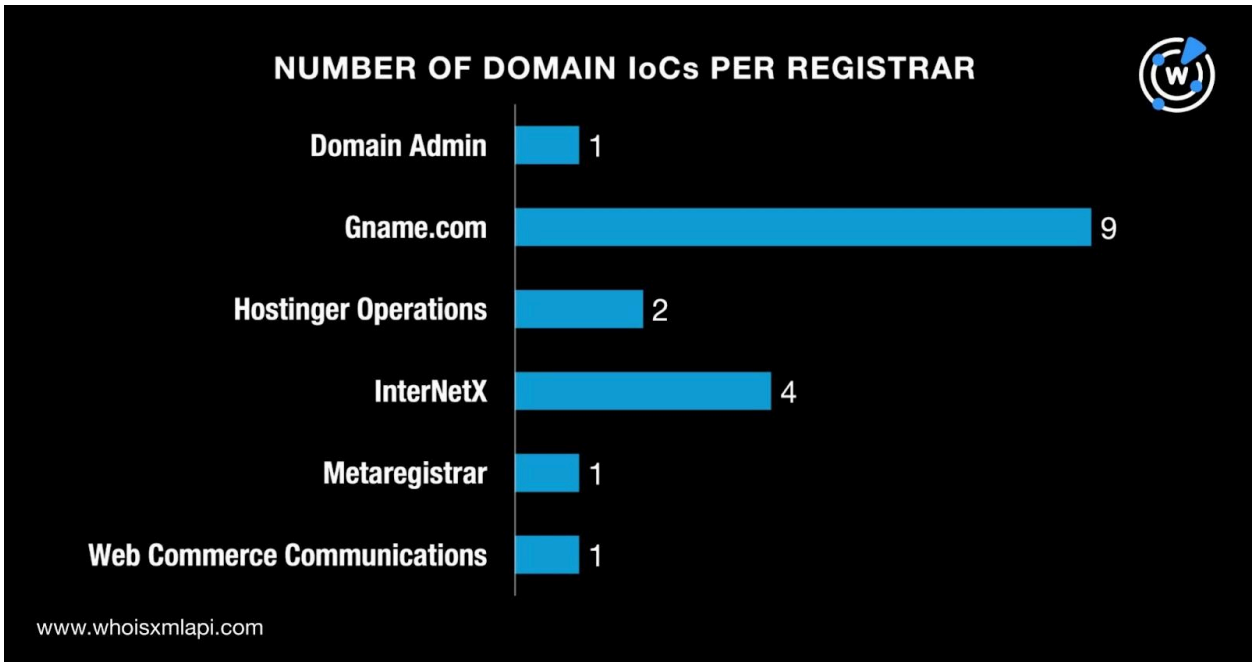
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE THE REPORT DATE
kkkgenieyesl[.]cn	12/30/24	339
teamszv[.]com	03/02/25	277
fjzwb[.]com	03/18/25	261
telegramgwxz[.]com	03/18/25	261
telegramtgxz[.]com	03/18/25	261

Next, we queried the 20 domains identified as IoCs on WHOIS API and discovered that only 18 had current WHOIS records. We limited our analysis for this section to the 18 domains with current WHOIS records. That said, we learned that:

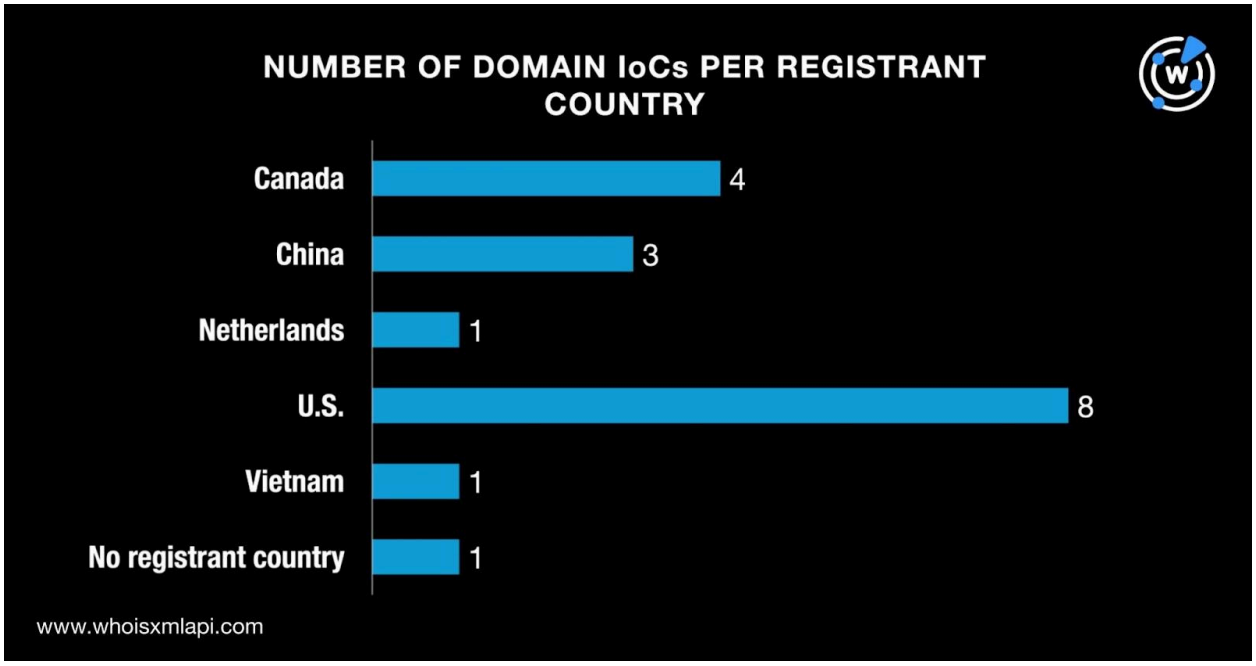
- They were created between 23 May 2011 and 9 April 2025. A majority of them, eight to be exact, were created in 2025; four in 2024; two in 2021; and one each in 2011, 2015, 2017, and 2022.



- They were administered by six registrars led by Gname.com, which accounted for nine domains. InterNetX administered four domains; Hostinger Operations managed two; and Domain Admin, Metaregistrar, and Web Commerce Communications managed one each.



- While one domain did not have a registrant country on record, the remaining 17 were registered in five countries topped by the U.S., which accounted for eight domains. Four domains were registered in Canada; three in China; and one each in the Netherlands and Vietnam.

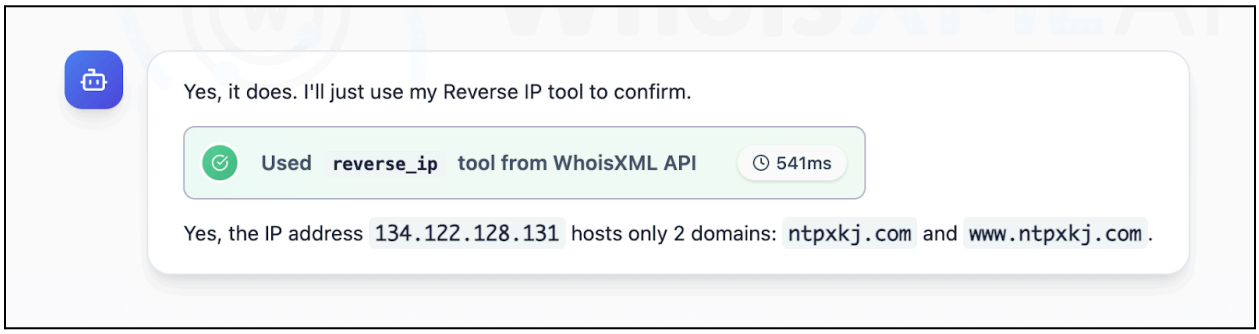


A DNS Chronicle API query for the 20 domains identified as IoCs revealed that only 18 had historical domain-to-IP resolutions. They posted a total of 2,729 resolutions over time. The domains baoyingkeji[.]com, fin-tastikantioch[.]com, and hardepc[.]com posted the oldest resolutions on 5 February 2017. Note that five other domains—chetanagarbatti[.]com, cpeakem[.]com, jqsnzp[.]com, kensun4a[.]com, and xclyd[.]com—posted resolutions in a matter of days after the first three did. This similarity could point to ownership by the same entity or, in this case, being part of the same attack infrastructure. Take a look at three examples below.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
baoyingkeji[.]com	260	02/05/17	02/10/25
fin-tastikantioch[.]com	492	02/05/17	01/09/24
hardepc[.]com	135	02/05/17	02/02/25

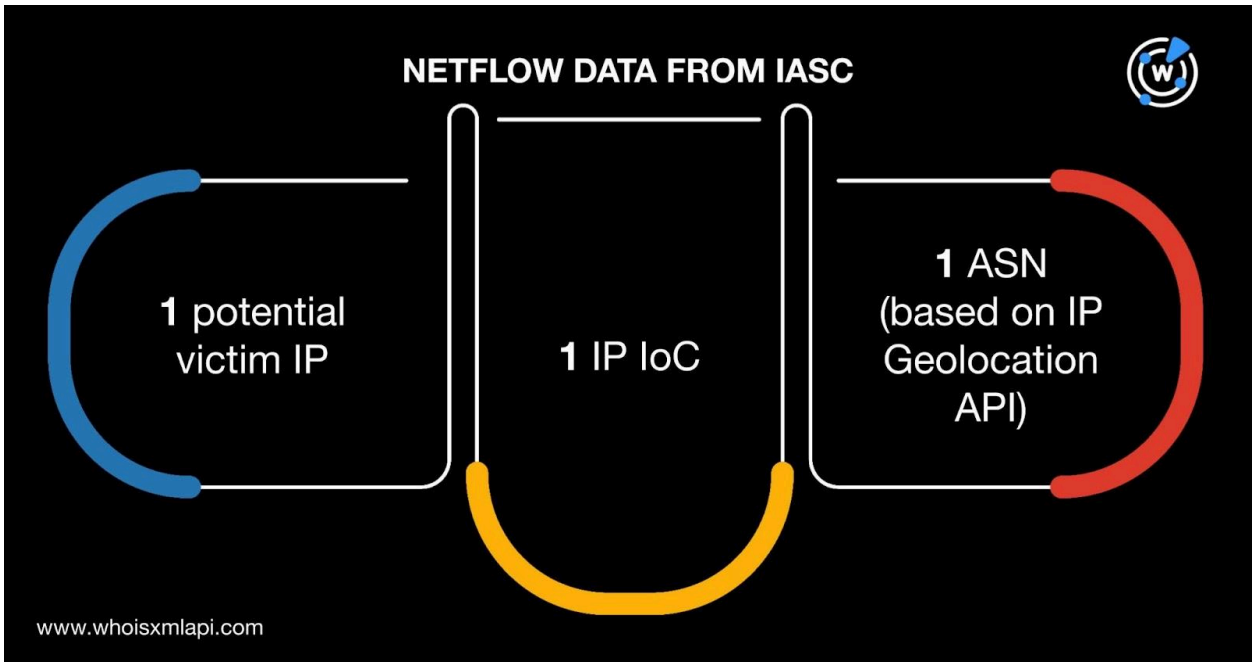
A Deep Dive into the IP Addresses Identified as ValleyRAT IoCs

Jake AI queries for the 18 IP addresses identified as IoCs revealed that 17 could be dedicated hosts.



Sample Jake AI result for the IP addresses identified as IoCs

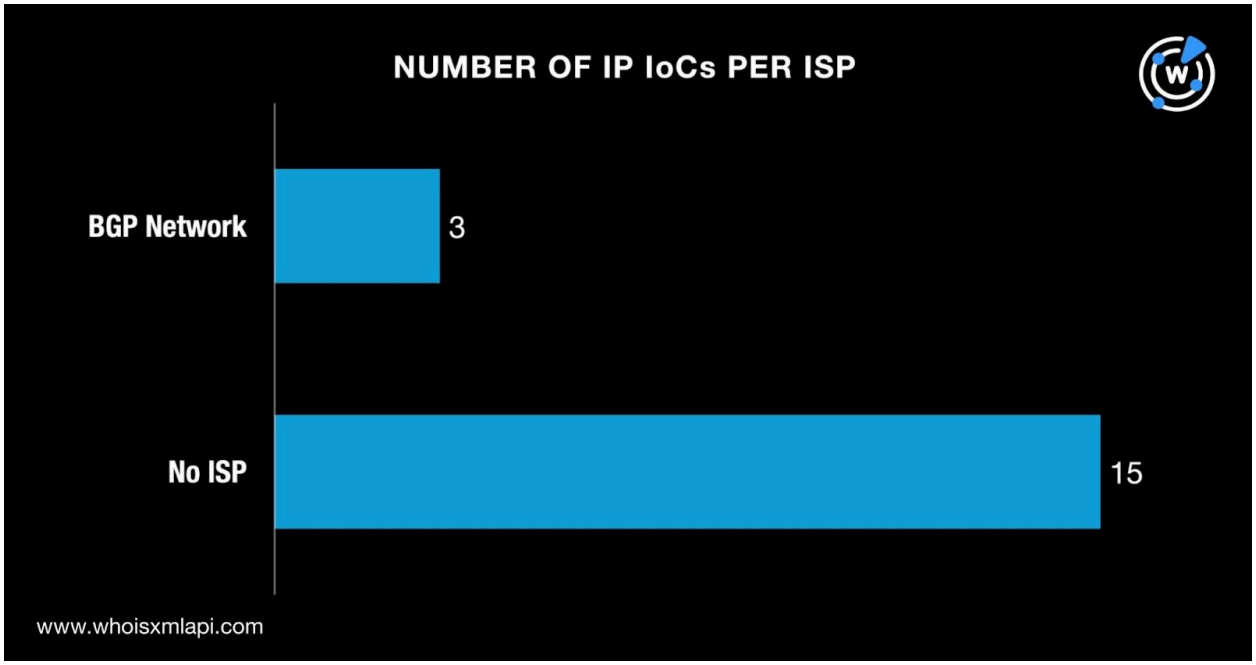
Sample IASC network traffic data for the 17 possibly dedicated IP addresses revealed an interesting finding. We learned that one potential victim IP address communicated with one IP address identified as an IoC on 9 December 2025.



Next, we queried the 18 IP addresses identified as IoCs on Bulk IP Geolocation Lookup and found out that:

- They were all geolocated in China, which is consistent with Silver Fox's home base.

- While 15 of them did not have ISPs on record, the remaining three were all administered by BGP Network.



A DNS Chronicle API query for the 18 IP addresses identified as IoCs showed that all of them had historical IP-to-domain resolutions. Altogether, they posted 6,349 resolutions over time, The IP address 43[.]226[.]125[.]112 recorded the oldest resolution on 25 January 2019.

IP IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
43[.]226[.]125[.]112	601	01/25/19	12/08/25
137[.]220[.]135[.]86	774	11/08/19	09/04/25
27[.]124[.]43[.]12	150	11/12/19	11/05/23
27[.]124[.]43[.]7	191	12/26/19	10/29/25
43[.]226[.]125[.]125	19	08/31/19	02/16/20

The Search for New ValleyRAT Artifacts

Our search for new artifacts began with a WHOIS History API query for the 20 domains identified as IoCs. We discovered that 16 of them had email addresses in their historical

WHOIS records. We unearthed 60 unique email addresses in all. Closer scrutiny showed that 33 were public email addresses.

A Reverse WHOIS API query for the 33 public email addresses showed that while none of them appeared in any domain's current WHOIS record, all of them did so in historical WHOIS records. Nine public email addresses could belong to domainers so they were excluded from further analysis. The 24 public email addresses led to the discovery of 45,949 unique email-connected domains after those already identified as IoCs were filtered out.

The results of our Threat Intelligence API query for the 45,949 email-connected domains revealed that 51 have already been weaponized for various attacks.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
aiaizz[.]com	Phishing Generic threat	08/27/25 08/28/25	10/29/25 10/13/25
chatrouletterus[.]com	Generic threat Phishing	09/21/25 09/20/25	10/13/25 09/20/25
echoblogger[.]com	Phishing Generic threat	08/07/25 08/08/25	12/19/25 09/20/25
laughtersoundhealing[.]com	Phishing Generic threat	09/26/25 04/06/23	11/29/25 10/13/25
0593cm[.]com	Generic threat	12/19/24	10/13/25

Next, we queried the 20 domains identified as IoCs on DNS Lookup API and found out that 18 actively resolved to various IP addresses. We obtained seven additional IP addresses.

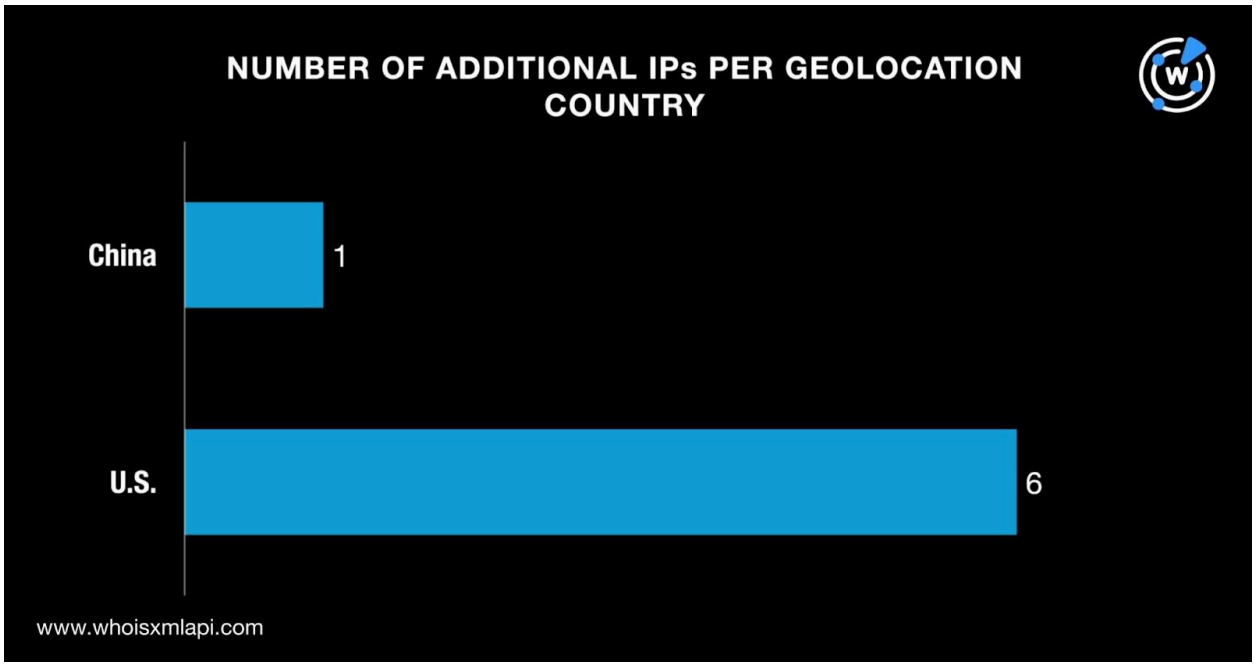
A Threat Intelligence API query for the seven additional IP addresses showed that all of them have already been weaponized for various attacks.

ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
172[.]67[.]148[.]126	C&C Malware distribution Phishing	04/07/24 07/06/23 05/21/23	12/20/25 11/06/25 10/21/25

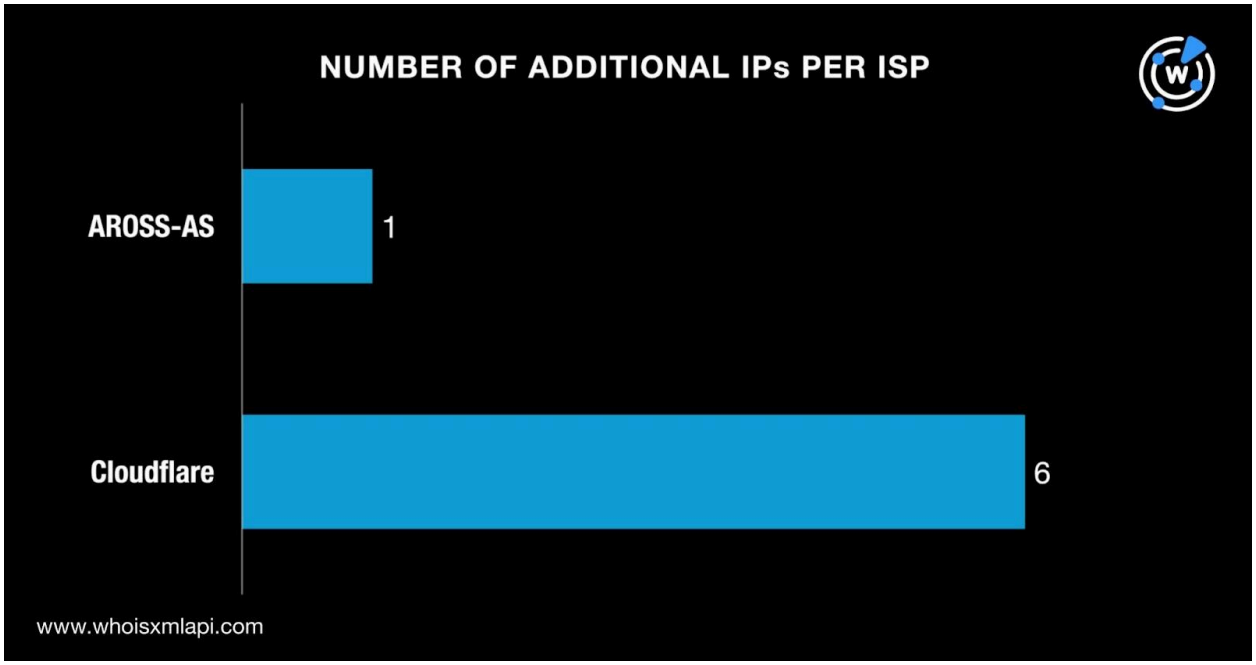
104[.]21[.]39[.]208	C&C Malware distribution Phishing	04/08/24 04/06/23 05/21/23	12/20/25 11/06/25 10/21/25
104[.]21[.]17[.]211	Generic threat Phishing Malware distribution	11/01/23 03/29/23 08/02/23	12/20/25 12/19/25 12/16/25
172[.]67[.]178[.]81	Generic threat Phishing Malware distribution	11/01/23 03/29/23 08/02/23	12/20/25 12/19/25 12/16/25
103[.]112[.]99[.]135	Malware distribution Generic threat	09/04/25 09/04/25	12/19/25 10/13/25

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

- They were geolocated in two countries led by the U.S., which accounted for six of the IP addresses. The sole remaining IP address originated from China like many of the IoCs.



- They were administered by two ISPs topped by Cloudflare, which accounted for six IP addresses. The remaining IP address was managed by AROSS-AS.



Adding together the 18 IP addresses identified as IoCs and the seven from the DNS Lookup API results, we now had 25 IP addresses in all for further analysis. A Reverse IP API query for them revealed that 15 were active domain hosts. We learned that only seven IP addresses could be dedicated hosts and limited our investigation to them. They hosted 20 unique IP-connected domains after those already tagged as IoCs and the email-connected domains were filtered out.

Next, we extracted 20 unique text strings from the 20 domains identified as IoCs. Domains & Subdomains Discovery searches for the 20 strings showed that nine appeared at the start of other domains—those not part of the IoC list—namely:

- baoyingkeji.
- binancegames.
- fjzwb.
- geroman.
- jqsnzp.
- qzjfxy.
- teamszv.
- telegramzwxz.
- xclyd.

Our searches also led to the discovery of 30 unique string-connected domains after those already identified as IoCs and the email- and IP-connected domains were filtered out.

A Threat Intelligence API query for the 30 string-connected domains revealed that one—binancegames[.]com[.]ua—has been associated with a generic threat between 29 April 13 October 2025.

—

Our in-depth investigation of the Silver Fox campaign leveraging ValleyRAT led us to discern that 2,357 unique client IP addresses under 20 distinct ASNs communicated with one domain identified as an IoC via 42,400 DNS queries made between 19 November and 18 December 2025. We also learned that four domains identified as IoCs were bulk-registered with 3–4 look-alikes each between 3 and 19 March 2025. In addition, seven domains identified as IoCs were deemed likely to turn malicious 239–339 days before they were dubbed as such on 4 December 2025. On top of all that, one potential victim IP address communicated with one domain identified as an IoC on 9 December 2025.

We were also able to collate 46,006 new artifacts comprising 45,949 email-connected domains, seven additional IP addresses, 20 IP-connected domains, and 30 string-connected domains. To date, 59 of the new artifacts we uncovered have already been weaponized for 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

- 0000www[.]com
- 0001uk[.]com
- 00038888[.]com
- a-ctl[.]com
- a-grip[.]com
- a-hope-bhagwati-vatica[.]com
- b1246[.]com
- b12vitamininjections[.]com
- b13595984888[.]com
- c-hl[.]com
- c-hooze[.]com
- c-kodama[.]com
- d-art[.]cc
- d-maldives[.]com
- d007[.]net
- e-alcala[.]com
- e-ao[.]com
- e-deepzone[.]com
- f-cheer[.]com
- f-windsor[.]com
- f0576[.]cn
- g-hirama[.]com
- g-scientific[.]biz
- g-tropin-aq[.]com
- h2013[.]com
- h2ispa[.]com
- h2j[.]net
- i-connectors[.]com
- i-dentical[.]com
- i-panelinc[.]com
- j-cena[.]com
- j-shogei[.]com
- j0007[.]com
- k-dousou[.]com
- k-p-k[.]com
- k2pchemicals[.]com
- l-coo[.]com
- l0089[.]com
- l22ba[.]cn
- m-lighting[.]net
- m-perm[.]com
- m-pson[.]com
- n-keitai2[.]com
- n5200[.]com
- n599[.]com
- o-movie[.]com
- o-yijia[.]com
- o1gg[.]com
- p-seosite[.]com
- p2dy[.]com
- p2pmailing[.]com
- q-song[.]com
- q8cpa[.]com
- q9909[.]com
- r1079[.]com
- r2sbot[.]com
- r4isdhc-no[.]com
- s-10xtreme[.]com
- s-kumarcompany[.]com
- s-shooting[.]com
- t-ber[.]com
- t-kittiwattana[.]com
- t-thailand[.]com
- u-mic[.]com
- u-pecker[.]com[.]cn
- u-teks[.]com[.]cn
- v-dimension[.]com
- v-transinternational[.]com
- v12010[.]com
- w-hao[.]com
- w00tastic[.]com
- w12315[.]com

- x-extreme[.]com
- x-profit[.]com
- x-sk[.]com
- y-jpg[.]com
- y-long[.]cn
- y-sun[.]net
- z-nyala[.]com
- z-tshirt[.]com
- z-xuefei[.]com

Sample Additional IP Addresses

- 103[.]112[.]99[.]135
- 104[.]21[.]39[.]208
- 172[.]67[.]148[.]126

Sample IP-Connected Domains

- 4hn42ik[.]cn
- alpha[.]superset[.]directindustry010[.]cfd
- b02kljj[.]com
- e7qx70j[.]com
- ftp[.]4hn42ik[.]cn
- gotonesmx[.]fit
- mail[.]4hn42ik[.]cn
- n9xbbfq[.]com
- panalobet999[.]com
- seo68888[.]vip
- wh96zsz[.]com

Sample String-Connected Domains

- baoyingkeji[.]cn
- binancegames[.]com
- fjzwb[.]icu
- geroman[.]com[.]br
- jqsnzp[.]cn
- qzjfxy[.]com
- teamszv[.]net
- telegramzwxz[.]org
- xclyd[.]cn