

Session 6B - Technical Means to Mitigate DNS Abuse

Ching Chiao, Head of APAC and Global Partnership
APTLD86 - Sep 19, 2024



WhoisXMLAPI

The Who Behind Domain, IP & Cyber Threat Intelligence

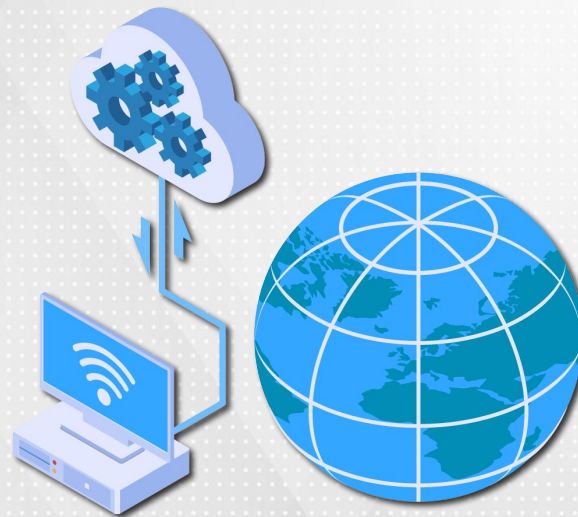
Overview

Part 1 - Descriptive Analysis of Native Language Characters in FQDNs

- A sample of 63,105 unique FQDNs containing native-language characters from more than 58 billion rows of data from a historical DNS file dated 6 June 2024
- The records were enriched with domain ownership and IP geolocation data

Part 2 - Technical Means to Study Suspicious FQDNs and IDN IoCs

- Clustering of the 63,105 FQDNs
- 4,000 identified domain IoCs containing the string "xn--"

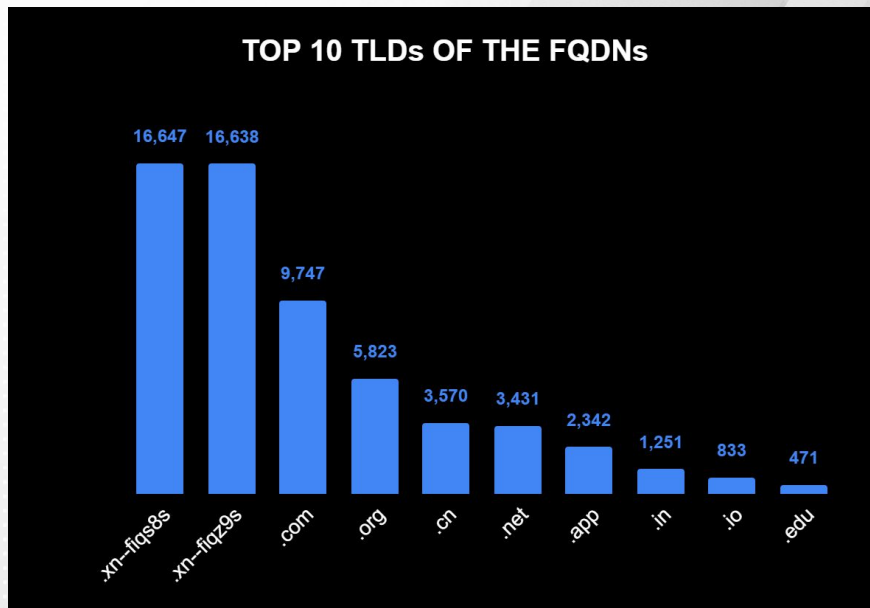


A woman with long dark hair, wearing a dark vest over a light-colored shirt and light-colored trousers, stands in a server room aisle. She is looking up and reaching towards a server rack on her right. The room is filled with rows of server racks, with many cables visible. The background shows more racks and a doorway. The entire image has a blue tint.

Part 1 - Descriptive Analysis of **Native** Language Characters in FQDNs

Presence Across Registries and TLDs

Our pDNS data highlighted the presence of native language characters in FQDNs across TLD types.

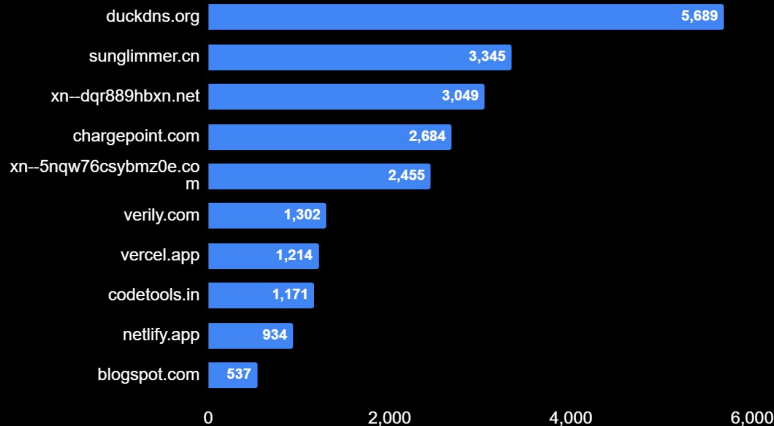


Top 10 ccTLDs	Volume
.xn--fiqs8s (.中国)	16647
.xn--fiqz9s (.中國)	16638
.cn	3570
.in	1251
.io	833
.cz	344
.ru	300
.ph	284
.ws	212

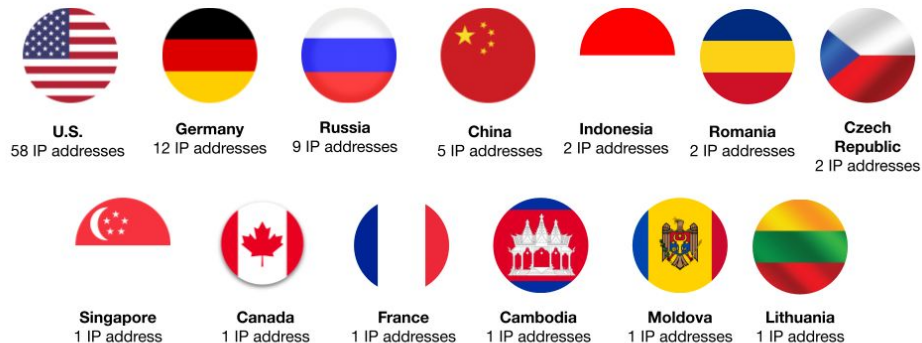
Found at Several Domain Levels

Native language characters were found at several domain levels though FQDNs could be grouped by most common root domains and their IP geolocation.

TOP 10 ROOT DOMAINS OF THE FQDNs



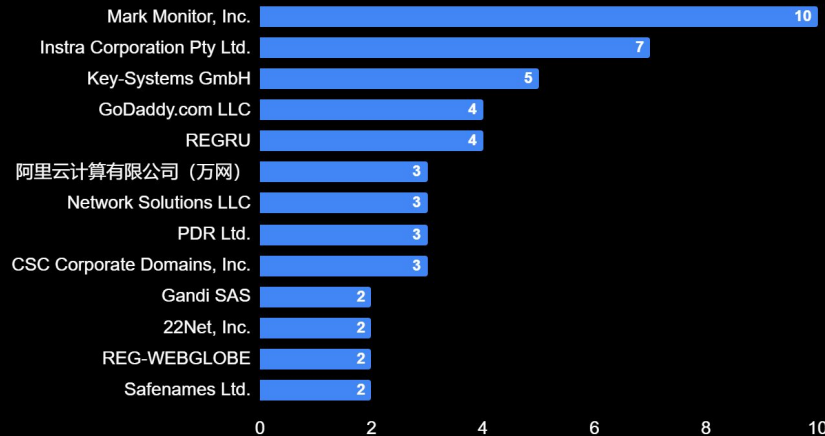
TOP GEOLOCATION COUNTRIES



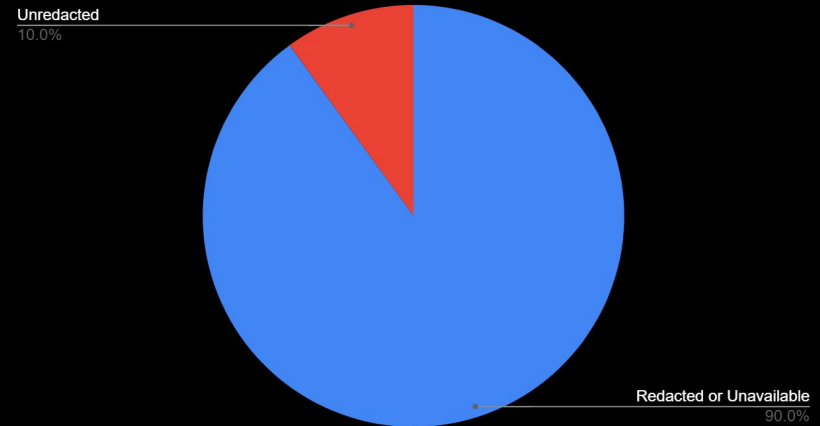
Widespread Registrar Administration

International and local registrars were found for the top 100 root domains. Most WHOIS records did not provide public domain ownership data.

TOP REGISTRARS OF THE TOP 100 MOST USED ROOT DOMAINS

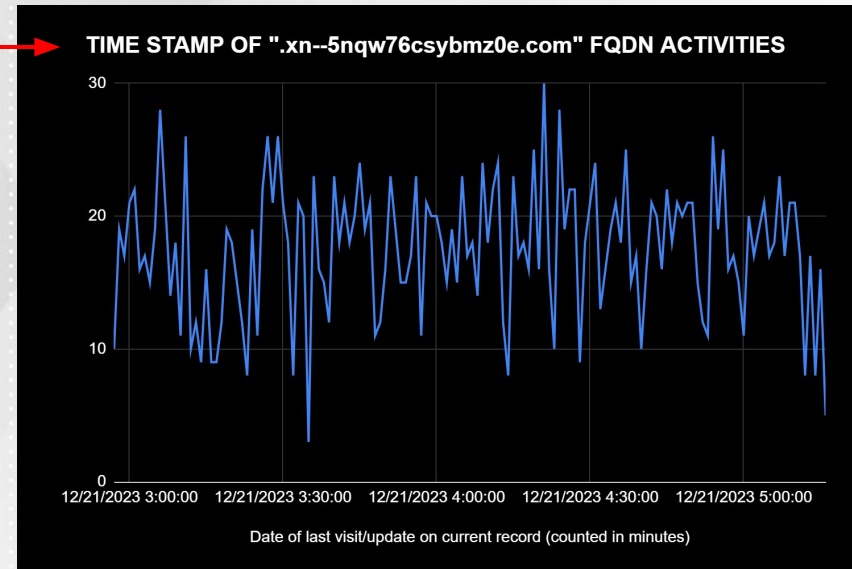
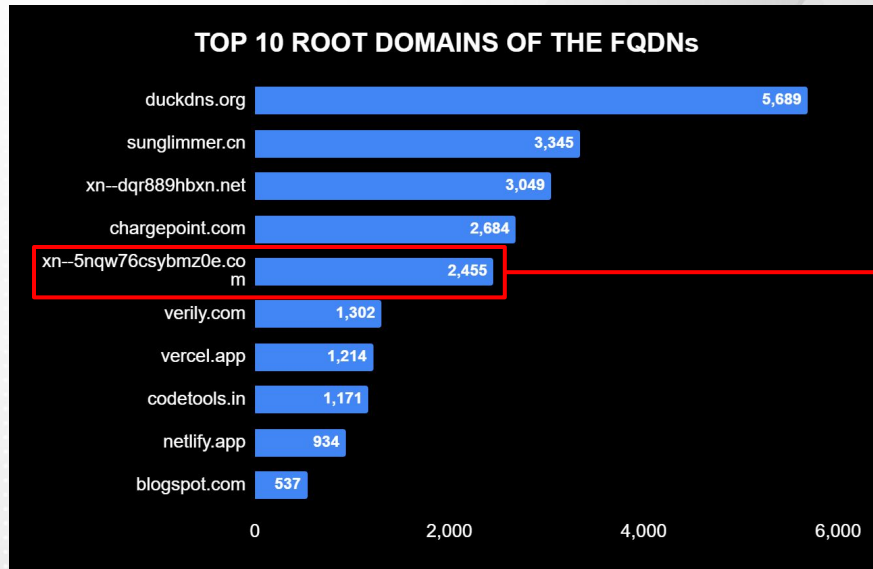


REDACTED OR UNAVAILABLE WHOIS RECORDS OF THE TOP 100 MOST USED ROOT DOMAINS



pDNS Activity Can Be Very Dynamic

The root domain xn--5nqw76csybmz0e.com (核新软件[.]com) has 2,455 FQDNs and logged several record visits and updates over only a few hours.



A woman with long dark hair, wearing a dark vest over a light-colored shirt and light-colored trousers, stands in a server room aisle. She is looking up and reaching out towards a server rack on the right. The room is filled with rows of server racks, with many cables visible. The lighting is dim, and the overall color scheme is dark blue. In the background, the numbers 4, 5, and 6 are visible on the wall above the server racks.

Part 2 - Technical Means to Study Suspicious FQDNs and IDN IoCs

Suspicious FQDNs and IDN IoCs

Technical means #1: Pay attention to clusters

A suspicious cluster may have the same TLD and resolve to the same IP address, but has different IDN variations of a word as their second-level domains (SLDs).


cluster	top_domain	timestamp	ip
56	a1financialservicēs.ph	1708737660	45.79.222.138
56	a1financialservicēs.ph	1708737660	45.79.222.138
56	a1financialsērvicēs.ph	1708772100	45.79.222.138
56	a1financiālservices.ph	1708737600	45.79.222.138
56	a1financiālsērvicēs.ph	1708737660	45.79.222.138
56	a1financialservices.ph	1708737660	45.79.222.138
56	a1fjncialservices.ph	1708737660	45.79.222.138
57	a1finānçiālsērvicēs.ph	1708737600	45.79.222.138

cluster	top_domain	timestamp	ip
4	1stcalgary.xn--fiqz9s	1715460420	218.241.105.10
4	1stcalgary.xn--fiqs8s	1715492340	218.241.105.10
4	1stcalgary.xn--fiqz9s	1715460420	218.241.105.10
4	1stcalgary.xn--fiqs8s	1715500800	218.241.105.10

cluster	top_domain	timestamp	ip
278	同花順.net	1705815960	100.127.132.229
278	同花順.net	1705819560	86.35.3.192 86.35.3.193
278	同花順.net	1705818600	36.86.63.182
278	同花順.net	1705820760	100.127.132.229
278	同花順.net	1705818120	86.35.3.192 86.35.3.193
278	同花順.net	1705823820	36.86.63.182

Suspicious FQDNs and IDN IoCs

Technical means #2: Look for listed domain IoCs



Search by Domain, URL, IP, CIDR, Hash Wildcard (*) is supported.

0: Object

firstSeen: "2024-04-03T00:00:00Z",
 lastSeen: "2024-09-05T00:00:00Z",
 threatType: "attack",
 iocType: "domain",
 value: "xn--myetherwallet-4j5f.com"

1: Object

firstSeen: "2024-04-03T00:00:00Z",
 lastSeen: "2024-09-05T00:00:00Z",
 threatType: "attack",
 iocType: "domain",
 value: "xn--rtblocks-7ya.net"

2: Object

Total records: 4,342

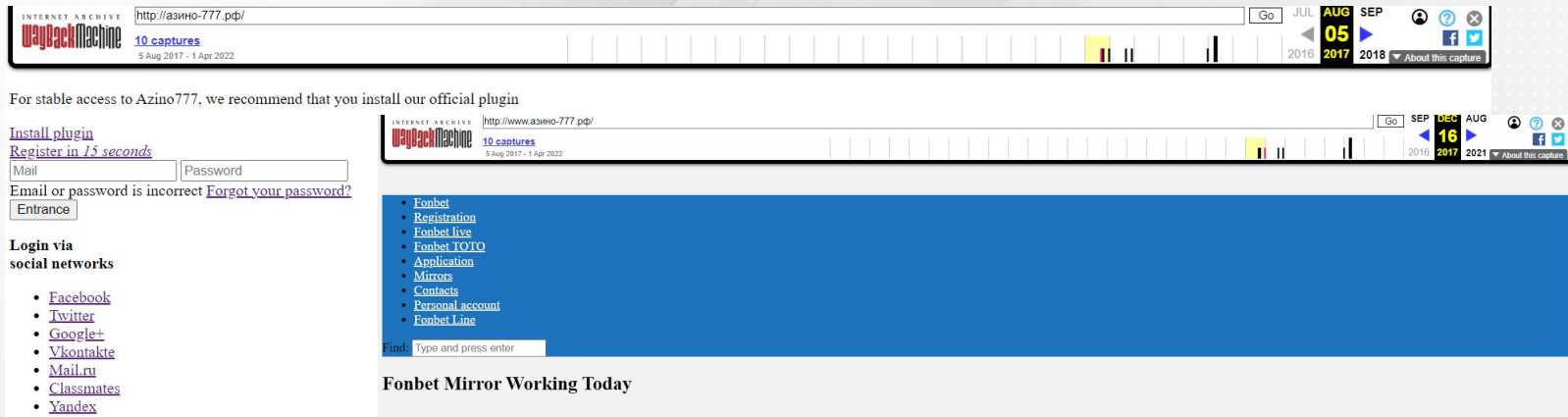
Decoded format

IDN IoCs	Punycode Version	Associated Threat Type
xn--myetherwallet-4j5f.com	myetherwallet.com	Attack
xn--onetgwat-dpb.pl	onetgwat.pl	Phishing
xn--h32b21ccvorra.xn--oi2b61z32a.xn--3e0b707e	메일정보.온라인.한국	Malware
xn--rtblocks-7ya.net	artblocks.net	Attack
xn--panakswap-s3a0c.finance	pancakswap.finance	Attack

Suspicious FQDNs and IDN IoCs

Technical means #3: Check hosted content history

The IoC xn---777-43d6bh4bj.xn--p1ai (азино-777.рф) historically hosted different content and promoted different services in a span of a few months only.



For stable access to Azino777, we recommend that you install our official plugin

[Install plugin](#)
[Register in 15 seconds](#)

Mail Password

Email or password is incorrect [Forgot your password?](#)

Entrance

Login via social networks

- [Facebook](#)
- [Twitter](#)
- [Google+](#)
- [Vkontakte](#)
- [Mail.ru](#)
- [Classmates](#)
- [Yandex](#)

[Fonbet](#)
[Registration](#)
[Fonbet live](#)
[Fonbet TOTD](#)
[Application](#)
[Mirrors](#)
[Contacts](#)
[Personal account](#)
[Fonbet Line](#)

Find: Type and press enter

Fonbet Mirror Working Today

Fonbet mirror!

Fonbet Mirror Site Working Today - will help you to the site of the bookmaker Fonbet and place a bet on sports whenever you want. The history of the Fonbet office dates back to 1994 in Moscow, when it was founded. The successful start of the company made it possible to quickly develop to a level when the limits of the capital were no longer enough to restrain the potential of the organization and like-minded people working in it. Thus, the structure of the bookmaker Fonbet has spread far beyond the Moscow Ring Road. Today, the company is very popular, many young bettors without hesitation choose the Fonbet office as their first and only platform for earning money on sporting events. So the popularity of the organization is growing and even negative reviews from competing offices do not spoil the reputation of the largest player in the sports betting market.

The owner of the bookmaker Fonbet is listed as OOO "FON". Sports bets are accepted here, and casinos and poker rooms disappeared without a trace after a series of blockages. The organizers even launched their own radio and video broadcast service called Fonbet TV. The service is available to citizens of Ukraine, Kazakhstan and Russia. The successful start and confident rise of the Fonbet company helped to decisively capture the top positions and the business grew far beyond the Moscow Ring Road. Of course, there is a lot of negativity towards the bookmaker, which does not affect the overall popularity of the office, since it is mainly written by people who, playing inadequately, lost money, and did not gain it.

Suspicious FQDNs and IDN IoCs

Technical means #4: Compare WHOIS records (even if redacted)

Historical NS and WHOIS data of
opensea.io (official domain) as of May
2023.

Name Servers

arch.ns.cloudflare.com >
nicole.ns.cloudflare.com >

Registrant Contact

Registrant Name: REDACTED FOR PRIVACY >
Registrant Organization: Opensea >
Registrant Street: REDACTED FOR PRIVACY >
Registrant City: REDACTED FOR PRIVACY >
Registrant State/Province: NY >
Registrant Postal Code: REDACTED FOR PRIVACY >
Registrant Country: UNITED STATES >
Registrant Email: ---
Registrant Phone: ---
Registrant Phone Extension: REDACTED FOR PRIVACY >
Registrant Fax: ---
Registrant Fax Extension: REDACTED FOR PRIVACY >

Historical NS and WHOIS data of
opensea.xn--q9jyb4c (opensea.みんな)
as of May 2023.

Name Servers

ns1.quickswap.us.com >
ns2.quickswap.us.com >

Registrant Contact

Registrant Name: REDACTED FOR PRIVACY >
Registrant Organization: ---
Registrant Street: REDACTED FOR PRIVACY >
Registrant City: REDACTED FOR PRIVACY >
Registrant State/Province: Madrid >
Registrant Postal Code: REDACTED FOR PRIVACY >
Registrant Country: SPAIN >
Registrant Email: ---
Registrant Phone: ---
Registrant Phone Extension: ---
Registrant Fax: ---
Registrant Fax Extension: ---



Thank you.

Any questions?

Email: ching.chiao@whoisxmlapi.com

Free WhoisXML API trial available on www.whoisxmlapi.com