Analysis of Internationalized Domain Names in Reputation Block List Data (Q4 2023 - Q3 2025)

1. Executive Summary 2
3. Comparison of Reported ASCII Domain Names vs. IDNs 3
4. Types of Security Threats Analysis 5
5. IDNs by Script Analysis 7
6. Conclusion 8

Global Domains and Strategy

February 2026

1. Executive Summary

This report analyses the relationship between Internationalized Domain Names (IDNs) under generic top-level domains (gTLDs) and security threats as defined in ICANN's DNS Abuse Mitigation Program. It examines IDN-related data drawn from third-party Reputation Block Lists (RBLs) of domain names associated with three kinds of DNS Abuse: botnets, malware and phishing, aligning with types of DNS Abuse tracked by the ICANN's Domain Metrica project. Data related to Country Code Top-Level Domains (ccTLDs), including IDN ccTLDs, is outside the scope of this report.

Based on the RBLs data analyzed from Q4 2023 to Q3 2025 (October 2023 - September 2025) under the gTLDs:

- 1,031,421 ASCII domain names were reported per quarter, or 0.47 percent of total ASCII domain names under gTLDs.
- 1,257 IDNs were reported per quarter, or 0.09 percent of total IDNs under gTLDs.

This represents a ratio of 5.3 to 1 for ASCII domain names and IDNs reported percentages under gTLDs. Both ASCII and IDN domain names have a similar distribution of the security threats across different threat types. Phishing is the most reported security threat type for both ASCII domain names (96.99 percent of reported ASCII domain names) and IDNs (98.98 percent of reported IDNs).

The majority of the reported IDNs consist of Latin script (0.26 percent of total Latin IDNs) followed by Chinese (Han) script (0.04 percent of total Chinese (Han) IDNs).

2. Introduction

\Reputation Block Lists (RBLs) reflect reports of malicious domain usage data from third party reputation providers.[1] Because RBL data concerns are reported, rather than verified or proven

[1] The RBLs analyzed in this report are as follows: **APWG** (https://apwg.org/) contains blocklisted phishing URLs that are submitted by accredited users through the eCrime Exchange (eCX) platform.
OpenPhish (https://openphish.com/) receives unfiltered URLs from multiple sources which it then uses to detect live phishing URLs.
PhishStats (https://phishstats.info/) gathers phishing feeds from a number of sources.
PhishTank (https://phishtank.org/) is a community driven source of phishing URLs.
Spamhaus (https://www.spamhaus.org/) provides data on domains with low reputation that are collected from spam payload URLs, spam senders and sources, known spammers, phishing, virus, and malware-related websites.
SURBL (https://www.surbl.org/) provides different blacklists containing malicious domain names. The data in these lists comes from various sources such as MailSecurity, PhishTank, and participating mail servers.
URLHaus (https://urlhaus.abuse.ch/) is a project operated by abuse.ch. It collects, tracks and shares malware URLs.

abuse, this analysis is based on the domain names being reported as abusive and NOT whether they are actually being used for abuse.

This analysis was conducted to gain a better understanding of security threats using IDNs registered under gTLDs. It uses the reported domain names in RBLs, which are analyzed and stored in a database managed by ICANN's Office of the Chief Technology Officer (OCTO) team. The following questions were analyzed:

- How do the reported IDNs with security threats compare with the reported American Standard Code for Information Interchange (ASCII) domain names?
- How are the reported IDNs distributed over the different types of security threats?
- How are the reported IDNs distributed over different scripts?

3. Comparison of Reported ASCII Domain Names vs. IDNs

The median daily number of domain names under gTLDs for each period, divided into ASCII domain names and IDNs, are shown in Table 1. Unless otherwise stated, all averages reported in this study are mean values.

Table 1: Median Daily Number of Domain Names Under gTLDs[2]

Reporting Period[3]	All	ASCII	IDN
Q4 2023	218,676,265	217,188,541	1,487,724
Q1 2024	219,896,116	218,423,926	1,472,190
Q2 2024	220,085,247	218,639,009	1,446,238
Q3 2024	219,689,236	218,266,520	1,422,716
Q4 2024	219,900,337	218,489,578	1,410,759
Q1 2025	221,561,850	220,164,907	1,396,943
Q2 2025	223,610,785	222,223,998	1,386,787
Q3 2025	227,916,464	226,546,776	1,369,688
Average	***221,417,038***	***219,992,907***	***1,424,131***

Table 2 presents the number of unique domain names reported in RBLs, broken down by ASCII domain names and IDNs. Each domain name is counted only once per reporting period, regardless of the number of times it appears across the RBLs.

WMC Global (https://www.wmcglobal.com/phishfeed/) provide data on phishing which has a focus on mobile phishing including phishing via SMS (smishing).

[2] Median of the daily values seen over the period in question.

[3] The periods refer to the calendar-year throughout the report.

Table 2: Number of Reported Domain Names Under gTLDs

Reporting Period	All	ASCII	IDN
Q4 2023	422,820	421,932	888
Q1 2024	787,443	786,388	1,055
Q2 2024	874,481	873,126	1,355
Q3 2024	851,614	850,443	1,171
Q4 2024	1,036,816	1,035,535	1,281
Q1 2025	1,302,367	1,300,824	1,543
Q2 2025	1,372,192	1,370,868	1,324
Q3 2025	1,603,636	1,602,201	1,435
Average	**1,031,421**	**1,030,165**	**1,257**

Based on Table 1 and Table 2, the percentage of reported domains to the total domains are shown in Table 3 and Figure1.

Table 3: Percentage of Reported Domain Names to Total Domain Names Under gTLDs

Reporting Period	% of Reported to Total for ASCII Domain	% of Reported to Total for IDN
Q4 2023	0.19%	0.06%
Q1 2024	0.36%	0.07%
Q2 2024	0.40%	0.09%
Q3 2024	0.39%	0.08%
Q4 2024	0.47%	0.09%
Q1 2025	0.59%	0.11%
Q2 2025	0.62%	0.10%
Q3 2025	0.71%	0.10%
Average	***0.47%***	***0.09%***

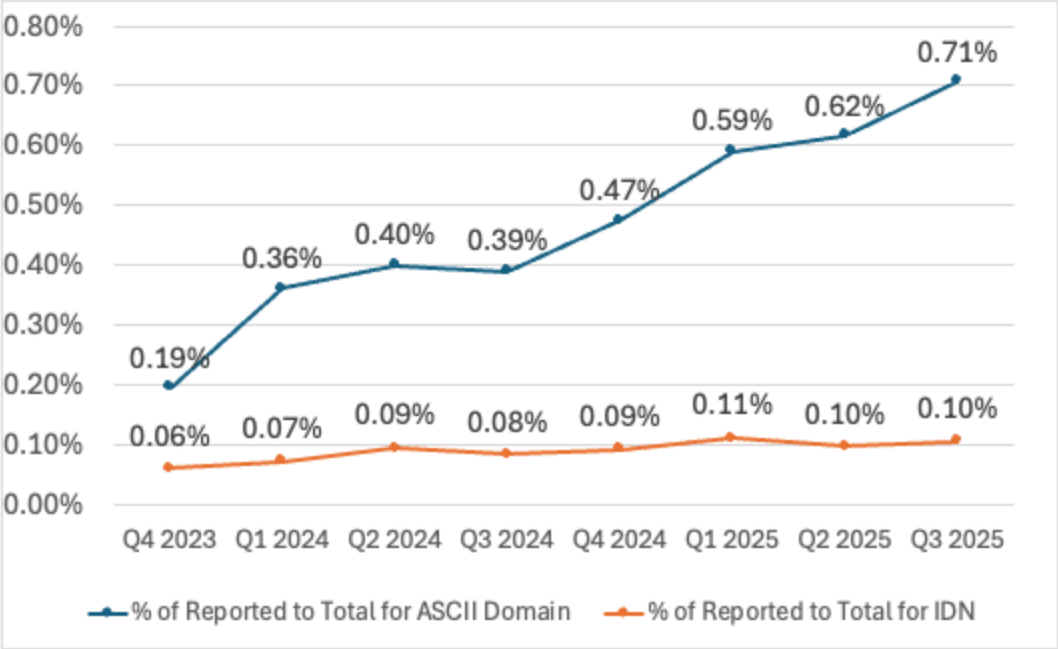

Figure 1: Trend of Percentage of Reported ASCII Domain Names and IDNs to Respective Total Domain Names under gTLDs

On average from Q4 2023 – Q3 2025:

- 1,031,421 ASCII domain names were reported per quarter, or 0.47 percent of total ASCII domain names under gTLDs.
- 1,257 IDNs were reported per quarter, or 0.09 percent of total IDNs under gTLDs.

Across the quarters in the reporting period, the ratio of percentage of ASCII domain names reported as security threats vs. percentage of IDNs reported as security threats was **5.3 to 1** (0.47 percent to 0.09 percent).

4. Types of Security Threats Analysis

Based on the data in RBLs, each reported domain name is associated with a security threat type as tracked by the ICANN's Domain Metrica project. The security threats are broken down into Botnet Command and Control (C&C), Malware, and Phishing as defined in DNS Abuse Mitigation Program.

In the following analysis, a domain name is counted once per security-threat type, regardless of how many times it is reported within the reporting period. If a domain name is associated with multiple security-threat types, it is counted once under each applicable type.

The reported ASCII domain names by security threat type are shown in Table 4 and the reported IDNs by security threat type are shown in Table 5.

Table 4: Number of Reported ASCII Domain Names by Security Threat Type

Reporting Period	Phishing	Malware	Botnet C&C
Q4 2023	398,136	26,508	3,138
Q1 2024	744,739	46,089	1,906
Q2 2024	848,207	29,612	1,813
Q3 2024	828,072	26,484	2,740
Q4 2024	1,011,751	26467	10,725
Q1 2025	1,283,278	18,078	10,313
Q2 2025	1,356,157	13,822	7,779
Q3 2025	1,586,055	13,472	10,907
Average	1,007,049	25,067	6,165
Percentage	***96.99%***	***2.41%***	***0.59%***

Table 5: Number of Reported IDNs by Security Threat Type

Reporting Period	Phishing	Malware	Botnet C&C
Q4 2023	877	12	0
Q1 2024	1,050	7	0
Q2 2024	1,351	6	0
Q3 2024	1,161	10	2
Q4 2024	1,265	18	5
Q1 2025	1,529	17	4
Q2 2025	1,318	10	2
Q3 2025	1,429	6	4
Average	1,248	11	2
Percentage	***98.98%***	***0.85%***	***0.17%***

Percentage values for the three security threat types in Table 4 and 5 were calculated using the average of each of the three security threats types over the quarters listed. For ASCII domains and IDNs, phishing was the most reported security threat. There is no significant difference in the distribution across the security threats types for ASCII domain names and IDNs.

5. IDNs by Script Analysis

The following analysis is based on the data of the latest reporting period, Q3 2025 which includes 1,435 reported IDNs (see Table 2). The script used in the labels for the second level domain name of the IDNs was analyzed. IDNs under gTLDs in the following two forms are included *IDN.ASCII* and *IDN.IDN*.

Table 6: Breakdown of Reported Second Level IDNs by Script for Q3 2025

Script	Number of Reported IDNs	Percentage
Latin	1,006	70.10%
Chinese (Han)	270	18.82%
Korean	72	5.02%
Thai	25	1.74%
Cyrillic	20	1.39%
Japanese	15	1.05%
Tamil	12	0.84%
Arabic	8	0.56%
Greek	5	0.35%
Hebrew	1	0.07%
Unified Canadian Aboriginal Syllabics	1	0.07%

Based on the data, the Latin script had the highest number of reported domain names at 1,006 (70.10 percent), followed by the Chinese (Han) script at 270 (18.82 percent).

For the Chinese (Han) and Latin scripts, the percentage of the reported IDNs to the total IDNs in the respective script is shown in Table 7. As a percentage of registered domains, Latin script IDNs are slightly higher than Chinese (Han) IDNs.

Table 7: Percentage of Reported IDNs to Total IDNs within the Script for Q3 2025

Script	Number of Reported IDNs	Number IDN Registrations of the Script[4]	Percentage
Latin	1,006	394,005	0.26%
Han	270	656,043	0.04%

6. Conclusion

Based on the data analyzed from Q4 2023 to Q3 2025, the percentage of ASCII domain names reported for security threats is 5.3 times higher than the percentage of IDNs. Both ASCII domain names and IDNs have similar distribution of the security threats across threat types, with phishing being the most reported security threat type. The majority of the reported IDNs are in Latin script (0.26 percent of total Latin IDNs) and Chinese (Han) script (with 0.04 percent of total Chinese (Han) IDNs).

[4] The number of registrations on 30 September 2025.