Sneaking a Peek into the Inner DNS Workings of Sneaky 2FA

Table of Contents

Executive Report

Sneaky 2FA, believed to be sold via the phishing-as-a-service (PhaaS) business model, recently figured in an adversary-in-the-middle (AitM) attack targeting Microsoft 365 users. Marketed as Sneaky Log by a full-featured bot on Telegram, Sneaky 2FA reportedly used fake Microsoft authentication pages with automatically filled-in email address fields to add to its sense of authenticity.

Sekoia published their in-depth investigation on Sneaky 2FA in "Sneaky 2FA: Exposing a New AitM Phishing-as-a-Service" and identified at least 61 indicators of compromise (IoCs) comprising 57 domains, two IP addresses, and two subdomains.

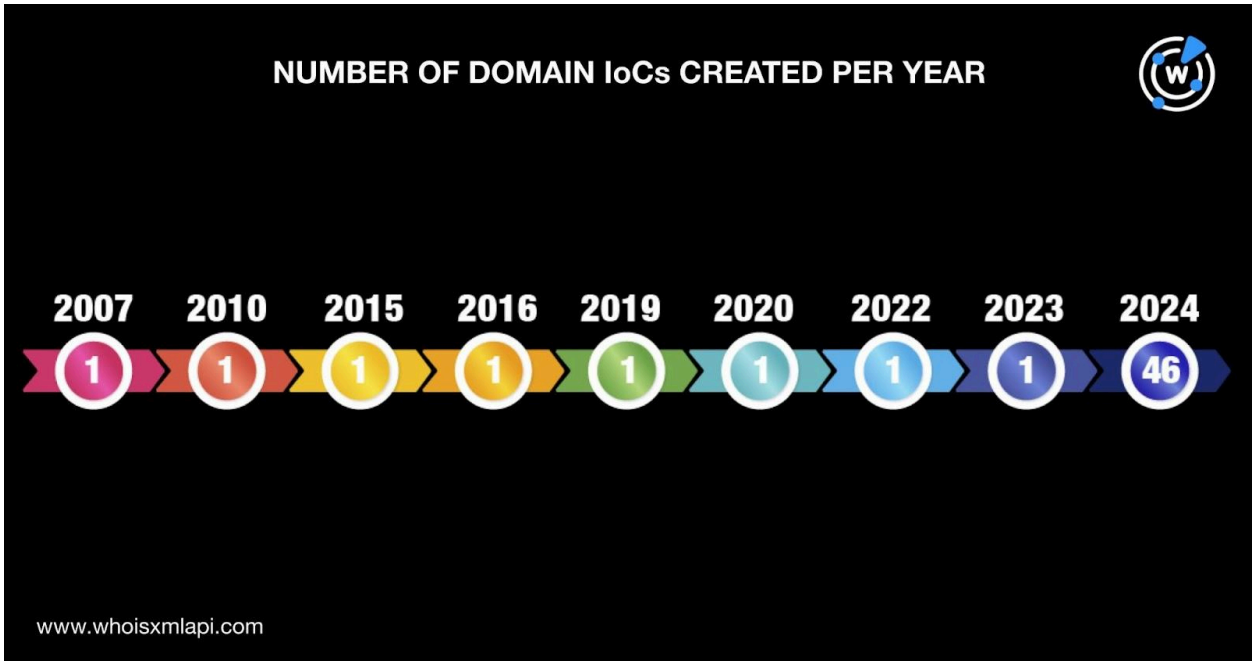
The WhoisXML API research team expanded the current list of IoCs in a bid to find more connected artifacts and uncovered:

- 342 email-connected domains based on historical WHOIS records, 14 of which have already been weaponized for various campaigns
- 49 additional IP addresses, 36 of which turned out to be malicious
- 235 IP-connected domains, two of which have already been tagged as malicious
- 216 string-connected domains, one of which has already figured in a malicious campaign
- 50 string-connected subdomains

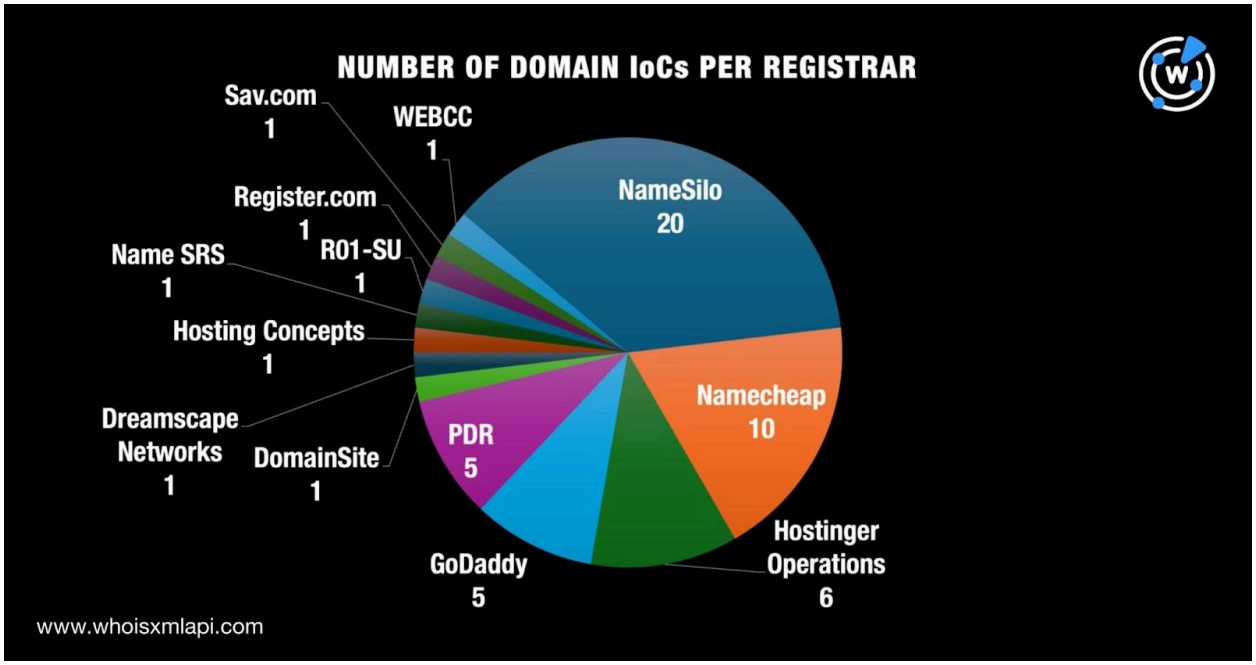
Facts about the Sneaky 2FA IoCs

To gather more information about the IoCs, we first queried the 57 domains identified as such on Bulk WHOIS API. We found that only 54 of them had current WHOIS records. Their records revealed the following:

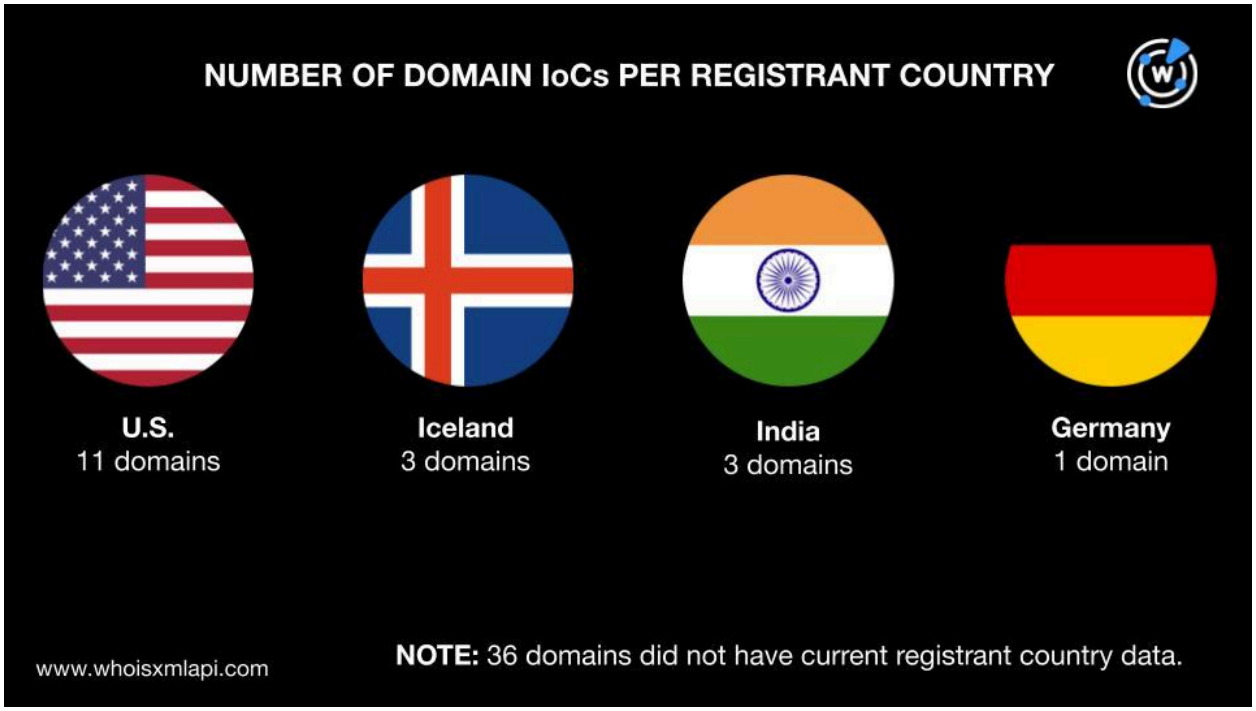
- A majority of the domains, 46 to be exact, were created in 2024. One domain each was created in 2007, 2010, 2015, 2016, 2019, 2020, 2022, and 2023.



- They were administered by 13 different registrars led by NameSilo, which accounted for 20 domains. Namecheap came in second place with 10 domains. In third place was Hostinger Operations with six domains. GoDaddy and PDR tied in fourth place with five domains each. Finally, DomainSite, Dreamscape Networks, Hosting Concepts, Name SRS, R01-SU, Register.com, Sav.com, and WEBCC accounted for one domain each.



- Only 18 of them had registrant countries listed in their current WHOIS records. The U.S. was the top registrant country, accounting for 11 domains. Iceland and India tied in second place with three domains each. Germany accounted for one domain.

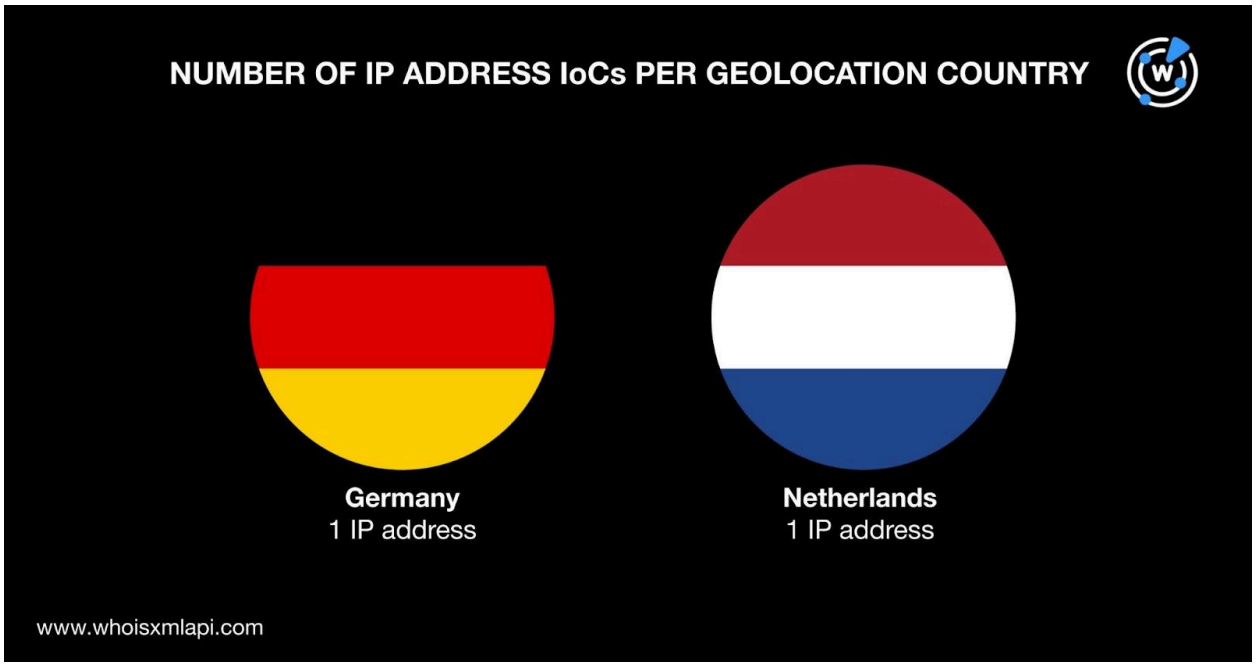


We also queried the 57 domains tagged as IoCs on DNS Chronicle API and found that only 53 had recorded historical IP resolutions. Altogether, they recorded 1,184 IP resolutions over time. The IoC usfightingsystems[.]com recorded the oldest IP resolution on 4 October 2019. Take a look at the DNS histories of five other examples below.

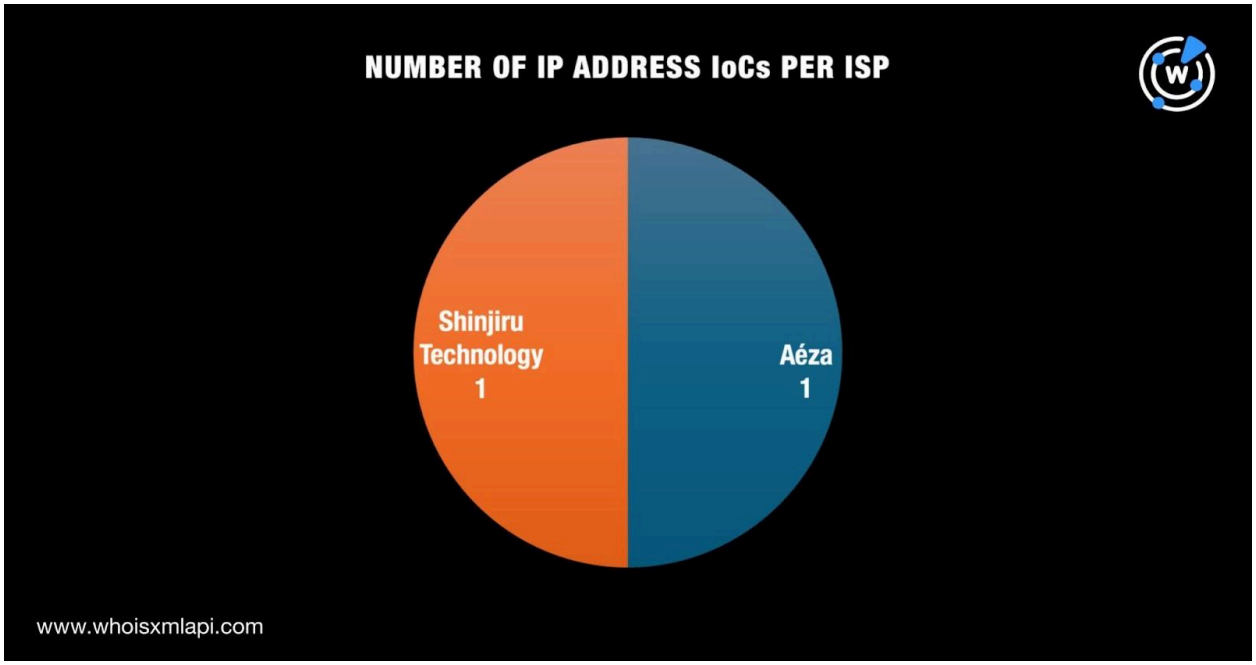
DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
advanceplastics-ke[.]com	13	11 January 2025
drop-project[.]top	4	3 December 2024
intertrustsgroup[.]com	43	11 October 2019
organichoicehome[.]com	4	7 December 2024
storageorder[.]sbs	14	18 December 2024

We then looked more closely at the two IP addresses identified as IoCs by querying them on Bulk IP Geolocation Lookup, which revealed that:

- Each was geolocated in a different country—one in Germany and the other in the Netherlands.



- They were also administered by two different ISPs—one by Shinjiru Technology and the other by Aéza.



As with the domains tagged as IoCs, we queried the two IP addresses on DNS Chronicle API. We found that only one recorded domain resolutions. In particular, 101[.]99[.]92[.]124 posted 14 domain resolutions over time starting on 6 February 2024.

Sneaky 2FA IoC List Expansion Findings

To find other web properties possibly connected to Sneaky 2FA, we began by querying the 57 domains tagged as IoCs on WHOIS History API. We discovered that 33 had 60 email addresses after duplicates were filtered out in their historical WHOIS records. Further scrutiny revealed that 12 of the email addresses were public.

We queried the 12 public email addresses on Reverse WHOIS API in a bid to uncover email-connected domains. Our search, however, revealed that none of them appeared in the current WHOIS records of other domains.

So, we dug deeper. We queried the 12 public email addresses on Reverse WHOIS Search using the **Historic** parameter and discovered that 11 had connections. In particular, the addresses appeared in the historical WHOIS records of 342 email-connected domains after duplicates and those already tagged as IoCs were filtered out.

Threat Intelligence API queries for the 342 email-connected domains revealed that 14 have already been weaponized for various campaigns. Take a look at five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREATS
4baeuty4you[.]com	Generic threat Phishing
brenntags-asia[.]com	Generic threat Phishing
nautadutlih[.]com	Generic threat Phishing
rawbles[.]com	Generic threat Phishing
sulyaks[.]net	Generic threat Phishing

As the next step, we queried the 57 domains identified as IoCs on DNS Lookup API and found that 38 resolved to 49 additional IP addresses after duplicates and those already tagged as IoCs were filtered out.

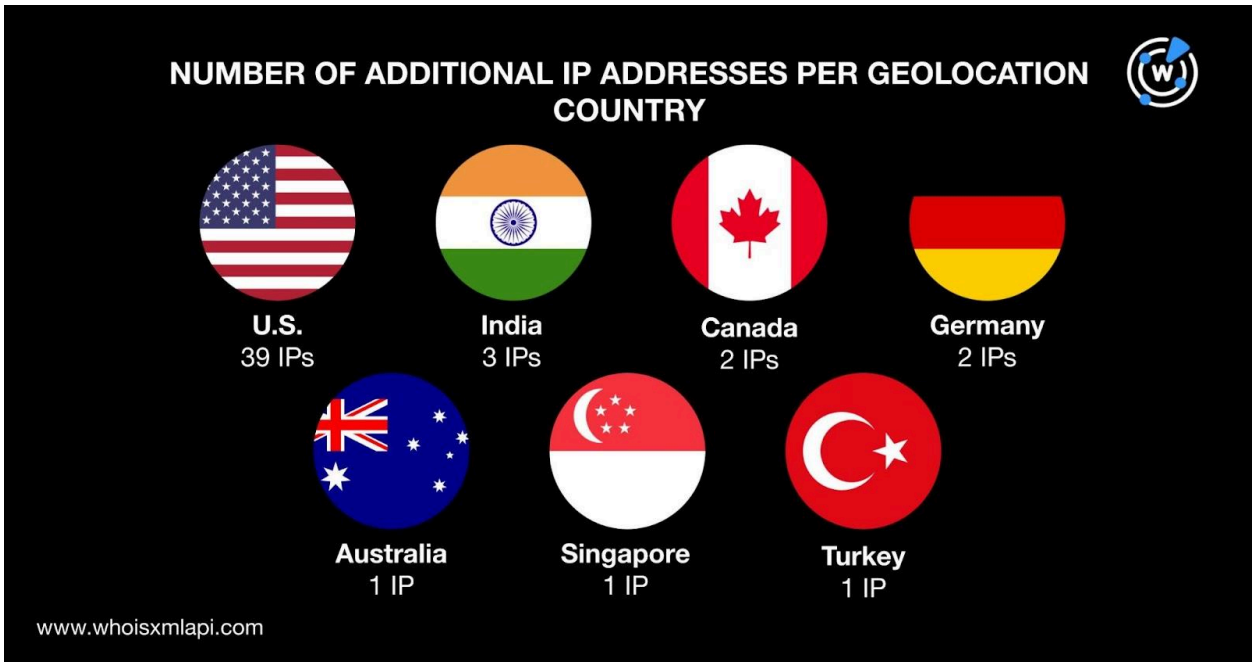
Threat Intelligence API queries for the 49 additional IP addresses showed that 36 have already been weaponized for various campaigns. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
103[.]83[.]194[.]55	Attack Generic threat Malware distribution Phishing
104[.]21[.]4[.]206	Malware distribution Phishing
104[.]21[.]80[.]1	Attack Command and control (C&C) Generic threat Malware distribution Phishing Suspicious activity

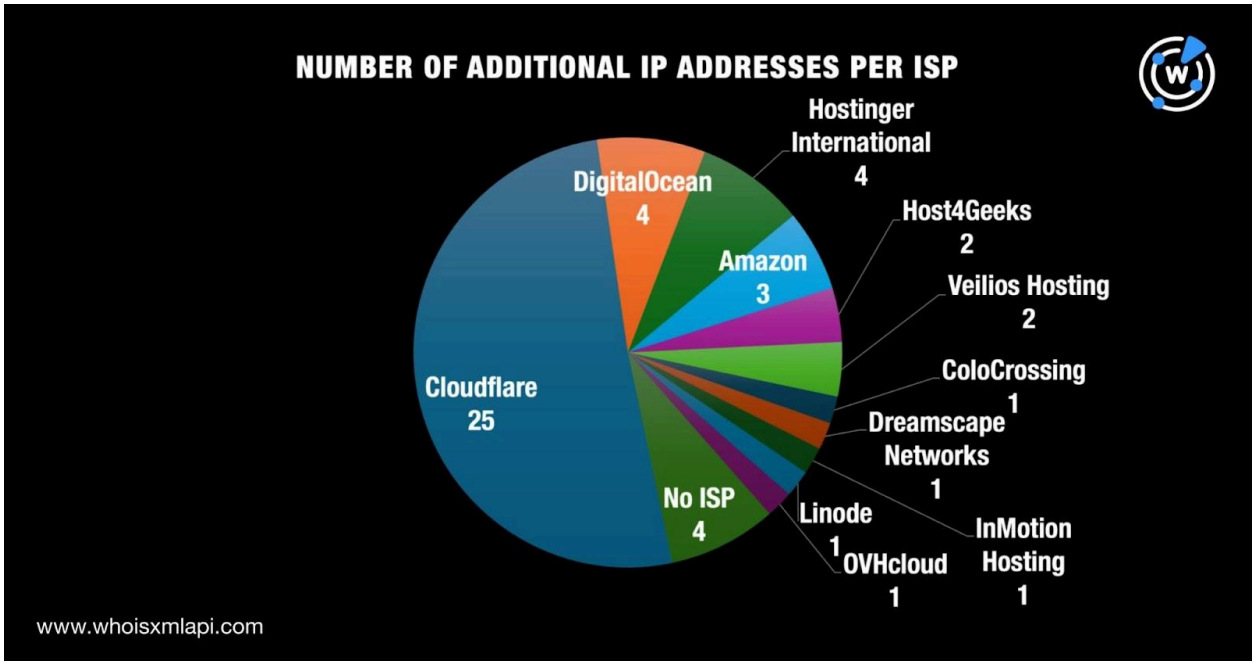
172[.]105[.]62[.]200	Generic threat
172[.]67[.]188[.]224	Malware distribution Suspicious activity

We also queried the 49 additional IP addresses on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in seven different countries led by the U.S., which accounted for 39 IP addresses. India came in second place with three IP addresses. Canada and Germany tied in third place with two IP addresses each. Australia, Singapore, and Turkey completed the list with one IP address each.



- Only 45 of them had ISP information in their A records. Cloudflare administered 25 IP addresses. DigitalOcean and Hostinger International accounted for four IP addresses each. Amazon took the next spot with three IP addresses. Host4Geeks and Veilios Hosting accounted for two IP addresses each. Finally, ColoCrossing, Dreamscape Networks, InMotion Hosting, Linode, and OVHcloud accounted for one IP address each.



We now had 51 IP addresses on our list (i.e., two identified as IoCs and 49 additional) for further analysis. A Reverse IP API query for them revealed that 13 could be dedicated hosts. These 13 IP addresses also hosted 235 other domains after duplicates, those already tagged as IoCs, and the email-connected domains were filtered out.

Threat Intelligence API queries for the 235 IP-connected domains showed that two have already been classified as malicious. The domain 1mam1[.]com, for instance, was associated with a generic threat.

Next, we looked for other domains that started with the same text strings as those already identified as IoCs using Domains & Subdomains Discovery. We found that these 38 strings appeared in other domains:

- africanagrirnarket.
- alliedhealthcaresolution.
- bhlergroup.
- claytoncontsruction.
- desirenetwork.
- docuinshare.
- dolh6growth.
- dreamwp.
- drop-project.
- emailsay.
- emea-nec.
- erhakalip.
- files42.
- glamorouslengths.
- greyscaleal.
- guardiansresearch.
- historischeverenigingmarum.
- intertrustsgroup.
- lovencareurology.
- matcocomponent.

- ms-consulting-dom.
- mypi.
- omnirayoprah.
- outsourcel.
- profitminers.
- reintergestna.
- rurrasqueamos.
- sneakylog.
- stillmanconsulting.
- storageorder.
- sysarchirnc.
- tvsyndciate.
- urbanumbrella.
- usfightingsystems.
- webitww.
- welcomehomeproject.
- windstreaim.
- wwgle.

Specifically, the 38 text strings listed above led to the discovery of 216 string-connected domains after duplicates, those already tagged as IoCs, and the email- and IP-connected domains were filtered out.

Threat Intelligence API queries for the 216 string-connected domains showed that one—mypi[.]co—has already figured in a malicious campaign featuring a generic threat.

As our last step, we searched for subdomains that started with the string **loginoffice365** akin to the two subdomains already identified as IoCs. We uncovered 50 string-connected subdomains that could figure in similar threats targeting Microsoft 365.

—

Our DNS deep dive into Sneaky 2FA led to the discovery of 892 potentially connected artifacts comprising 342 email-connected domains, 49 additional IP addresses, 235 IP-connected domains, 216 string-connected domains, and 50 string-connected subdomains. Security teams may wish to be especially wary of 53 of these artifacts since they 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

- 0bsadoo[.]com
- 1gld1[.]com
- 1pho1[.]com
- a1ahli[.]com
- a1naksa[.]com
- abahsainweldings[.]com
- babasibiherbs[.]com
- babassidiherbs[.]com
- bakerybazaar[.]com
- candvv-lc[.]com
- candw-lc[.]com
- carg0fe[.]com
- danvillemartialarts[.]com
- dbmscsteel-ae[.]com
- deedsofdignity[.]com
- ecctowers[.]com
- ei8m[.]com
- ei8support[.]com
- familydefensetips[.]com
- ff-e-t[.]com
- fkexp0rt[.]com
- getadcoin[.]com
- getinvitedintoschools[.]com
- getviraltees[.]com
- hansafinances[.]com
- herbsamix[.]com
- himi1e[.]com
- innovatorreport[.]com
- internationalcombustion-in[.]com
- internetvideoaudio[.]com
- j0ma-sport[.]com
- jkleebeyourbest[.]com
- joezimjs[.]com
- kangsacademy[.]com
- kangsblackbelt[.]com
- kanpurcabs[.]com
- leemedpharmaceuticals[.]com
- lindenhurstmartialarts[.]com
- lirnakskopje[.]com
- madvet[.]in
- maenetwork[.]com
- maisoncouture[.]shop
- nautadutlih[.]com
- nbmingsings[.]com
- nbrningsing[.]com
- obasdoo[.]com
- oleyinsights[.]com
- oleysgurus[.]com
- pacificprirne[.]com
- packerhalloffamers[.]com
- parampastries[.]com
- qsdk0rea[.]com
- r0qers[.]com
- r0senbauer[.]com
- radverbaljudodiscount[.]com
- salesmarketingreport[.]com
- sasitm[.]org
- sasjournals[.]com
- taccomtips[.]com
- taccomusa[.]com
- taekwondophoenix[.]com
- ultarfilterindia[.]com
- united-irnaging[.]com
- uniteds-imaging[.]com
- vam1[.]com
- vanarkel[.]legal
- varmarnarine[.]com
- wallstreetgang777[.]com
- walnutcreekmartialarts[.]com
- wasabisakelounge[.]com
- yadavrealestate[.]com
- yellowraintechnologies[.]com

- yiyingdaplastics[.]com
- zealotbiotech[.]com
- zubairsfurnishing[.]com

Sample Additional IP Addresses

- 103[.]83[.]194[.]17
- 103[.]83[.]194[.]55
- 104[.]21[.]112[.]1
- 104[.]21[.]16[.]1
- 104[.]21[.]22[.]171
- 104[.]21[.]24[.]140
- 104[.]21[.]27[.]249
- 104[.]21[.]32[.]1
- 104[.]21[.]4[.]206
- 104[.]21[.]40[.]65
- 104[.]21[.]48[.]1
- 104[.]21[.]50[.]48
- 104[.]21[.]64[.]1
- 104[.]21[.]65[.]110
- 104[.]21[.]71[.]115
- 104[.]21[.]80[.]1
- 104[.]21[.]9[.]14
- 104[.]21[.]96[.]1
- 108[.]179[.]192[.]93
- 122[.]201[.]127[.]228

Sample IP-Connected Domains

- 1glm1[.]com
- 1mam1[.]com
- biglik[.]site
- blackbeltfamily[.]com
- calleme[.]site
- cpanel[.]1mam1[.]com
- cpanel[.]baptihealth[.]com
- elecnors[.]es
- ftp[.]1glm1[.]com
- ftp[.]1mam1[.]com
- ftp[.]baptihealth[.]com
- glmhost[.]com
- health-proheritage[.]com
- hobbive[.]site
- kodit[.]site
- lginnotek[.]site
- localhost[.]baptihealth[.]com
- localhost[.]dolh6growth[.]online
- mail[.]1glm1[.]com
- mail[.]1mam1[.]com
- mail[.]baptihealth[.]com
- neowiz[.]site
- nltto[.]com
- npsgov[.]org
- pop[.]1mam1[.]com
- pop[.]baptihealth[.]com
- pop[.]dolh6growth[.]online
- remhann[.]com
- riconengineering[.]com
- sapphirrecaregroup[.]com
- servor[.]site
- siteacess[.]site
- theeffectivelandlord[.]com
- thiccbaush[.]site
- volmconpanies[.]com
- webdisk[.]1mam1[.]com
- webdisk[.]baptihealth[.]com
- webdisk[.]dolh6growth[.]online

Sample String-Connected Domains

- africanagrirnarket[.]ph
- alliedhealthcaresolution[.]ph

- bhlergroup[.]ws
- claytoncontsruction[.]ws
- desirenetwork[.]co[.]in
- desirenetwork[.]co[.]uk
- desirenetwork[.]com
- docuinshare[.]ws
- dolh6growth[.]ph
- dreamwp[.]com[.]br
- dreamwp[.]ir
- dreamwp[.]net
- drop-project[.]co[.]uk
- drop-project[.]com
- drop-project[.]eu
- emailsay[.]bid
- emea-nec[.]co
- erhakalip[.]ws
- files42[.]nl
- glamorouslengths[.]co
- glamorouslengths[.]co[.]uk
- glamorouslengths[.]com
- greyscaleal[.]ws
- guardiansresearch[.]com
- historischeverenigingmarum[.]nl
- historischeverenigingmarum[.]sbs
- intertrustsgroup[.]net
- lovencareurology[.]com
- matcocomponent[.]ws
- ms-consulting-dom[.]xn--kprw13d
- ms-consulting-dom[.]xn--kpry57d
- mypi[.]agency
- mypi[.]ai
- mypi[.]app
- omnirayoprah[.]ph
- omnirayoprah[.]ws
- outsourcel[.]com
- profitminers[.]biz
- profitminers[.]cc
- profitminers[.]co
- reintergestna[.]ph
- rurrasqueamos[.]ph
- rurrasqueamos[.]us
- sneakylog[.]com
- stillmanconsulting[.]com
- stillmanconsulting[.]online
- storageorder[.]com
- storageorder[.]xyz
- sysarchirnc[.]ph
- tvsyndciate[.]ph
- urbanumbrella[.]ca
- urbanumbrella[.]co
- urbanumbrella[.]co[.]in
- usfightingsystems[.]ws
- webitww[.]ph
- welcomehomeproject[.]co
- welcomehomeproject[.]com
- windstreaim[.]net
- wwgle[.]co

Sample String-Connected Subdomains

- loginoffice365online-ny8mlcke2yhow9frm0p3[.]pcl-ss[.]com
- loginoffice365online[.]400index[.]live
- loginoffice365[.]office[.]microsoft[.]online[.]fluffy-corp[.]com
- loginoffice365online[.]ddosk-login[.]live
- loginoffice365[.]southpolehvca[.]com
- loginoffice365[.]bigqond[.]com
- loginoffice365[.]surveysparrow[.]com
- loginoffice365[.]hpcontosdesk1[.]site
- loginoffice365[.]com[.]ipaddress[.]com

- loginoffice365online[.]aaaldelia[.]com
- loginoffice365online[.]zerol0[.]app
- loginoffice365onlines[.]mb-194[.]xyz
- loginoffice365online[.]msf-365[.]xyz
- loginoffice3654576123457678945624533567[.]duckdns[.]org
- loginoffice365online[.]wwips[.]xyz
- loginoffice365online[.]ag-65[.]xyz
- loginoffice365online[.]101-201-001[.]live
- loginoffice365[.]aged2perfection[.]site
- loginoffice365online-api[.]at-tt[.]xyz
- loginoffice365onlinep[.]servoicapital[.]com
- loginoffice365[.]centoslinuxhp1[.]live
- loginoffice365[.]highprocomptech[.]online
- loginoffice365online[.]msftlogin[.]live
- loginoffice365online[.]apps101[.]live
- loginoffice365online[.]sgmexinternational[.]com