WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Under the DNS Hood of an Ongoing Legacy MSHTA Tool Attack

Threat Report

Table of Contents

Executive Report

Bitdefender recently detailed how attackers continued to abuse Microsoft's legacy MSHTA tool as a delivery mechanism across multiple malware campaigns. In one of the most prominent clusters, threat actors used the HTA-based loader CountLoader to deploy the infostealers LummaStealer and Amatera onto victims' systems. As a result, affected users could lose sensitive data, including their credentials, browser-stored information, session tokens, and cryptocurrency-related information, to the attackers.

The Bitdefender study identified 128 network IoCs comprising subdomains, domains, and IP addresses.

We extracted domains from the subdomain IoCs then filtered out those owned by legitimate organizations and were inactive from the resulting list aided by the WhoisXML API MCP Server. We ended up with 81 domain IoCs for further analysis. Combining that with the 11 subdomain and 28 IP IoCs, we had a total of 120 network IoCs for our investigation.

Our DNS deep dive into the ClickFix attack targeting MSHTA users led to these discoveries:

- 17 unique client IP addresses that communicated with 28 of the domain IoCs
- Four domain IoCs that appeared in three typosquatting groups with 3–9 members each
- 20 domain IoCs that were likely registered with malicious intent
- 618 unique IP addresses potentially owned by victims that communicated with 25 of the IP IoCs
- 2,260 email-connected domains, 56 of which were confirmed malicious
- 42 additional IP addresses, all of which were confirmed malicious
- 96 IP-connected domains, 17 of which were confirmed malicious
- 1,571 string-connected domains, five of which were confirmed malicious

A Study of the MSHTA Attack Subdomain IoCs

We began our analysis by querying the 11 subdomain IoCs on the WhoisXML API MCP Server and discovered that:

- The .pw domains with random strings fit a common malware distribution or phishing pattern.
- The **pool** string with hostnames (e.g., d1 and us1) and datacenter or region labels are reminiscent of classic cryptomining pool or proxy infrastructure naming

conventions. And since the subdomains resolve to the same IP address, they could be on a shared mining proxy or C&C host.
- Attacker-controlled OSS or S3 buckets are frequently used to host second-stage payloads or droppers.
- The .shop domains with various hostnames match algorithmically generated throwaway domains used in malvertising and phishing campaigns.

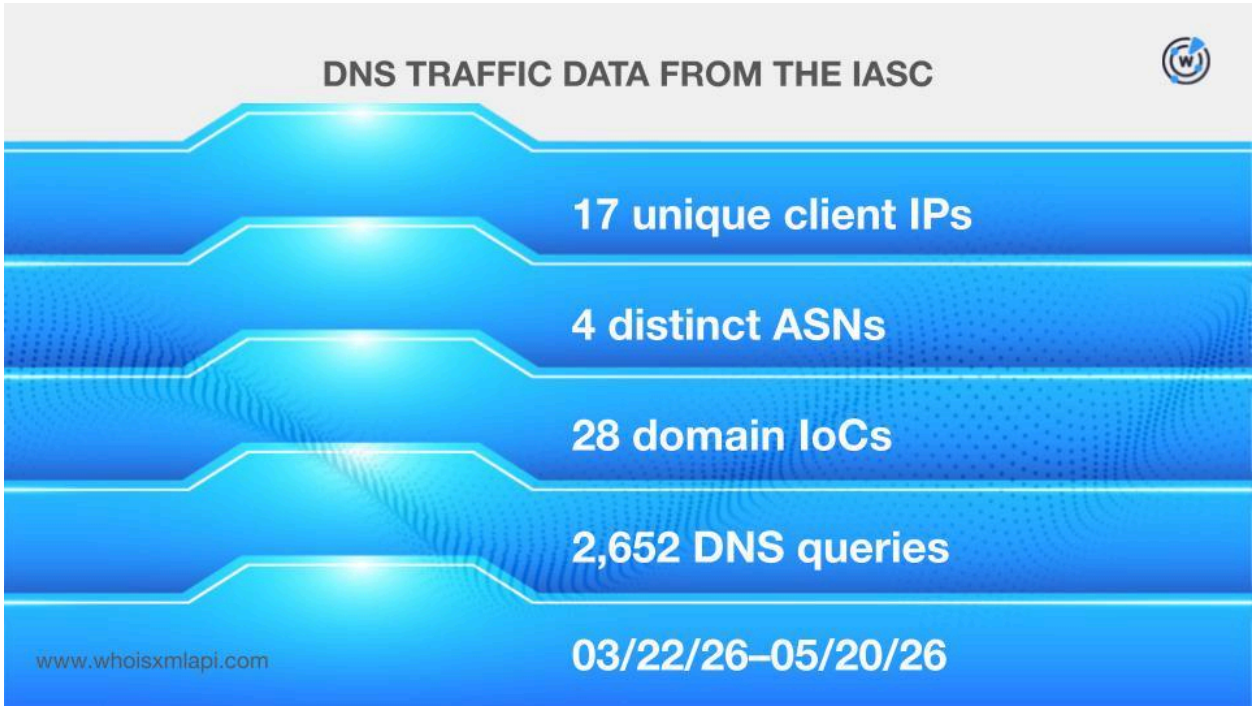
Here are more details on five examples.

SUBDOMAIN IoC	WXA MCP SERVER FINDING
asd[.]s7610rir[.]pw	Shares the IP address of asq[.]d6shiiwz[.]pw
asq[.]d6shiiwz[.]pw	Shares the IP address of asd[.]s7610rir[.]pw
buck2nd[.]oss-eu-central-1[.]aliyuncs[.]com	While hosted on a legitimate Alibaba Cloud OSS bucket, this could have been specially crafted for hosting second-stage payloads or droppers
check[.]qlkwr[.]com	Shares the IP address of d1[.]pool4883[.]pw
d1[.]pool4883[.]pw	Shares the IP address of check[.]qlkwr[.]com

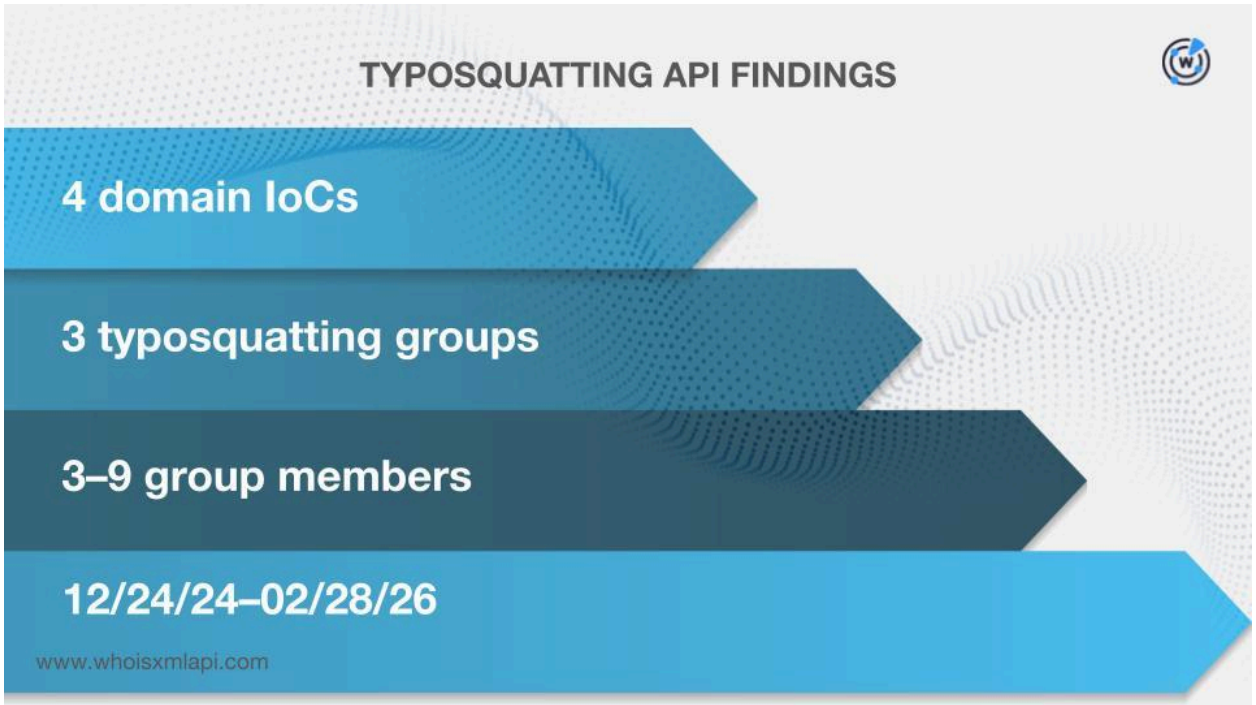
A Deep Dive into the MSHTA Attack Domain IoCs

We then looked more closely at the 81 domain IoCs.

First, sample network traffic data from the IASC showed that 17 unique client IP addresses under four distinct ASNs communicated with 28 of the domain IoCs via 2,652 DNS queries made between 22 March and 20 May 2026.



We then queried the domain IoCs on Typosquatting API and found out that four appeared in three typosquatting groups.



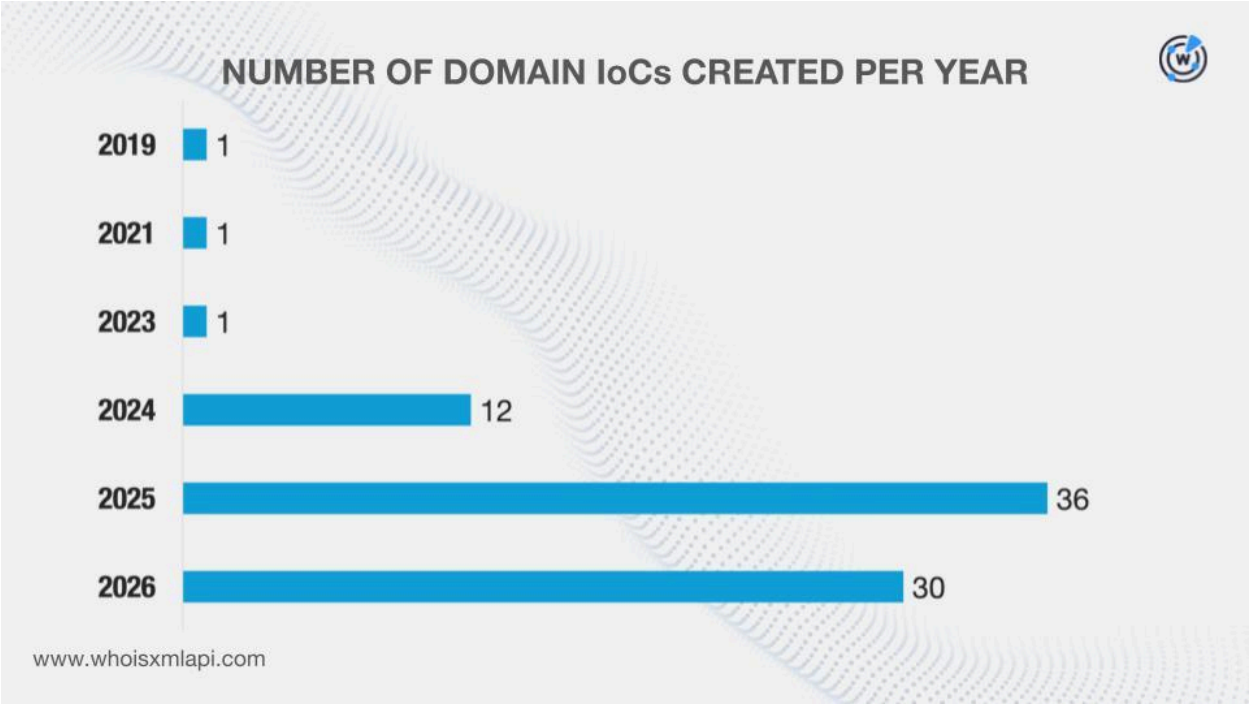
It is interesting to note that the domains simplerwebs[.]world and simplerwebs[.]space appeared in the same typosquatting group with nine members. They were bulk-registered with the domains simplerways[.]shop, simplerwebs[.]website, simplerwebs[.]online, simplerwebs[.]site, simpleweb[.]ai, simplerwebs[.]sbs, and simplerwebs[.]click on 2 January 2025.

Based on the results of our First Watch Malicious Domains Data Feed searches for the domain IoCs, 20 of them were likely registered with malicious intent 90–501 days before they were dubbed as IoCs on 19 May 2026. Here are five examples.

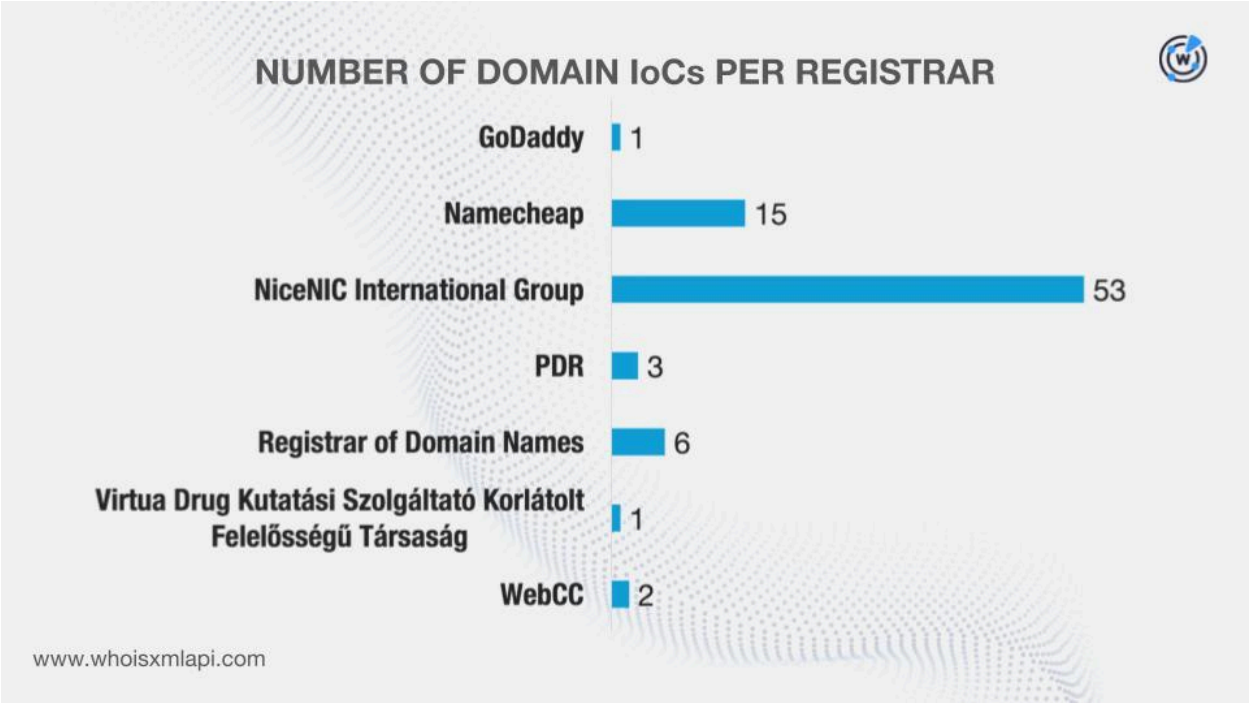
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE THE REPORT DATE
qlkwr[.]com	01/03/25	501
propofgustestyle[.]info	01/21/25	483
ms-team-ping6[.]com	08/25/25	267
holiday-updateservice[.]com	11/16/25	184
health-smooth-eu3[.]com	11/18/25	182

Next, we queried the domain IoCs on WHOIS API and discovered that:

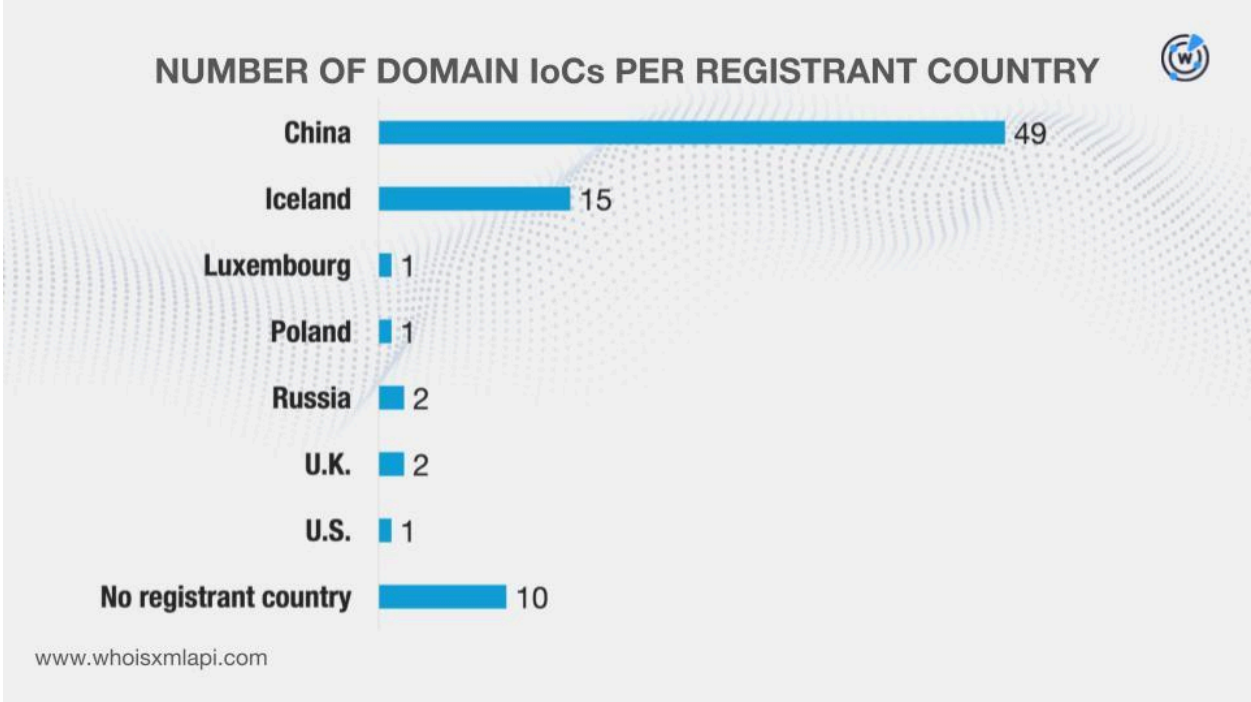
- They were created between 11 October 2019 and 14 April 2026, possibly indicating the threat actors did not have a specific preference with regard to domain age.



- They were administered by seven different registrars.



- While 10 did not have registrant countries on record, the remaining 71 were registered in seven different countries.



DNS Chronicle API queries for the domain IoCs revealed that 76 of them recorded 2,480 historical domain-to-IP resolutions over time. Take a look at more information for five examples below.

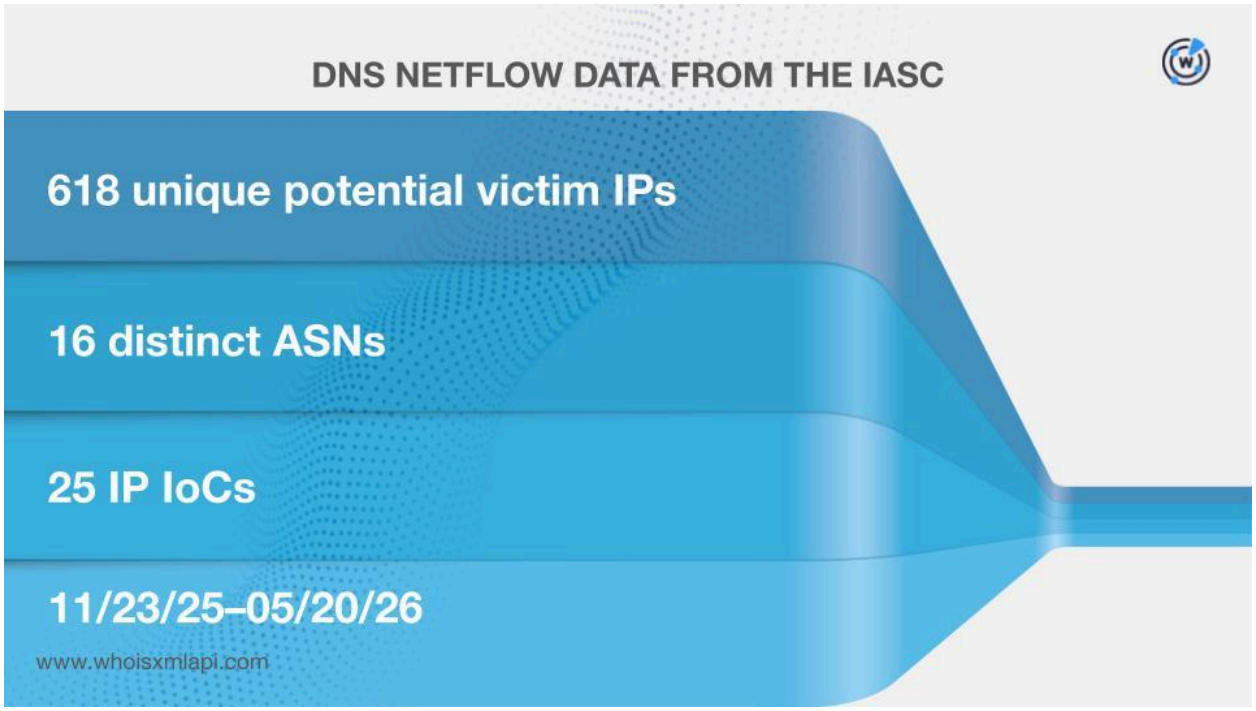
DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
ms-team-ping6[.]com	205	08/25/25–05/09/26
alphazero1-endscape[.]cc	121	11/23/25–05/10/26
s3-updatehub[.]cc	110	12/02/25–05/17/26
globalsnn1-new[.]cc	106	11/23/25–05/10/26
my-smart-house1[.]com	101	11/12/25–05/20/26

A total of 49 of the domain IoCs continue to post resolutions this May.

An Investigation of the MSHTA Attack IP IoCs

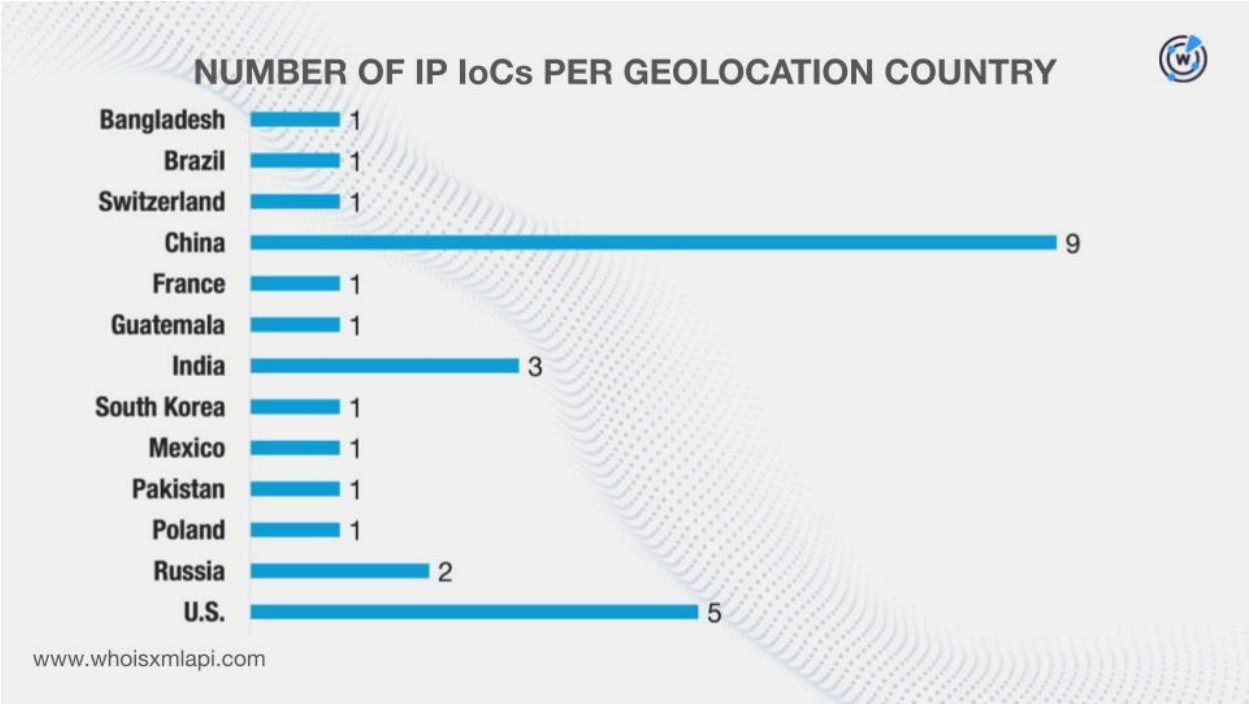
Next, we studied the 28 IP IoCs further.

Sample network traffic data from the IASC revealed that 618 unique IP addresses that could belong to victims under 16 distinct ASNs communicated with 25 of the IP IoCs between 23 November 2025 and 20 May 2026.

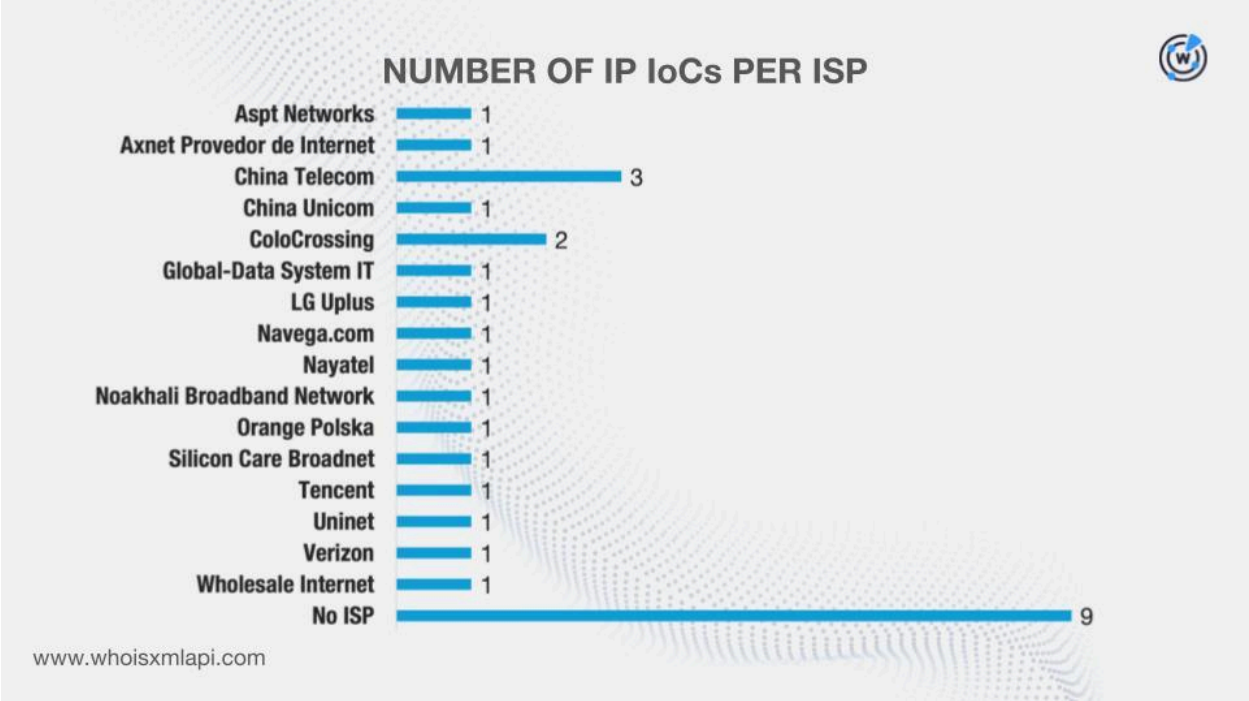


We then queried the IP IoCs on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in 13 different countries.



- While nine did not have ISPs on record, the remaining 19 were administered by 16 different ISPs.



Lastly, we queried the IP IoCs on DNS Chronicle API and found out that 15 of them posted 2,564 historical IP-to-domain resolutions over time. Here are more details for five examples.

IP IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	DATES SEEN
103[.]115[.]17[.]90	1,000	02/15/19–09/04/20
100[.]1[.]121[.]27	520	02/07/17–05/20/26
87[.]96[.]21[.]84	260	02/06/17–08/15/24
107[.]175[.]187[.]11	140	06/24/17–08/16/20
222[.]73[.]29[.]92	119	10/22/19–02/04/22

As of May 2026, only one IP IoC continued to resolve domains.

The Search for New Artifacts Related to the MSHTA Attack

To kick off our IoC list expansion, we queried the 81 domain IoCs on WHOIS History API and found out that 16 of them had 29 unique email addresses in their historical records. Further scrutiny allowed us to discern that 13 were public email addresses.

Reverse WHOIS API queries for the public email addresses showed that two could be owned by domainers and one was no longer active so they were excluded from the next step. This step also led to the discovery of 2,260 unique email-connected domains after those already tagged as IoCs were filtered out.

We then queried the email-connected domains on Threat Intelligence API, which revealed that 56 have already been confirmed malicious. Take a look at more information for five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
all-instructions[.]com	Malware distribution	10/19/24–05/20/26
bragwe[.]com	Malware distribution	03/09/23–05/20/26
chrone-intsall[.]com	Malware distribution	03/09/23–05/20/26

dfgh[.]online	Malware distribution	01/01/25–05/20/26
extraguestreview[.]com	Malware distribution	12/19/24–05/20/26

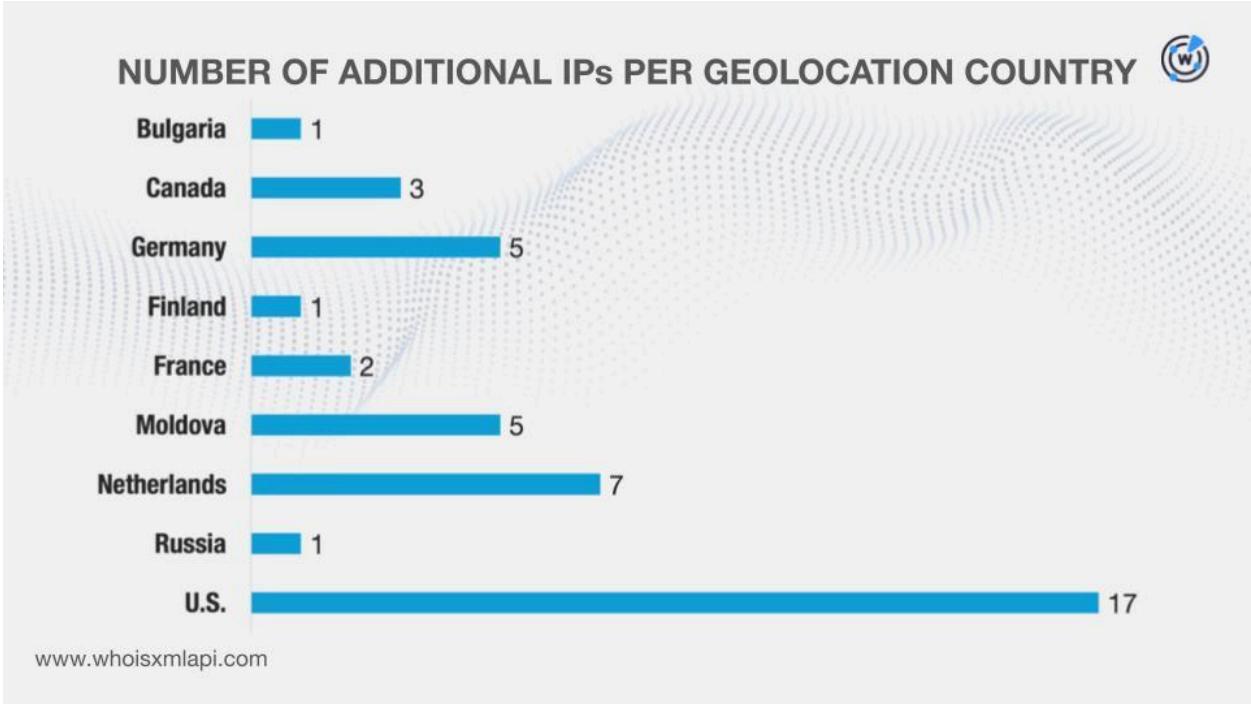
We then queried the domain IoCs on DNS Lookup API and uncovered 42 unique additional IP addresses after those already identified as IoCs were filtered out.

Threat Intelligence API queries for the additional IP addresses showed that all of them have already been weaponized for various attacks. Here are more details for five examples.

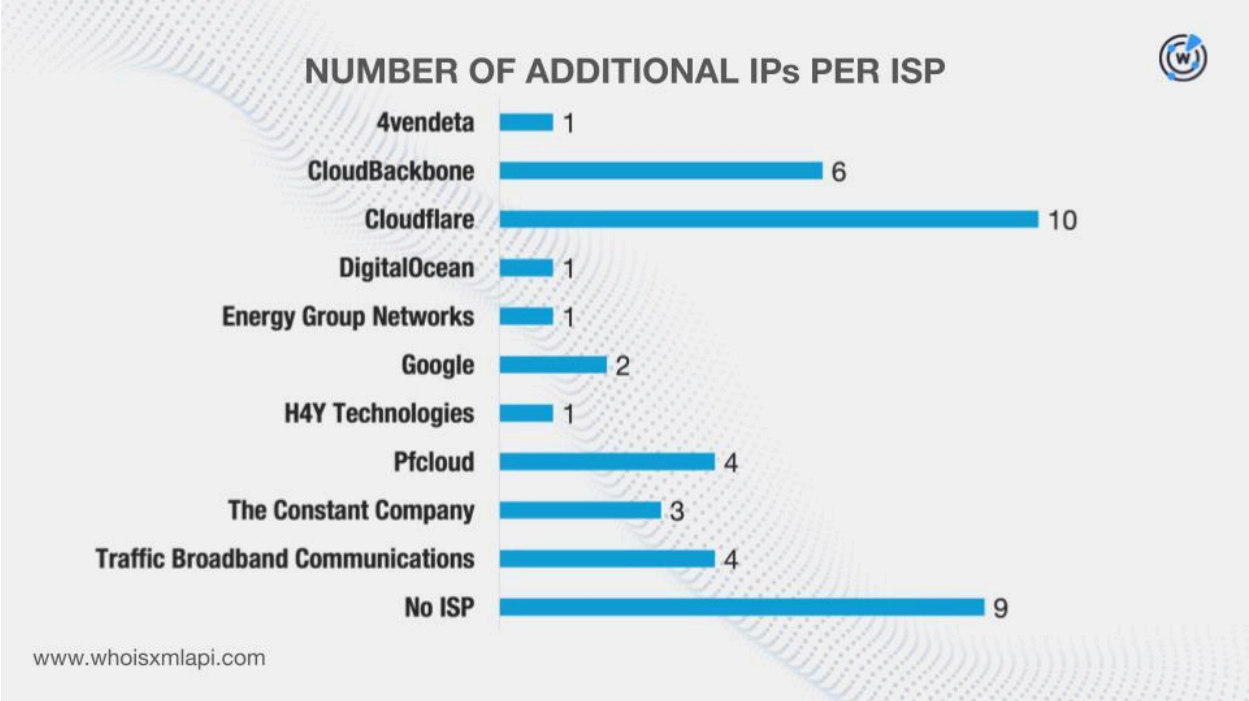
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
104[.]21[.]17[.]53	Malware distribution Phishing Generic threat	03/29/23–05/20/26 05/31/24–05/20/26 05/30/24–04/01/26
104[.]21[.]23[.]175	Phishing Malware distribution	12/10/23–05/21/26 03/09/24–05/19/26
104[.]21[.]74[.]84	Malware distribution	03/29/23–05/20/26
104[.]252[.]53[.]249	Malware distribution Generic threat	04/16/26–05/19/26 04/24/26–05/09/26
146[.]190[.]24[.]11	Phishing Attack Generic threat	01/27/26–05/19/26 05/06/25–03/18/26 01/28/26–03/03/26

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

- They were geolocated in nine different countries. Note that three of these locations—France, Russia, and the U.S.—were also among the IP IoCs' geolocation countries.



- While nine of them did not have ISPs on record, the remaining 33 were administered by 10 different ISPs.



After adding the additional IP addresses to the IP IoCs, we now had 70 IP addresses in all to further investigate.

Reverse IP API queries for all of the IP addresses revealed that 33 could be dedicated hosts. This step led to the discovery of 96 unique IP-connected domains after those already named as IoCs and the email-connected domains were filtered out.

We then queried the IP-connected domains on Threat Intelligence API and found out that 17 have already figured in various malicious campaigns. Take a look at more information for five examples below.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
dorisgrillbar[.]com	Phishing Generic threat	01/27/26–05/21/26 01/28/26–02/27/26
node1-py-store[.]com	Malware distribution	12/14/25–05/20/26
node2-py-store[.]com	Malware distribution Generic threat	12/14/25–05/20/26 03/12/26–03/12/26
npm-storage[.]cc	Malware distribution	02/17/26–05/20/26
s1-rarlab[.]com	Malware distribution Generic threat	12/14/25–05/20/26 03/12/26–03/12/26

As our final step, we extracted 80 unique text strings from the domain IoCs. We then used Domains & Subdomains Discovery to search for other domains not yet dubbed as IoCs that started with them. We found results for 43 strings, including but not limited to the following:

- alpha-centavr.
- bigbrainsholdings.
- ccleaner.
- d6shiiwz.
- echoicedeals.
- fileless-market.
- geo-foundation.
- hardware-office.
- immortal-service.
- jenj.
- kizmond.
- local-wanderer.
- macphotoeditor.
- network-defender.
- offshore-storage.
- parent-control.
- qlkwr.
- readit-carfanatics.
- s3-microservice-updatehub.
- topofsuper.
- urugvai.
- web3-walletnotify.

We unearthed 1,571 unique string-connected domains after those already confirmed as 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.

Threat Intelligence API queries for the string-connected domains revealed that five have already been weaponized for various threats. An example would be ccleaner[.]host, which has been affiliated with malware distribution between 9 March 2023 and 20 May 2026.

Conclusion

Our in-depth DNS investigation of the campaigns targeting users of the legacy tool MSHTA with LummaStealer, Amatera, and CastleLoader revealed interesting new insights, such as that 17 unique client IP addresses communicated with 28 of the domain IoCs. Four of the domain IoCs also appeared in three typosquatting groups with 3–9 members each. In addition, 20 of the domain IoCs were likely registered with malicious intent. Finally, 618 unique IP addresses potentially owned by victims communicated with 25 of the IP IoCs.

Our IoC list expansion, meanwhile, uncovered 3,969 new artifacts comprising 2,260 email-connected domains, 42 additional IP addresses, 96 IP-connected domains, and 1,571 string-connected domains. Users are also advised to take the utmost caution as 120 of them have already been confirmed 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

- 08u073852[.]online
- 09smile[.]click
- 0rohyp5yu[.]online
- a-zon[.]online
- abservatory-home[.]com
- aclz9[.]online
- b2-ra[.]online
- b3×1p[.]online
- b8a2[.]online
- c-lntera[.]com
- c0h9w[.]online
- c2y8[.]online
- d-09-r[.]online
- d09r[.]online
- d1a8[.]online
- e-hongsengg[.]live
- e-inter1c[.]cfd
- e-inter1c[.]live
- f-42-s[.]online
- f05t[.]online
- f2g5q[.]online
- g-69-p[.]online
- g-lim[.]online
- g-lnterracc[.]com
- h-73-n[.]online
- h73n[.]online
- h8y0[.]online
- i-jntercca[.]cfd
- i-jntercca[.]top
- i-jntercca[.]world
- j1g3k[.]online
- j2e6[.]online
- j5-ol[.]online
- k0v1p[.]online
- k25q[.]online
- k4tem[.]online
- l8o6[.]online
- l9a5[.]online
- la9q[.]online
- m-lnretca[.]com
- m-lnterracc[.]com
- m-lnterrc[.]com
- n-96-f[.]online
- n-jur[.]online
- n2-ke[.]online
- o-inter24[.]com
- oafj[.]wang
- oaqc[.]wang
- p2-om[.]online
- p2j4k[.]online
- p9v7g[.]online
- q-0-spi[.]online
- q-len[.]online
- q0spi[.]online
- r0-mx[.]online
- r0z8r[.]online
- r1a4[.]online
- s2-ly[.]online
- s3i1[.]online
- s4-ti[.]online
- t4a4[.]online
- t4c5d[.]online
- t4g9w[.]online
- ugle[.]wang
- uht-3-o[.]online
- uht3o[.]online
- v1n4n[.]online
- v3sa[.]online
- v4h3t[.]online
- w-1nterac[.]cfd
- w-1nterac[.]cyou
- w-1nterac[.]icu
- x-vo4[.]online
- x0a3[.]online

- x0e8[.]online
- yayf[.]wang
- yeyn[.]wang
- yffl9[.]online
- z15d[.]online
- z3-lu[.]online
- z99l[.]online

Sample Additional IP Addresses

- 104[.]21[.]10[.]159
- 142[.]250[.]184[.]14
- 146[.]190[.]24[.]11
- 149[.]248[.]61[.]108
- 155[.]138[.]150[.]91
- 172[.]67[.]156[.]103
- 176[.]65[.]132[.]173
- 178[.]255[.]222[.]234
- 193[.]84[.]71[.]233
- 194[.]58[.]112[.]174
- 216[.]58[.]212[.]174
- 31[.]56[.]176[.]201
- 37[.]221[.]66[.]103
- 45[.]153[.]34[.]163
- 78[.]128[.]114[.]182
- 82[.]29[.]71[.]183
- 85[.]121[.]148[.]13
- 94[.]183[.]183[.]156

Sample IP-Connected Domains

- 0fd14881-789e-449f-8106-6df009461563[.]random[.]xiangyangtools[.]com
- a03b52ca-2cfa-440d-a695-8a287fb71472[.]random[.]timeportalgames[.]com
- be93d38e-37e5-44fb-9934-2e1c57df2350[.]random[.]wow-coupons[.]com
- c1222162-684a-4ef3-ad29-ca6b4b46a895[.]random[.]vivarilearninglounge[.]com
- dbd9fffe-dfc5-43f4-8038-7db8c3ca093a[.]random[.]xiangyangtools[.]com
- e58318ec-a8b5-4a34-85e6-ba67642d089f[.]random[.]wow-coupons[.]com
- f5a5f770-1bc4-4ef4-959c-3a1400e98266[.]random[.]vivarilearninglounge[.]com
- gaslightinnredhook[.]com
- h232[.]wow-coupons[.]com
- info[.]wap[.]wow-coupons[.]com
- karenhosmertutoring[.]com
- lailasbookthief[.]wow-coupons[.]com
- mail[.]dorisgrillbar[.]com
- netsiapps[.]com
- ochan[.]wow-coupons[.]com
- pknjeegqnve[.]xiangyangtools[.]com
- run-home[.]cc
- s1-rarlab[.]com
- tangrenjieyulechengguanwang[.]wow-coupons[.]com
- ulg[.]wow-coupons[.]com
- video[.]www[.]xiangyangtools[.]com
- wow-coupons[.]com
- yytrr[.]ns[.]asriranfun[.]ir
- zaixianduboqipaiyouxi[.]wow-coupons[.]com

Sample String-Connected Domains

- antibot-check[.]sbs
- ccleaner[.]africa
- ccleaner[.]app
- ccleaner[.]asia
- checkpageonce[.]ph
- checkpageonce[.]ws
- critical-service[.]app
- critical-service[.]com
- critical-service[.]es
- debank-api[.]com
- deluxe[.]academy
- deluxe[.]ad
- deluxe[.]ae
- domain-monitoring[.]app
- domain-monitoring[.]ch
- domain-monitoring[.]com
- driftcharm[.]com
- echoicedeals[.]com
- etrademart[.]co[.]uk
- etrademart[.]com
- etrademart[.]in
- explorer[.]ac
- explorer[.]ac[.]cn
- explorer[.]academy
- files-storage[.]biz
- files-storage[.]cf
- files-storage[.]co[.]uk
- geo-foundation[.]com
- geo-foundation[.]org
- geo-foundation[.]ru
- gevaq[.]asia
- gevaq[.]cn
- gevaq[.]link
- google-services[.]cf
- google-services[.]ch
- google-services[.]co
- hardware-office[.]bid
- hardware-office[.]com
- health-smooth-eu2[.]ph
- health-smooth-eu2[.]ws
- holiday-forever[.]com
- holiday-forever[.]de
- holiday-forever[.]ru
- holypriest[.]com
- holypriest[.]cz
- holypriest[.]de
- hosting-control[.]be
- hosting-control[.]biz
- hosting-control[.]com
- jenj[.]art
- jenj[.]be
- jenj[.]buzz
- local-wanderer[.]ph
- local-wanderer[.]ws
- macphotoeditor[.]com
- macphotoeditor[.]ws
- melody-wave[.]com
- memory-scanner[.]com
- memory-scanner[.]uk
- microservice[.]academy
- microservice[.]agency
- microservice[.]ai
- msedge[.]app
- msedge[.]asia
- msedge[.]biz
- network-defender[.]com
- network-defender[.]net
- network-defender[.]pro
- offshore-storage[.]ch
- offshore-storage[.]com
- onceletthemcheck[.]ph
- onceletthemcheck[.]ws
- parent-control[.]co[.]uk
- parent-control[.]com
- parent-control[.]info
- polystore9-servicebucket[.]ph
- py-installer[.]ph
- py-installer[.]ws

- qlkwr[.]tk
- qlkwr[.]vip
- qlkwr[.]ws
- readit-carfanatics[.]ws
- retrosome[.]com
- savecoupons[.]ca
- savecoupons[.]club
- savecoupons[.]co
- scrutinycheck[.]com
- silverhost[.]ae
- silverhost[.]africa
- silverhost[.]biz
- simplerwebs[.]click
- simplerwebs[.]com
- simplerwebs[.]online
- system-monitor[.]bb
- system-monitor[.]co[.]uk
- system-monitor[.]com
- topofsuper[.]com
- topofsuper[.]store
- urugvai[.]autos
- urugvai[.]com
- urugvai[.]org