A DNS Exploration of the Latest Educated Manticore Attack

Table of Contents

Executive Report

Check Point Research published an in-depth analysis of the recent spearphishing attack launched by Iranian threat group Educated Manticore. The attackers targeted Israeli journalists, high-profile cybersecurity experts, and computer science professors from leading Israeli universities.

The threat actors directed victims who engaged with them to fake Gmail login pages or Google Meet invitations. The credentials the victims entered on phishing pages were sent to the attackers, enabling them to intercept passwords and two-factor authentication (2FA) codes and gain unauthorized access to the victims' accounts.

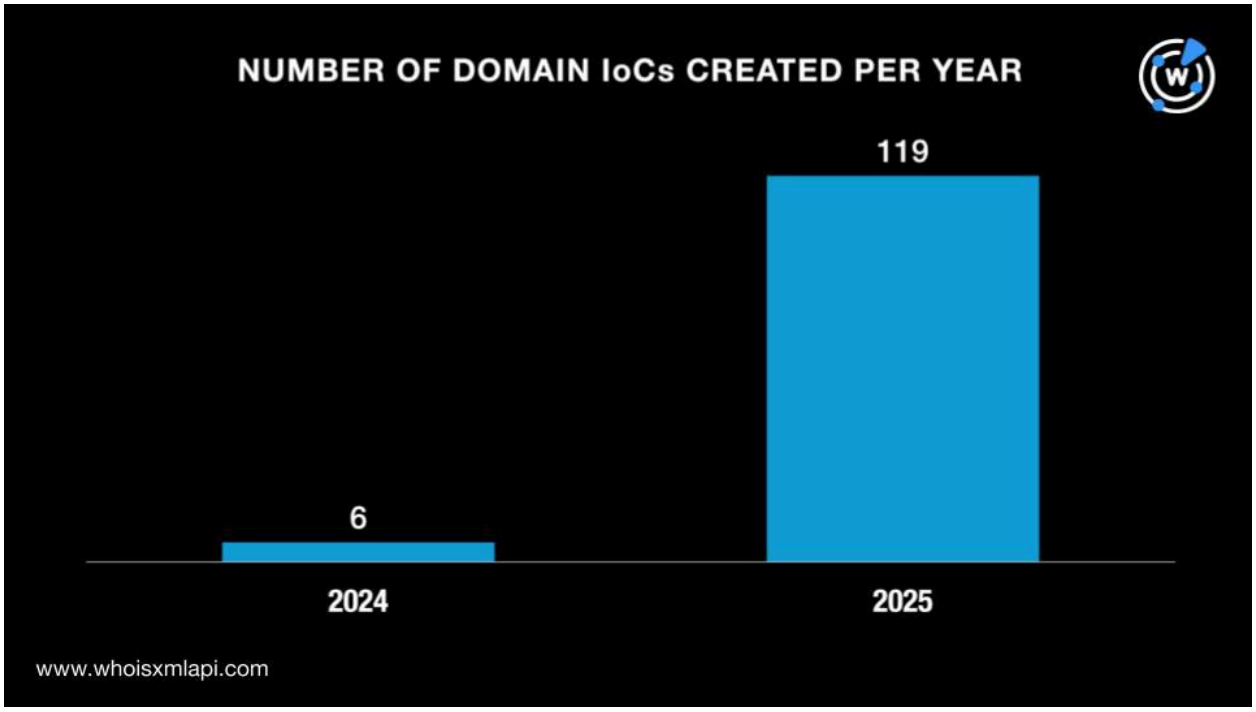
The researchers identified 141 indicators of compromise (IoCs) comprising 129 domains and 12 IP addresses in their report "Iranian Educated Manticore Targets Leading Tech Academics." We analyzed the IoCs in greater depth and uncovered:

- 1,753 alleged victim IP records obtained from the Internet Abuse Signal Collective (IASC) tied to two Autonomous System (AS) numbers
- 72 of the domains tagged as IoCs appeared on First Watch Malicious Domains Data Feed upon registration
- One of the IP addresses tagged as IoCs communicated with one source IP based on IASC data
- 217 email-connected domains, one of which was malicious
- One additional IP address that was malicious
- 460 IP-connected domains, three of which were malicious
- 1,176 string-connected domains, one of which was malicious

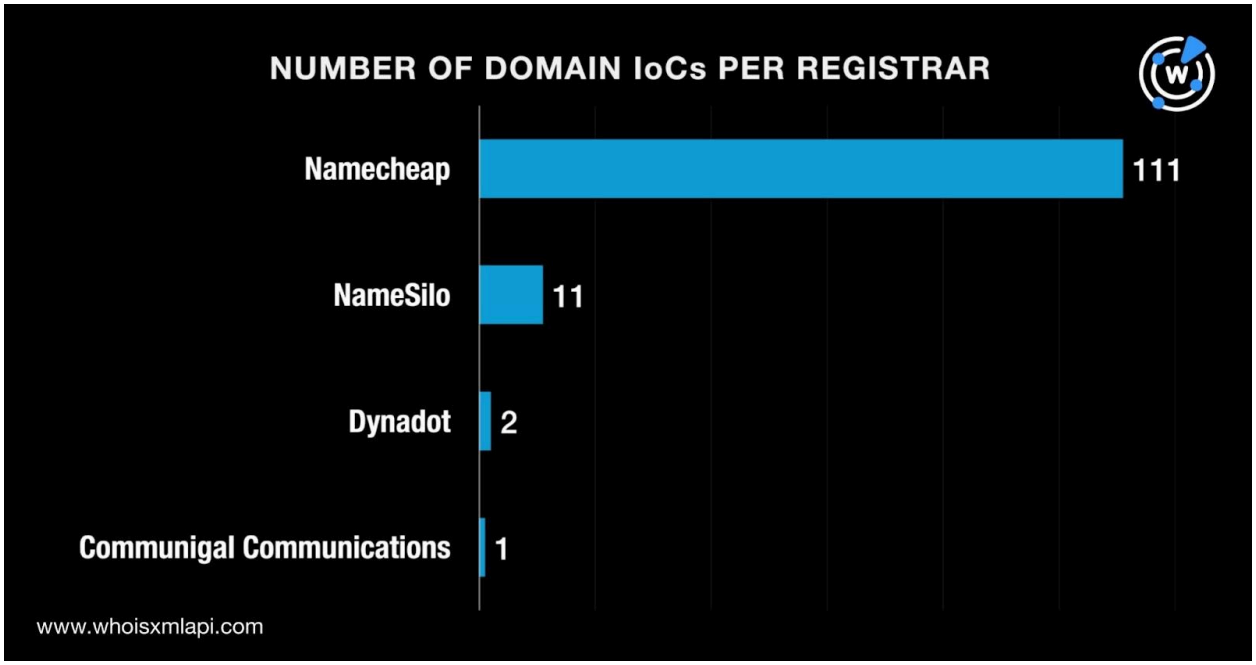
More on the Educated Manticore Attack IoCs

We began our analysis by looking deeper into the IoCs by querying the 129 domains tagged as IoCs on Bulk WHOIS API. We discovered that 125 of them had current WHOIS records. Further analysis of the 125 domains showed that:

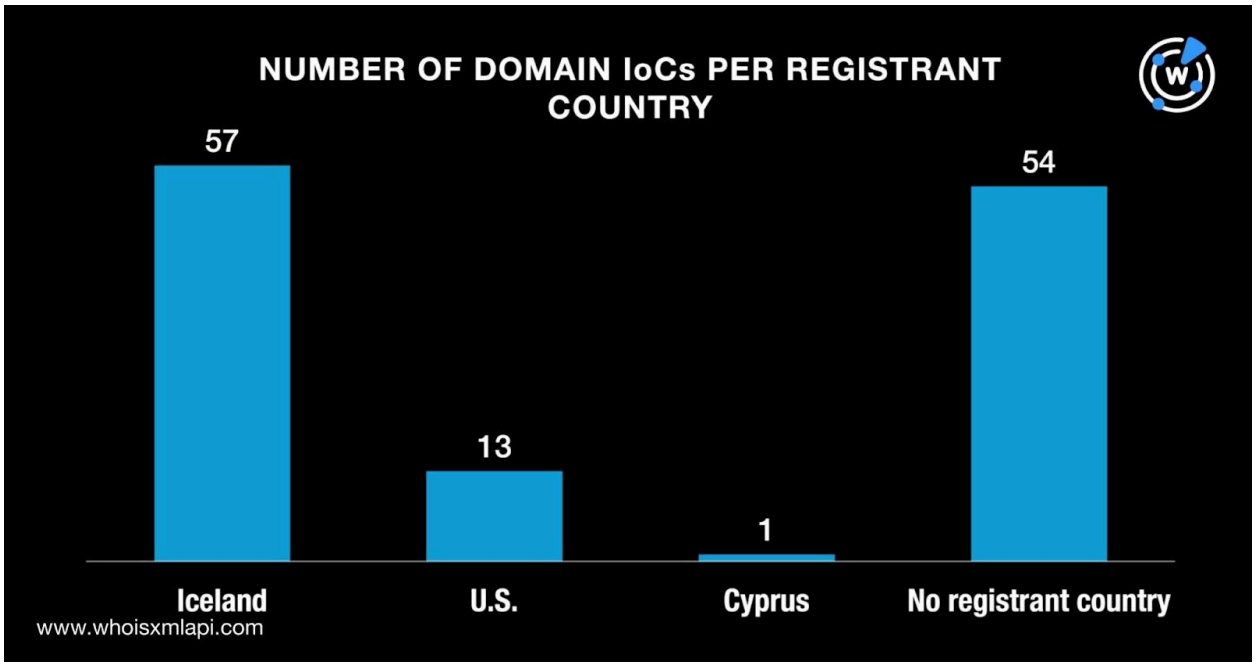
- They were created between 28 March 2024 and 23 June 2025. Specifically, six domains were created in 2024 while 119 were created in 2025.



- They were split among four registrars led by Namecheap, which accounted for 111 domains. NameSilo came in second place with 11 domains. Dynadot placed third with two domains. Finally, Communigal Communications accounted for one domain.



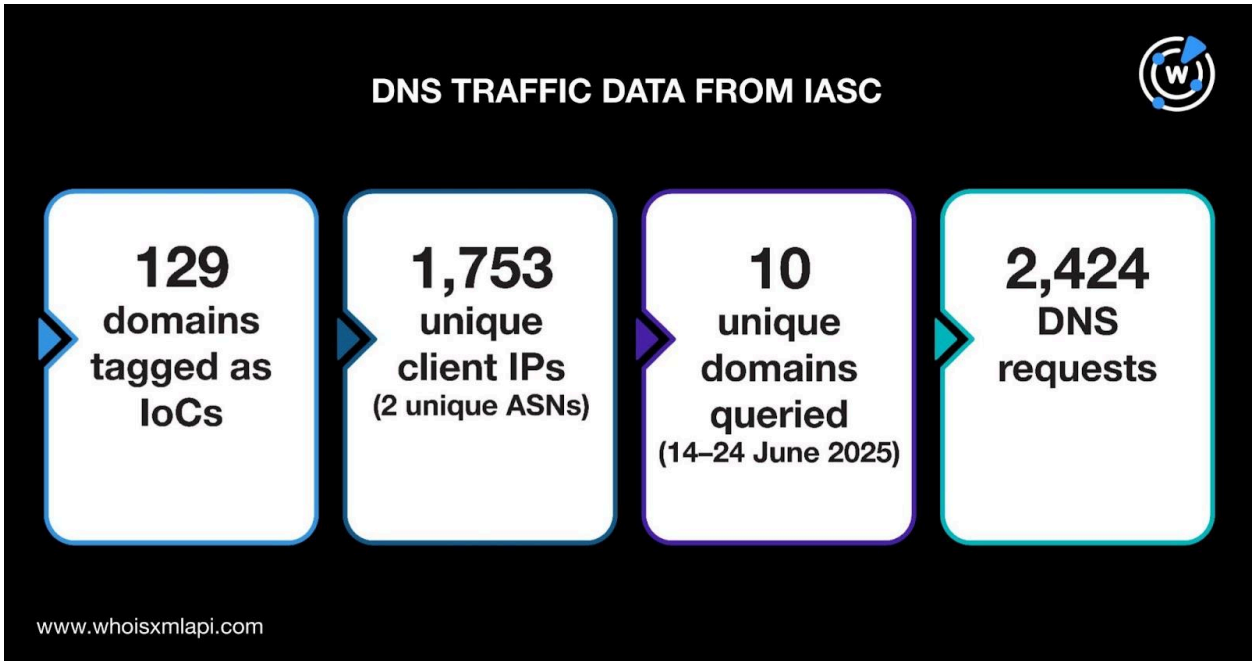
- Only 71 of the 125 domains had registrant countries on record. They were registered in three countries topped by Iceland, which accounted for 57 domains. The U.S. took the second spot with 13 domains. Cyprus placed third with one domain. The remaining 54 domains did not have registrant countries in their current WHOIS records.



A DNS Chronicle API query for the 129 domains tagged as IoCs showed that 123 of them had historical domain-to-IP resolutions. Specifically, the 123 domains recorded 2,630 resolutions over time. The IoC alpha-man[.]info posted the oldest domain-to-IP resolution on 5 February 2017. Take a look at more details for five other domains below.

DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	FIRST RESOLUTION DATE
conn-ectionor[.]cfd	1	24 June 2025
becker624[.]online	1	16 June 2025
steve-brown[.]info	3	6 April 2025
network-show[.]online	1	4 February 2025
suite-moral[.]info	3	26 April 2025

Using sample DNS traffic data our researchers obtained from the IASC, we further analyzed the 129 domains tagged as IoCs. The sample data revealed that 1,753 unique client IP addresses tied to two unique AS numbers queried 10 distinct domains on 14–24 June 2025 via 2,424 DNS requests.

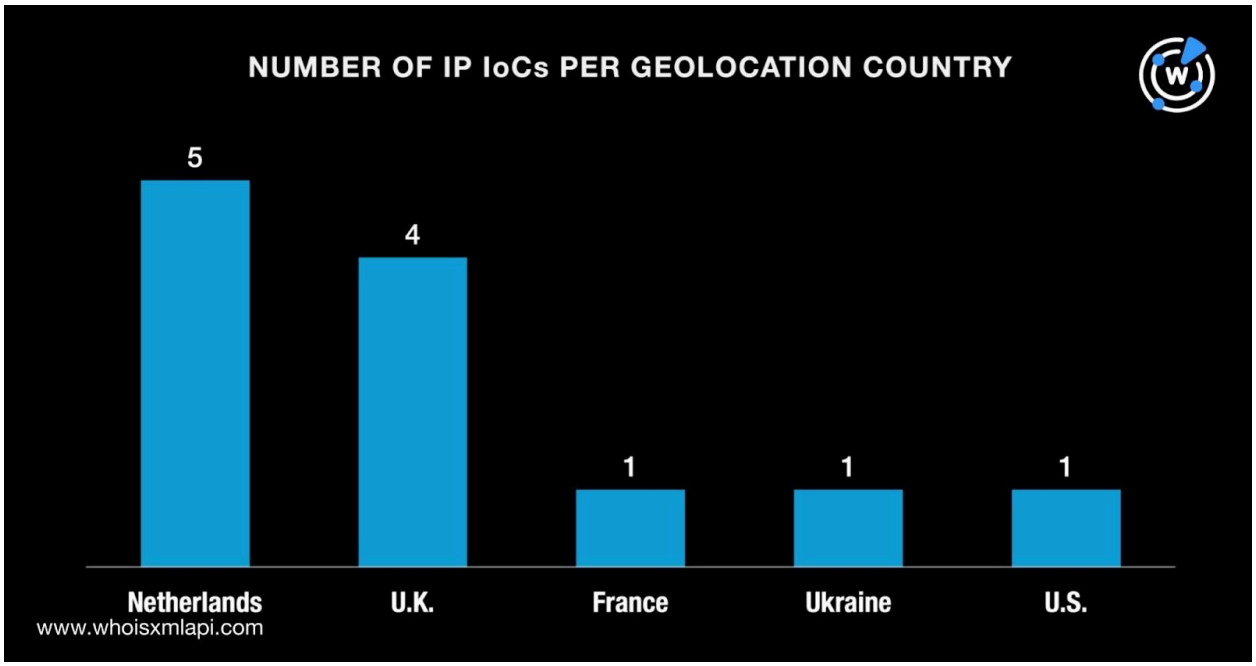


We then queried the 129 domains on First Watch and found that 72 of them appeared on various feeds 5–454 days before they were reported as attack IoCs on 25 June 2025. Take a look at five examples below.

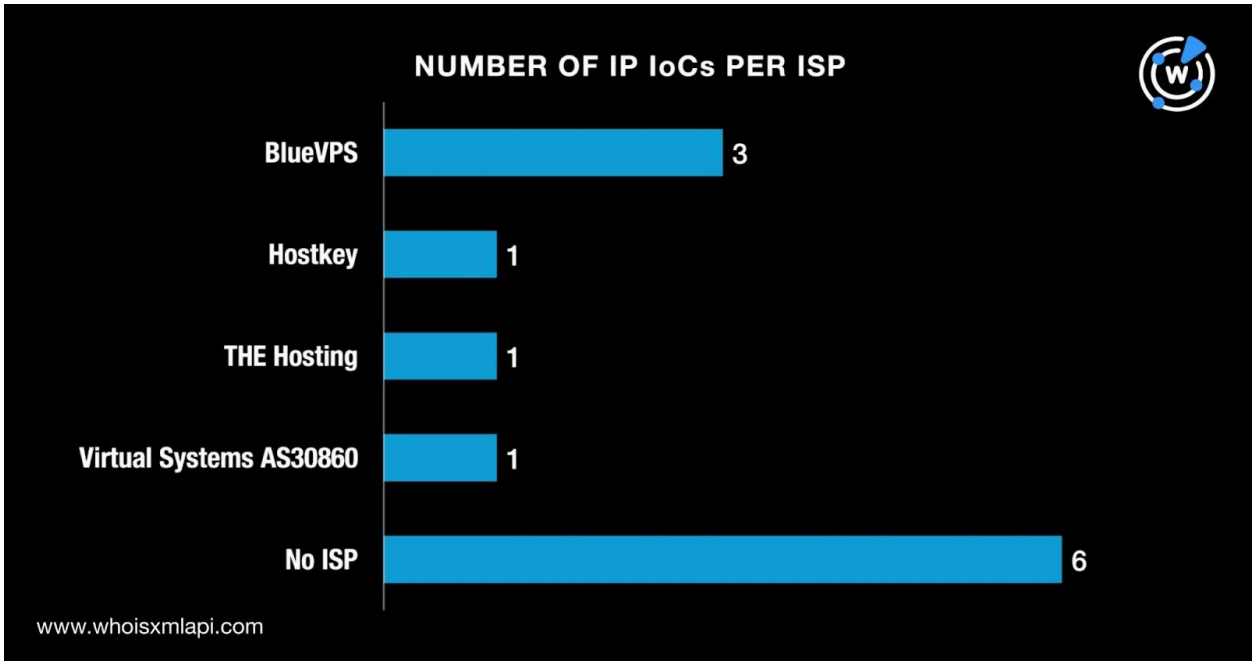
DOMAIN IoC	FIRST WATCH DATE ADDED	NUMBER OF DAYS PRIOR TO REPORTING DATE
world-shop[.]online	28 March 2024	454
spring-club[.]info	9 March 2025	108
nsim-ph[.]info	10 April 2025	76
yamal-group[.]online	27 April 2025	59
optio-nalynk[.]online	20 June 2025	5

Next, we queried the 12 IP addresses tagged as IoCs on Bulk IP Geolocation Lookup and found that:

- They originated from five countries led by the Netherlands, which accounted for five IP addresses. The U.K. took the second spot with four domains. Finally, one IP address each was geolocated in France, Ukraine, and the U.S.



- While six of them did not have ISPs on record, the other six were administered by four ISPs topped by BlueVPS, which accounted for three IP addresses. Finally, one IP address each was administered by Hostkey, THE Hosting, and Virtual Systems AS30860.



A DNS Chronicle API query for the 12 IP addresses revealed that all of them had historical IP-to-domain resolutions. Specifically, the 12 IoCs recorded 6,860 resolutions over time. The IP address 195[.]66[.]213[.]132 posted the oldest IP-to-domain resolution on 4 February 2017.

IP IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	FIRST RESOLUTION DATE
146[.]19[.]254[.]238	1,000	6 April 2025
194[.]11[.]226[.]29	1,000	1 October 2024
194[.]11[.]226[.]5	1,000	10 March 2025
194[.]61[.]120[.]185	1,000	23 November 2019
45[.]12[.]2[.]158	121	18 January 2022

We also looked for more information on the 12 IP addresses tagged as IoCs using traffic data we obtained from IASC and discovered that one of them—185[.]130[.]226[.]71—communicated with one source IP.

Expanding the List of Educated Manticore Attack IoCs

We started our in-depth analysis by querying the 129 domains tagged as IoCs on WHOIS History API and discovered that seven of them had email addresses in their historical WHOIS records. In particular, the seven domains had 14 email addresses, six of which were public addresses.

While our Reverse WHOIS API query for the six public email addresses showed they did not appear in any current WHOIS records, all of them did appear in historical records. Specifically, the six addresses were present in the historical WHOIS records of 217 email-connected domains after duplicates and those already tagged as IoCs were filtered out.

A Threat Intelligence API query for the 217 email-connected domains revealed that one of them—top-game[.]online—already figured in malware distribution.

After that, we queried the 129 domains tagged as IoCs on DNS Lookup API and discovered that 54 of them had current IP resolutions. After duplicates and those already identified as IoCs were filtered out, we were left with one additional IP address.

A Threat Intelligence API query for the IP address 198[.]54[.]117[.]242 showed that it has already figured in malware distribution, generic threats, phishing, suspicious activity, and command and control (C&C).

Next, an IP Geolocation API query for the additional IP address revealed that it was geolocated in the U.S. and administered by Namecheap. While it shared one IP IoC's geolocation country, it did not share any of the IoCs' ISPs.

We now had 13 IP addresses for further analysis—12 tagged as IoCs and one additional from our DNS lookup earlier. We queried the 13 IP addresses on Reverse IP API and found that seven of them could be dedicated and played host to 460 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

A Threat Intelligence API query for the 460 IP-connected domains revealed that three of them have already been weaponized for attacks. One example—burjog[.]com—served as a C&C domain.

As our final step, we looked for domains that looked like the 129 IoCs using Domains & Subdomains Discovery. We discovered 124 unique text strings, and of them, 61 appeared in other domains. Take a look at the list below.

- albert-company.
- alpha-man.
- anna-blog.
- arizonaclub.
- backback.
- bestshopu.
- beta-man.
- black-friday-store.
- city-splash.
- clothes-show.
- connect-room.
- cook-tips.
- course-math.
- cyberlattice.
- everything-here.
- exir-juice.
- expressmarket.
- first-course.
- gallery-shop.
- good-news.
- good-student.
- healthy-lifestyle.
- idea-home.
- infinit-world.
- live-coaching.
- live-conn.
- live-content.
- live-meet.
- live-message.
- make-house.
- master-club.
- meet-work.
- message-live.
- network-game.
- network-review.
- network-show.
- nice-goods.
- online-room.
- panel-network.
- ph-work.
- rap-art.
- reading-course.
- reg-d.
- royalsoul.
- shadow-network.
- sky-writer.
- socks.
- spring-club.
- steve-brown.
- storm-wave.
- thomas-mark.
- top-game.
- warplogic.
- wash-less.
- white-car.
- white-life.
- wood-house.
- word-course.
- work-meeting.
- world-shop.
- yamal-group.

Our search led to the discovery of 1,176 string-connected domains after duplicates, those already tagged as IoCs, and the email- and IP-connected domains were filtered out.

A Threat Intelligence API query for the 1,176 string-connected domains showed that one—healthy-lifestyle[.]pl—is connected to a generic threat.

—

Our in-depth analysis of the 141 Educated Manticore attack IoCs led to the discovery of 1,854 potentially connected artifacts comprising 217 email-connected domains, one additional IP address, 460 IP-connected domains, and 1,176 string-connected domains. It is also worth noting that six of them have already been weaponized for various attacks.

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

- 100-dosok[.]com
- alfa-bonus[.]info
- alfa-bonus[.]website
- alfa-football-survey[.]info
- best4hair[.]net
- bonus-social-smg[.]site
- cloverv2[.]info
- cloverv2[.]pro
- cloverv2[.]site
- easy-bonus[.]fun
- easy-bonus[.]site
- easy-prise[.]site
- fifa-club[.]online
- fifa-club[.]website
- fifa-lige-cup[.]info
- give-me-bonus-smg[.]info
- give-me-bonus-smg[.]site
- give-me-prise-like[.]info
- iab-rating-news[.]website
- iab-rating[.]site
- iab2018[.]site
- just-order[.]pro
- just-order[.]pw
- keramist[.]org
- lacky-gretest-bonus[.]fun
- lacky-gretest-bonus[.]site
- lacky-instamedia[.]site
- maikmueller[.]net
- master-club[.]space
- master-club[.]website
- newsinformers[.]fun
- newsinformers[.]space
- newsinformers[.]website
- on-mail[.]net
- online-promouter[.]com
- online-promouter[.]net
- pay-gen[.]xyz
- pay-gen1[.]info
- pay-gen1[.]site
- ref01-payoffers[.]site
- ref01-useroffers[.]site
- ref02-infopay[.]site
- sberonline[.]site
- sberonline[.]website
- sbsurvey[.]pw
- top-5[.]biz
- top-game[.]online
- trust-seo[.]com
- ubs-bank[.]info
- union-money[.]site
- union-money[.]website
- vibory2018[.]site
- vostokzapad[.]su
- x1-payfree[.]site
- x2-greatfaro[.]site
- x3-faropaymenrs[.]site
- z2-payfree[.]site
- z3-userreferal[.]site
- zbr-online[.]xyz

Sample IP-Connected Domains

- 0ad1bd76-66b5-459e-ba4e-6d70b7daabd5[.]random[.]cloth-model[.]blog
- 0f260069-3834-4e5b-9eb9-17b11ba3b762[.]random[.]cloth-model[.]blog

- 195-66-213-132[.]dynamic-ip[.]hinet[.]net
- admin[.]cloth-model[.]blog
- anzhuo[.]cloth-model[.]blog
- api[.]cloth-model[.]blog
- b7966597-405f-4c1a-800c-26f04728008c[.]random[.]cloth-model[.]blog
- backback[.]cloth-model[.]blog
- backoffice[.]cloth-model[.]blog
- c9a9e374-4293-4f41-8ebd-d358bef583b9[.]random[.]cloth-model[.]blog
- cb5f56a0-c54b-48a8-a52d-94f7f38babb6[.]random[.]cloth-model[.]blog
- cbukkfneix528nl7r0jhuv9v8[.]cloth-model[.]blog
- d6fd092d-a90d-4730-8705-301d42477b0e[.]cloth-model[.]blog
- de[.]cloth-model[.]blog
- demo[.]cloth-model[.]blog
- e-menu[.]me
- ec846778-7b6d-4e21-907f-4aec020fd4f0[.]random[.]cloth-model[.]blog
- email[.]cloth-model[.]blog
- fbgrasjdxuz[.]cloth-model[.]blog
- final-move[.]store
- forum[.]cloth-model[.]blog
- gitlab[.]cloth-model[.]blog
- home[.]cloth-model[.]blog
- hs3[.]cloth-model[.]blog
- imap[.]cloth-model[.]blog
- info[.]cloth-model[.]blog
- ios[.]cloth-model[.]blog
- localhost[.]albert-company[.]online
- localhost[.]becker624[.]online
- localhost[.]black-friday-store[.]online
- m[.]cloth-model[.]blog
- magento[.]cloth-model[.]blog
- mail[.]albert-company[.]online
- news[.]cloth-model[.]blog
- noreo-po[.]online
- ns1[.]cloth-model[.]blog
- office[.]cloth-model[.]blog
- old[.]cloth-model[.]blog
- optionyou[.]online
- panel[.]cloth-model[.]blog
- pay[.]cloth-model[.]blog
- pop[.]albert-company[.]online
- random[.]cloth-model[.]blog
- reflex-po[.]online
- remote[.]cloth-model[.]blog
- s[.]cloth-model[.]blog
- serve[.]cloth-model[.]blog
- shop[.]cloth-model[.]blog
- test[.]cloth-model[.]blog
- time-quest[.]online
- update[.]cloth-model[.]blog
- ups[.]cloth-model[.]blog
- vpn[.]cloth-model[.]blog
- wap[.]cloth-model[.]blog
- web-kreacija[.]e-menu[.]me
- web[.]cloth-model[.]blog
- ysuoh8rtf40clagtxijw7gmiuzdstt88[.]cloth-model[.]blog

Sample String-Connected Domains

- albert-company[.]com
- alpha-man[.]club
- alpha-man[.]co
- alpha-man[.]co[.]uk
- anna-blog[.]bid
- anna-blog[.]com
- anna-blog[.]cricket
- arizonaclub[.]by
- arizonaclub[.]cn
- arizonaclub[.]co

- backback[.]be
- backback[.]business
- backback[.]club
- bestshopu[.]com
- bestshopu[.]net
- beta-man[.]co[.]uk
- beta-man[.]com
- black-friday-store[.]com
- black-friday-store[.]de
- black-friday-store[.]ga
- city-splash[.]com
- clothes-show[.]co[.]uk
- clothes-show[.]com
- clothes-show[.]uk
- connect-room[.]com
- connect-room[.]net
- connect-room[.]ru
- cook-tips[.]com
- cook-tips[.]ru
- cook-tips[.]space
- course-math[.]ru
- cyberlattice[.]club
- cyberlattice[.]co
- cyberlattice[.]com
- everything-here[.]club
- everything-here[.]com
- everything-here[.]eu
- exir-juice[.]ws
- expressmarket[.]am
- expressmarket[.]be
- expressmarket[.]bg
- first-course[.]co[.]uk
- first-course[.]com
- first-course[.]info
- gallery-shop[.]ba
- gallery-shop[.]ch
- gallery-shop[.]co[.]uk
- good-news[.]accountant
- good-news[.]agency
- good-news[.]ai
- good-student[.]cf
- good-student[.]cn
- good-student[.]com
- healthy-lifestyle[.]academy
- healthy-lifestyle[.]africa
- healthy-lifestyle[.]app
- idea-home[.]cn
- idea-home[.]co
- idea-home[.]co[.]il
- infinit-world[.]com
- infinit-world[.]ir
- live-coaching[.]at
- live-coaching[.]be
- live-coaching[.]co[.]uk
- live-conn[.]com
- live-conn[.]net
- live-content[.]co[.]uk
- live-content[.]com
- live-content[.]de
- live-meet[.]click
- live-meet[.]club
- live-meet[.]co[.]uk
- live-message[.]ch
- live-message[.]co
- live-message[.]co[.]jp
- make-house[.]co[.]jp
- make-house[.]co[.]kr
- make-house[.]com
- master-club[.]at
- master-club[.]cf
- master-club[.]ch
- meet-work[.]com
- meet-work[.]de
- meet-work[.]fr
- message-live[.]click
- message-live[.]com
- network-game[.]cn
- network-game[.]com
- network-game[.]com[.]pl
- network-review[.]club

- network-review[.]co[.]uk
- network-review[.]com
- nice-goods[.]cc
- nice-goods[.]com
- nice-goods[.]com[.]ua
- online-room[.]cf
- online-room[.]com
- online-room[.]ga
- panel-network[.]com
- panel-network[.]vip
- ph-work[.]com
- ph-work[.]de
- ph-work[.]ru
- rap-art[.]com
- rap-art[.]de
- reading-course[.]com
- reading-course[.]ru
- reading-course[.]tk
- reg-d[.]com
- reg-d[.]org
- reg-d[.]ru
- royalsoul[.]city
- royalsoul[.]co
- royalsoul[.]co[.]uk
- shadow-network[.]cf
- shadow-network[.]com
- shadow-network[.]de
- sky-writer[.]com
- sky-writer[.]net
- sky-writer[.]no
- socks[.]ac
- socks[.]ae
- socks[.]africa
- spring-club[.]com
- spring-club[.]de
- spring-club[.]net
- steve-brown[.]co[.]uk
- steve-brown[.]com
- steve-brown[.]eu
- thomas-mark[.]com
- thomas-mark[.]de
- thomas-mark[.]dk
- top-game[.]app
- top-game[.]bid
- top-game[.]biz
- warplogic[.]com
- warplogic[.]pl
- wash-less[.]com
- white-car[.]ch
- white-car[.]co
- white-car[.]co[.]uk
- white-life[.]co[.]kr
- white-life[.]com
- white-life[.]de
- wood-house[.]at
- wood-house[.]be
- wood-house[.]bg
- word-course[.]com
- work-meeting[.]com
- world-shop[.]at
- world-shop[.]biz
- world-shop[.]by
- yamal-group[.]ru