Down the DNS Funnel and into the Funnull Infrastructure

Table of Contents

Executive Report

The Federal Bureau of Investigation (FBI) issued a FLASH report to disseminate indicators of compromise (IoCs) for the Funnull infrastructure that threat actors used to manage domains related to cryptocurrency investment fraud scams between October 2023 and April 2025. The report provided links to two lists.

The first list contained 549 Funnull CNAMEs from which we extracted 19 unique domains. The second list, meanwhile, contained 332,696 URLs believed to be part of the Funnull infrastructure, totaling 333,245 web properties, from which we extracted 176,637 root domains. Combining the two lists, we had a total of 176,656 root domains for analysis.

WhoisXML API ran the dataset through several of our tools, which allowed us to gather these findings for the first part of our analysis:

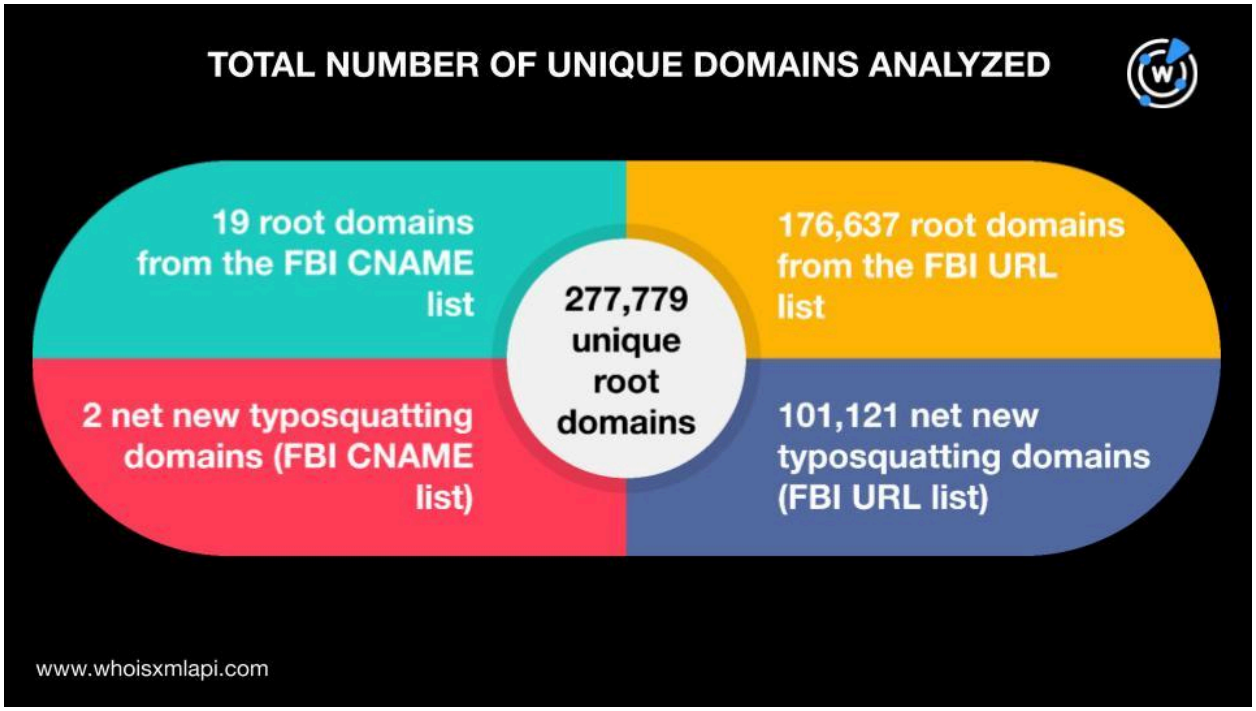
- 176,656 root domains extracted from the FBI's IoC lists
- 101,123 net new typosquatting domains uncovered, bringing the total number of domains to analyze to 277,779
- 82,261 out of the 277,779 domains dubbed "likely to turn malicious" as soon as they were created
- Sample DNS traffic data from the Internet Abuse Signal Collective (IASC) collected for the 277,779 domains recorded 22,772 unique client IP addresses querying 1,062 distinct domains between 6 May and 4 June 2025 through 189,640 DNS requests

We then paid closer attention to the 101,123 net new typosquatting domains, along with the 44,834 FBI domains these were derived from, and identified the following findings for the latter part of our analysis:

- Hong Kong was the top geolocation country of the resolving IP addresses while the top ISP varied for the IPs of the net new typosquatting domains versus FBI domains.
- The U.S. was the top current registrant country while 146 was their top IANA ID.
- The U.S. was the top historical registrant country (i.e., when the domains were first created) while the top historical IANA ID varied for the net new typosquatting domains versus FBI domains.

Hunting for Look-Alike Domains

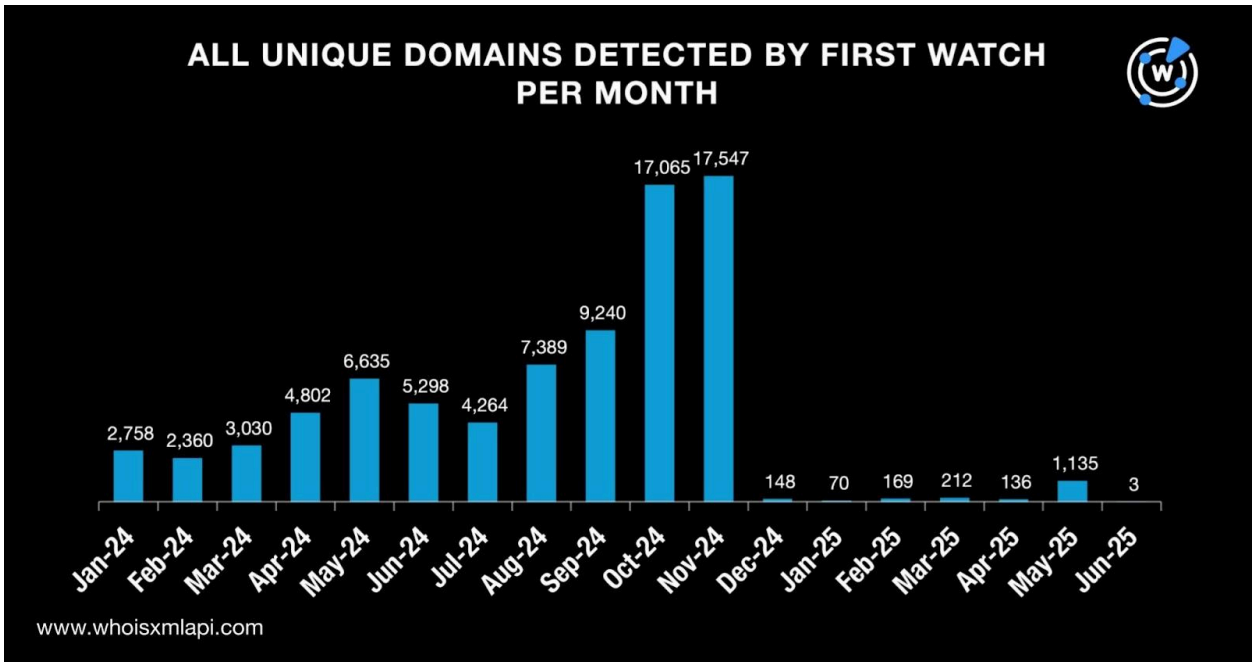
We began our analysis by uncovering more domains that could be part of the Funnull infrastructure, specifically by looking for look-alikes via the Typosquatting Data Feed. Using the combined list of 176,656 root domains from the FBI lists as search terms, we obtained 101,123 net new typosquatting domains. That brought our total dataset to 277,779 domains.



Examining the Combined List of FBI and Typosquatting Domains

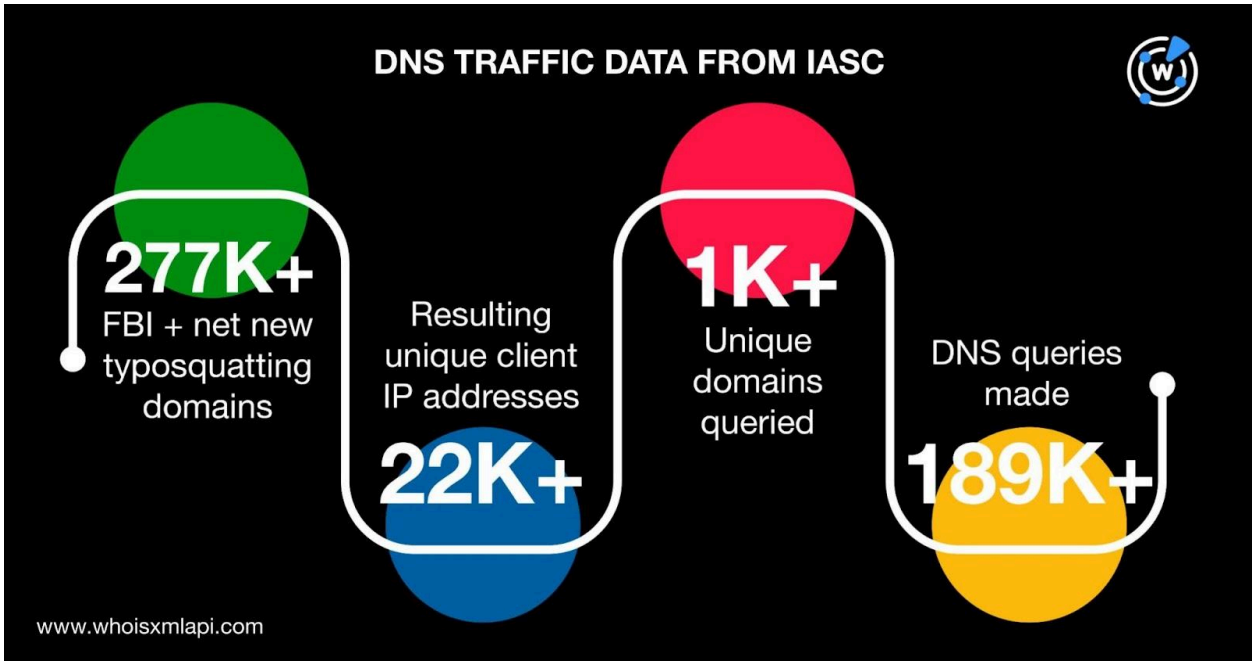
Determining Which Domains Were Likely to Turn Malicious

After expanding our dataset, we sought to determine if any of the 277,779 domains were deemed likely to turn malicious as soon as they were created. Our First Watch Malicious Domains Data Feed searches provided us with 82,261 matches from January 2024 to June 2025, which makes up nearly 30% of the total number. Take a look at the domain volume breakdown by month below.

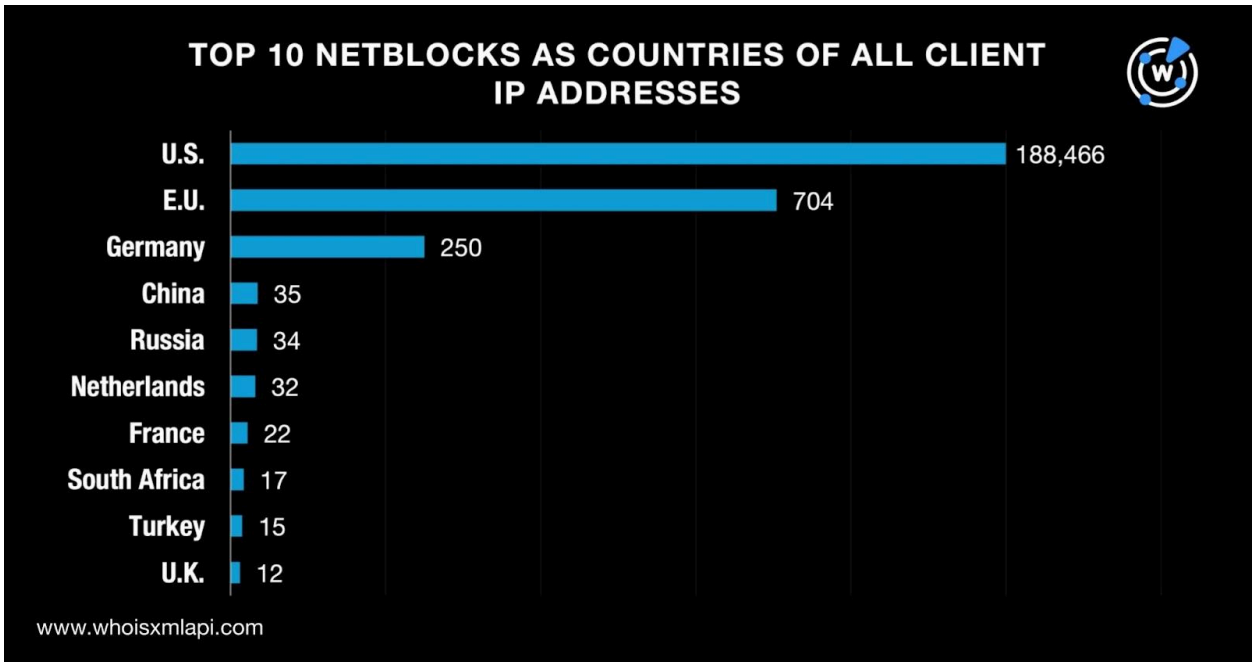


Uncovering Active DNS Connections

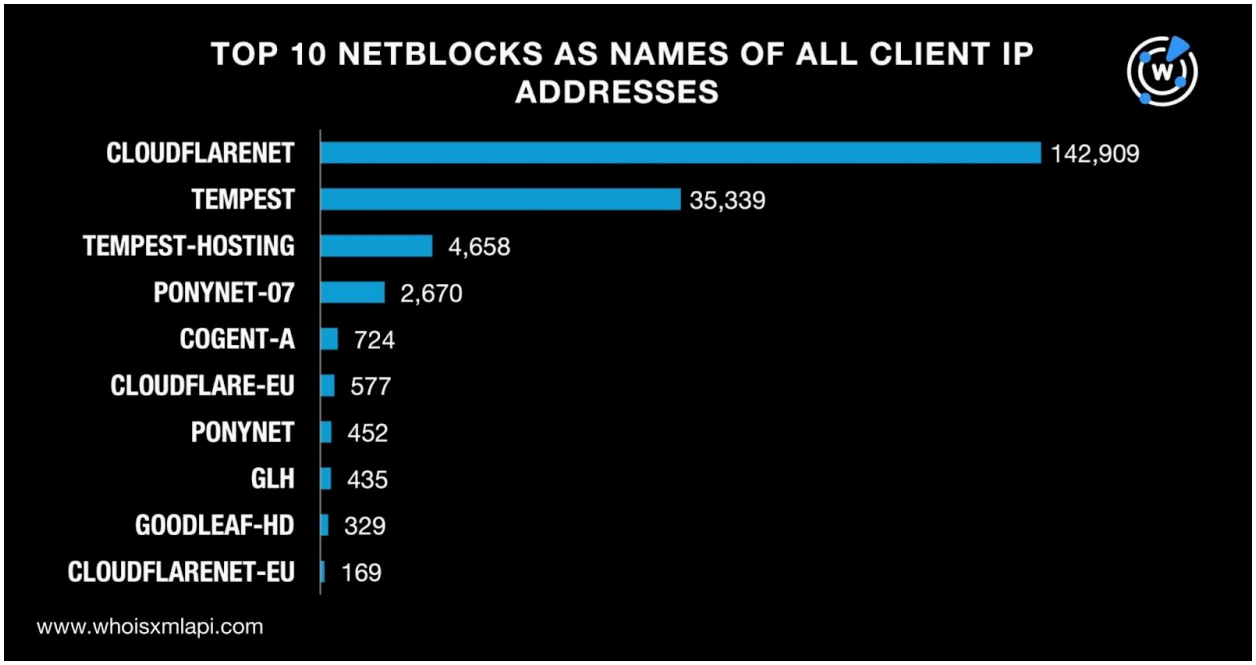
Using sample DNS traffic data our researchers obtained from the IASC, we further analyzed the 277,779 domains. The sample data revealed that 22,772 unique client IP addresses queried 1,062 distinct domains between 6 May and 4 June 2025 through a total of 189,640 DNS requests.



We further examined the DNS traffic data to determine the top 10 netblocks Autonomous System (AS) countries of the client IP addresses and found they were the U.S., the E.U., Germany, China, Russia, the Netherlands, France, South Africa, Turkey, and the U.K. Take a look at the breakdown below.



We also identified the top 10 netblocks AS names pertaining to the providers of the client IP addresses. CLOUDFLARENET topped the list, followed by TEMPEST, TEMPEST-HOSTING, PONYNET-07, COGENT-A, CLOUDFLARE-EU, PONYNET, GLH, GOODLEAF-HD, and CLOUDFLARENET-EU. Take a look at the details below.



Digging Deeper into the Typosquatting Domains

Our search for typosquatting domains, including those that were already part of the FBI lists, actually turned up 145,957 domains in all, three for the FBI CNAMEs list and 145,954 for the FBI infrastructure-related subdomains and domains list.

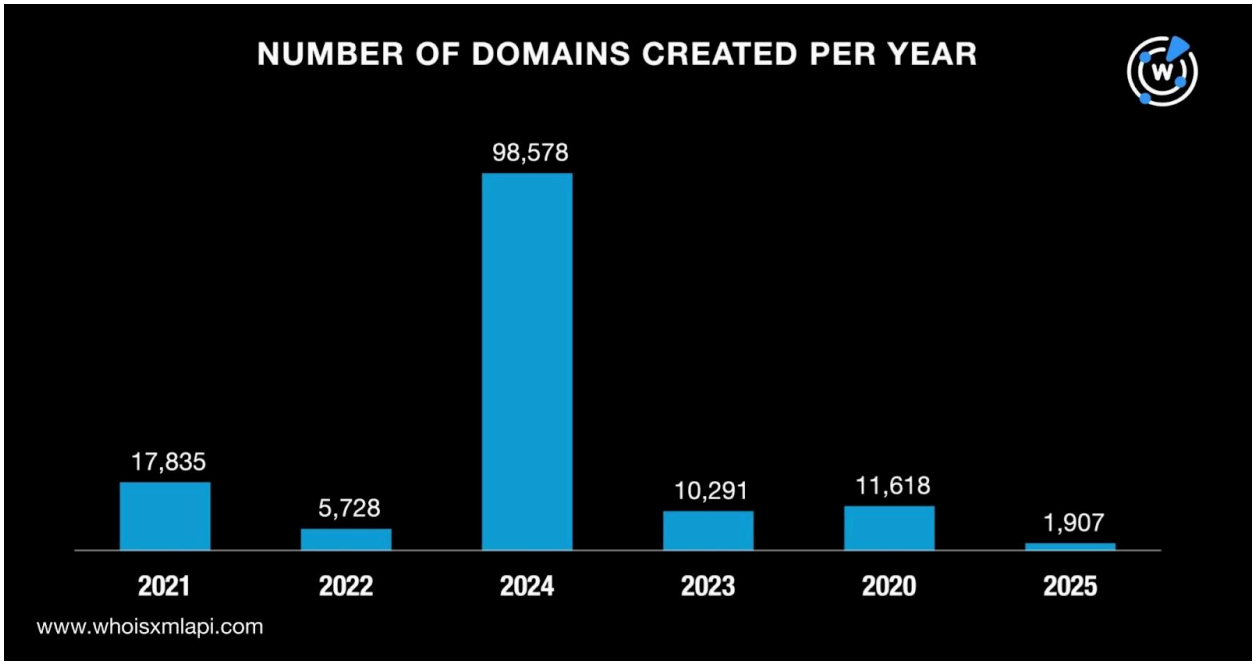
More specifically, 44,834 of the 176,656 root domains extracted from the FBI's IoC lists were used with domain clustering techniques to identify multiple groups of similar-looking domains with matching registration dates, resulting in the discovery of 101,123 net new typosquatting domains.

To illustrate, let us take a look at an extract sample from our Typosquatting Data Feed, alongside some enrichments, specifically a snippet showing data points for group number 51 comprising 176 domains spotted on 22 May 2024.

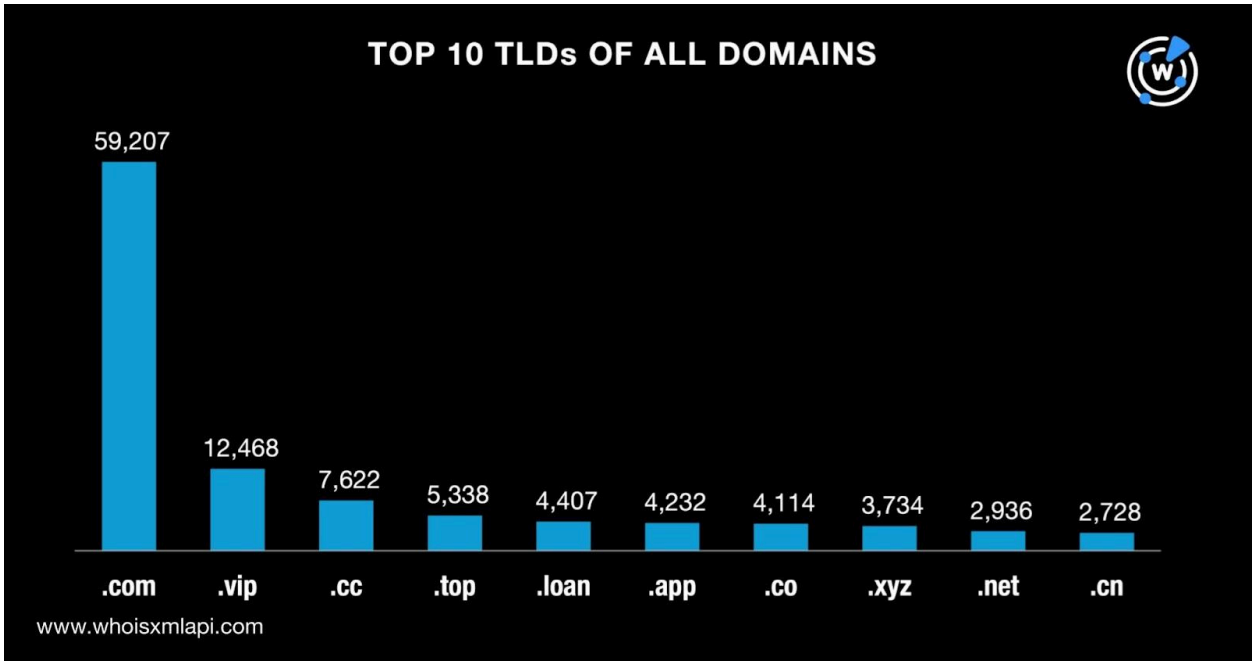
Typosquatting Data Feed					Bulk IP Geolocation Lookup		Bulk WHOIS API		WHOIS History API	
Date	Domain	Group Number	Group Size	Source	Geolocation Country	ISP	Registrar IANA ID	Registrant Country	Registrar IANA ID	Registrant Country
2024-05-22	67331.club	51	176	Net new typosquatting	US	Amazon.com			472	UNITED STATES
2024-05-22	67282.club	51	176	Net new typosquatting	US	Amazon.com			472	UNITED STATES
2024-05-22	62310.ooo	51	176	Net new typosquatting	US	Amazon.com	472	UNITED STATES	472	UNITED STATES
2024-05-22	67276.club	51	176	Net new typosquatting	US	Amazon.com			472	UNITED STATES
2024-05-22	67607.cc	51	176	Net new typosquatting	US	Amazon.com	472	UNITED STATES	472	UNITED STATES
2024-05-22	67305.club	51	176	Net new typosquatting	US	Amazon.com			472	UNITED STATES
2024-05-22	67383.club	51	176	Net new typosquatting	US	Amazon.com			472	UNITED STATES
2024-05-22	67379.club	51	176	Net new typosquatting	US	Amazon.com			472	UNITED STATES
2024-05-22	67632.cc	51	176	Net new typosquatting	US	Amazon.com	472	UNITED STATES	472	UNITED STATES
2024-05-22	67350.ooo	51	176	Net new typosquatting	US	Amazon.com	472	UNITED STATES	472	UNITED STATES
2024-05-22	67339.club	51	176	Net new typosquatting	US	Amazon.com			472	UNITED STATES
2024-05-22	67328.club	51	176	Net new typosquatting	US	Amazon.com			472	UNITED STATES
2024-05-22	67696.cc	51	176	Net new typosquatting	US	Amazon.com	472	UNITED STATES	472	UNITED STATES
2024-05-22	67228.pro	51	176	Net new typosquatting	US	Amazon.com	472	UNITED STATES	472	UNITED STATES
2024-05-22	67639.cz	51	176	FBI original	CN, HK	CNSERVERS, Microsoft		UNITED STATES	0	UNITED STATES

As shown, the 14 sample typosquatting domains resembled the domain 67639[.]cz from the FBI's infrastructure-related domains list in that they all began with **6**, comprised five random numbers, and sported new gTLD extensions. Many of them also shared the FBI domain's registrant country—the U.S.—at the time they were first created based on data gleaned from WHOIS History API and their current WHOIS record details.

Moving on with our analysis of the 145,957 domains, a closer look at their creation dates showed that a majority, 98,578 to be exact, were created in 2024. Altogether, the domains were created between 2021 and 2025. Take a look at the breakdown below.



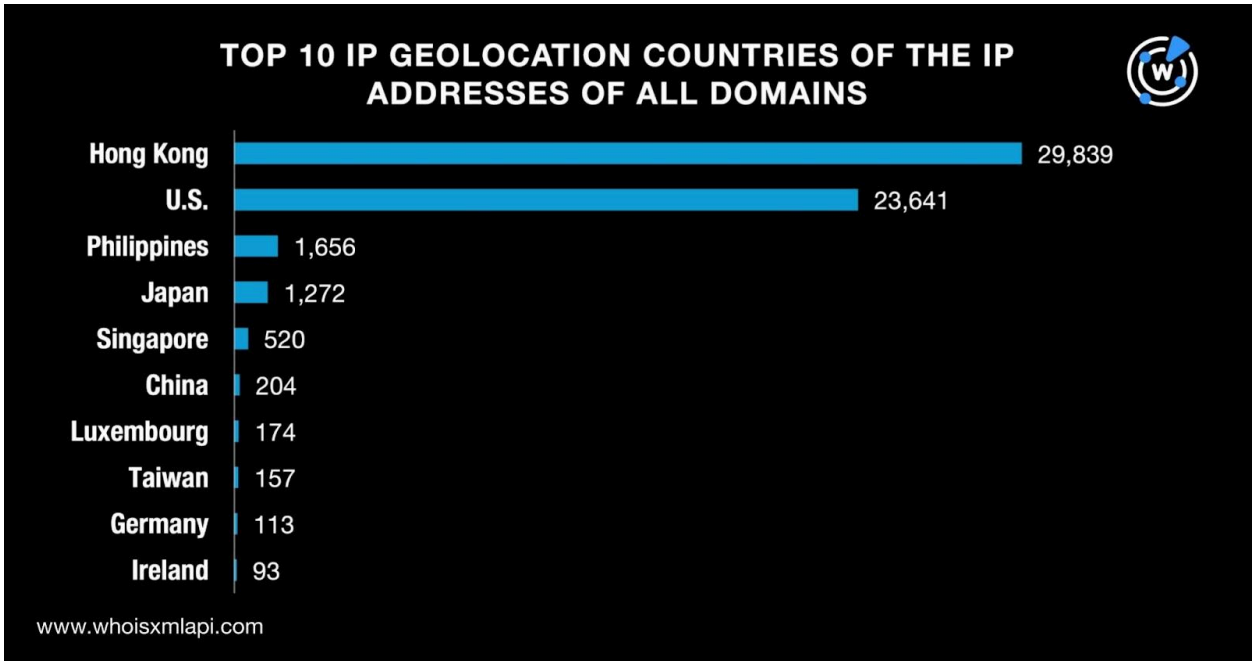
We also scrutinized the domains in terms of TLD extension and found that a majority, 59,207 to be exact, sported the .com gTLD. Eight of the other TLDs were gTLDs, namely, .vip, .cc, .top, .loan, .app, .co, .xyz, and .net while one was the .cn ccTLD. Take a look at the details below.



We then sought to dig even deeper into the 145,957 domains' resolving IP addresses and current and historical information in a bid to find overlaps between the domains on the FBI lists and those obtained from Typosquatting Data Feed.

IP Origins and Service Providers

The data we collated from Bulk IP Geolocation Lookup revealed that the top 10 geolocation countries for the combined list of 145,957 domains were Hong Kong, the U.S., the Philippines, Japan, Singapore, China, Luxembourg, Taiwan, Germany, and Ireland. All in all, they were geolocated in 45 countries. Take a look at the detailed breakdown below.



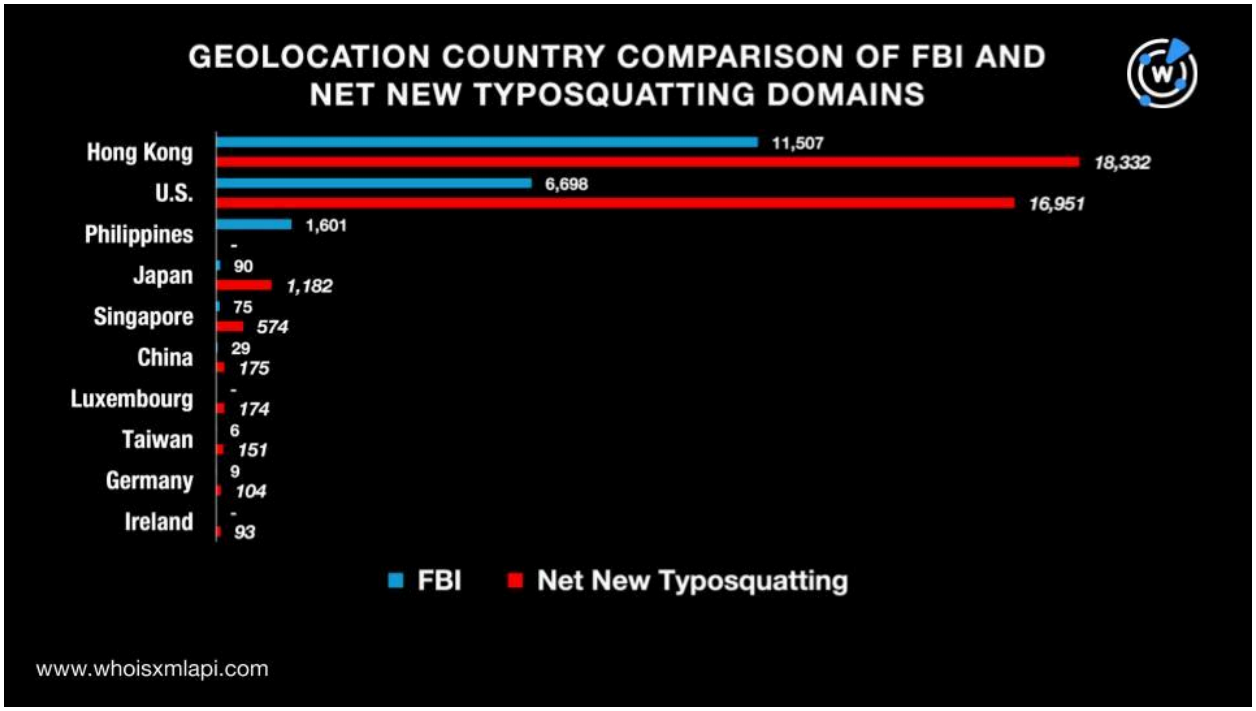
More specifically, 18,255 of the IP addresses of the 44,834 FBI domains had geolocation countries on record. They were spread across 14 countries led by Hong Kong, which accounted for 11,507 of the resolving IP addresses. The rest of the top 10 countries were the U.S., the Philippines, Japan, Singapore, China, France, Germany, Taiwan, and India.

Meanwhile, 38,363 of the IP addresses of the 101,123 net new typosquatting domains had geolocation country information. They were split among 45 countries led by Hong Kong, which accounted for 18,332 of the resolving IP addresses. The rest of the top 10 countries were the U.S., Japan, Singapore, China, Luxembourg, Taiwan, Germany, Ireland, and Malaysia.

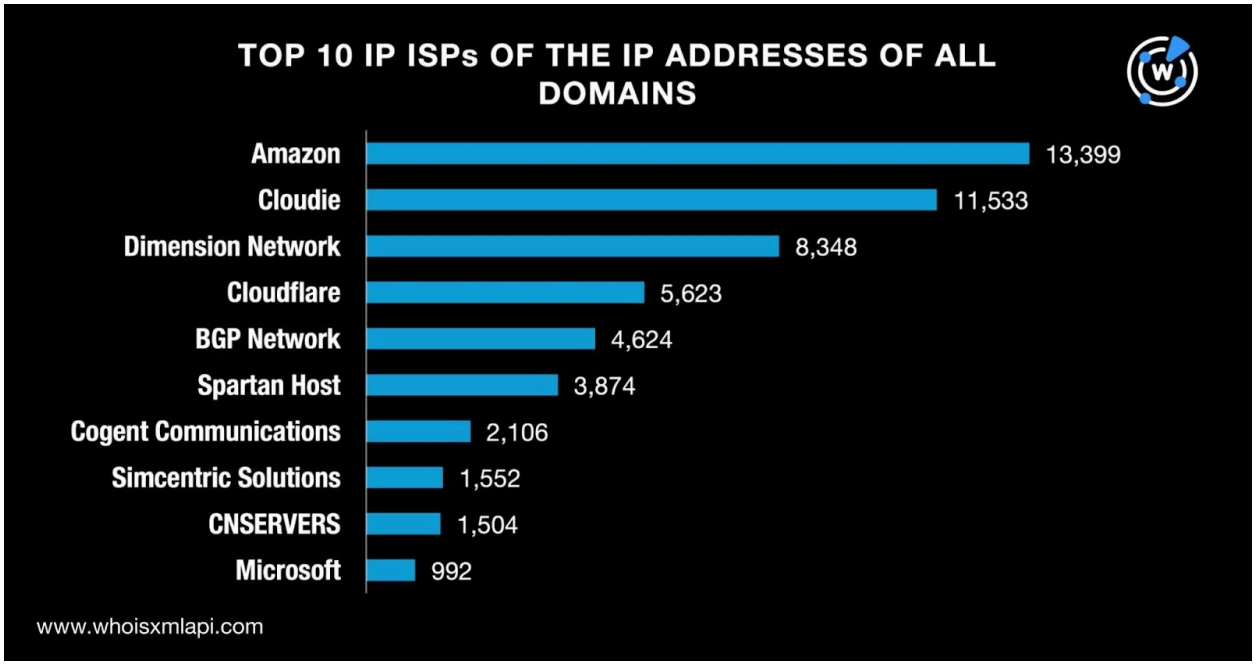
GEOLOCATION COUNTRY	FBI DOMAINS	ALL DOMAINS	NET NEW TYPOSQUATTING DOMAINS
Hong Kong	1st	1st	1st
U.S.	2nd	2nd	2nd
Philippines	3rd	3rd	
Japan	4th	4th	3rd
Singapore	5th	5th	4th
China	6th	6th	5th

Luxembourg		7th	6th
Taiwan	9th	8th	7th
Germany	8th	9th	8th
Ireland		10th	9th

A comparison of the top 10 geolocation countries for the FBI and net new typosquatting domains showed a 70% overlap. Both lists had seven countries in common. Take a look at the details below.



Looking at the ISPs, we discovered that the top 10 were Amazon, Cloudie, Dimension Network, Cloudflare, BGP Network, Spartan Host, Cogent Communications, Simcentric Solutions, CNSERVERS, and Microsoft. The domains' resolving IP addresses were administered by 192 ISPs. Take a look at the detailed breakdown below.



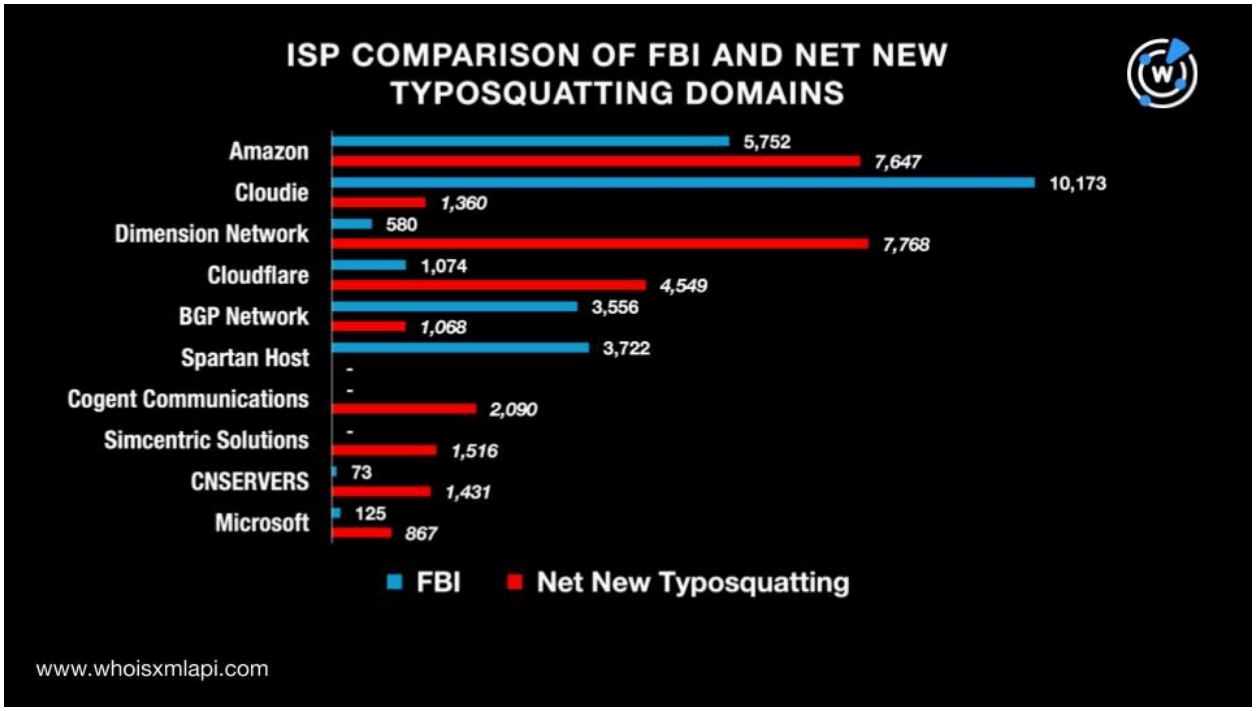
More specifically, the top 10 ISPs for the FBI domains were Cloudie, Amazon, Spartan Host, BGP Network, Cloudflare, Dimension Network, DXTL, Microsoft, CNSERVERS, and Alibaba and MultaCOM that tied in tenth place. The domains' resolving IP addresses were administered by 53 ISPs.

Meanwhile, the top 10 ISPs for the net new typosquatting domains were Dimension Network, Amazon, Cloudflare, Cogent Communications, Simcentric Solutions, CNSERVERS, Cloudie, BGP Network, Microsoft, and OWS. The domains' resolving IP addresses were administered by 192 ISPs.

ISP	FBI DOMAINS	ALL DOMAINS	NET NEW TYPOSQUATTING DOMAINS
Amazon	2nd	1st	2nd
Cloudie	1st	2nd	7th
Dimension Network	6th	3rd	1st
Cloudflare	5th	4th	3rd
BGP Network	4th	5th	8th
Spartan Host	3rd	6th	

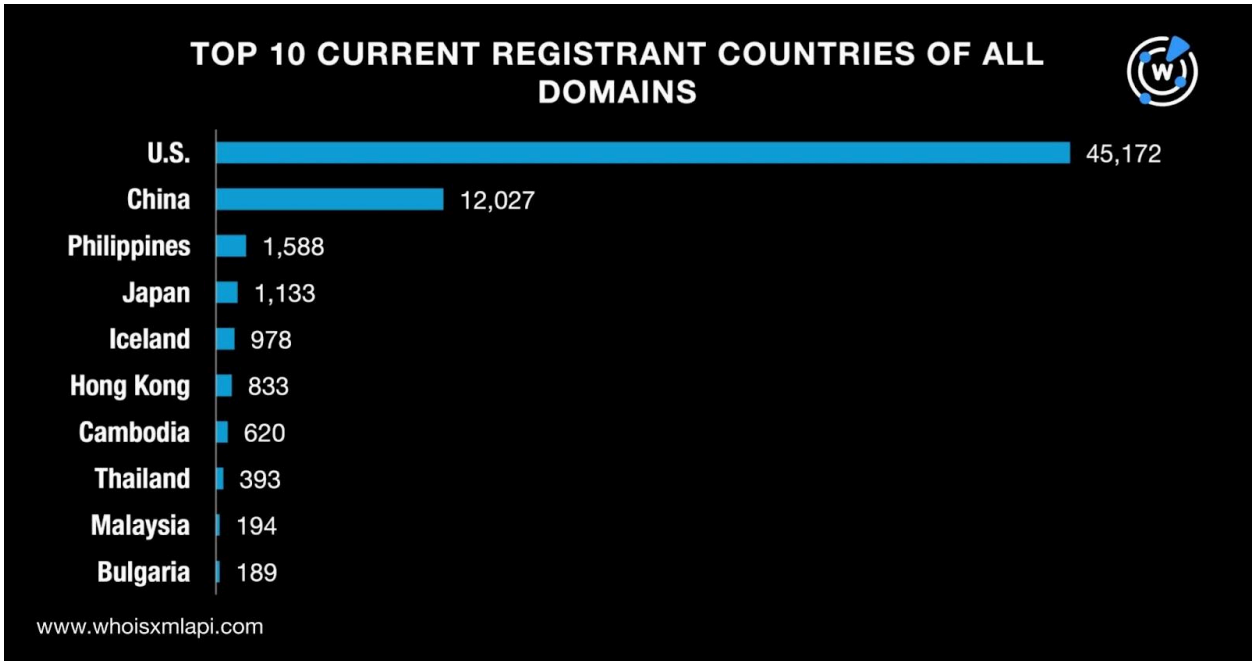
Cogent Communications		7th	4th
Simcentric Solutions		8th	5th
CNSERVERS	9th	9th	6th
Microsoft	8th	10th	9th

A comparison of the top 10 ISPs for the FBI and net new typosquatting domains showed a 70% overlap. Both lists had seven ISPs in common. Take a look at the details below.



Current Domain Registrant Countries and Registrars

The data we collated from Bulk WHOIS API revealed that the top 10 registrant countries for the combined list of 145,957 domains were the U.S., China, the Philippines, Japan, Iceland, Hong Kong, Cambodia, Thailand, Malaysia, and Bulgaria. All in all, they were registered in 70 countries. Take a look at the detailed breakdown below.



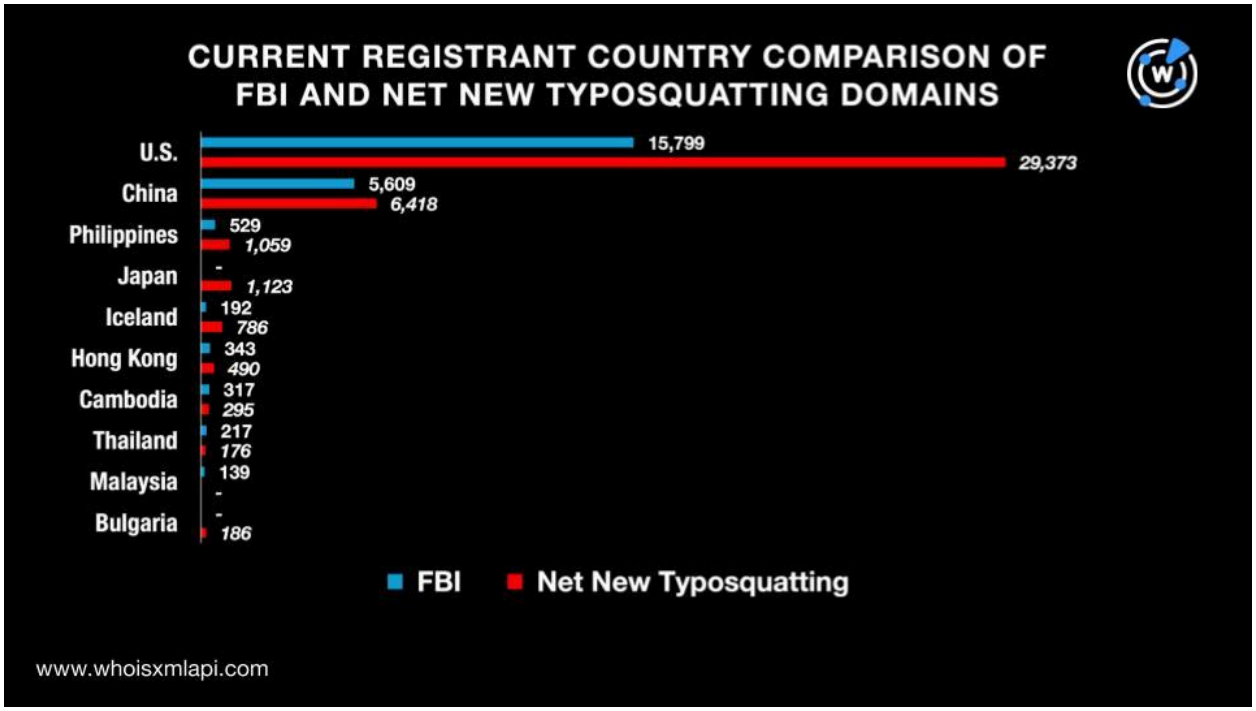
More specifically, 23,342 of the 44,834 FBI domains had registrant countries on record. They were spread across 28 countries led by the U.S., which accounted for 15,799 domains. The rest of the top 10 registrant countries were China, the Philippines, Hong Kong, Cambodia, Thailand, Iceland, Malaysia, the Czech Republic, and Canada.

Meanwhile, 40,947 of the 101,123 net new typosquatting domains had registrant country information. They were split among 69 countries led by the U.S., which accounted for 29,373 domains. The rest of the top 10 registrant countries were China, Japan, the Philippines, Iceland, Hong Kong, Cambodia, Bulgaria, Senegal, and Thailand.

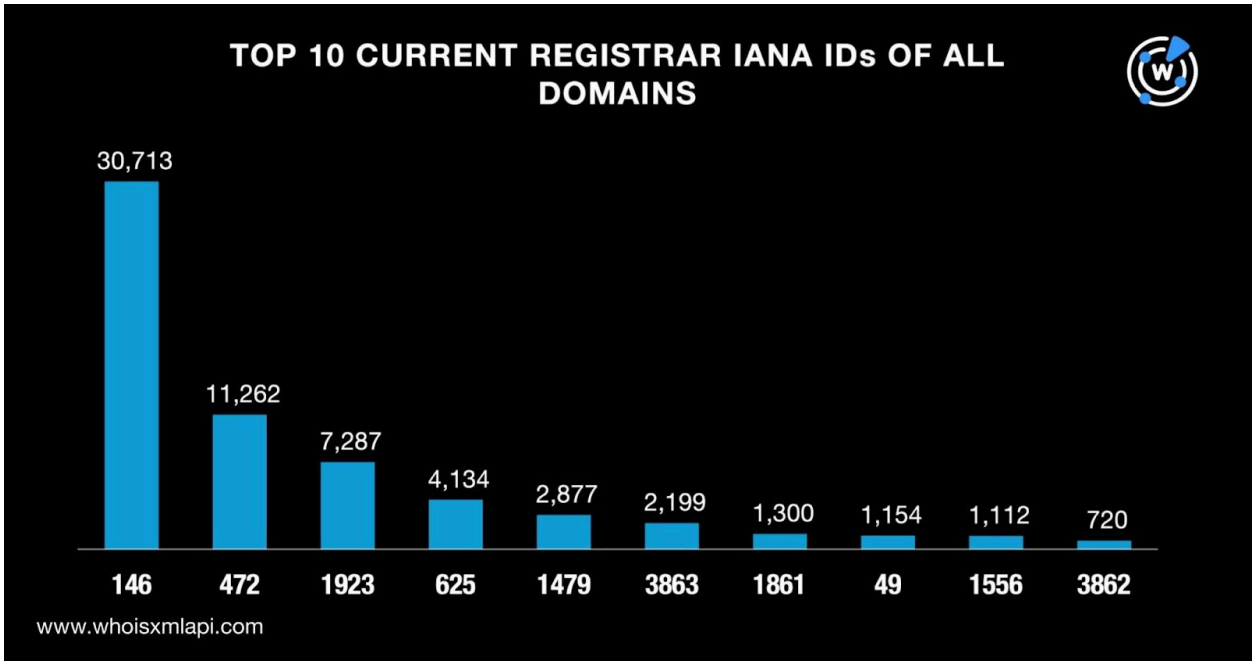
CURRENT REGISTRANT COUNTRY	FBI DOMAINS	ALL DOMAINS	NET NEW TYPOSQUATTING DOMAINS
U.S.	1st	1st	1st
China	2nd	2nd	2nd
Philippines	3rd	3rd	4th
Japan		4th	3rd
Iceland	7th	5th	5th
Hong Kong	4th	6th	6th

Cambodia	5th	7th	7th
Thailand	6th	8th	10th
Malaysia	8th	9th	
Bulgaria		10th	8th

A comparison of the top 10 registrant countries for the FBI and net new typosquatting domains showed a 70% overlap. Both lists had seven countries in common. Take a look at the details below.



Next, we looked into all the domains' current registrar Internet Assigned Numbers Authority (IANA) IDs and discovered that the top 10 were 146, 472, 1923, 625, 1479, 3863, 1861, 49, 1556, and 3862. We found 185 unique IDs in all. Take a look at the detailed breakdown below.



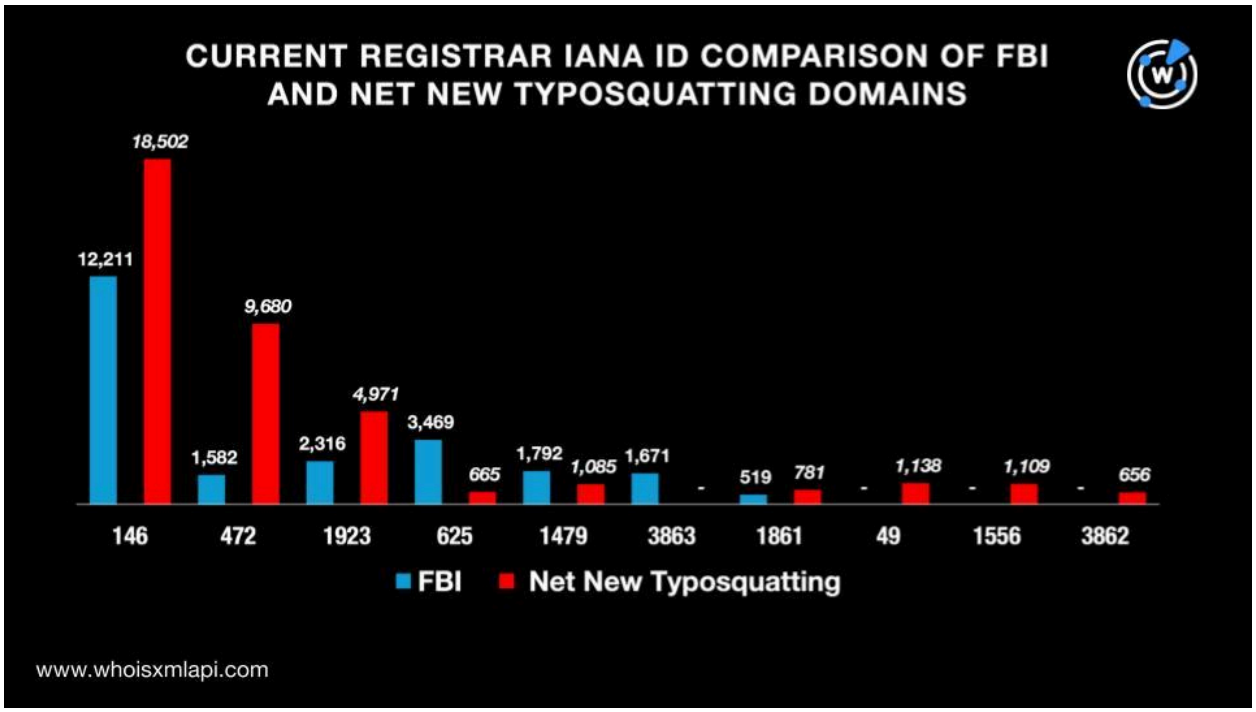
The top 10 current IANA IDs for the FBI domains, on the other hand, were 146, 625, 1923, 1479, 3863, 472, 1861, 460, 1491, and 1068. We uncovered 46 unique IDs in all.

Finally, the top 10 current IANA IDs for the net new typosquatting domains were 146, 472, 1923, 49, 1556, 1479, 1861, 625, 3862, and 1068. We found 182 IDs in all.

CURRENT IANA ID	FBI DOMAINS	ALL DOMAINS	NET NEW TYPOSQUATTING DOMAINS
146	1st	1st	1st
472	6th	2nd	2nd
1923	3rd	3rd	3rd
625	2nd	4th	8th
1479	4th	5th	6th
3863	5th	6th	
1861	7th	7th	7th
49		8th	4th

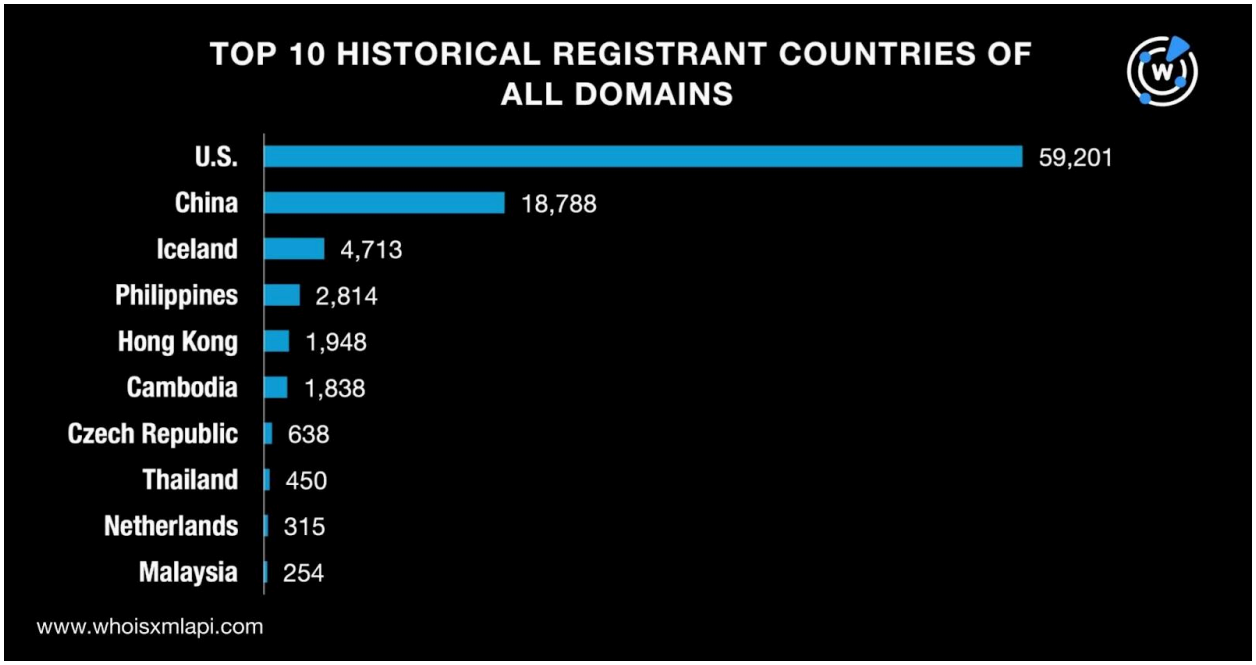
1556		9th	5th
3862		10th	9th

A comparison of the top 10 current registrar IANA IDs for the FBI and net new typosquatting domains showed a 60% overlap. Both lists had six IANA IDs in common. Take a look at the details below.



Historical Domain Registrant Countries and Registrars

The data we collated from WHOIS History API revealed that the top 10 registrant countries for the combined list of 145,957 domains at the time they were first created were the U.S., China, Iceland, the Philippines, Hong Kong, Cambodia, the Czech Republic, Thailand, the Netherlands, and Malaysia. All in all, they were registered in 69 countries. Take a look at the detailed breakdown below.



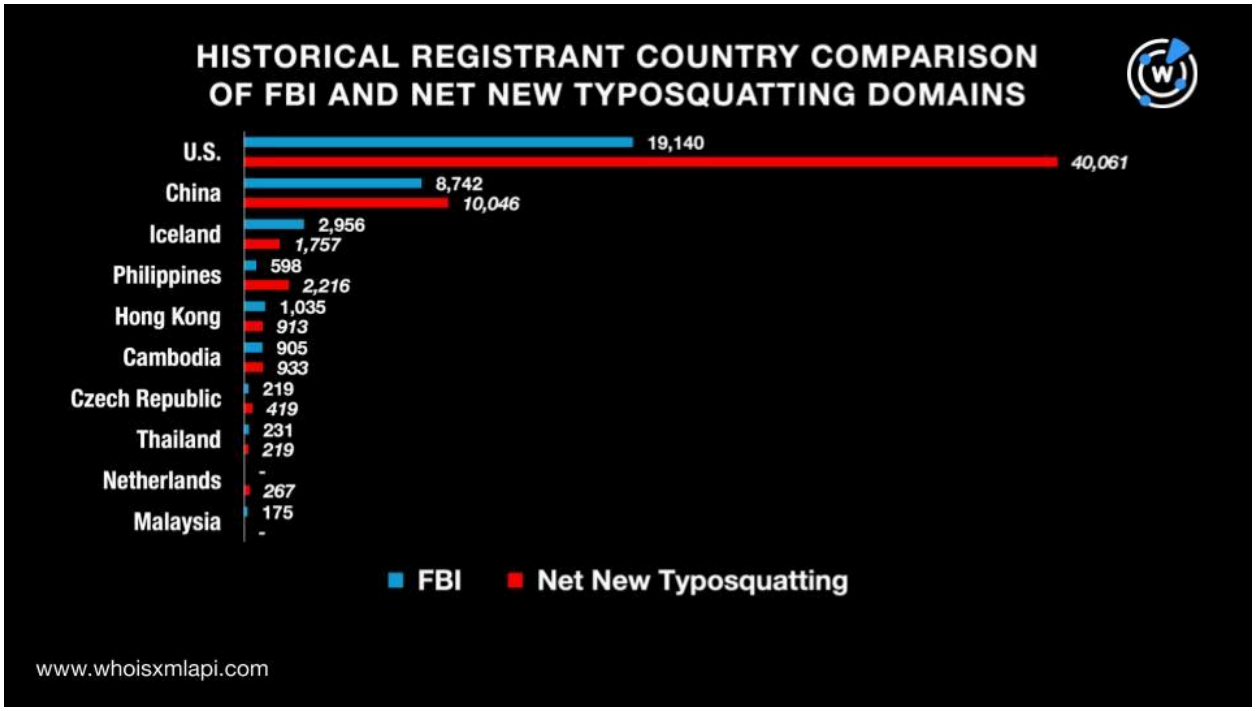
Meanwhile, 34,222 of the 44,834 FBI domains had registrant countries in their historical WHOIS record at the time of their creation. They were spread across 34 countries led by the U.S., which accounted for 19,140 domains. The rest of the top 10 countries were China, Iceland, Hong Kong, Cambodia, the Philippines, Thailand, the Czech Republic, Malaysia, and Croatia.

Finally, 58,772 of the 101,123 net new typosquatting domains had historical registrant country information. They were split among 66 countries led by the U.S., which accounted for 40,061 domains. The rest of the top 10 countries were China, the Philippines, Iceland, Cambodia, Hong Kong, the Czech Republic, the Netherlands, Thailand, and Taiwan.

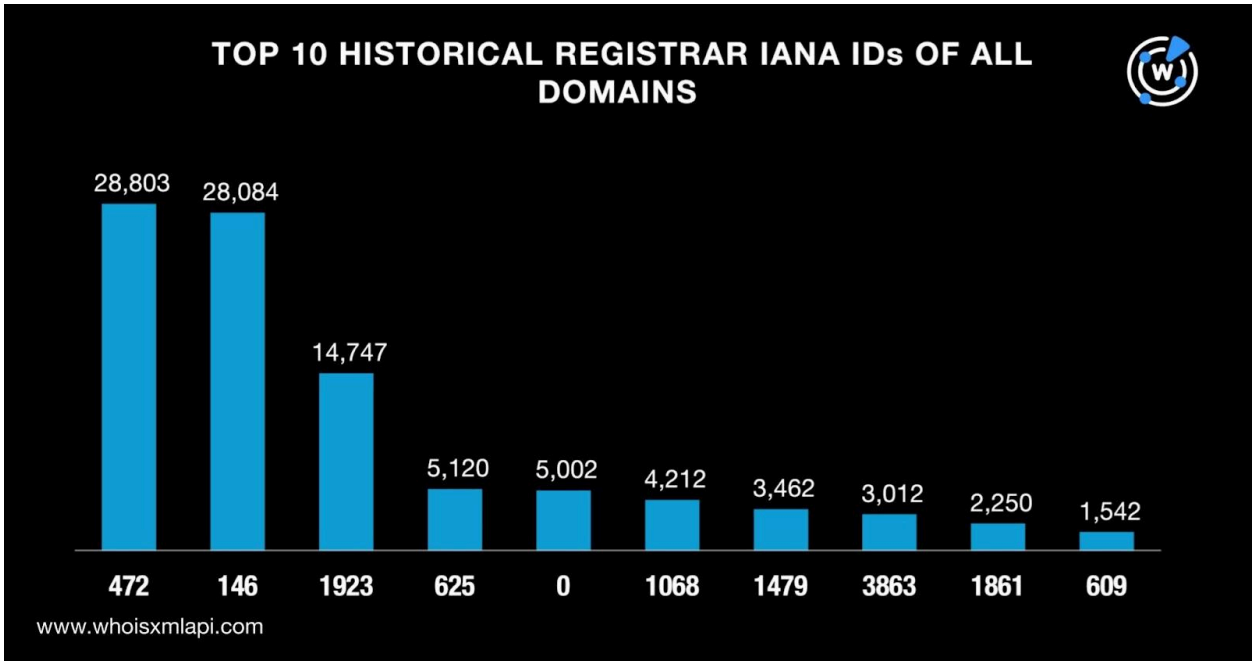
HISTORICAL REGISTRANT COUNTRY	FBI DOMAINS	ALL DOMAINS	NET NEW TYPOSQUATTING DOMAINS
U.S.	1st	1st	1st
China	2nd	2nd	2nd
Iceland	3rd	3rd	4th
Philippines	6th	4th	3rd
Hong Kong	4th	5th	6th
Cambodia	5th	6th	5th

Czech Republic	8th	7th	7th
Thailand	7th	8th	9th
Netherlands		9th	8th
Malaysia	9th	10th	

A comparison of the top 10 historical registrant countries for the FBI and net new typosquatting domains showed an 80% overlap. Both lists had eight countries in common. Take a look at the details below.



Next, we looked into all the domains' historical registrar IANA IDs and discovered that the top 10 were 472, 146, 1923, 625, 0, 1068, 1479, 3863, 1861, and 609. We found 236 unique IDs in all. Take a look at the detailed breakdown below.



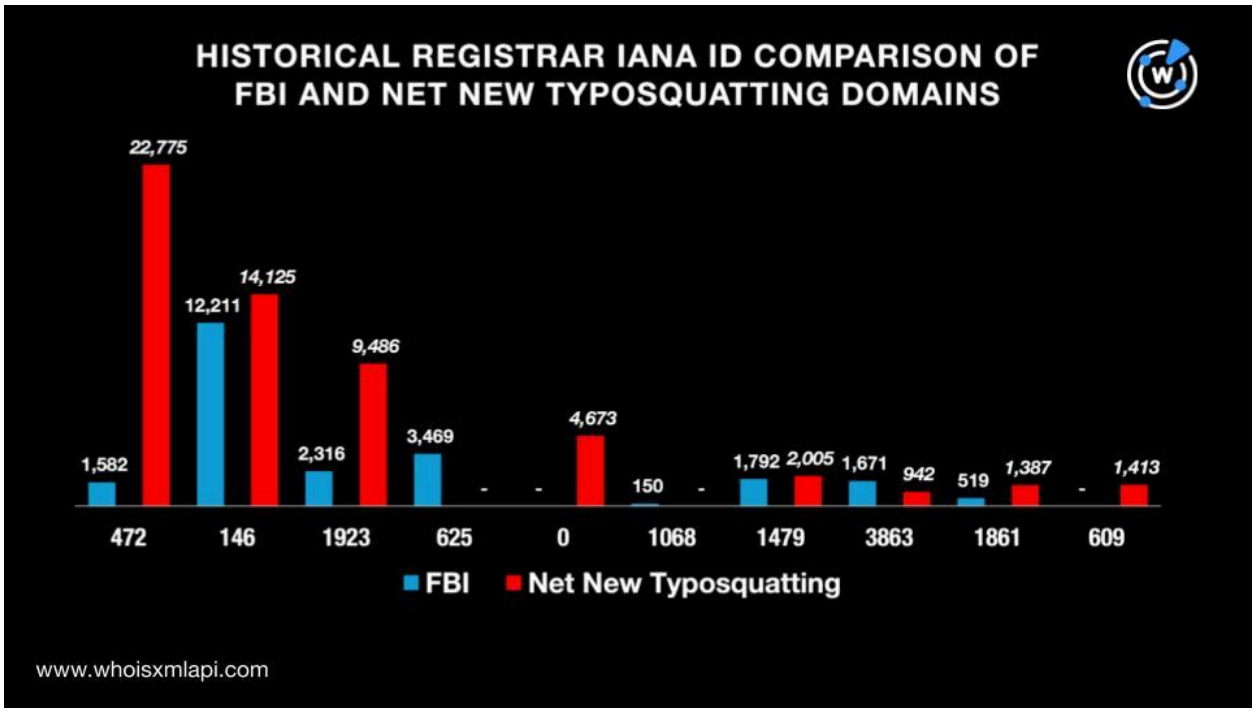
More specifically, the top 10 historical IANA IDs for the FBI domains were 146, 625, 1923, 1479, 3863, 472, 1861, 460, 1491, and 1068. We uncovered 46 unique IDs in all.

Meanwhile, the top 10 historical IANA IDs for the net new typosquatting domains were 472, 146, 1923, 0, 1479, 609, 1861, 1556, 3862, and 3863. We found 231 IDs in all.

HISTORICAL IANA ID	FBI DOMAINS	ALL DOMAINS	NET NEW TYPOSQUATTING DOMAINS
472	6th	1st	1st
146	1st	2nd	2nd
1923	3rd	3rd	3rd
625	2nd	4th	
0		5th	4th
1068	10th	6th	
1479	4th	7th	5th
3863	5th	8th	10th

1861	7th	9th	7th
609		10th	6th

A comparison of the top 10 current registrar IANA IDs for the FBI and net new typosquatting domains showed a 60% overlap. Both lists had six IANA IDs in common. Take a look at the details below.



—

Our more in-depth investigation into the Funnull dataset using several of our tools allowed us to gather these findings for the first part of our analysis:

- 176,656 root domains extracted from the FBI's IoC lists
- 101,123 net new typosquatting domains uncovered, bringing the total number of domains to analyze to 277,779
- 82,261 out of the 277,779 domains dubbed "likely to turn malicious" as soon as they were created
- Sample DNS traffic data from the IASC collected for the 277,779 domains recorded 22,772 unique client IP addresses querying 1,062 distinct domains between 6 May and 4 June 2025 through 189,640 DNS requests

We then paid closer attention to the 101,123 net new typosquatting domains, along with the 44,834 FBI domains these were derived from, and identified the following findings for the latter part of our analysis:

- Hong Kong was the top geolocation country of the resolving IP addresses while the top ISP varied for the IPs of the net new typosquatting domains versus FBI domains.
- The U.S. was the top current registrant country while 146 was their top IANA ID.
- The U.S. was the top historical registrant country (i.e., when the domains were first created) while the top historical IANA ID varied for the net new typosquatting domains versus FBI domains.

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 Domains from the Typosquatting Data Feed

- funnull-accelerate[.]com
- funnullaccelerate[.]vip
- funnull-accelerate[.]vip
- 80095[.]bet
- 80095[.]org
- 80095[.]info
- hth1752[.]com
- hth6598[.]com
- hth7547[.]com
- yhty239[.]app
- yhty187[.]vip
- ytty90[.]com
- bet5765[.]com
- bet5685[.]com
- bet5985[.]com
- x000511[.]com
- x000211[.]com
- x000311[.]com
- alibabacloud-cloud-huawei-qsedc-meiqia-zhihui01[.]com
- alibabacloud-cloud-huawei-qsedc-meiqia-bfclpz1[.]com
- alibabacloud-cloud-huawei-qsedc-meiqia-juw01[.]com
- 88816xx[.]com
- 88856xx[.]com
- 88827xx[.]com
- yicau04[.]com
- yicau02[.]com
- yicau05[.]com
- zhxw668[.]com
- zhxw660[.]com

- zhxw661[.]com
- suiliao27[.]xyz
- suiliao29[.]xyz
- suiliao24[.]xyz

Sample Domains from First Watch Malicious Domains Data Feed

- qdty168[.]com
- 00kykf13[.]com
- 00kykf14[.]com
- 04960976[.]com
- 04528702[.]com
- 04612267[.]com
- 04696979[.]com
- 04614679[.]com
- 04681071[.]com
- 04304491[.]com
- 04756486[.]com
- 04588530[.]com
- 52663t[.]com
- 53695t[.]com
- 53365x[.]com
- xvu707[.]cn
- rpm621[.]cn
- wyp769[.]cn
- pg8087ww[.]com
- qfy021[.]cn
- byz132[.]cn
- tzb690[.]cn
- viq693[.]cn
- vxq123[.]cn
- pnckgkkof[.]top
- apppnc5[.]top
- coinmetrogkkof[.]top
- fdge06trf[.]com
- fcw039[.]cn
- fau562[.]cn