Investigating the UNC2975 Malvertising Campaign Infrastructure

Table of Contents

Executive Report

Mandiant's Managed Defense Threat Hunting Team recently published an in-depth study of the malware distributed via what they have dubbed the "UNC2975 malvertising campaign." Users who have been tricked into clicking poisoned sponsored search engine results and social media posts ended up with computers infected with either the DANABOT or DARKGATE backdoor.

Mandiant's in-depth analysis of the threat led to the identification of 28 indicators of compromise (IoCs), specifically 19 domains and nine IP addresses. The WhoisXML API research team, in an effort to find more information and possibly connected artifacts that have not been identified to date, expanded the list of IoCs and uncovered:

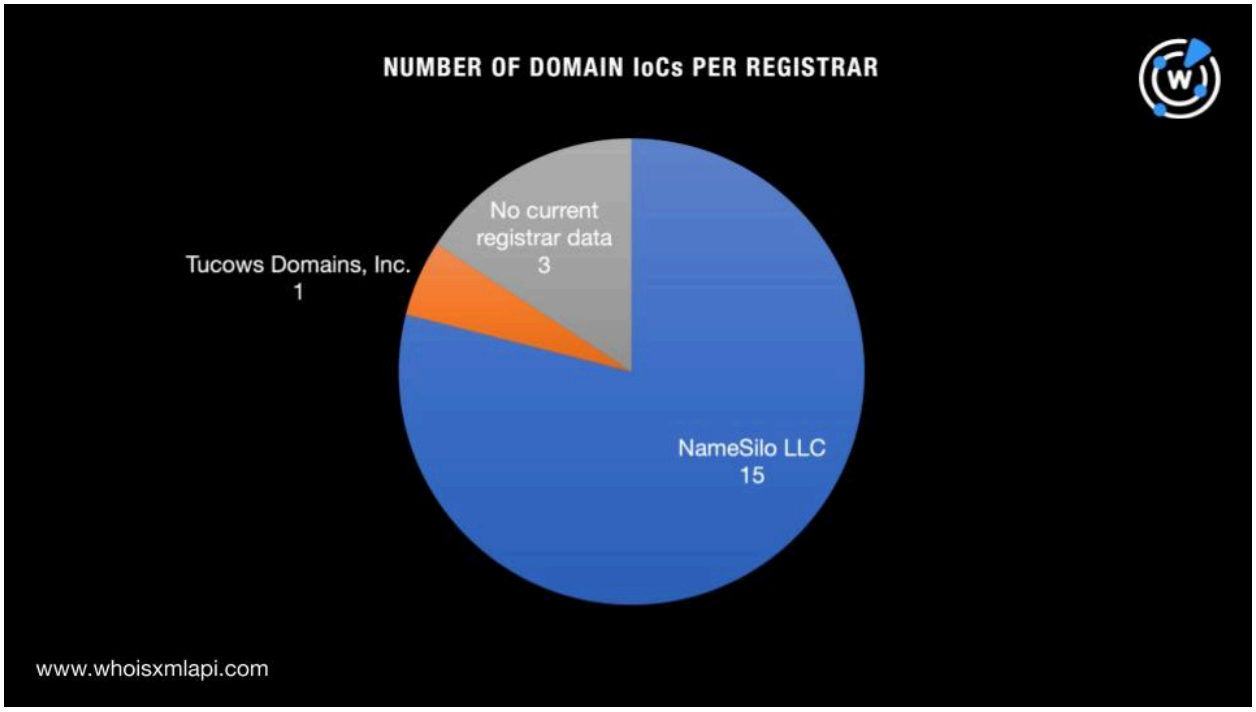
- 239 email-connected domains
- 13 IP addresses to which the domains identified as IoCs resolved
- Three IP-connected domains
- 2,772 string-connected domains

A Closer Look at the UNC2975 IoCs

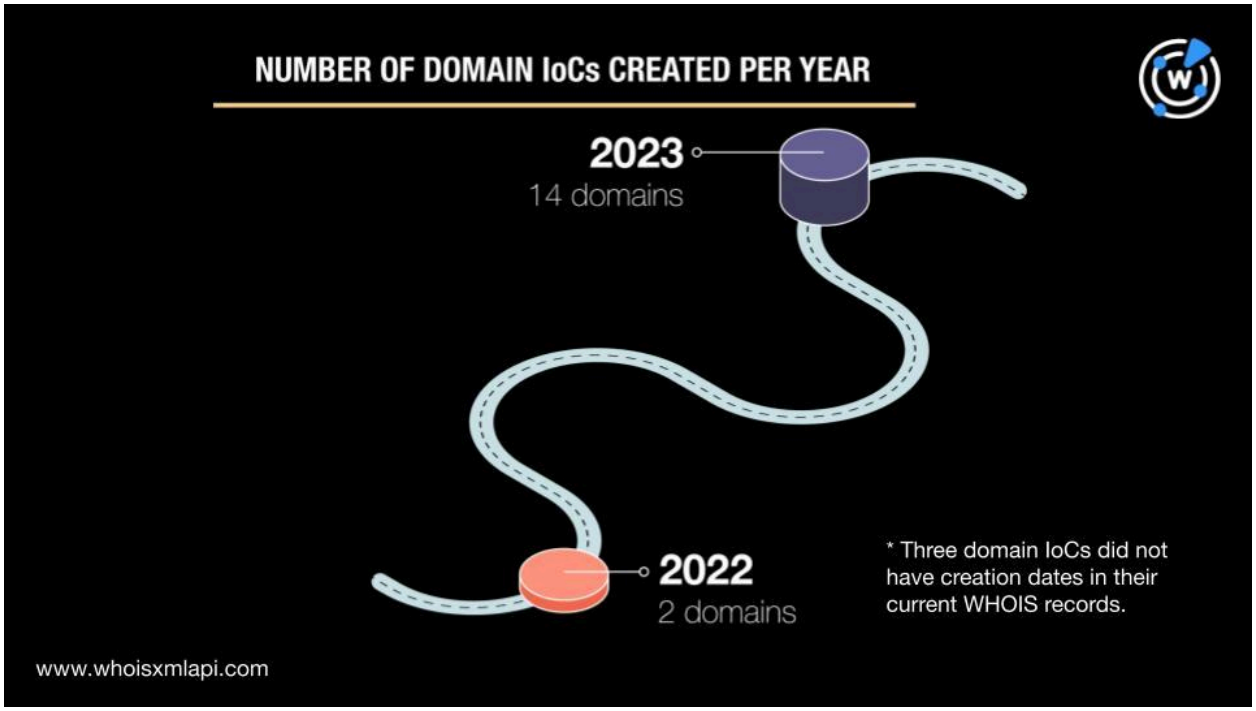
As is our usual first step, we sought to find more information on the domains and IP addresses that Mandiant identified as IoCs.

We began by performing a bulk WHOIS lookup on the 19 domains and found that:

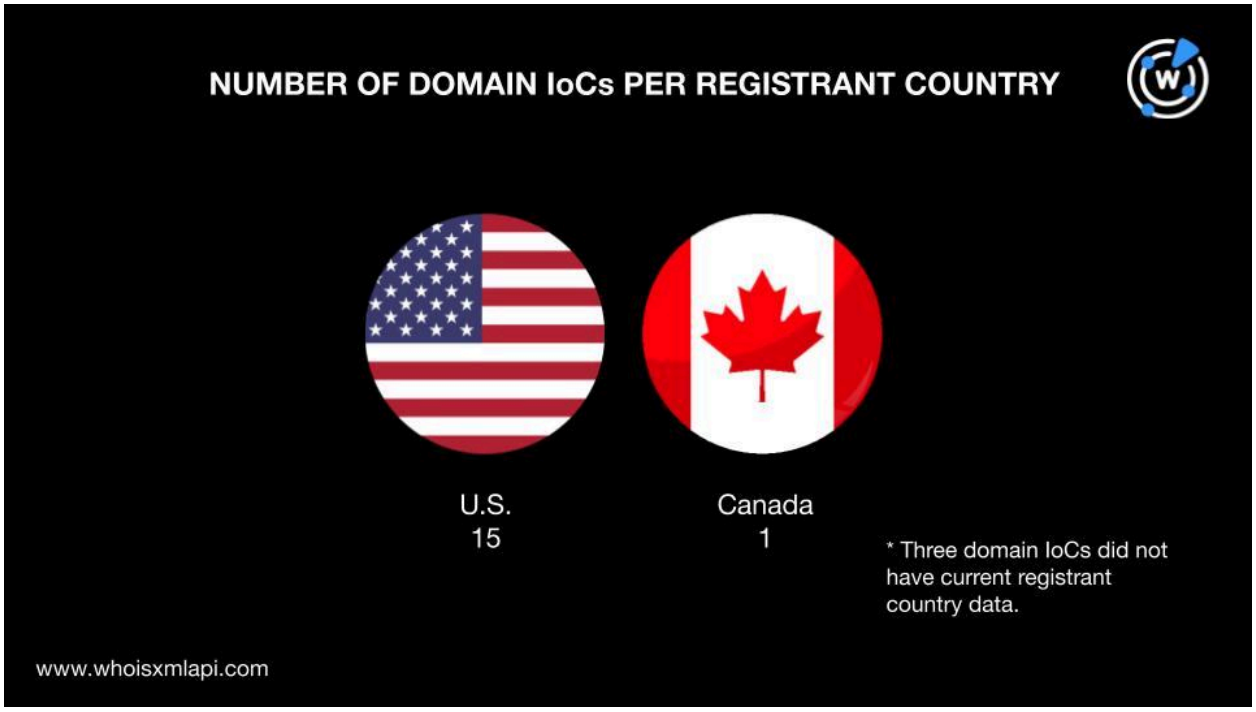
- They were administered by two registrars—NameSilo LLC, which accounted for 15 domains, and Tucows Domains, Inc., which accounted for one domain. The remaining three domains did not have current registrar data.



- A majority of them were relatively new—14 were created in 2023 and two in 2022. The remaining three domains did not have creation dates retrievable from current WHOIS records.

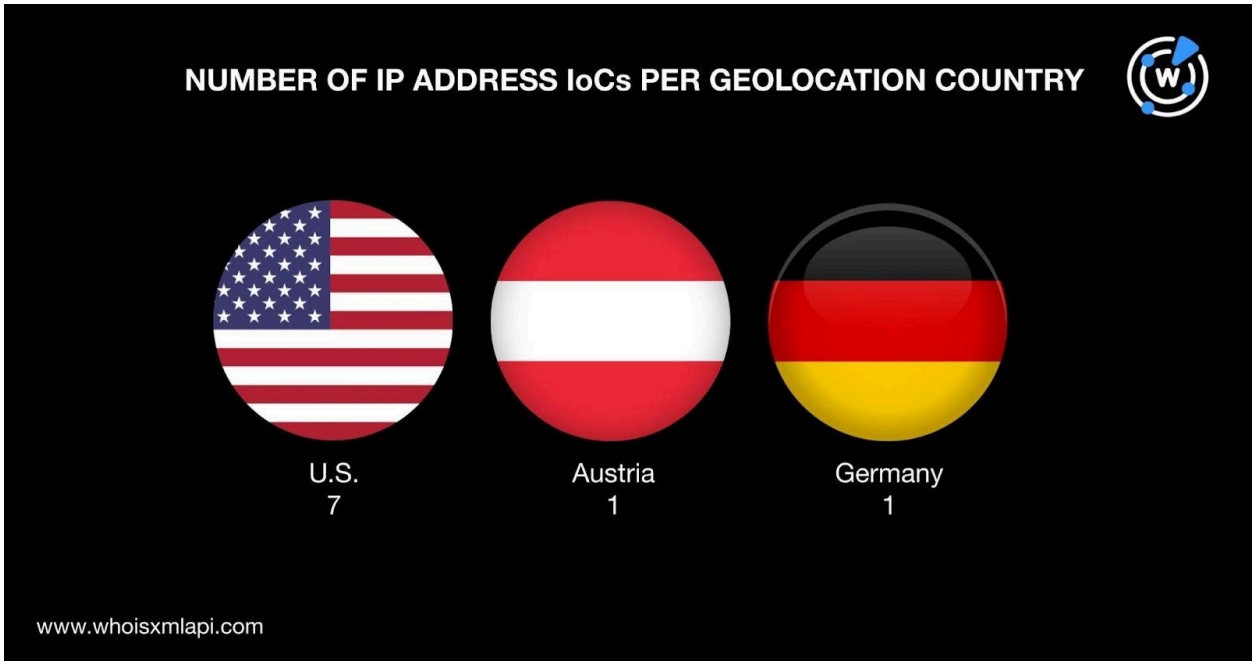


- They were spread across two registrant countries—15 domains were supposedly registered in the U.S. and one in Canada. Three domains did not have current registrant country data.

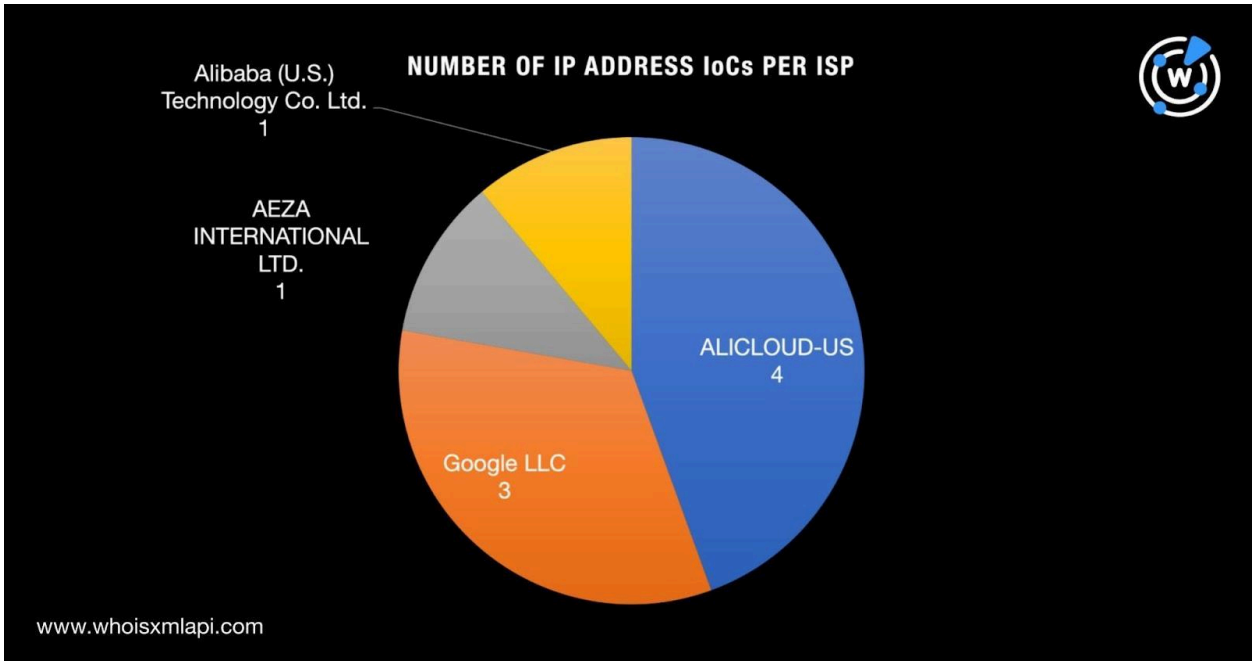


Next, we subjected the nine IP addresses to a bulk IP geolocation lookup, which revealed that:

- They were spread across three geolocation countries—seven in the U.S. and one each in Austria and Germany.



- They were administered by four Internet service providers (ISPs) topped by ALICLOUD-US with four IP addresses. Google LLC handled three IP addresses and AEZA INTERNATIONAL LTD. and Alibaba (U.S.) Technology Co. Ltd. managed one IP address each.



UNC2975 DNS Connections

To unveil as many potentially connected UNC2975 artifacts as possible, we looked at the WHOIS records of the 19 domains identified as IoCs first.

WHOIS History API searches showed that seven of them had 15 email addresses in total in their WHOIS records, 13 of which were public.

Next, Reverse WHOIS API searches for the 13 public email addresses revealed that only five were present in the current WHOIS records of 239 other domains after duplicates and the IoCs were filtered out.

Screenshot API searches for the 239 email-connected domains showed that only one continued to host live content as of this writing.

Screenshot of email-connected domain nasheradio[.]us

We then subjected the 19 domains identified as IoCs to DNS lookups and found that 10 of them actively resolved to 13 IP addresses after duplicates and those already identified as IoCs were removed.

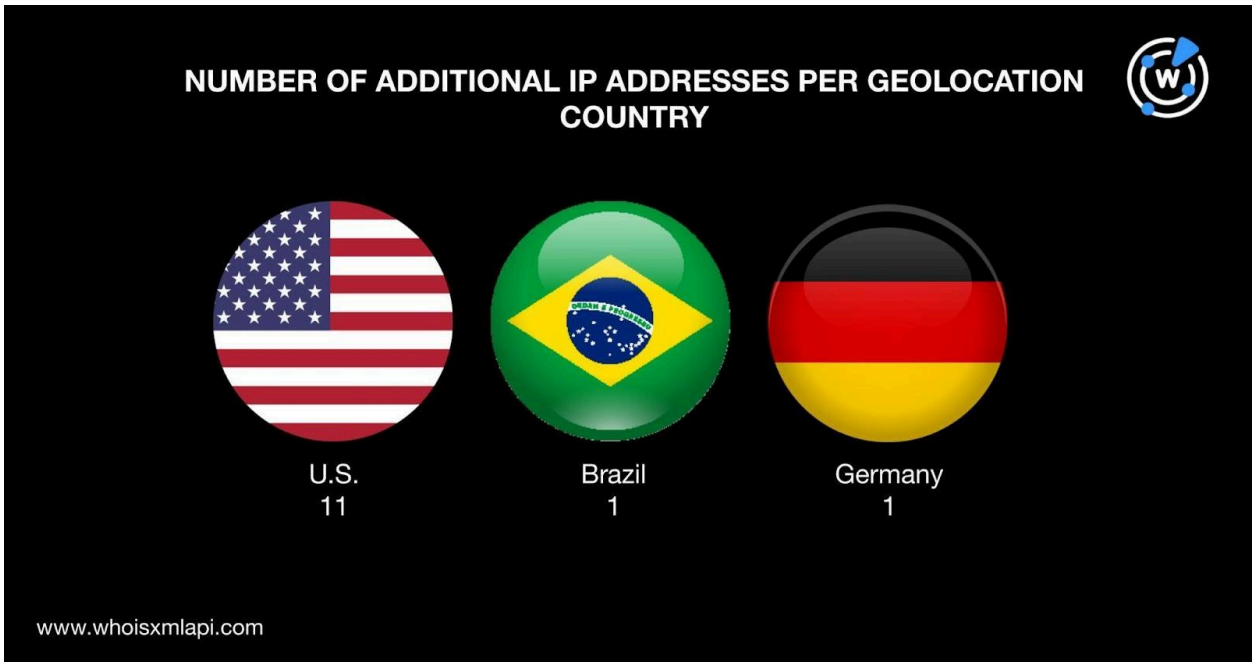
Threat Intelligence API searches for the 13 additional IP addresses showed that all of them were associated with various threats. Take a look at our specific findings for each below.

IP ADDRESS	NUMBER OF ASSOCIATED THREATS	ASSOCIATED THREAT TYPES
104[.]21[.]29[.]244	3	Generic Phishing Malware
104[.]21[.]4[.]50	3	Malware Phishing Generic
104[.]21[.]43[.]177	3	Malware Phishing Generic
104[.]21[.]62[.]212	1	Malware
104[.]21[.]65[.]69	1	Malware
104[.]21[.]69[.]249	3	Phishing Malware Generic
172[.]67[.]131[.]172	3	Malware Phishing Generic
172[.]67[.]139[.]87	1	Malware
172[.]67[.]150[.]3	3	Generic Phishing Malware
172[.]67[.]182[.]165	3	Malware Phishing Generic
172[.]67[.]189[.]35	1	Malware

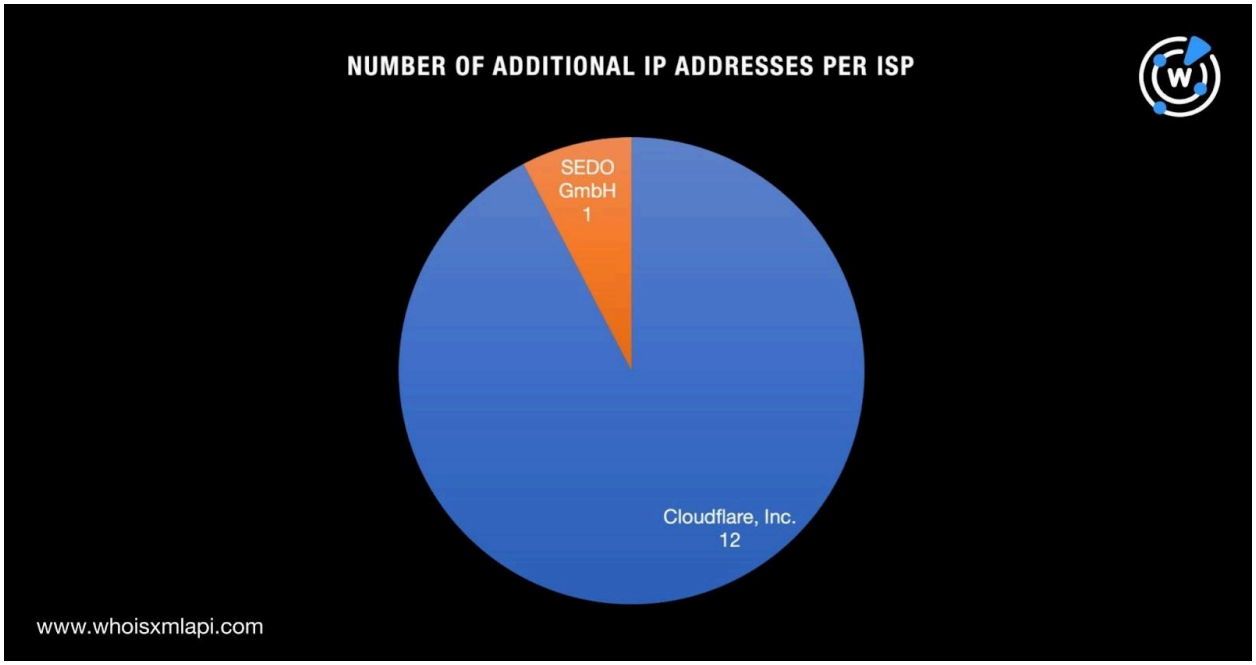
172[.]67[.]216[.]21	3	Phishing Malware Generic
91[.]195[.]240[.]12	5	Malware Phishing Generic Suspicious C2

A bulk IP geolocation lookup for the additional 13 IP addresses revealed that:

- Like the IP addresses identified as IoCs, a majority of them, 11 to be exact, seemed to be geolocated in the U.S. One each appeared to originate from Brazil and Germany.



- A huge chunk of them, 12 to be exact, were administered by Cloudflare, Inc. One was under the purview of SEDO GmbH. None of them had the same ISP as any of the IP addresses identified as IoCs.



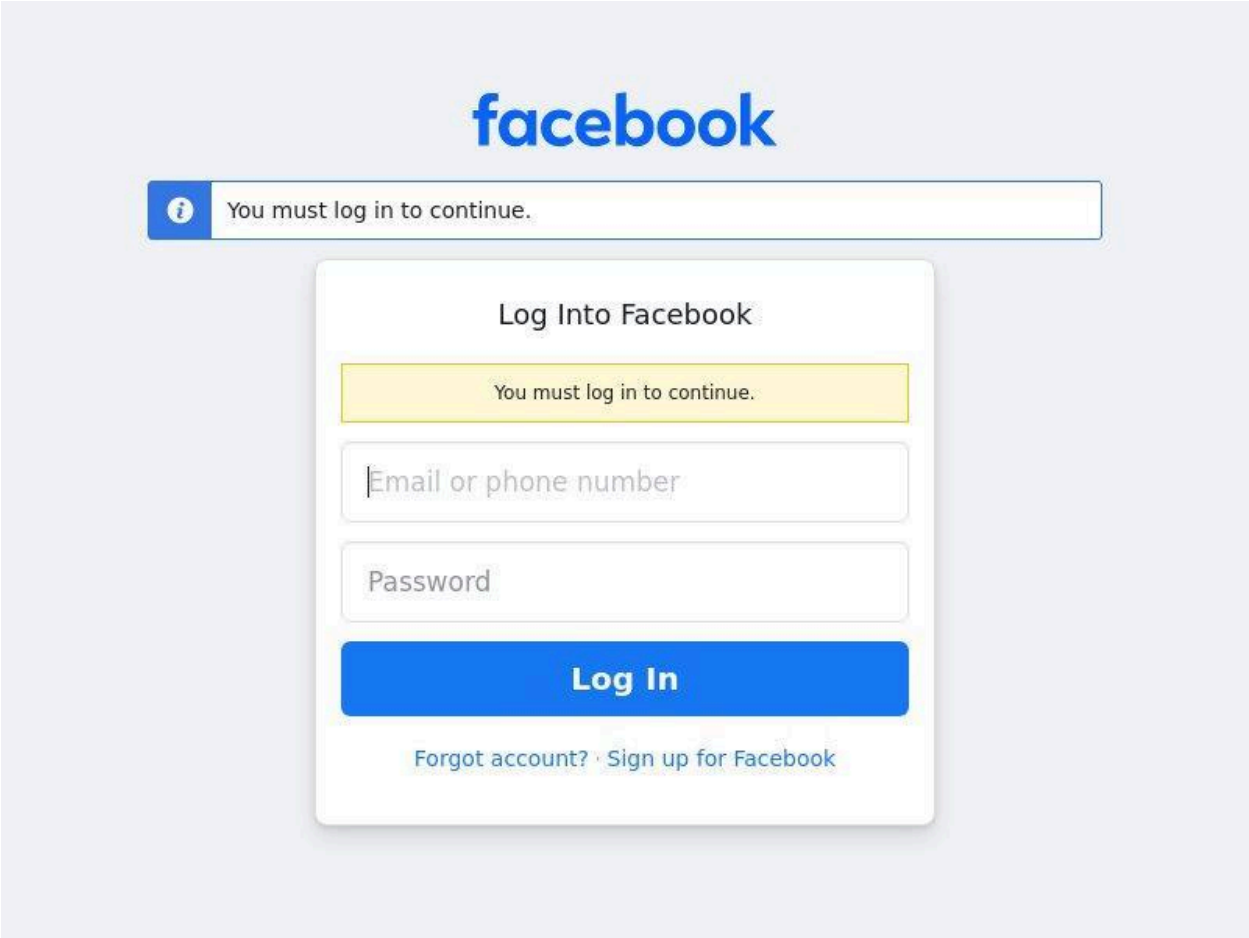
Next, we subjected the 22 IP addresses, the nine identified as IoCs and 13 additional, to reverse IP lookups and found that three of them seemed to be dedicated hosts. Altogether, they hosted three additional domains after the duplicates, IoCs, and email-connected domains were filtered out.

To cover all of our bases, we further scrutinized the 19 domains identified as IoCs and found that they contained text strings that appeared in 2,772 other domains after duplicates, the IoCs, and email- and IP-connected domains were removed. We specifically used the following as search strings on Domains & Subdomains Discovery using the **Starts with** parameter:

- **assetfinder**
- **barracudas**
- **bikeontop**
- **capitalfinders**
- **claimprocessing**
- **claimunclaimed**
- **dreamteamup**
- **freelookup**
- **gfind**
- **halibut**
- **infocatalog**
- **lewru**
- **lugbara**
- **myunclaimedcash**
- **positivereview**
- **soulcarelife**
- **thebesttime**
- **treasurydept**
- **whatup**

Screenshot lookups for the string-connected domains revealed that 379 continued to host live content to date. String-connected domain whatuptrepstars[.]com, in particular, proved

interesting in that it led to what seemed to be a Facebook login page even if it could not be publicly attributed to the social media platform based on its WHOIS record details.



Screenshot of string-connected domain whatuptrepstars[.]com

In addition, based on Threat Intelligence API checks, the string-connected domain halibut[.]site was associated with one threat, specifically malware.

—

Our follow-up investigation on UNC2975 led to the discovery of 3,027 email-, IP-, and string-connected artifacts. It is also worth noting that 14 of them—13 IP addresses and one string-connected domain—were associated with threats or have already been classified as malicious.

If you wish to perform a similar investigation or 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 and IoCs

UNC2975 IoCs

DOMAINS	IP ADDRESSES
assetfinder[.]org barracudas[.]sbs bikeontop[.]shop capitalfinders[.]org claimprocessing[.]org claimunclaimed[.]org dreamteamup[.]shop freelookup[.]org gfind[.]org halibut[.]sbs infocatalog[.]pics lewru[.]top lugbara[.]top myunclaimedcash[.]org positivereview[.]cloud soulcarelife[.]org thebesttime[.]buzz treasurydept[.]org whatup[.]cloud	34[.]16[.]181[.]0 35[.]203[.]111[.]228 35[.]247[.]194[.]72 47[.]252[.]33[.]131 47[.]252[.]45[.]173 47[.]253[.]141[.]12 47[.]253[.]165[.]1 8[.]209[.]99[.]230 94[.]228[.]169[.]143

Sample Email-Connected Domains

- academic-advising[.]org
- admissionsrequirements[.]net
- alvincommunitycollege[.]net
- americanacademyofaudiology[.]org
- americanacademyofdermatology[.]org
- americanboardofpediatrics[.]org
- americanindiancollege[.]org
- americansocietyofradiologictechnologists[.]com
- associatedstudents[.]net
- athenstechnicalcollege[.]org
- athleticdept[.]org
- atlantadevelopmentauthority[.]com

- beaumontadultschool[.]com
- bentleycollege[.]org
- bethune-cookmancollege[.]com
- bethune-cookmanuniversity[.]com
- boblogan[.]us
- bollingairforcebase[.]com
- brownmackiecollege[.]org
- building-inspector[.]org
- bureauoflaborstatistics[.]org
- butlercountycommunitycollege[.]com
- cadlang[.]org
- californiavirtualcampus[.]com
- campus-security[.]org
- capitolcenterforthearts[.]com
- capt-kirk[.]org
- charter-school[.]org
- checkpageranking[.]org
- checkpagerankings[.]org
- chemicalphysics[.]net
- chemistryteacher[.]net
- choaterosemaryhall[.]org
- christian-college[.]org
- city-data[.]biz
- citycollegecoventry[.]com
- citycollegenorwich[.]com
- citydata[.]mobi
- citydatabase[.]org
- cityofaiken[.]org
- cityofakron[.]net
- cityofaventura[.]org
- cityofbathcollege[.]com
- cityofbend[.]org
- cityofkennewick[.]org
- cityoflubbock[.]net
- cityofpomona[.]org
- cityofrifle[.]com
- cityofsanford[.]net
- cityofunioncity[.]org

Sample Additional IP Addresses

- 104[.]21[.]29[.]244
- 104[.]21[.]4[.]50
- 104[.]21[.]43[.]177
- 104[.]21[.]62[.]212
- 104[.]21[.]65[.]69
- 104[.]21[.]69[.]249

Sample IP-Connected Domains

- 94[.]228[.]169[.]143[.]sslip[.]io
- lifesoul[.]top

Sample String-Connected Domains

- assetfinder-rws[.]com
- assetfinder[.]biz
- assetfinder[.]cl
- assetfinder[.]club
- assetfinder[.]cn
- assetfinder[.]co
- assetfinder[.]co[.]uk
- assetfinder[.]com
- assetfinder[.]com[.]au
- assetfinder[.]de
- assetfinder[.]expert
- assetfinder[.]ie
- assetfinder[.]in
- assetfinder[.]info
- assetfinder[.]net
- assetfinder[.]net[.]au

- assetfinder[.]online
- assetfinder[.]services
- assetfinder[.]sh
- assetfinder[.]uk
- assetfinder[.]us
- assetfinder[.]xyz
- assetfinder02[.]com
- assetfinder02[.]ph
- assetfinder1[.]com
- assetfinder123[.]com
- assetfinder18[.]com
- assetfinder20[.]com
- assetfinder4[.]com
- assetfinder49[.]com
- assetfinder4u[.]com
- assetfinder4unow[.]com
- assetfinder56[.]com
- assetfinder56[.]ws
- assetfinder72[.]com
- assetfinder88[.]com
- assetfinderandrecovery[.]com
- assetfinderassociates[.]com
- assetfindercloud[.]com
- assetfinderco[.]com
- assetfinderconsultant[.]com
- assetfinderexperts[.]com
- assetfinderexperts[.]ws
- assetfindergroup[.]com
- assetfinderhub[.]com
- assetfinderllc[.]com
- assetfindernetwork[.]com
- assetfinderonline[.]com
- assetfinderonus[.]com
- assetfinderplus[.]com
- assetfinderpro[.]com
- assetfinderproject[.]com
- assetfinderpros[.]com
- assetfinderpros[.]net
- assetfinderr[.]com
- assetfinderrecovery[.]com
- assetfinders[.]biz
- assetfinders[.]com
- assetfinders[.]eu
- assetfinders[.]ie
- assetfinders[.]info
- assetfinders[.]net
- assetfinders[.]org
- assetfinders[.]us
- assetfinders007[.]com
- assetfinders123[.]com
- assetfinderservice[.]com
- assetfinderservices[.]com
- assetfindersgroup[.]com
- assetfindersinc[.]com
- assetfindersllc[.]com
- assetfindersllc[.]net
- assetfindersltd[.]com
- assetfindersnetwork[.]com
- assetfindersofamerica[.]com
- assetfindersofamerica[.]us
- assetfindersplus[.]com
- assetfindersrus[.]com
- assetfindersusa[.]com
- assetfindersusa1[.]com
- assetfinderteam[.]com
- assetfinderteam[.]info
- assetfinderteam[.]net
- assetfinderteam[.]org
- assetfindertoolkit[.]com
- assetfinderunlimited[.]com
- assetfinderunlimitedllc[.]com
- assetfinderusa[.]com
- assetfinderz[.]com
- barracudas-ambassadors[.]com
- barracudas-aquarama[.]co[.]za
- barracudas-aquarama[.]com
- barracudas-baseball[.]com
- barracudas-comms[.]co[.]uk
- barracudas-dive[.]ru
- barracudas-hotel[.]ru

- barracudas-hotel[.]xn--kprw13d
- barracudas-hotel[.]xn--kpry57d
- barracudas-hurricanes[.]dk
- barracudas-nue[.]de