Exploring the SideWinder APT Group's DNS Footprint

Table of Contents

Executive Report

The SideWinder advanced persistent threat (APT) group, also known as "T-APT-04" or "RattleSnake," has been active since 2012. It launched attacks against military and government entities in Asia.

SecureList analyzed the inner workings of SideWinder in great depth and identified 100 domain names as indicators of compromise (IoCs) as of 15 October 2024. The WhoisXML API research team expanded the IoC list in a bid to uncover other potentially connected artifacts.

Our analysis led to the discovery of:

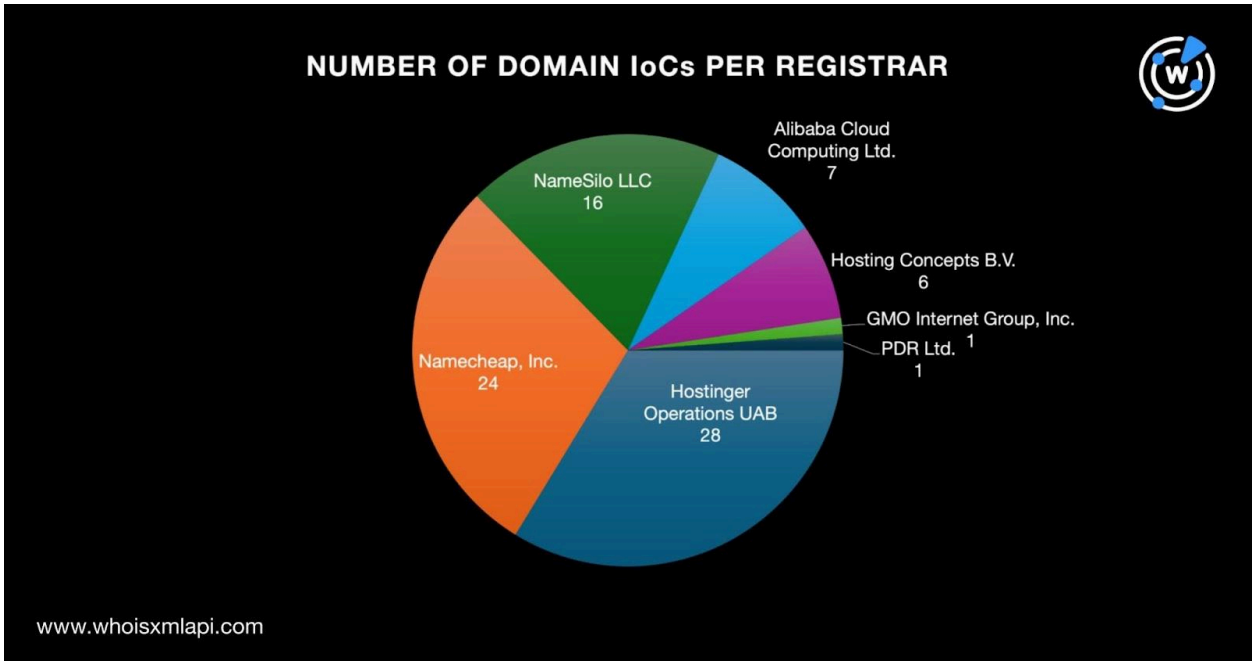
- Six email-connected domains
- 22 IP addresses, 20 of which turned out to be malicious
- 176 IP-connected domains, 130 of which turned out to be associated with various threats
- 370 string-connected domains, 21 of which have already figured in malicious campaigns

A Closer Look at the SideWinder IoCs

As per usual, we began our analysis by performing a bulk WHOIS lookup for the 100 domains identified as IoCs. We found out that only 83 had current WHOIS record details. Here is a breakdown of our findings for them.

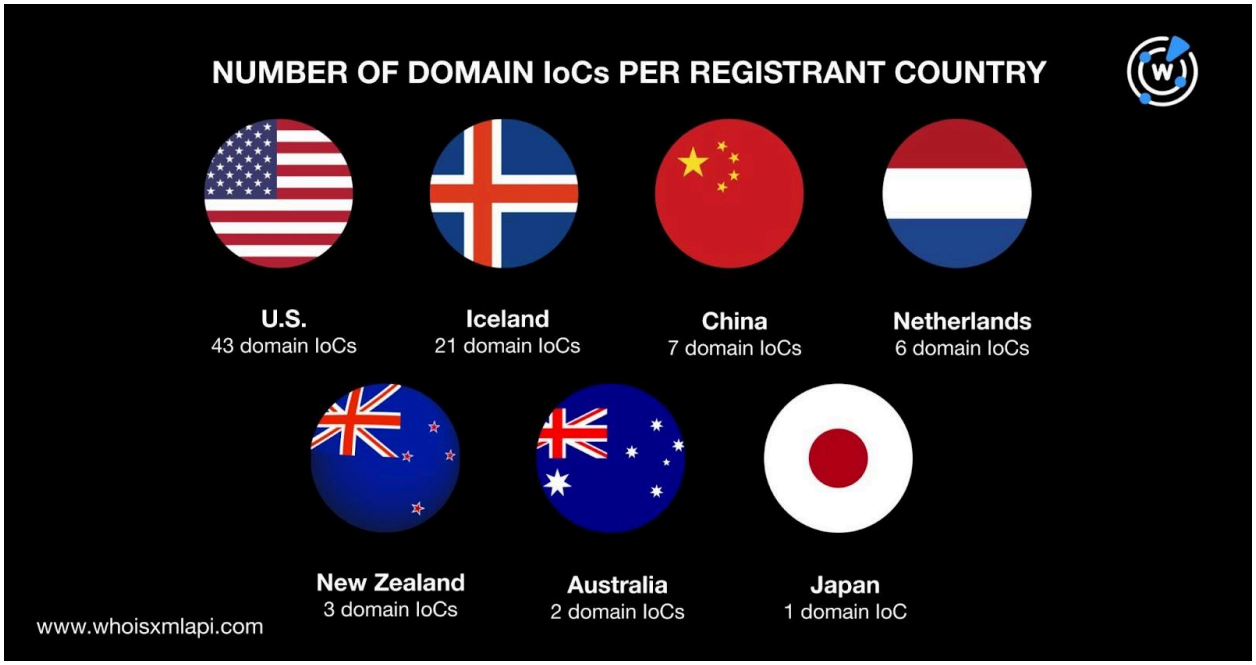
- They were administered by seven registrars led by Hostinger Operations UAB with 28 domain IoCs. Namecheap, Inc. took the second spot, accounting for 24 domains. NameSilo LLC came in third with 16 IoCs. The 15 domain IoCs left were administered

by Alibaba Cloud Computing Ltd. (seven); Hosting Concepts B.V. (six); and GMO Internet Group, Inc. and PDR Ltd. (one each).



- Thirty-one domain IoCs were created in 2023, while 52 were created in 2024.

- The domain IoCs were seemingly registered in seven countries topped by the U.S., which accounted for 43 domain IoCs. Iceland came in second place with 21 domains. China took the third spot with seven IoCs. The Netherlands (six), New Zealand (three), Australia (two), and Japan (one) completed the list of registrant countries.



On the Hunt for SideWinder-Connected Artifacts

As the first step to expand the list of domain IoCs, we queried them on WHOIS History API. That led to the discovery of 45 email addresses, 15 of which were public.

Querying the 15 public email addresses on Reverse WHOIS API revealed that two could belong to domainers, given the high number of connected domains we found, leaving us with 13 email addresses for further analysis. These 13 public email addresses appeared in the current WHOIS records of six domains after duplicates and the IoCs were filtered out.

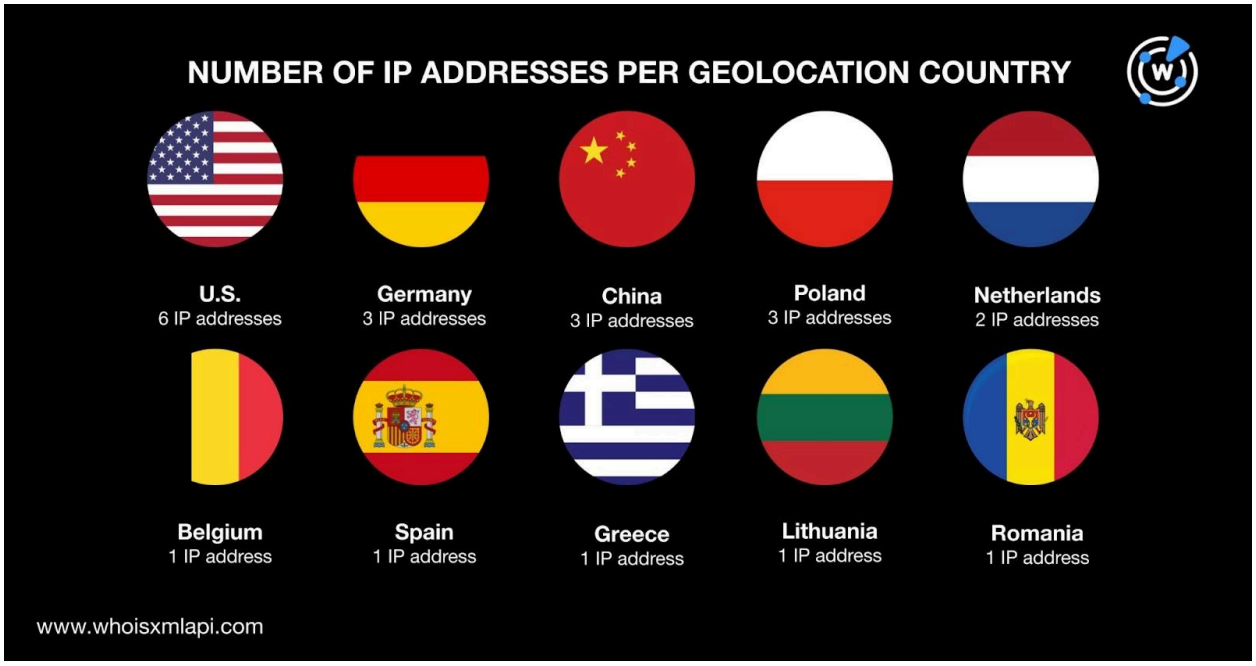
Next, we performed DNS lookups for the 83 domain IoCs and found that while 55 did not have active resolutions, 28 resolved to 22 unique IP addresses.

Threat Intelligence API showed that 20 of the 22 IP addresses were associated with various threats. Take a look at five examples below.

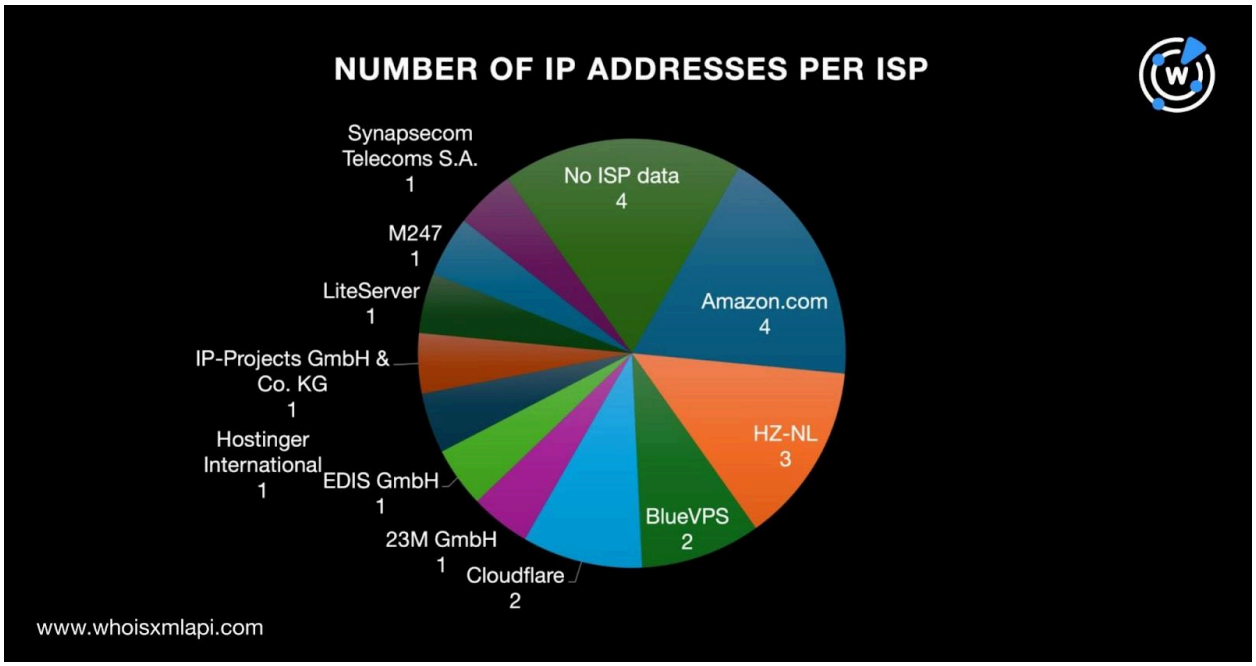
MALICIOUS IP ADDRESS	ASSOCIATED THREAT TYPE
13[.]248[.]252[.]114	Attack Command and control (C&C) Generic Malware Phishing Suspicious
172[.]67[.]208[.]176	Malware
23[.]235[.]163[.]147	Generic Malware
43[.]240[.]239[.]76	C&C Generic Malware
45[.]86[.]229[.]78	Malware

A bulk IP geolocation lookup for the 22 IP addresses revealed that:

- They were spread across 10 countries led by the U.S., which accounted for six IP addresses. The remaining countries were Germany, China, and Poland (three each); the Netherlands (two); and Belgium, Spain, Greece, Lithuania, and Romania (one each).

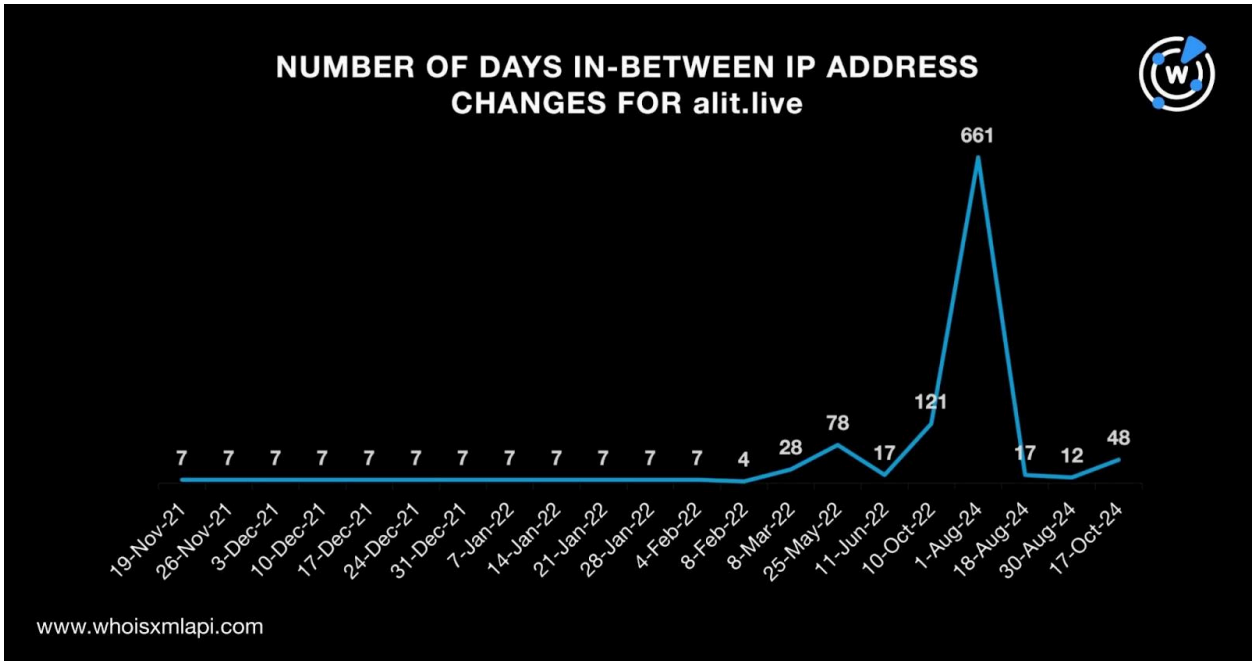


- Eighteen of them were administered by 11 ISPs led by Amazon.com, which accounted for four IP addresses. The remaining ISPs were HZ-NL (three); BlueVPS and Cloudflare (two each); 23M GmbH, EDIS GmbH, Hostinger International, IP-Projects GmbH & Co., LiteServer, M247, and Synapsecom Telecoms S.A. (one each). Four IP addresses did not have ISP information.



As the next step, we dove deeper into the historical A records of the domain IoCs using DNS Chronicle Lookup and found that 81 domain IoCs resolved to 563 IP addresses with some overlaps between 4 October 2019 and 31 October 2024.

We looked more closely at one domain IoC in particular—alit[.]live—and found that it resolved to 21 IP addresses from 19 November 2021 to 31 October 2024. It seemingly changed from one IP address to another every seven days from 19 November 2021 to 4 February 2022. Then the number of days varied widely after that.



Continuing our IoC list expansion, we performed reverse IP lookups for the 22 IP addresses and found that 14 of them could be dedicated. They hosted 176 domains after duplicates, the IoCs, and email-connected domains were filtered out.

Threat Intelligence API queries for the 176 IP-connected domains showed that 130 were associated with various threats. Take a look at five examples below.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT TYPE
adobearm[.]com	Malware
beanx99[.]xyz	Malware
calvya[.]xyz	Malware
danwza05[.]top	Malware
easycldshare[.]xyz	Malware

As the last step, we performed Domains & Subdomains Discovery searches for the 72 unique strings found among the domain IoCs, which revealed that only 47 appeared in other domains. These were:

- 126-com.
- 163inc.
- afmat.
- alit.

- aliyum.
- cnsa-gov.
- comptes.
- condet.
- conft.
- detru.
- dgps-govpk.
- dirctt88.
- direct888.
- donwloaded.
- dowmload.
- download-file.
- dynat.
- e1ix.
- e1x.
- fia-gov.
- govpk.
- gtrec.
- jmicc.
- kernet.
- mfa-gov.
- mfa-govt.
- mfagov.
- mfas.
- mofa.
- moittpk.
- navy-mil.
- newmofa.
- newoutlook.
- nopler.
- ntcpk.
- numpy.
- office-drive.
- paknavy-govpk.
- pmd-office.
- sjfu-edu.
- support-update.
- tazze.
- tni-mil.
- tsinghua-edu.
- tumet.
- u1x.
- widge.

Note that we used the **Domains only** and **Starts with** parameters to limit our search results. We uncovered 370 string-connected domains after filtering out duplicates, the IoCs, and the email- and IP-connected domains.

According to Threat Intelligence API, 21 of the 370 string-connected domains were associated with various threats. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT TYPE
163inc[.]org	Malware
alit[.]com[.]mx	Malware
aliyum[.]org	Malware
dgps-govpk[.]org	Malware

dirctt88[.]org	Malware

—

Our in-depth DNS investigation of the SideWinder IoCs led to the discovery of 574 potentially connected artifacts comprising six email-connected domains, 22 IP addresses, 176 IP-connected domains, and 370 string-connected domains. Interestingly, 171 of them have already figured in various 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

- 3315[.]com[.]cn
- 6189[.]com[.]cn
- 7286[.]com[.]cn

Sample IP Addresses

- 104[.]21[.]85[.]178
- 13[.]248[.]252[.]114
- 15[.]197[.]130[.]221
- 172[.]67[.]208[.]176
- 172[.]93[.]185[.]127
- 192[.]71[.]166[.]63
- 193[.]142[.]58[.]112
- 193[.]200[.]16[.]197
- 193[.]29[.]59[.]29
- 193[.]42[.]36[.]16

Sample IP-Connected Domains

- 32689657[.]xyz
- adobearm[.]com
- afcat[.]xyz
- afrepublic[.]xyz
- aismedu[.]com
- alligatorsviolottabackyard[.]top
- altriors[.]xyz
- anticlean[.]xyz

- appplace[.]life
- appsrv[.]live
- assbutt[.]xyz
- autodiscover[.]dualexport[.]com
- azzoodijdhgdr[.]com
- beanx99[.]xyz
- bgevin[.]live
- bingoplant[.]live
- blesis[.]live
- blingin[.]xyz
- bol-north[.]com
- bookservices[.]xyz
- breat[.]info
- bydthkk[.]top
- calvya[.]xyz
- casadomarceneiro[.]store
- cerebrovascular[.]net
- chandhor[.]top
- check-fix[.]com
- chr15[.]shop
- cikcre[.]info
- ciscohelpcenter[.]com
- cjbwsrmc[.]info
- countpro[.]info
- cpcpipe[.]com
- credmg[.]xyz
- crushter[.]info
- cssc[.]live
- cusara[.]xyz
- danwza05[.]top
- daoqaz[.]cn
- dawnon[.]live
- ddxikhexkfl[.]info
- deriksystemspartens[.]com
- docusserve[.]cc
- douyin866[.]com
- dsmes[.]xyz
- easycldshare[.]xyz
- ecstasycode[.]xyz
- enricowilli[.]top
- erdosyzd[.]com
- esrservice[.]top

Sample String-Connected Domains

- 126-com[.]cc
- 126-com[.]com
- 126-com[.]org
- 126-com[.]website
- 126-com[.]xyz
- 163inc[.]org
- afmat[.]cn
- afmat[.]or[.]tz
- afmat[.]org
- alit[.]ai
- alit[.]app
- alit[.]arab
- alit[.]ca
- alit[.]chat
- alit[.]cloud
- alit[.]cn
- alit[.]co[.]uk
- alit[.]com
- alit[.]com[.]au
- alit[.]com[.]br
- alit[.]com[.]co
- alit[.]com[.]mx
- alit[.]com[.]vn
- alit[.]cz
- alit[.]de
- alit[.]digital
- alit[.]edu[.]au
- alit[.]ee
- alit[.]fit
- alit[.]fo
- alit[.]fr
- alit[.]global

- alit[.]go[.]pw
- alit[.]int[.]la
- alit[.]is
- alit[.]jp
- alit[.]mil[.]ph
- alit[.]my[.]id
- alit[.]net[.]au
- alit[.]nl
- alit[.]one
- alit[.]org
- alit[.]org[.]cn
- alit[.]ph
- alit[.]pub
- alit[.]ru
- alit[.]se
- alit[.]tech
- alit[.]us
- alit[.]xyz
- aliyum[.]cam
- aliyum[.]co
- aliyum[.]email
- aliyum[.]fun
- aliyum[.]info
- aliyum[.]live
- aliyum[.]online
- aliyum[.]org
- aliyum[.]tk
- aliyum[.]xyz
- cnsa-gov[.]ws
- comptes[.]de
- comptes[.]il
- comptes[.]ma
- comptes[.]online
- comptes[.]org
- comptes[.]today
- condet[.]fun
- condet[.]id
- condet[.]info
- condet[.]my[.]id
- condet[.]xn--mxtq1m
- conft[.]ai
- conft[.]cf
- conft[.]dev
- conft[.]info
- conft[.]io
- conft[.]it
- conft[.]no
- conft[.]org
- conft[.]pl
- conft[.]site
- conft[.]tk
- detru[.]cn
- detru[.]org
- dgps-govpk[.]org
- dirctt88[.]com
- dirctt88[.]info
- dirctt88[.]org
- dirctt88[.]ws
- direct888[.]com
- direct888[.]org
- donwloaded[.]cfd
- dowmload[.]buzz
- dowmload[.]co
- dowmload[.]com
- dowmload[.]de
- dowmload[.]info
- dowmload[.]link
- dowmload[.]live