WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

An Analysis of the AtlasCross RAT Network IoCs

Threat Report

Table of Contents

Executive Report

Hexastrike Cybersecurity discovered and analyzed a multistage AtlasCross RAT campaign that used domains impersonating trusted software brands. The threat affected VPN clients, encrypted messengers, videoconferencing tools, cryptocurrency trackers, and e-commerce applications. The domains they used mimicked brands including Surfshark VPN, Signal, Telegram, Zoom, Microsoft Teams, and others. And after careful examination, the attack was attributed to the Silver Fox APT group.

The Hexastrike report identified 13 network IoCs comprising 12 domains and one IP address. Note that none of the domain IoCs belonged to legitimate organizations based on the results of our domain legitimacy checks via the WhoisXML API MCP Server.

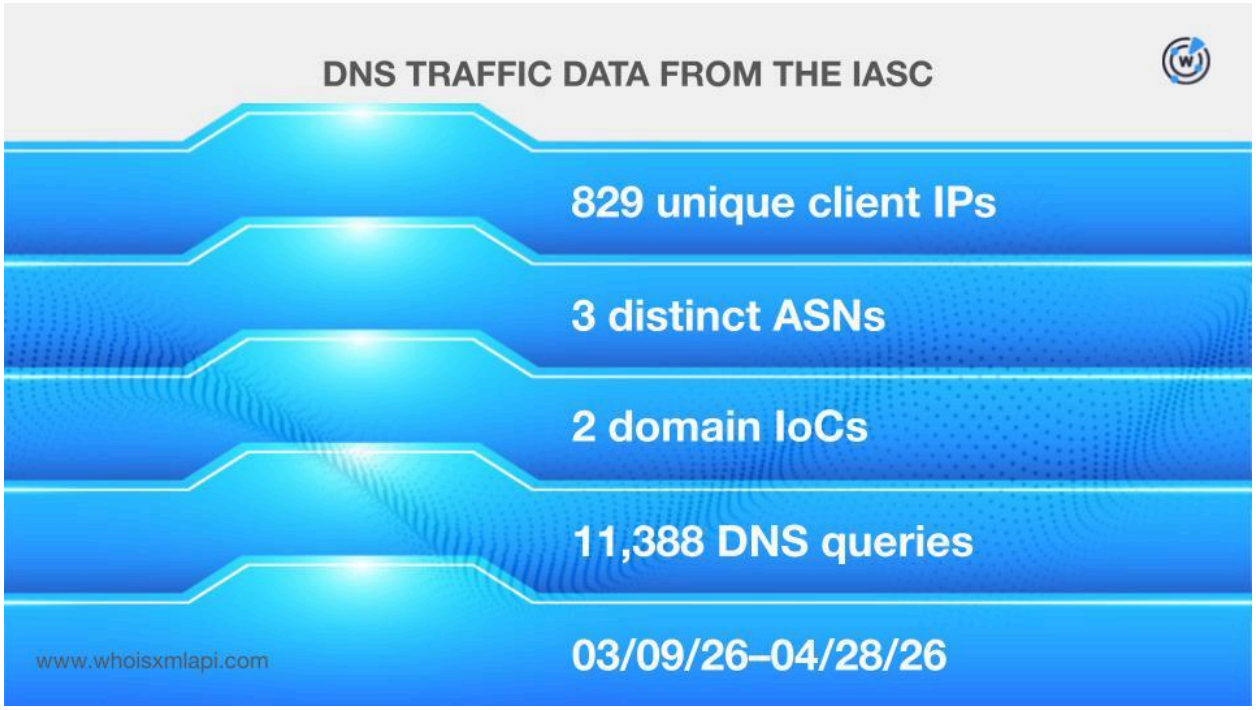
Our DNS deep dive into these IoCs led to these discoveries:

- 829 unique client IP addresses that communicated with two of the domain IoCs
- One domain IoC that was bulk-registered with six look-alike domains
- Five domain IoCs that were likely registered with malicious intent
- 33 IP addresses potentially owned by victims that communicated with one of the IP IoCs
- 2,584 email-connected domains
- 10 additional IP addresses, seven of which were confirmed malicious
- 33 IP-connected domains
- 35 string-connected domains, three of which were confirmed malicious

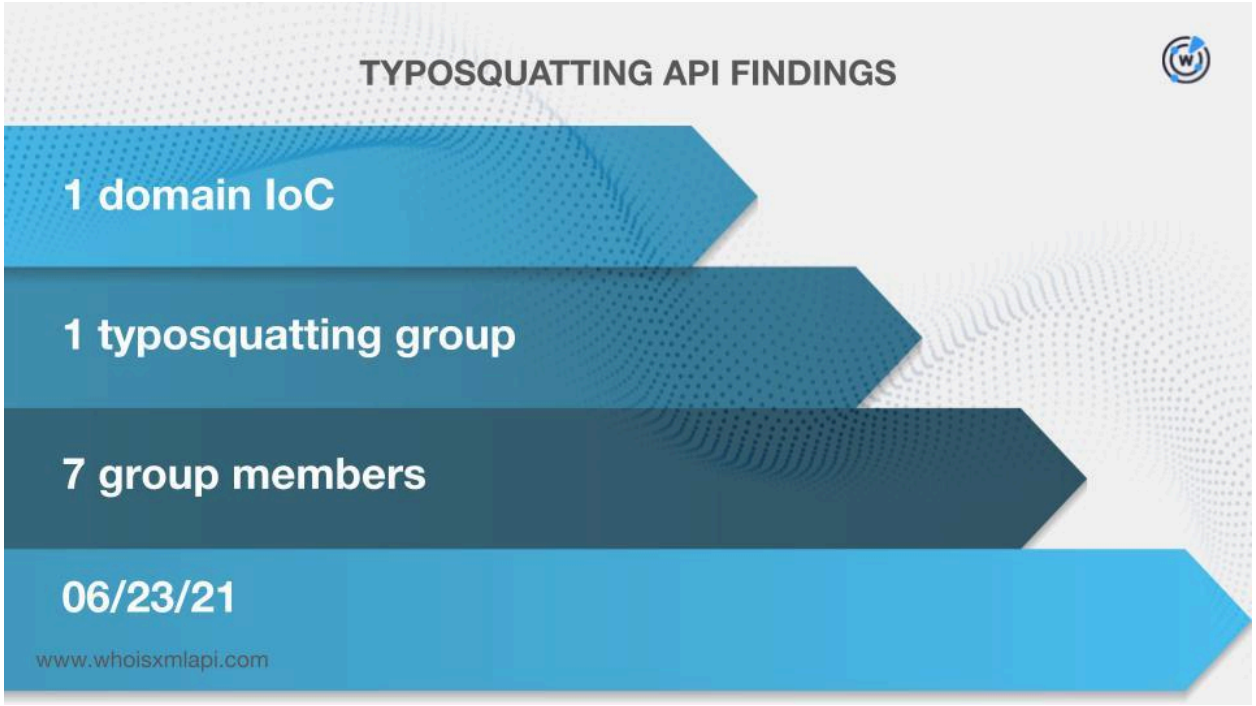
Dissecting the AtlasCross RAT Domain IoCs

We began our analysis by taking a closer look at the 12 domain IoCs.

First off, sample network traffic data from the IASC revealed that 829 unique client IP addresses under three ASNs communicated with two of the domain IoCs via 11,388 DNS queries made between 9 March and 28 April 2026.



We then queried the domain IoCs on Typosquatting API and discovered that the domain bifa668[.]com appeared in one typosquatting group made up of seven members all registered on 23 June 2021.



This domain IoC was registered alongside these six look-alikes:

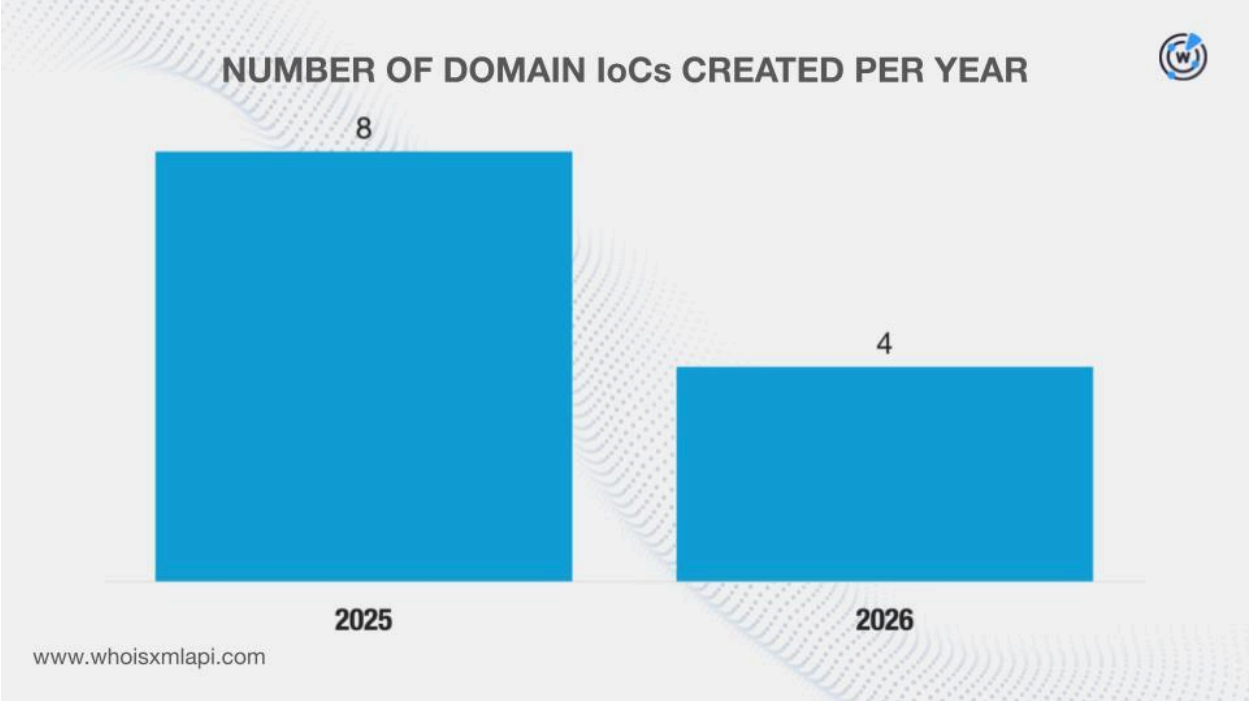
- bifa6868[.]com
- bifa0588[.]com
- bifa668[.]com
- bifa1688[.]com
- bifa688[.]com
- bifa0888[.]com

Next up, First Watch Malicious Domains Data Feed showed that five domain IoCs were likely registered with malicious intent as they showed up on the database 26–594 days before being identified as IoCs on 25 March 2026. Take a look at more details for three examples below.

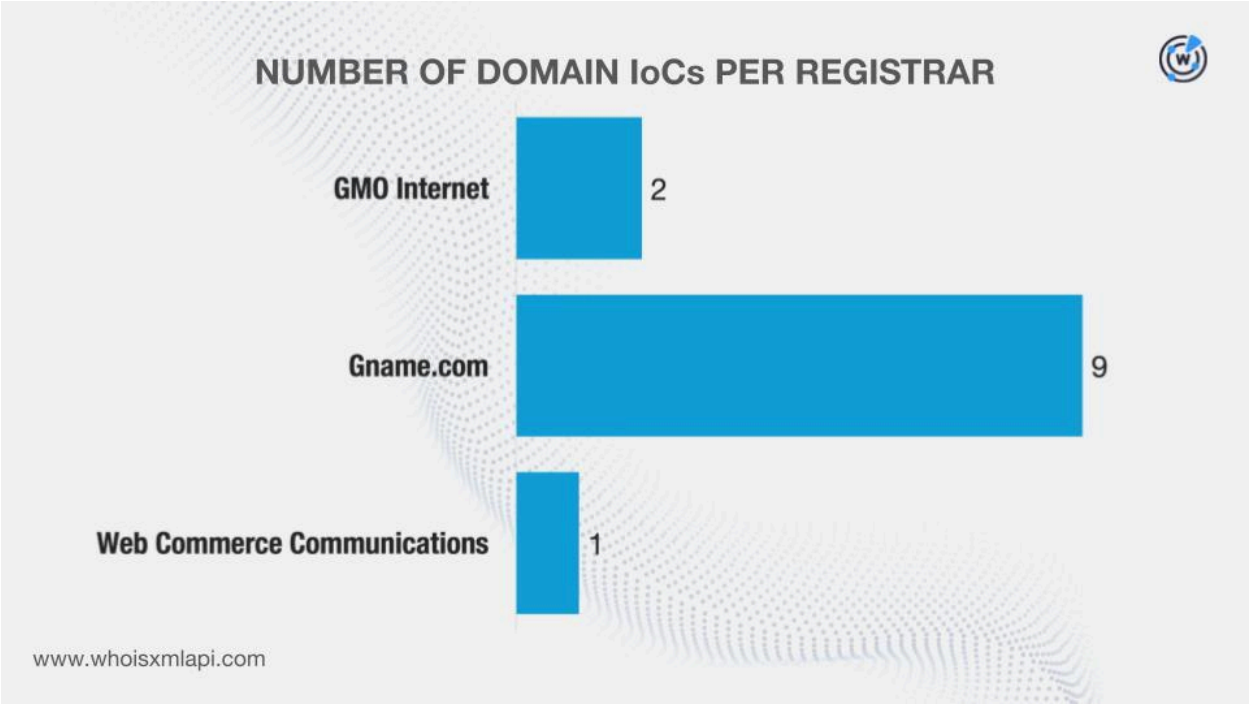
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE THE REPORT DATE
quickq-quickq[.]com	08/08/24	594
www-teams[.]com	11/14/25	131
wwtalk-app[.]com	11/28/25	117

After that, we queried the domain IoCs on WHOIS API and learned that:

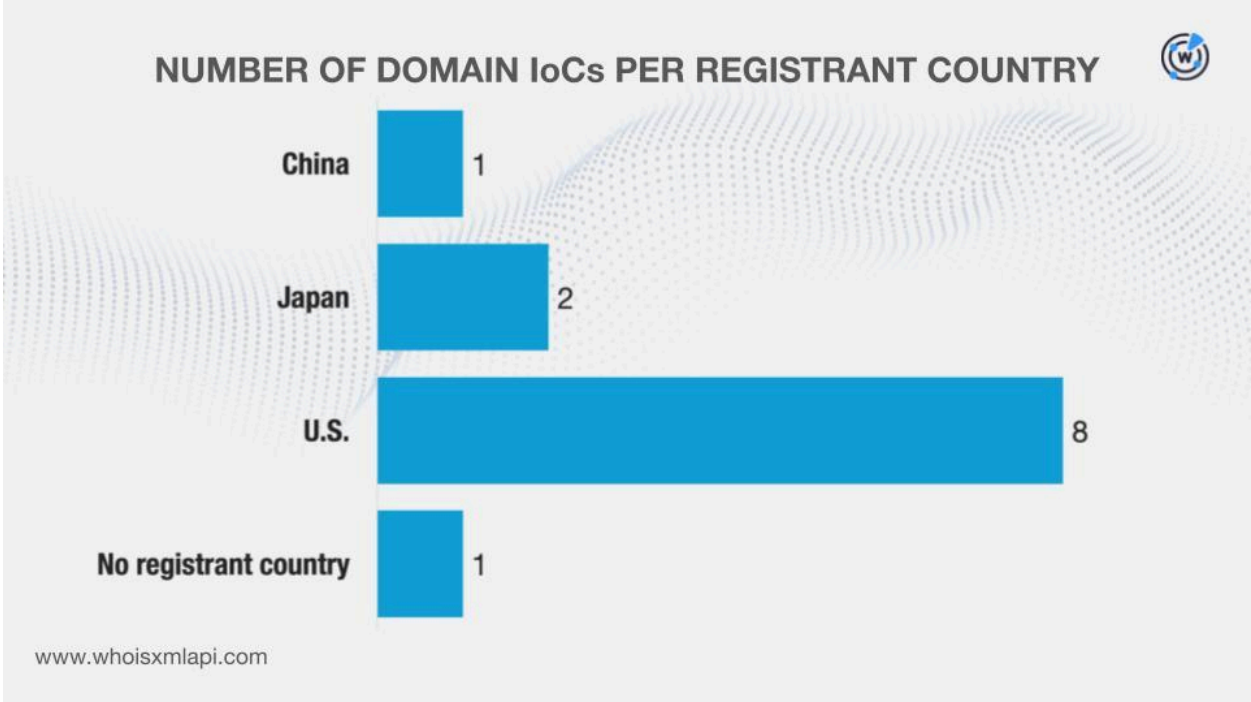
- They were created between 27 October 2025 and 1 March 2026.



- They were administered by three registrars.



- While one did not have a registrant country on record, the remaining 11 were registered in three countries.



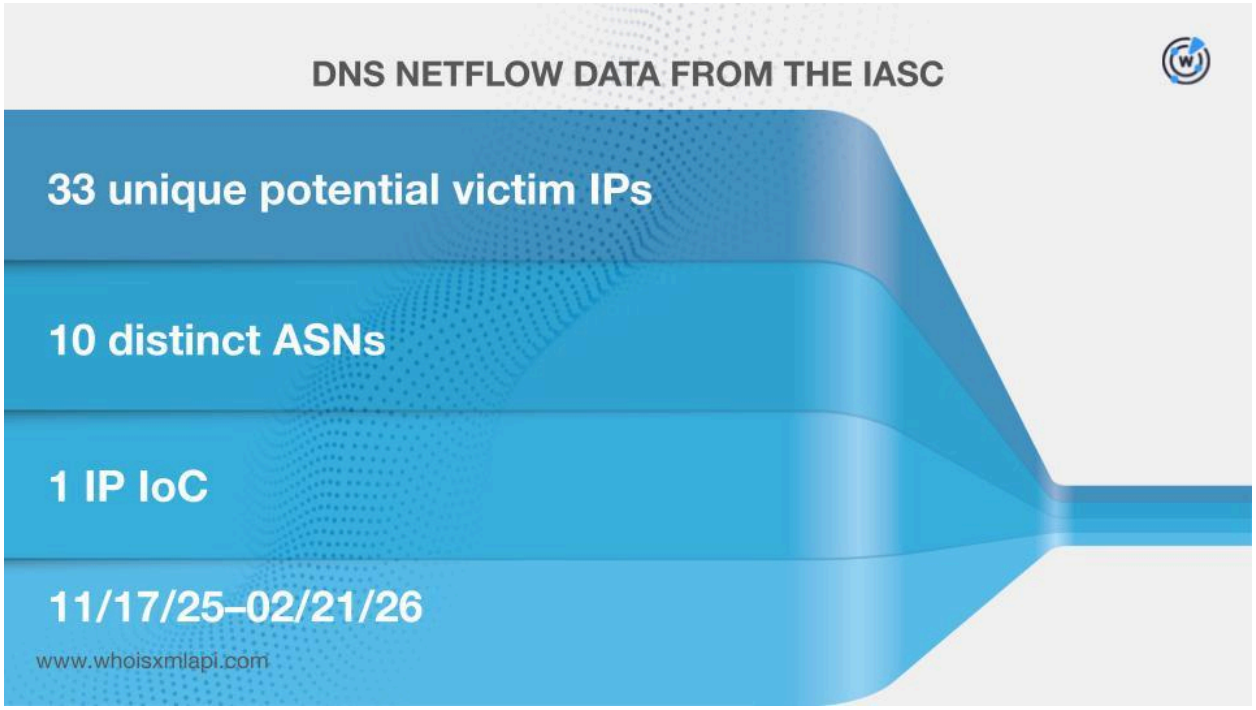
Finally, we queried the domain IoCs on DNS Chronicle API and discovered that 11 had recorded 316 historical domain-to-IP resolutions over time. Here are more details about five examples.

DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
bifa668[.]com	155	02/05/17–12/27/25
app-zoom[.]com	138	10/20/17–03/30/26
quickq-quickq[.]com	6	08/08/24–01/09/26
ultraviewer-cn[.]com	2	11/06/25–03/11/26
kefubao-pc[.]com	2	11/21/25–01/12/26

Investigating the AtlasCross RAT IP IoCs

After learning more about the domain IoCs, we further investigated the sole IP IoC.

First, sample network traffic data from the IASC revealed that 33 unique potentially victim-owned IP addresses under 10 ASNs communicated with the IP IoC between 17 November 2025 and 21 February 2026.



We then queried the IP IoC on IP Geolocation API and found out that it was geolocated in South Korea and administered by MOACK.

DNS Chronicle API, meanwhile, revealed that it only recorded one historical IP-to-domain resolution over time.

Amassing New AtlasCross RAT Artifacts

We started our search for new artifacts by querying the domain IoCs on WHOIS History API. We discovered that six of them had 11 email addresses in their historical WHOIS records.

Further scrutiny revealed that five were public email addresses. Of these, one could belong to a domainer, hence, it was excluded from the next step.

We then queried the four public email addresses on Reverse WHOIS API, which led to the discovery of 2,584 unique email-connected domains after the domain IoCs were filtered out.

After that, we queried the domain IoCs on DNS Lookup API and uncovered 10 unique additional IP addresses.

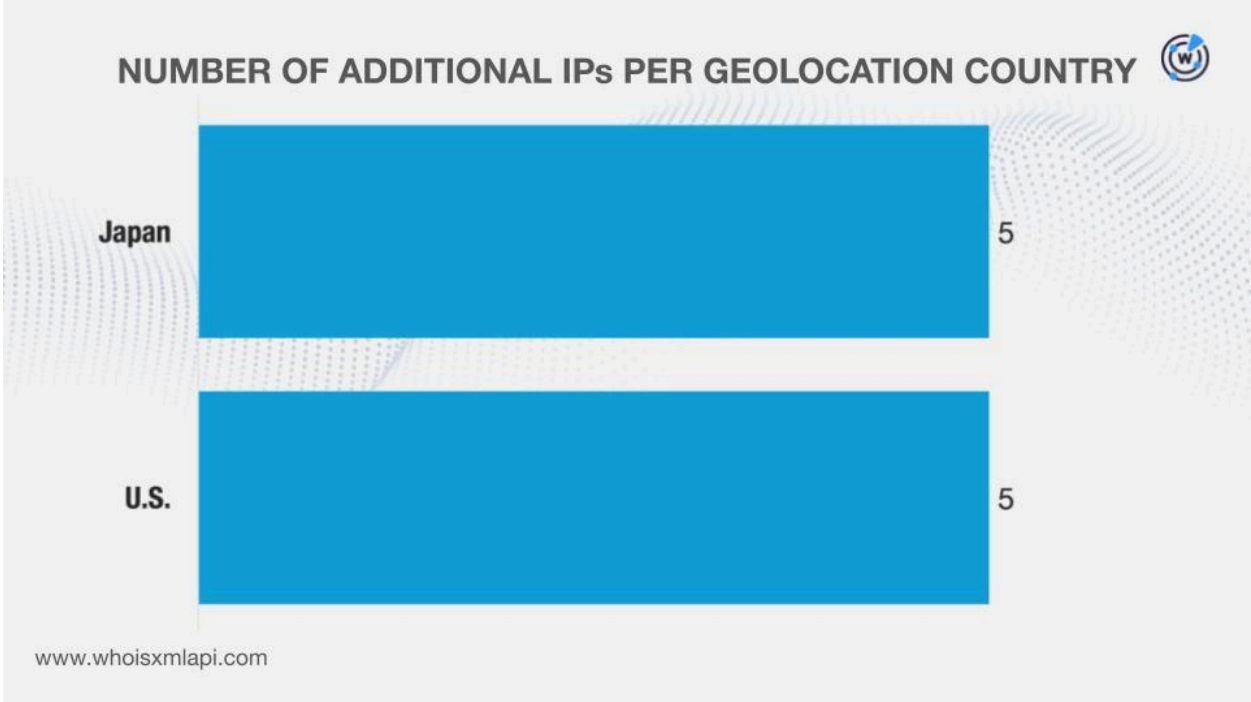
The results of our Threat Intelligence API queries for the additional IP addresses revealed that seven have already been weaponized for various attacks. Take a look at more information on three examples below.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
154[.]193[.]232[.]229	Malware distribution	03/30/26
154[.]193[.]232[.]231	Malware distribution	03/30/26
156[.]235[.]106[.]141	Malware distribution	03/30/26

It is interesting to note that almost all of the malicious additional IP addresses only served as malware hosts for about a day. One was detected for malware distribution for about three days.

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

- They were geolocated in two countries that did not match that of the sole IP IoC.



- They were all administered by a single ISP—AROSS-AS—that also did not match that of the sole IP IoC.

At this point, we had 11 IP addresses (one IoC and 10 additional) for the next step. We queried them on Reverse IP API and found out that four could be dedicated hosts. Together, they hosted 33 unique IP-connected domains after the domain IoCs and the email-connected domains were filtered out.

Finally, we scoured the DNS for other domains that started with the same text strings as the domain IoCs using Domains & Subdomains Discovery. Of the 12 unique strings extracted from the domain IoCs, these eight had results:

- app-zoom.
- bifa668.
- eyy-eyy.
- quickq-quickq.
- signal-signal.
- telegrtam.
- wwtalk-app.
- www-surfshark.

This step of our hunt led to the discovery of 35 unique string-connected domains after the domain 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. Since they mimic known software brands, the results may include legitimate domains.

We queried the string-connected domains on Threat Intelligence API and discovered that three have already been weaponized for various attacks. An example is app-zoom[.]website, which has already been associated with malware distribution between 13 March 2025 and 31 March 2026.

Conclusion

Our analysis of the latest Silver Fox attack leveraging AtlasCross RAT revealed that 829 unique client IP addresses communicated with two of the domain IoCs. We also learned that one domain IoC was bulk-registered with six look-alike domains. In addition, five domain IoCs were likely registered with malicious intent. Finally, 33 IP addresses potentially owned by victims communicated with one of the IP IoCs.

We also unearthed 2,662 new artifacts comprising 2,584 email-connected domains, 10 additional IP addresses, 33 IP-connected domains, and 35 string-connected domains. Of these, 10 have already figured in different malicious 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

- 024byyy[.]com
- 0573fz[.]net
- 086isp[.]net
- acti1[.]info
- ahmj4[.]info
- ambq0[.]info
- b2bjob[.]net
- baih2[.]info
- bainiankangle[.]com
- cdlanyu[.]net
- ceaikit[.]com
- cep13[.]info
- dabv5[.]info
- danrivertechnologies[.]com
- dcdzsw[.]com
- eack4[.]info
- edisonlighting-led[.]com
- eduf4[.]info
- fgv67[.]info
- fhmjjd[.]com
- fow99[.]info
- gcy86[.]info
- gdplt[.]com
- gdsailang[.]com
- hbxfnzxn[.]com
- hefeilixia[.]com
- hello-xhl[.]com
- icce4[.]info
- idc-hosting[.]net
- igs79[.]info
- jao66[.]info
- jawt7[.]info
- jcsi3[.]info
- kaolu88[.]com
- kcbh8[.]info
- kefu-eyy250cn[.]com[.]cn
- la-venda[.]com
- laienmenye[.]com
- lanqiubbs[.]com
- mamahoho[.]com
- mcm52[.]info
- metexss[.]com
- ncay2[.]info
- ndm45[.]info
- ney21[.]info
- oais5[.]info
- obdh6[.]info
- obfo4[.]info
- pbx59[.]info
- pfun8[.]info
- pieraboots[.]com
- qcet4[.]info
- qd-batter[.]com
- qeg16[.]info
- rbn85[.]info
- rdop5[.]info
- reliance-industry[.]com
- s-wavetech[.]com
- sahy8[.]info
- saibeibj[.]com
- taau8[.]info
- taogoogle[.]com
- tcjm9[.]info
- uay35[.]info
- udl63[.]info
- ula99[.]info
- vbax2[.]info
- vdxe4[.]info
- veb51[.]info
- wangjiewl[.]com
- wangshangliaoxz[.]com[.]cn
- wero9[.]info
- xbet108[.]com
- xbet118[.]com

- xbet128[.]com
- yanxiang88[.]com
- yasi51[.]com
- ybw96[.]info
- zbdianyuan[.]com
- zdkg2[.]info
- zhmingtong[.]com

Sample Additional IP Addresses

- 154[.]193[.]232[.]229
- 154[.]193[.]232[.]231
- 156[.]235[.]106[.]141

Sample IP-Connected Domains

- 51909de5-4091-48af-9f31-74075d71ecbe[.]random[.]sdmingmou[.]com
- 53e2e72e-92ec-45bd-b5bf-5230e35c1564[.]random[.]sdmingmou[.]com
- admin[.]wq12325[.]com
- api[.]wq12325[.]com
- app[.]wq12325[.]com
- cef331d9-c605-4d06-aa84-b25d5c7662ac[.]random[.]belatrova[.]com
- core[.]harbor[.]sdmingmou[.]com
- cpanel[.]wq12325[.]com
- dev[.]wq12325[.]com
- election[.]sdmingmou[.]com
- ftp[.]wq12325[.]com
- localhost[.]wq12325[.]com
- m[.]kristinspitznogle[.]sdmingmou[.]com
- m[.]wq12325[.]com
- mail[.]wq12325[.]com
- parkeerproducten[.]sdmingmou[.]com
- pay[.]wq12325[.]com
- pop[.]wq12325[.]com
- random[.]wq12325[.]com
- smtp[.]wq12325[.]com
- smtp[.]xiaokequan[.]com
- u[.]sdmingmou[.]com
- webdisk[.]wq12325[.]com
- webmail[.]wq12325[.]com
- webmail[.]xiaokequan[.]com

Sample String-Connected Domains

- app-zoom[.]cloud
- app-zoom[.]com[.]cn
- app-zoom[.]live
- bifa668[.]cn
- bifa668[.]work
- eyy-eyy[.]com[.]cn
- quickq-quickq[.]cn
- quickq-quickq[.]com[.]cn
- quickq-quickq[.]hl[.]cn
- signal-signal[.]com[.]cn
- signal-signal[.]de
- signal-signal[.]net
- telegrtam[.]club
- telegrtam[.]com
- telegrtam[.]com[.]ph
- wwtalk-app[.]top
- www-surfshark[.]ru