WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Exploring the DNS Flipside of SideWinder

Table of Contents

Executive Report

The SideWinder advanced persistent threat (APT) group, active since 2012 and known for targeting government, military, and business entities throughout Asia, primarily Pakistan, China, Nepal, and Afghanistan, has struck once again.

This time around, the threat actors updated their toolset and created new infrastructure to spread malware and control compromised systems. They also significantly increased attacks against maritime and logistics companies notably in Djibouti and Egypt and nuclear power plants in South Asia and Africa.

Securelist identified 35 domains as indicators of compromise (IoCs) in connection with the latest SideWinder attack. WhoisXML API jumped off their list of IoCs in a bid to find more connected artifacts through an expansion analysis and uncovered:

- 35 email-connected domains
- Two IP addresses, one of which turned out to be malicious
- 10 IP-connected domains
- 532 string-connected domains, 16 of which have already figured in cyber attacks

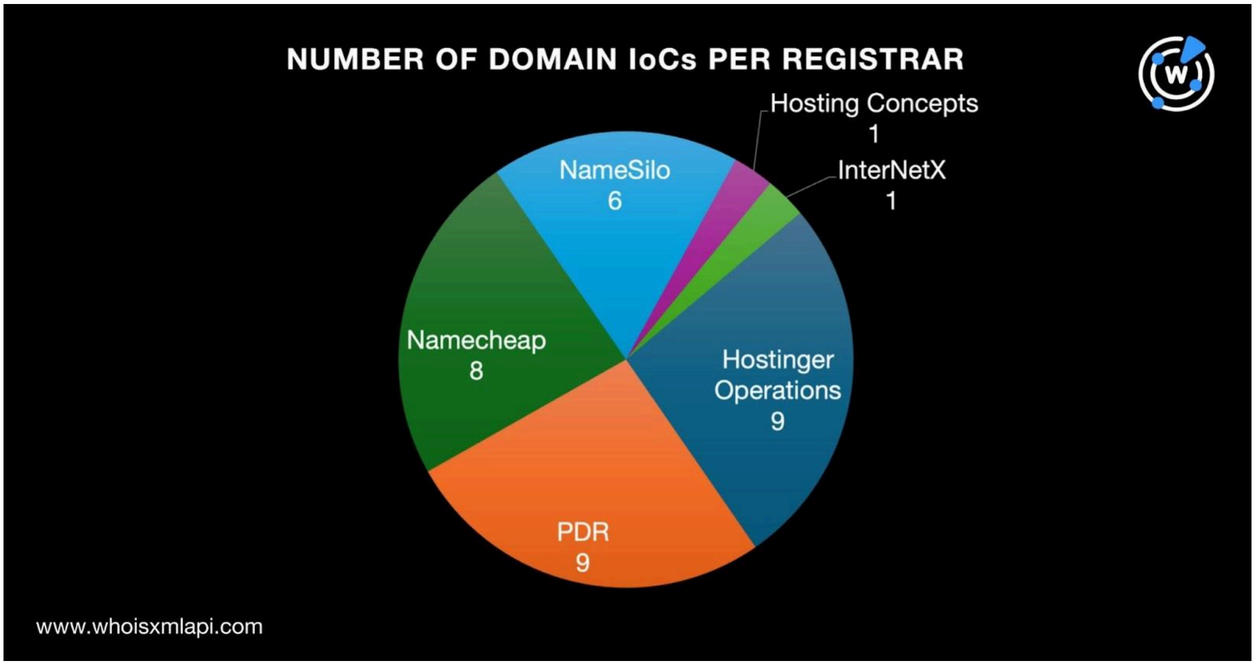
On the Flipside of the SideWinder IoCs

We started our analysis of the most recent SideWinder attack by looking more closely at IoCs.

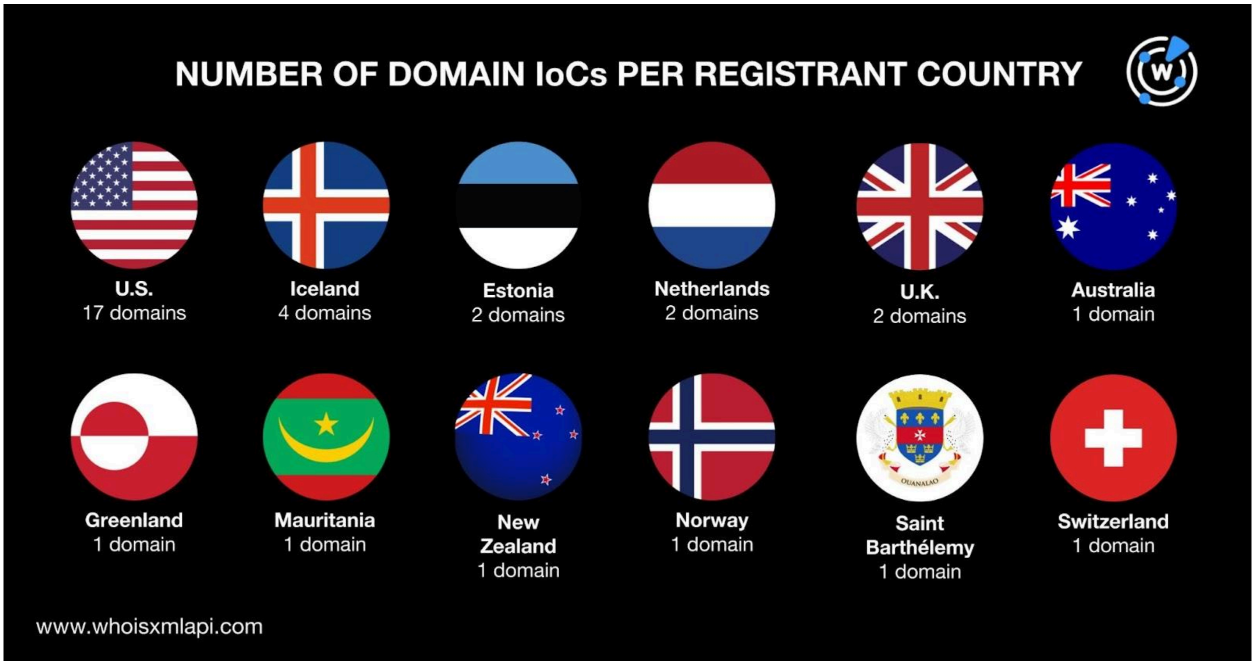
A Bulk WHOIS API query for the 35 domains identified as IoCs revealed that only 34 of them had current WHOIS records. The results also showed that:

- The 34 domains were all created in 2024.
- They were administered by six registrars led by Hostinger Operations and PDR, which accounted for nine domains each. Namecheap took the second spot with eight

domains. NameSilo placed third with six domains. Finally, Hosting Concepts and InterNetX administered one domain each.



- They were registered in 12 countries topped by the U.S., which accounted for 17 domains. Four were registered in Iceland while two each were registered in Estonia, the Netherlands, and the U.K. Finally, one domain each was registered in Australia, Greenland, Mauritania, New Zealand, Norway, Saint Barthélemy, and Switzerland.



We then queried the 35 domains tagged as IoCs on DNS Chronicle API and found that only 32 of them had historical domain-to-IP address resolutions. In fact, they had 146 resolutions in all. The domain documentviewer[.]info posted the oldest resolution date—3 April 2020. Given that documentviewer[.]info was created on 8 August 2024 according to its current WHOIS record, it could have been reregistered specifically for the SideWinder attack.

Take a look at details for five other domains identified as IoCs below.

DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
aliyum[.]email	6	5 August 2024
depo-govpk[.]com	2	18 October 2024
dowmloade[.]org	1	21 August 2024
ms-office[.]app	6	29 March 2023
veorey[.]live	8	27 November 2024

SideWinder Attack IoC List Expansion Findings

We kicked off our analysis by querying the 35 domains identified as IoCs on WHOIS History API, which showed that six of them had 10 email addresses in their current WHOIS records after filtering out duplicates. Two of the 10 email addresses were public.

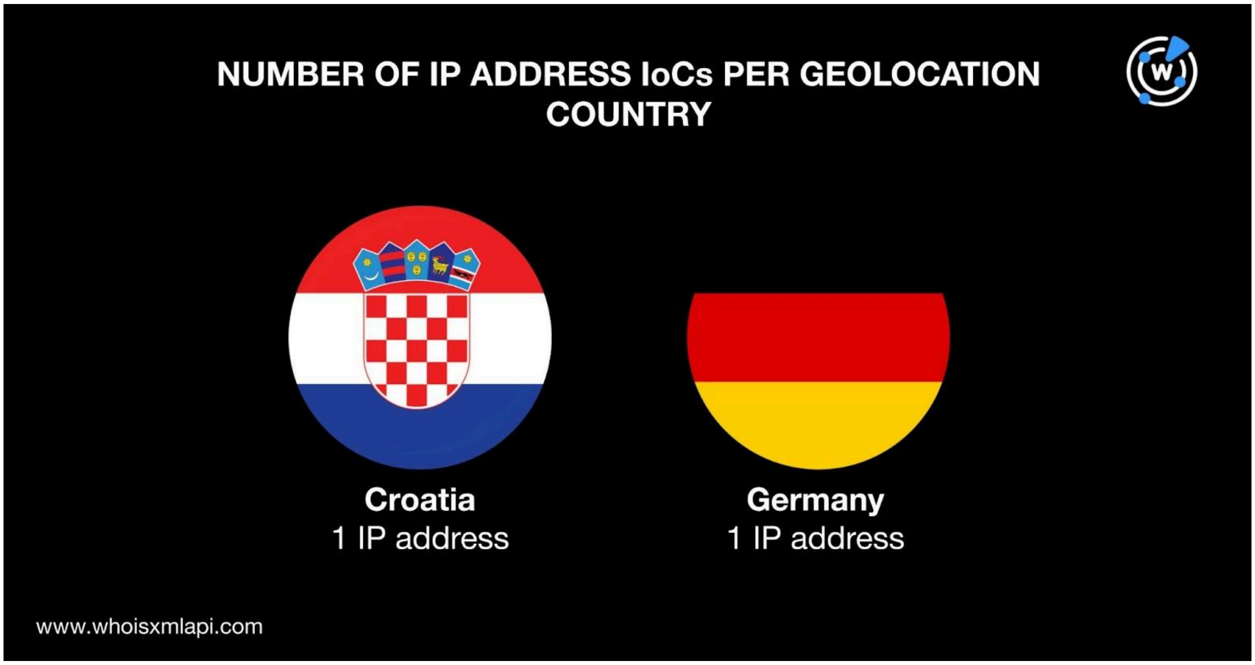
Next, we queried the two public email addresses on Reverse WHOIS API and found that while they did not appear in the current WHOIS records of any domain, they did so in the historical records of 35 email-connected domains after duplicates and those already identified as IoCs were filtered out.

We then queried the 35 domains identified as IoCs on DNS Lookup API. Two of them had active domain-to-IP address resolutions. Specifically, two domains resolved to two unique IP addresses.

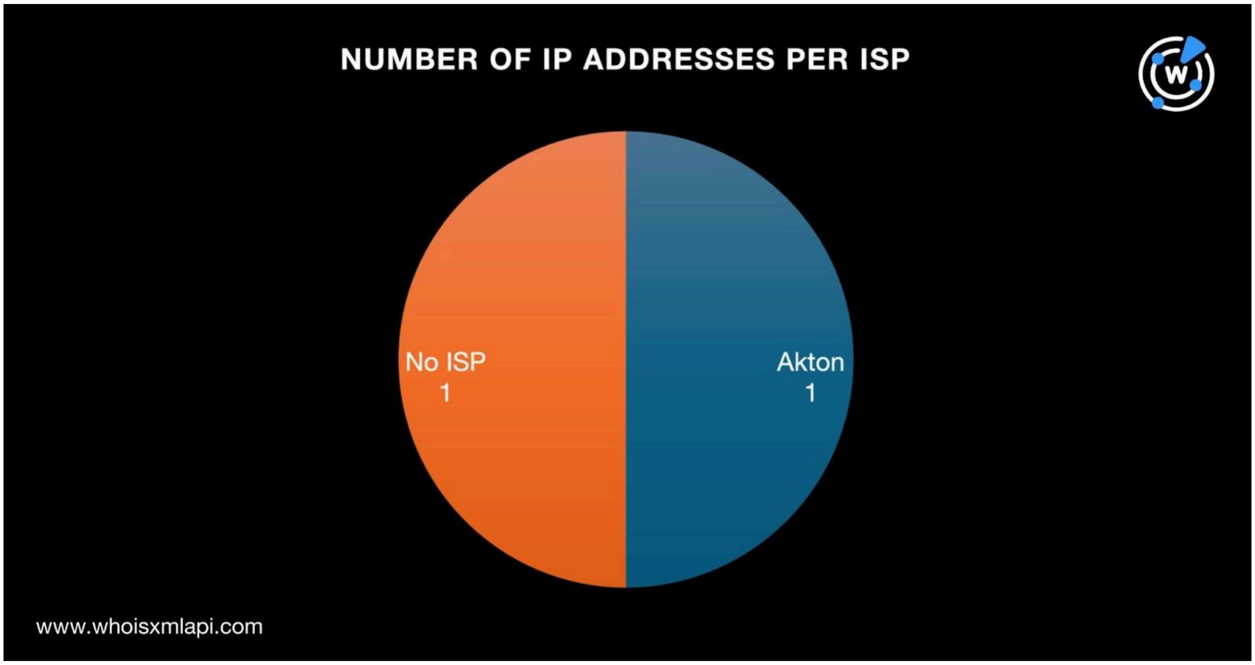
A Threat Intelligence API query for the two IP addresses revealed that one of them—91[.]195[.]240[.]12—has already been weaponized in connection with generic threats, phishing, command and control (C&C), attacks, malware distribution, and suspicious activity.

Querying the two IP addresses on Bulk IP Geolocation Lookup next, we found that:

- One IP address each was geolocated in Croatia and Germany.



- One IP address was administered by Akton while the other did not have an ISP on record.



We also queried the two IP addresses on Reverse IP API and discovered that they had 311 IP address-to-domain resolutions. Further scrutiny revealed that only one of the addresses—46[.]183[.]184[.]83—could be dedicated. Specifically, it hosted 10 unique IP-connected domains.

Next, we scoured the DNS for domains that contained these 32 unique text strings found in the 35 domains identified as IoCs:

- aliyum.
- crontec.
- d0cumentview.
- d0wnlaod.
- debcon.
- defencearmy.
- depo-govpk.
- dirctt88.
- dirctt888.
- directt88.
- document-viewer.
- documentviewer.
- dowmload.
- dowmloade.
- downl0ad.
- file-dwnld.
- mevron.
- mod-kh.
- modpak-info.
- modpak.
- mods.
- ms-office.
- mteron.
- pmd-offc.

- pmd-office.
- pncert.
- portdedjibouti.
- session-out.
- veorey.
- zeltech.
- ziptec.

Our Domains & Subdomains Discovery query uncovered 532 string-connected domains after filtering out duplicates, those already identified as IoCs, and the email- and IP-connected domains.

A Threat Intelligence API query for the 532 string-connected domains showed that 16 of them have already figured in various cyber attacks. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT
aliyum[.]org	Malware distribution
dirctt88[.]net	Malware distribution
directt88[.]org	Malware distribution
dowmload[.]org	Malware distribution
ms-office[.]services	Malware distribution

We queried the 16 malicious string-connected domains on Screenshot API and found that two of them—dirctt88[.]co and dirctt88[.]net—remained accessible to date.

It is also interesting to note that two malicious string-connected domains—ms-office[.]org ms-office[.]services—contained strings that could be mistaken for belonging to Microsoft. However, WHOIS API query results for both domains showed they were not publicly attributable to the tech giant.

—

Our DNS deep dive into the latest SideWinder attack led to the discovery of 579 potentially connected artifacts comprising 35 email-connected domains, two IP addresses, 10 IP-connected domains, and 532 string-connected domains. Further investigation into these artifacts revealed that 17—one IP address and 16 domains—have already been considered malicious to date.

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

- 128[.]xyz
- black-rock[.]xyz
- coreathletics[.]club
- eye-and-brain[.]xyz
- fivedragonsllc[.]xyz
- geeks[.]xyz
- hyperdrive[.]xyz
- jamesdcase[.]xyz
- location[.]xyz
- madrid[.]xyz
- niqla[.]xyz
- obstacleguard[.]xyz
- printers[.]xyz
- ricardomeier[.]design
- safaris[.]xyz
- taillight[.]xyz
- us-china-trade-and-innovation-center[.]xyz
- vespa[.]work

Sample IP-Connected Domains

- cpanel[.]veorey[.]live
- ftp[.]veorey[.]live
- localhost[.]veorey[.]live
- mail[.]veorey[.]live
- pop[.]veorey[.]live

Sample String-Connected Domains

- aliyum[.]biz
- crontec[.]at
- d0cumentview[.]ph
- d0wnlaod[.]ph
- debcon[.]be
- defencearmy[.]cf
- depo-govpk[.]ph
- dirctt88[.]co
- dirctt888[.]net
- directt88[.]org
- document-viewer[.]ca
- documentviewer[.]ai
- dowmload[.]buzz
- dowmloade[.]ph
- downl0ad[.]club
- file-dwnld[.]org[.]ws
- mevron[.]com
- mod-kh[.]ph
- modpak-info[.]ph
- modpak[.]ca
- mods[.]ac
- ms-office[.]academy
- mteron[.]com
- pmd-offc[.]ph
- pmd-office[.]com
- pncert[.]com
- portdedjibouti[.]com
- session-out[.]ws
- veorey[.]ph
- zeltech[.]be
- ziptec[.]ca