Interisle

26 June 2026

Tripti Sinha
Chair, Board of Trustees
Internet Corporation for Assigned Names and Numbers

Re: Submission of Interisle research report

Dear Tripti:

On behalf of Interisle Consulting Group, we are pleased to submit our report, *Malicious Registrations in the Domain Name Market: An Analysis of 2025 gTLD Registrations and Cybercriminal Demand*, for the information of the ICANN Board. A copy of the executive summary and full report are attached.

Among its principal findings, we found that 10% of all gTLD domains registered during 2025 have already been blocklisted for malicious activity by security providers. Applying conservative projections for additional future blocklistings and associated domains (based, in part, on work published by ICANN's OCTO research team), we found the actual number of gTLD domains registered by bad actors last year may be close to 16.8 million, or 20% of all domains created. The report also examines the concentration of malicious registrations among certain gTLDs and registrars, contains case studies on associated domain name checks, and discusses economic factors and market practices that may allow abusive registrations to persist.

We presented the report during ICANN86 in Seville and had constructive and useful discussions with a range of participants and stakeholder groups across the ICANN community. We appreciated the thoughtful engagement with the research and the interest expressed in its findings and implications.

We believe the report's findings are relevant to the Board's consideration of abuse issues, including the effectiveness of existing and future policy measures aimed at abuse prevention and mitigation, contractual compliance and enforcement, and the effect that abuse and the harms it facilitates have on the public interest. The report explains our data sources and methodology in detail and is offered as an evidence-based contribution to the ICANN community's ongoing work on these issues.

We respectfully request that this letter, the executive summary, and the full report be circulated in full to all members of the ICANN Board so that they have an opportunity to review the findings directly.

Interisle would welcome an opportunity to brief the Board and to answer questions regarding the report's data, methodology, findings, and policy implications.

Thank you for your consideration and for the Board's attention to these important issues.

Sincerely,

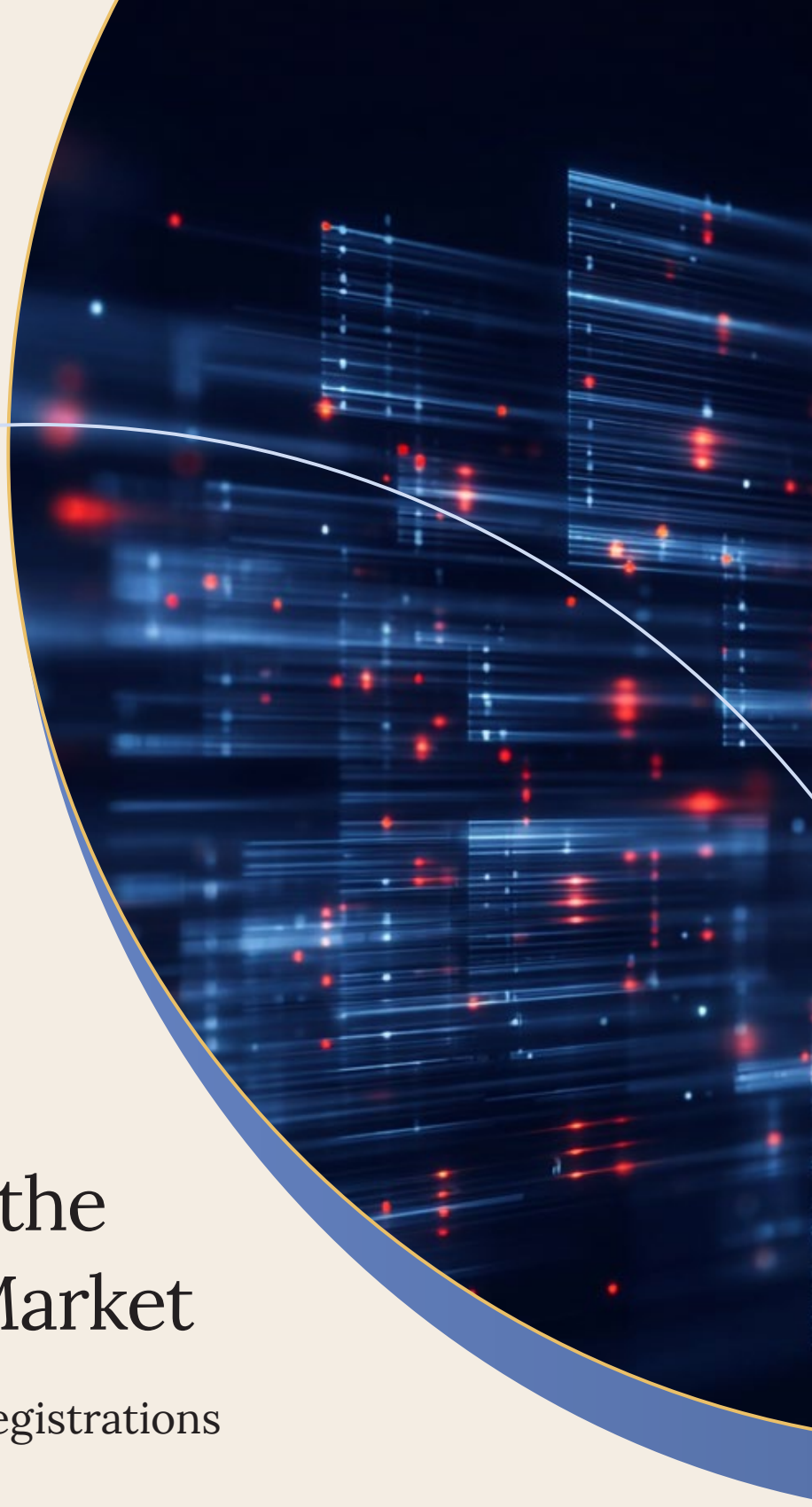
Karen Rose
Partner

Greg Aaron
Partner

Enc:
Executive Summary
Full Report

Interisle Consulting Group
https://interisle.net
info@interisle.net

Interisle



Malicious Registrations in the Domain Name Market

An Analysis of 2025 gTLD Registrations and Cybercriminal Demand

INTERISLE CONSULTING GROUP JUNE 2026

CONTENTS

Executive Summary

Cybercrime is a professionalized, multinational industry that relies on a steady supply of cheap, disposable domain names to perpetrate malicious attacks at scale. This study measures the extent to which malicious actors drove new registrations in the gTLD market in 2025.

Using publicly and commercially available data, it shows that cybercriminal demand constitutes a significant share of the domain name market.

KEY FINDINGS:

Malicious actors purchased between 10% and 20% of all gTLD domain names created in 2025. This report establishes that 10% is the floor, documenting that 8.5 million of the 85 million domains created in 2025 have already been blocklisted for malicious activity. However, blocklists miss many domains registered by bad actors. Applying conservative projections for additional future blocklistings and associated domains that were not identified by blocklists, the actual number of domains registered by malicious actors in 2025 may be closer to 16.8 million, or 20% of all domains created that year. **[see pages 6-8]**

Abuse is widespread across the market, but highly concentrated at specific gTLDs, registrars, and corporate families in the industry. Five registrars accounted for 50% of all blocklisted domains; at one registrar, 88% of new registrations were blocklisted. Multiple open gTLDs saw more than half of their new registrations used for malicious activity. Two gTLDs had nearly two million new registrations flagged for abuse. **[see pages 9–16]**

Criminal organizations purchased domains at scale. The detection, prevention, and mitigation of this activity was partial and far from effective. Case studies in this report detail how criminal gangs registered hundreds of thousands of domain names to conduct phishing, malware, and scam campaigns. Even after U.S. government sanctions were imposed on the criminal FUNNULL organization in May 2025, it continued to acquire domain names. Small percentages of blocklisted domains were suspended by registrars and registries. **[see pages 17–22]**

Low renewal rates are an indicator of abuse. gTLDs used by cybercriminals posted renewal rates as low as

0.5%, indicating that legitimate use was negligible.
[see pages 18–20 and 23–24]

The market provides incentives for registrars and registry operators to take or tolerate abusive registrations. Sales and incentive programs designed to drive growth and market share encourage sales to high-volume, repeat customers. Some registrars and registry operators appear to derive commercial benefits from selling large numbers of domains to bad actors. Even when abusive domains generate little revenue, there still may be an incentive to tolerate them when deterrence is more costly or risks losing higher-margin legitimate customers. The resulting social costs of cybercrime, however, including financial losses, business disruption, and eroded public trust, are borne by victims, businesses, and society at large. This is a classic negative externality that distorts the market and undermines the broader benefits of competition.
[See pages 25–27]

Abuse is not inevitable, however. Some registries and registrars grew without attracting outsized levels of abuse. Pricing strategies, provider practices, and abuse mitigation choices can materially affect whether growth is driven by legitimate demand or by cybercriminal registrations.

Improvements in domain name policies and practices are needed to reduce cybercriminals' access to domains while supporting legitimate market growth. Additional new, open gTLDs will be introduced in the coming year and beyond. Absent more effective controls, the increase in competition and domain name supply will likely exacerbate the current situation, shifting greater costs and harm to the public.

Introduction

Cybercrime is a pervasive, professionalized, and multinational industry that causes billions of dollars of losses and damage each year.[1] Almost anyone can become a victim at any time. Domain names are an essential resource for committing all types of cybercrime. They provide the locations for phishing, malware, scam and fraud sites, are used to control botnets, and to advertise abusive activities through email, on social media, and via text messages.

Understanding how many domain names are being used for abusive activities, and how bad actors acquire and use those domains, is essential. This study establishes how many gTLD domain names that were registered in 2025 have been blocklisted for malicious activity. It reveals how many domain names were sold to bad actors, and provides case studies revealing what they did with them. This report places the domain abuse problem into perspective, and provides reliable data so that participants in the broader Internet community, including policy-makers, can make informed decisions.

It is possible to study domain abuse in this way in the "generic Top Level Domains," or gTLDs, because rich data about domain registrations, transactions, and abuse are available. gTLD domains are 63% of the entire TLD space[2], and approximately 82% of all blocklisted domains have been in the gTLDs.[3] The gTLD space is overseen by ICANN, the Internet Corporation for Assigned Names and Numbers. ICANN determines what gTLDs exist, and awards the contractual right to operate each gTLD to a registry operator. ICANN also accredits the registrars who sell domains in the gTLDs. ICANN determines what policies govern the gTLD space, including under what circumstances registry operators and registrars must respond to abuse complaints. ICANN publishes the numbers of domain transactions made by each registrar in every gTLD[4] , and requires registrars and registry operators to make basic data about individual domain names available via the Registration Data Access Protocol (RDAP).

These kinds of transaction and registration data are only partially available (and often not available at all) for the country-code TLDs.

To understand what domains are being used for abusive activities, Interisle collects data from prominent Reputation Block Lists (RBLs). These blocklists contain domain names and/or the URLs of dangerous and unwanted content, including known phishing, malware, and scam and fraud sites. RBLs are widely used as a defensive measure. Internet service providers, email providers, web browser providers, Domain Name System (DNS) resolvers, and other organizations use these RBLs to block access to (and traffic and email from) these domains and URLs, protecting their users from online threats. The RBLs we use are provided by professional security threat-reporting sources, and are used to protect literally billions of users across the world.

Blocklist data therefore provides a practical measurement of what is happening in the "real world," the Internet ecosystem that uses the DNS. It shows what domain names that professional anti-abuse sources have identified as harmful, and what domains are being blocked by security administrators at private and public networks and services around the world. ICANN takes a similar approach with its Metrica abuse measurement system. ICANN's security and research team notes: "We believe that it is beneficial to collect the same DNS abuse data that is reported to industry and Internet users. Security systems such as anti-spam or anti-malware gateways or firewalls that protect billions of users incorporate these data into their DNS abuse mitigation measures."[5]

Interisle uses only publicly and commercially available data. Our findings and reporting can be independently validated by any party who collects the same data and applies the same general methods. For details about what data we collect, and our research methodologies, please see the Methodology section at the end of this report.

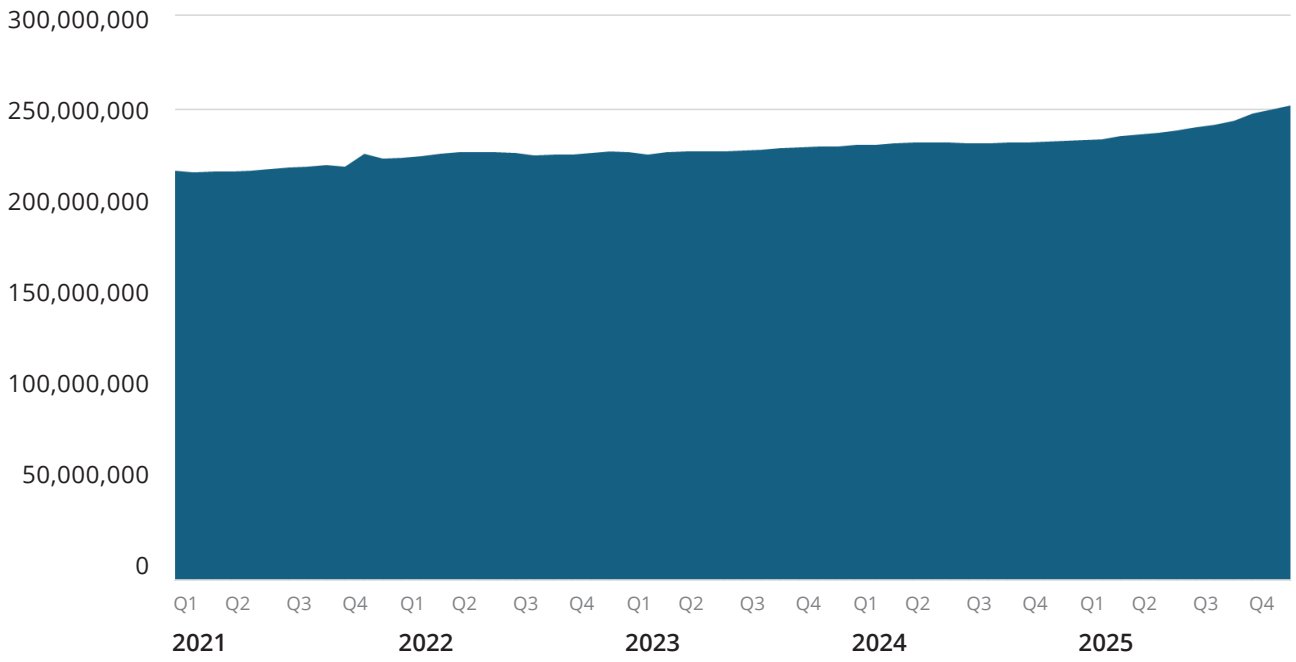
Malicious Registrations as a Share of the gTLD Market

Cybercriminals continually register new domain names to carry out their malicious activities. Various studies have analyzed the factors that drive domain abuse and malicious domain registrations. They have established that low prices tend to attract abuse, and this especially occurs in "open" gTLDs – those that are open to all registrants and have no registration limitations or requirements.[6, 7, 8, 9, 10, 11] One major study established that each dollar reduction in domain price corresponds to a 49% increase in malicious domain registrations, that free bundled services such as web hosting drive an 88% surge in phishing domains, and that API access provided by registrars for domain registration or account creation is associated with a "staggering" 401% rise in malicious domains.[12]

The registration of domains in batches is a well-known tactic among cybercriminals, who use them to perpetrate DNS abuse at scale. The ability to easily register domains in bulk enables attackers to quickly establish disposable infrastructure, evade detection, and scale their operations. From a security perspective, the identification and characterization of bulk domain registrations are of critical importance for abuse mitigation.[13]

What part does this malicious activity play in the domain name market? The overall gTLD market has been growing slowly, and most newly registered domains replace domains lost through non-renewal. From 2021 through 2024, the market grew by a total of 6.2%. In 2023 the entire TLD market only grew by 1%,[14] and the benchmark .COM TLD shrank every quarter in 2023 and 2024.[15] 2025 saw greater growth, as registry operators and registrars placed emphasis on gaining new registrations. During 2025 the gTLDs grew by 8.1%, increasing from 233 million to just under 252 million total domains.[16]

gTLD Domains Under Management
2021–2025

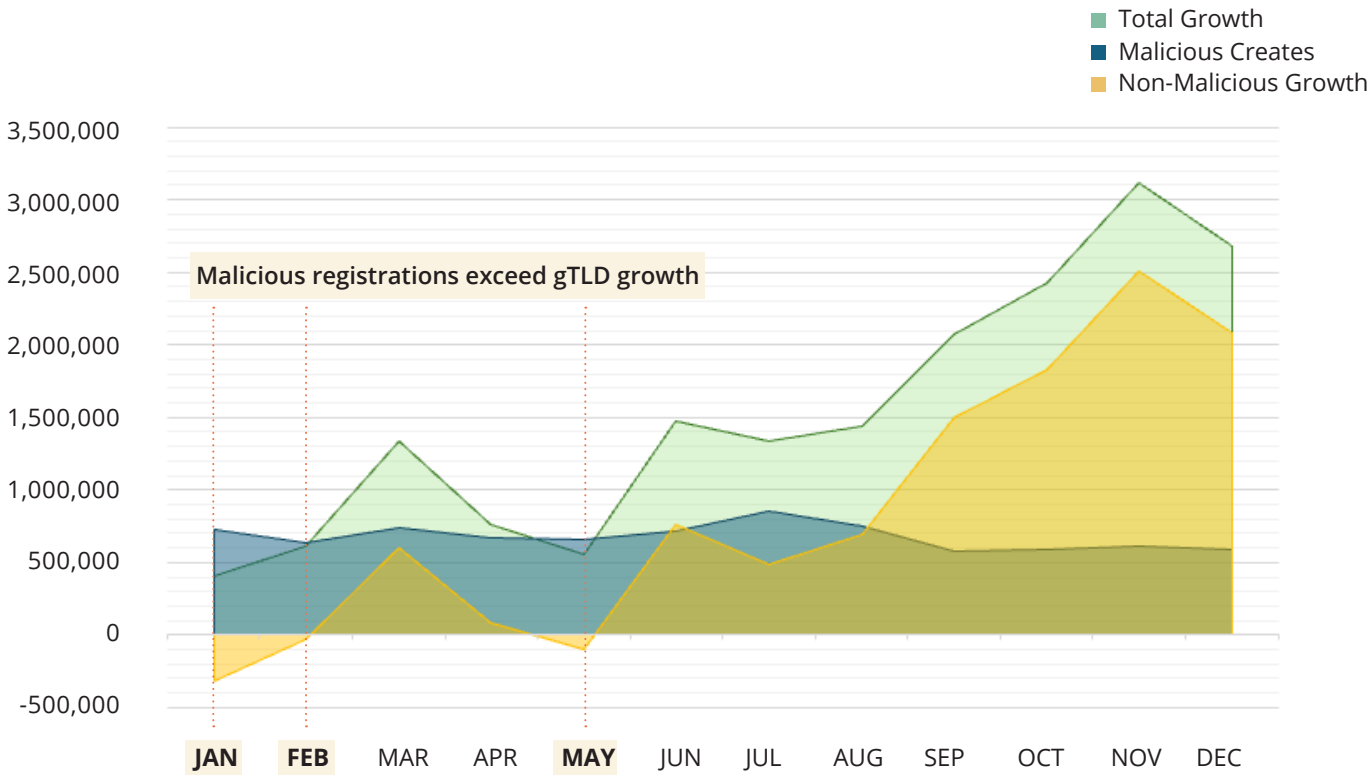


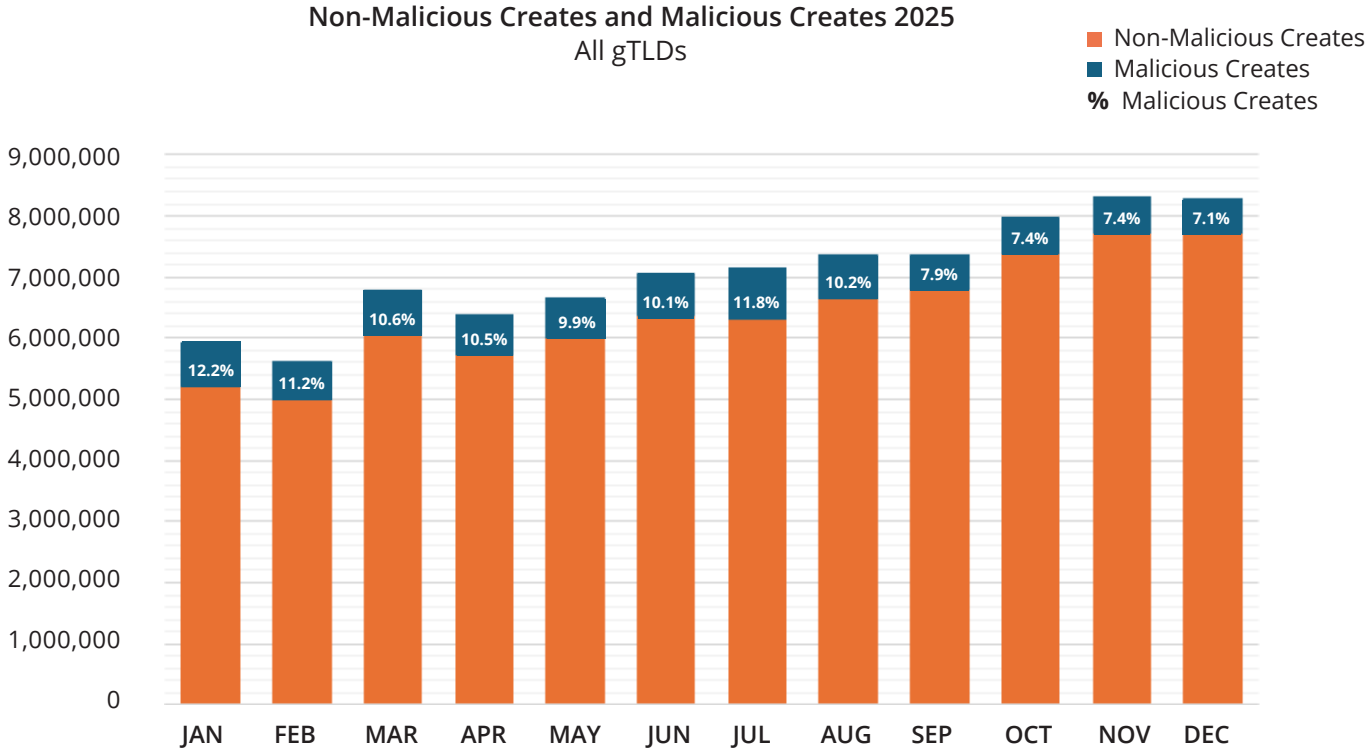
A total of 84,961,989 gTLD domains were created in 2025. These new registrations are the market activity most relevant to cybercrime. Cybercriminals register domains, use them, and then abandon them, registering more domains as they need. Cybercriminals very rarely renew their domain names when they reach their one-year anniversary. Renewals, and the total number of domains in any TLD or at any registrar, are not a measure of new sales or new demand in the market.

As of 18 May 2026, 8,496,811 of the domains created in 2025 had been added to blocklists — 10% of all gTLD domains sold during 2025. About 98% of these appear to have been maliciously registered, rather than compromised after creation. (For more about malicious versus compromised domains, see the Methodology section.)

Those malicious domain registrations were a significant contributor to the growth of the gTLDs in 2025. In January 2025, 5.9 million gTLD domains were created and 5.5 million domains were deleted, resulting in a net growth of 408,000 domains. But 723,000 domains created in January 2025 were subsequently blocklisted, eclipsing overall growth. The number of malicious domains registered in the gTLDs also exceeded overall gTLD growth in February and May 2025:

Total Growth, Malicious Creates, and Non-Malicious Growth 2025
All gTLDs





8.5 million is the number of blocklisted domains so far, establishing a conservative floor of how many domains were registered by bad actors in 2025. What might the actual numbers look like?

The number of new domain names being used for abusive purposes is significantly higher than 10%, for two reasons:

1. The blocklist providers do not detect or list all the abusive domain registrations. For more about this, see the "Case Studies" section below.
2. More domains that were created in 2025 will be added to the blocklists through the rest of 2026. Additional domains registered in late May 2025 through December 2025 will be blocklisted; the total will rise through December 2026.

We project that an additional 2% of 2025's registrations may get blocklisted by the end of December 2026, raising the total to around 12% of all new registrations, or 10.1 million domains. This is because some criminals strategically "age" their domains, not using them for months in order to evade blocklist scoring systems that place less trust in recently registered young domains.[17,18] We base our projection on what happened the year before: 2.32 million domains created in 2024 were added to blocklists between June and December 2025.

What about maliciously registered domains that were missed by the blocklist providers? A recent study of batch registrations made by ICANN's Office of the CTO provides a clue. It found that **for every three domains appearing on blocklists, two additional domains appear to have been registered within the same registration batches–** or an "80% increase in the volume of newly registered RBL domains." In other words, bad actors may register 66% more domains than the blocklists indicate.[19] The blocklist providers simply miss some domains purchased by bad actors. For more about this, see the "Case Studies" section later in this report.

We predict that approximately 10.1 million domains registered in 2025 will be blocklisted by the end of 2026. **When we apply the associated domains projection (an additional two-thirds of blocklisted domains), this suggests that 16.8 million domains were potentially purchased by bad actors in 2025, or 20% of the total gTLD new registration market in 2025.**

The 20% figure is a projection only, but it is notable that the ICANN analysis was conservative in some ways. Those researchers stated that "the true rate is likely to be higher"

since they excluded "many valid batches" such as those containing more than 1,000 domains. (In later sections of this report we document that large batches far in excess of 1,000 are regular occurrences.) The ICANN researchers stated that their results "indicate that batch registrations are prevalent, significantly predict overall abuse rates, and are useful for pivoting and expanding from known malicious 'seed' domain sets, particularly in certain TLDs and registrar environments."

These numbers are not out of line with what other sources observe. Threat intelligence company Infoblox provides a widely used protective DNS solution. In 2025 Infoblox identified 100.8 million newly observed second-level domains (in both gTLDs and ccTLDs), and classified 25.1% (25 million) of them as malicious or suspicious.[20]

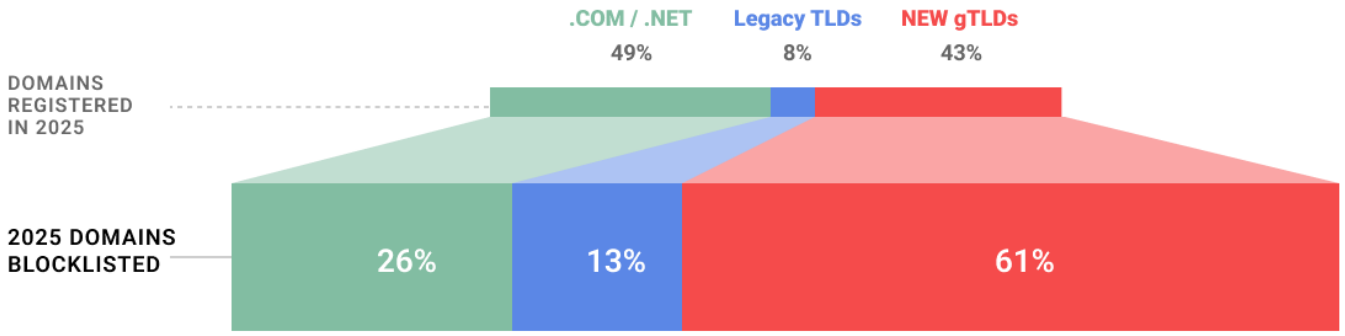
In the case studies later in this report, we performed similar "expansion analyses" of several gTLDs. We found that cybercriminals registered far more domains than the blocklists indicated.

Malicious registrations were pervasive across the gTLD space. In 2025, domains were blocklisted in 566 gTLDs–in almost all of the non-brand gTLDs. Malicious registrations were created at 2,684 registrars – 88% of the 3,022 currently accredited registrars.[21] But as detailed below, abuse was concentrated disproportionately in certain TLDs and at certain registrars.

Unless otherwise noted, blocklisting figures below for domains registered in 2025 were as of 30 April 2026.

Malicious Registrations by TLD

Malicious registrations were made disproportionately in the new, open gTLDs:



Which gTLDs and registrars had the largest numbers of maliciously registered domains, and significant percentages of malicious registrations, in 2025? Below, "malicious registrations" is the number of domains created in a TLD (or by a registrar) in 2025 that were blocklisted some time after creation and by 30 April 2026, and the domains met our "malicious registration" criteria (see the Methodology section for details). The data indicates that certain TLDs and registrars are disproportionately associated with malicious registrations.

The gTLDs with the most blocklisted domains were:

gTLDS WITH HIGHEST NUMBER OF NEW BLOCKLISTED (MALICIOUS) DOMAINS, 2025

2025 RANK	gTLD	OPERATOR	NEW DOMAINS CREATED (NET ADDS) IN 2025	NEW DOMAINS CREATED IN 2025, BLOCKLISTED, AND MALICIOUS (MINIMUM 100,000)	% OF NEW DOMAINS BLOCKLISTED, AND MALICIOUS
1	.COM	Verisign	39,469,949	**1,927,917**	4.9%
2	.TOP	Jiangsu Bangning Science & Technology*	5,193,483	**1,793,822**	34.6%
3	.INFO	Identity Digital	2,615,401	**561,614**	21.5%
4	.BOND	ShortDot SA	1,701,566	**514,197**	30.2%
5	.VIP	Registry Services LLC *(GoDaddy Registry)*	1,064,741	**354,690**	33.3%
6	.XYZ	XYZ.COM LLC	7,236,034	**275,896**	3.8%
7	.SHOP	GMO Registry, Inc.	3,308,236	**243,660**	7.4%
8	.PRO	Identity Digital	714,875	**174,184**	24.4%
9	.ICU	ShortDot SA	526,433	**149,861**	28.5%
10	.SBS	ShortDot SA	1,280,067	**144,403**	11.3%
11	.MOBI	Identity Digital	225,180	**141,483**	62.8%
12	.NET	Verisign	2,226,300	**129,357**	5.8%
13	.CFD	Identity Digital	490,977	**124,386**	25.3%
14	.CYOU	ShortDot SA	388,161	**116,812**	30.1%
15	.ORG	PIR	2,529,826	**100,110**	4.0%

***Sponsorship transferred to Hong Kong Zhongze International Limited in January 2026.**
https://www.iana.org/domains/root/db/top.html

Thirteen gTLDs had the majority of their new domains blocklisted, indicating significant purchases by bad actors. Twelve of the 20 gTLDs with the highest blocklisting rates were operated by Identity Digital. **The gTLDs that were most highly blocklisted were:**

gTLDS WITH HIGHEST PERCENTAGE OF NEW DOMAINS BLOCKLISTED, 2025

2025 RANK	gTLD	OPERATOR	DUM DEC 2025	NEW DOMAINS CREATED (NET ADDS) IN 2025	NEW DOMAINS CREATED IN 2025, BLOCKLISTED, AND MALICIOUS (MINIMUM 100,000)	% OF NEW DOMAINS BLOCKLISTED, AND MALICIOUS
1	.LOCKER	Orange Domains LLC	23,612	22,201	16,192	72.9%
2	.LGBT	Identity Digital	18,102	9,859	7,116	72.2%
3	.TOWN	Identity Digital	35,872	31,018	21,760	70.2%
4	.GDN	Joint Stock Co "Navigation-information systems"	49,747	45,395	30,545	67.3%
5	.MOBI	Identity Digital	429,361	225,180	141,483	62.8%
6	.XIN	Elegant Leader Limited	127,902	111,875	65,834	58.8%
7	.LOAN	dot Loan Limited *(PwC, Gibraltar)*	118,486	79,653	45,786	57.5%
8	.PICTURES	Identity Digital	32,051	6,122	3,437	56.1%
9	.QPON	DOTQPON LLC	55,749	58,704	32,317	55.1%
10	.MOV	Charleston Road Registry *(Google)*	6,357	2,570	1,371	53.3%
11	.BID	dot Bid Limited *(PwC, Gibraltar)*	69,578	32,082	16,858	52.5%
12	.PIZZA	Identity Digital	35,877	9,258	4,794	51.8%
13	.AUCTION	Identity Digital	12,419	6,742	3,457	51.3%
14	.PINK	Identity Digital	26,690	8,810	4,239	48.1%
15	.REVIEWS	Identity Digital	13,256	3,744	1,780	47.5%
16	.CLAIMS	Identity Digital	6,072	2,760	1,310	47.5%
17	.PET	Identity Digital	26,618	12,889	6,000	46.6%
18	.FORSALE	Identity Digital	5,472	2,292	1,051	45.9%
19	.DATE	dot Date Limited *(PwC, Gibraltar)*	11,107	5,198	2,190	42.1%
20	.LOANS	Identity Digital	11,376	4,061	1,705	42.0%

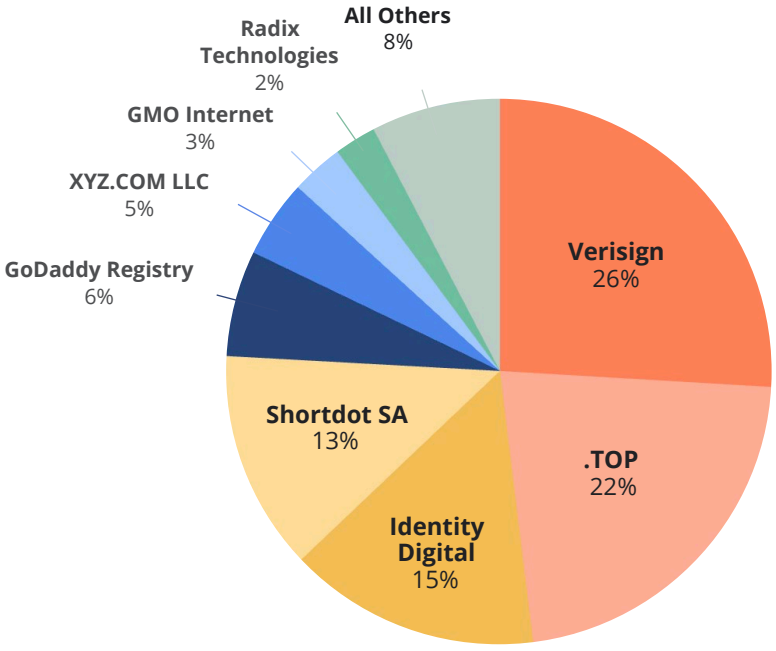
There is great variability in the percentages of malicious registrations in various TLDs. The absolute numbers are important, though–each blocklisted domain represents some amount of risk and potential damage.

An interesting case is .XYZ, which grew significantly in 2025, from 4.4 million to 8.7 million domains. Its 2025 renewal rate was only 18.7%, so it had to add a large number of new domains to make up for its losses due to non-renewal. .XYZ had 7.2 million net-adds during the year, of which 275,896 of its 2025 registrations blocklisted. That is a significant number for any TLD, but a relatively low percentage of its overall new registrations. It appears that XYZ.COM was somehow able to replace its losses and grow the TLD without attracting outsized abuse. We are not able to analyze the contributing factors in this case, but it suggests that it is possible to craft incentives, marketing programs, and/or deterrents that manage abuse levels.

Another way of examining registrations is by "registry family." Some companies operate multiple gTLDs, delegated to them by contract with ICANN. TLDs in a "family" are under the common legal, operational, and marketing control of one entity. We do not consolidate TLDs by back-end operator, only by sponsorship control as listed in the IANA root zone record.[22] For example, Identity Digital is the "TLD manager" of hundreds of gTLDs. It holds the ICANN contracts for them under subsidiaries such as Binky Moon LLC, Dog Beach LLC, and Identity Digital Limited.

We researched the ownership of the gTLDs and consolidated their numbers below. **About 92% of the domains that were created in 2025 and then blocklisted were in gTLDs operated by just eight companies:**

REGISTRY FAMILIES WITH MOST BLOCKLISTED (MALICIOUS) DOMAINS, 2025



Verisign	**26%**	2,103,454
.TOP (Jiangsu Bangning / Hong Kong Zhongze)	**22%**	1,793,822
Identity Digital	**15%**	1,206,412
Shortdot SA	**13%**	1,049,659
GoDaddy Registry	**6%**	507,048
XYZ.COM LLC	**5%**	374,047
GMO Internet	**3%**	251,824
Radix Technologies	**2%**	201,493
All Others	**8%**	622,815

Malicious Registrations by Registrar

The registrars with the most blocklisted domains created in 2025 are below. Dynadot registered 12.7% of all blocklisted gTLD domains created in 2025. **The top five registrars below registered 50% of all the blocklisted gTLD domains created in 2025.**

REGISTRARS WITH HIGHEST NUMBER OF NEW DOMAINS BLOCKLISTED, 2025

RANK	REGISTRAR	IANA ID	NEW DOMAINS CREATED (NET ADDS) 2025	NEW DOMAINS CREATED IN 2025 BLOCKLISTED, AND MALICIOUS	% OF NEW DOMAINS BLOCKLISTED, AND MALICIOUS
1	Dynadot	472	4,900,809	**1,029,018**	21.0%
2	Gname	1923	2,481,620	**997,771**	40.2%
3	NameCheap	1068	10,204,514	**816,805**	8.0%
4	NameSilo	1479	3,028,042	**621,268**	20.5%
5	GoDaddy	146	12,369,981	**586,799**	4.7%
6	Key-Systems, LLC	1345	745,084	**435,136**	58.4%
7	Dominet (HK)	3775	1,060,169	**357,398**	33.7%
8	Spaceship, Inc.	3862	3,882,989	**344,306**	8.9%
9	GMO	49	7,291,336	**244,060**	3.3%
10	Namemart Limited	3863	420,326	**215,100**	51.2%
11	Hosting Concepts B.V. dba Registrar.eu	1647	730,938	**213,225**	29.2%
12	NICENIC	3765	180,404	**157,970**	87.6%
13	Eranet	1868	815,751	**145,455**	17.8%
14	Web Commerce dba WebNic.cc	460	485,159	**127,567**	26.3%
15	West263 International	1915	1,333,091	**118,932**	8.9%
16	Alibaba Cloud dba HiChina	1599	1,723,281	**117,981**	6.8%
17	Aceville Pte. Ltd.	3858	119,896	**99,072**	82.6%
18	URL Solutions, Inc.	1449	139,882	**93,693**	67.0%
19	eName Technology Co., Ltd.	1331	361,526	**93,613**	25.9%
20	PDR Ltd. dba PublicDomainRegistry.com	303	1,067,281	**82,672**	7.7%

There is great variability in the percentages of malicious registrations in registrar portfolios. The absolute numbers are important, however – each blocklisted domain represents some amount of risk and potential damage.

The largest registrar, GoDaddy, created 12.3 million domains in 2025, but only 4.3% of them were blocklisted and malicious.

Eight individual registrars had more than half of their new registrations blocklisted:

REGISTRARS WITH HIGHEST PERCENTAGE OF NEW DOMAINS BLOCKLISTED, 2025

RANK	REGISTRAR	IANA ID	NEW DOMAINS CREATED (NET ADDS) 2025	NEW DOMAINS CREATED IN 2025 BLOCKLISTED, AND MALICIOUS (MINIMUM 10,000)	% OF NEW DOMAINS BLOCKLISTED, AND MALICIOUS
1	NICENIC INTERNATIONAL	3765	180,404	157,970	**87.6%**
2	MainReg Inc.	1917	29,666	25,435	**85.7%**
3	Aceville Pte. Ltd.	3858	119,896	99,072	**82.6%**
4	URL Solutions, Inc.	1449	139,882	93,693	**67.0%**
5	Key-Systems, LLC	1345	745,084	435,136	**58.4%**
6	Ultahost, Inc.	4331	31,034	17,759	**57.2%**
7	Hefei Juming Network Tech Co.	3758	148,439	79,018	**53.2%**
8	Namemart Limited	3863	420,326	215,100	**51.2%**
9	Devexpanse Ltd	4342	27,859	11,317	**40.6%**
10	Gname	1923	2,481,620	997,771	**40.2%**
11	Dominet (HK) Limited	3775	1,060,169	357,398	**33.7%**
12	Hosting Concepts B.V. dba Registrar.eu	1647	730,938	213,225	**29.2%**
13	Web Commerce dba WebNic.cc	460	485,159	127,567	**26.3%**
14	eName Technology Co., Ltd.	1331	361,526	93,613	**25.9%**
15	Nicnames, Inc.	4156	49,985	10,860	**21.7%**
16	Dynadot Inc	472	4,900,809	1,029,018	**21.0%**
17	NameSilo, LLC	1479	3,028,042	621,268	**20.5%**
18	Zhengzhou Century Connect	2805	81,366	16,065	**19.7%**
19	July Name Limited	3855	138,406	25,696	**18.6%**
20	Eranet International Limited	1868	815,751	145,455	**17.8%**

Another way of examining registrations is by "registrar family." Some registrars own multiple registrar companies or brands, each of which has its own ICANN accreditation. ICANN legally considers each a "Registrar Family" and the individual companies "Affiliates" of each other when they are under the common control of one entity.[23] The registrars in a family often have their legal, sales and marketing, and anti-abuse operations handled in common by the same parent company and personnel. For example, NameCheap (IANA ID 1068) started a separate registrar brand called Spaceship Inc. (IANA ID 3862).[24] Since they have separate accreditations, their registration numbers are reported by ICANN separately, but NameCheap and Spaceship are commonly controlled and members of the same registrar family.

We have researched the ownership of registrar families and consolidated their numbers below. **The top five registrar families registered 53.1% of the domains that were created in 2025 and blocklisted:**

REGISTRAR FAMILIES WITH HIGHEST NUMBER OF NEW DOMAINS BLOCKLISTED, 2025

RANK	REGISTRAR FAMILY	# OF ACCREDITATIONS	NEW DOMAINS CREATED (NET ADDS) 2025	NEW DOMAINS CREATED IN 2025 BLOCKLISTED, AND MALICIOUS	% OF NEW DOMAINS BLOCKLISTED, AND MALICIOUS, 2025	% OF ALL MALICIOUS REGISTRATIONS CREATED IN 2025 IN ALL gTLDS BY ALL REGISTRARS
1	NameCheap	2	14,087,503	**1,161,111**	**8.2%**	13.9%
2	Gname	501	3,143,739	**1,036,853**	**33.0%**	12.4%
3	Dynadot	24	4,913,367	**1,029,282**	**20.9%**	12.3%
4	NameSilo, LLC	1	3,028,042	**621,268**	**20.5%**	7.4%
5	GoDaddy	12	12,875,929	**595,684**	**4.6%**	7.1%
6	Team Internet	10	1,544,544	**477,808**	**30.9%**	5.7%
7	Alibaba Group	4	2,783,760	**475,397**	**17.1%**	5.7%
8	GMO	3	7,291,336	**314,196**	**4.3%**	3.8%
9	Namemart	2	506,966	**223,704**	**44.1%**	2.7%
10	Hosting Concepts B.V. dba Registrar.eu	1	730,938	**213,225**	**29.2%**	2.5%

cont'd on following page

REGISTRAR FAMILIES WITH HIGHEST NUMBER OF NEW DOMAINS BLOCKLISTED, 2025 (CONT'D)

RANK	REGISTRAR FAMILY	# OF ACCREDITATIONS	NEW DOMAINS CREATED (NET ADDS) 2025	NEW DOMAINS CREATED IN 2025 BLOCKLISTED, AND MALICIOUS	% OF NEW DOMAINS BLOCKLISTED, AND MALICIOUS, 2025	% OF ALL MALICIOUS REGISTRATIONS CREATED IN 2025 IN ALL gTLDS BY ALL REGISTRARS
11	NICENIC INTERNATIONAL	1	180,404	**157,970**	**87.6%**	1.9%
12	Eranet International Limited	1	815,751	**145,455**	**17.8%**	1.7%
13	Web Commerce Comm's dba WebNic.cc	1	485,159	**127,567**	**26.3%**	1.5%
14	West263 International	1	1,333,091	**118,932**	**8.9%**	1.4%
15	Tencent	2	522,746	**105,974**	**20.3%**	1.3%
16	Newfold Digital	582	2,500,558	**97,837**	**3.9%**	1.2%
17	URL Solutions, Inc.	1	139,882	**93,693**	**67.0%**	1.1%
18	eName Technology Co	1	361,526	**93,613**	**25.9%**	1.1%
19	Tucows	3	2,657,721	**80,150**	**3.0%**	1.0%
20	Hefei Juming Network Technology Co.	1	148,439	**79,018**	**53.2%**	0.9%

Note that some registrar families have a significant number of domains under management, but relatively fewer blocklisted domains. For example, Newfold Digital (the parent of 582 accredited registrars, notably Network Solutions, Register.com, and SnapNames) has achieved high annual renewal rates of 74% to 80%, and has relatively low domain abuse. Tucows has managed its businesses, which include both reseller-oriented and public-facing registrars (Tucows/OpenSRS, eNom, EPAG, and Ascio) in a manner that has controlled abuse numbers.

Malicious registrations make up a significant portion of the market, and permeate the gTLD space. But they tend to be concentrated at certain providers. Below we examine several TLDs to quantify their levels of malicious registrations, and some of the criminal activity that took place using those domains.

Case Studies: Associated Domains & Organized Criminal Activity

We examined four TLDs—LOAN, .PINK, .BOND, and .GIFT—as case studies. There we identified hundreds of thousands of domains registered by professional criminal organizations, accounting for most of the domains in three of the four TLDs.

We found thousands of associated domains registered by the bad actors that were never blocklisted, illustrating how the criminal registration problem is notably larger than the blocklisting numbers indicate. **Starting with blocklisted domains as indicators, we found 38% to 63% more associated domains that were likely registered by the bad actors.** We found significant numbers of associated domains even in heavily blocklisted TLDs.

When TLDs had high numbers of malicious registrations, their renewal rates plummeted a year later. This emphasizes the exceptionally low legitimate use of those TLDs.

Security researchers have tracked how threat actors have used programmatic mechanisms to register millions of domain names to perpetrate abuse at scale.[25, 26] Once blocklist providers find an indicator of abuse, they analyze infrastructures and registration data to find "associated domain names" – the additional domains in the batches that are registered for malicious purposes. Registry operators can access those same kinds of data. Domain registrars have significantly greater data with which to perform these checks that other parties do not, including registrant contact data, payment details, and registrant IP addresses.

Associated Domains

A recent study about associated domains was performed by the research team in ICANN's Office of the CTO (OCTO).[27] This study found that "at least 16% of newly registered gTLD domains, [created] in the first quarter of 2025, exhibited batch registration patterns." Starting with an initial set of "seed" RBL-listed domains, the researchers **found an additional 80% more domains that were associated with the blocklisted ones.** This "indicates that for every three newly registered malicious domains reported through RBL feeds, batch expansion (using conservative filtering) identifies an additional two neighboring domains." The researchers stated that "the true rate is likely to be higher" since they excluded "many valid batches" such as those containing more than 1,000 domains. The results "indicate that batch registrations are prevalent, significantly predict overall abuse rates, and are useful for pivoting and expanding from known malicious 'seed' domain sets, particularly in certain TLDs and registrar environments."

We performed "associated domain checks" or "expansion analysis" of four TLDs, using blocklisted domains to point us to potentially associated domains. We obtained registration data for all the domains in these TLDs, based on the contents of their zone files at two points (30 July and 2 September 2025), and for all the blocklisted domains. Our criteria shared similarities with the ones used in the ICANN OCTO study. We considered domains to be associated when they shared the following characteristics:

1. At least one domain in the set was blocklisted for abuse, AND
2. the domains were created by the same registrar(s), AND
3. the domains were registered within a time-bound manner (typically less than 10 minutes between consecutive registrations), AND
4. the domains used the same hosting (same nameserver pair, and/or same IP address/A record), AND
5. the domains followed the same distinctive string pattern. These are lexical similarities often produced by domain generation algorithms. These include same

string length, reoccurring or progressive characters or substrings, use of all digits, use of all letters, and use of hyphens.

We then performed manual validation of the data, examining every record for every domain. This allowed us to find and confirm certain registration patterns, some of which we describe below.

FUNNULL: Professional Criminal Domain Registrations

Some of the registrations in these case studies were the work of FUNNULL, a criminal content delivery system that is a key infrastructure provider for Southeast Asia's cybercriminal ecosystem. FUNNULL offers one-stop services that have been used to perpetrate billions of dollars in financial losses since 2022, through cryptocurrency investment fraud and "pig butchering" scams, phishing campaigns, malware attacks, and other illicit activities.[28, 29, 30] FUNNULL has registered and supported perhaps more than a million domain names for cybercriminals using domain generation algorithms (DGAs).

FUNNULL is linked to the majority of the virtual currency investment scam websites reported to the Federal Bureau of Investigation (FBI). U.S.-based victims of these scam websites have reported over $200 million in losses, with average losses of over $150,000 per individual, although investigators believe the actual losses are much higher. Among others, FUNNULL also hosted thousands of illegal gambling sites for the Suncity Group, a transnational Chinese crime syndicate involved in laundering billions of dollars for Chinese criminal groups, and has been linked to North Korea's Lazarus Group, a state-sponsored hacking group.[31, 32] In the second half of 2024 alone, Quad9 blocked more than 570 million queries to the domains attributed to FUNNULL's Polyfill.io attack.[33] FUNNULL and its associated groups continue to be threats in 2026.[34, 35]

On 29 May 2025, the U.S. government placed FUNNULL and its administrator Lui Lizhi on its sanctions list. This required that all assets of FUNNULL in the United States (or in the possession or control of American entities) be blocked and reported to the financial intelligence and enforcement agency of the United States Treasury Department, and the sanctions prohibited U.S. entities from transacting with any entities related to FUNNULL.[36]

In connection with the sanctions, the FBI released a list of more than 332,000 domain names it had documented on FUNNULL's infrastructure.[37] FUNNULL spread its activity across multiple TLDs, registrars, and hosting infrastructure. **Only 56.6% of the domains on the FBI's list made their way onto the blocklists we monitored, either before or after the FBI released its list. This is an example of how malicious registrations can be missed by RBLs,** especially when the activity involves large sets of domain names, and the malicious activity is distributed.

Case Study: .LOAN

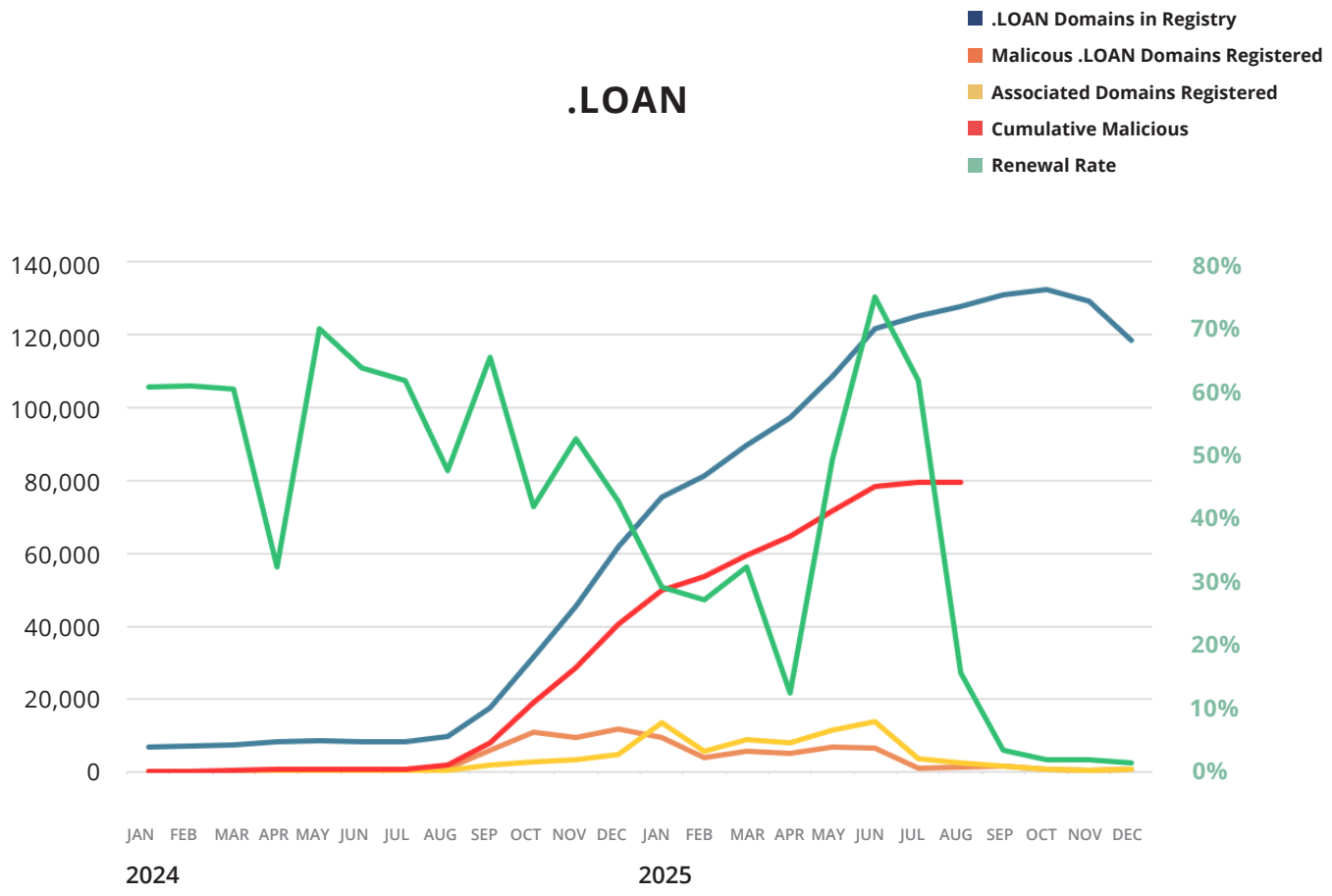
We chose to study .LOAN because it experienced unusual growth. This open gTLD was operated by Domain Venture Partners PCC Limited (DVP) of Gibraltar until 2018, when it was placed into administration following disputes with investors. The court-appointed administrator is a Gibraltar-based accountant at PricewaterhouseCoopers.[38, 39, 40]

.LOAN was historically a small TLD – there were only 7,000 domains in it in January 2024. Its growth surged beginning in August 2024, and by September 2025 there were 132,258 .LOAN domains in the registry, or growth of 1,880%. Of those domains, 76,892 had been blocklisted in 2025 and 2026 – about 58% of the TLD.

Using those blocklisted domains as a starting point, our expansion analysis found 31,777 additional associated domains (41% more). We therefore believe that more than 108,600 .LOAN domains were registered for abuse, or more than 82% of the domains in the TLD as of September 2025. It appears that FUNNULL made at least 100,000 of those registrations.

The following chart shows how that surge in malicious registration drove .LOAN's fast growth, beginning in August 2024. A year later, as malicious registrations began to expire, .LOAN's renewal rate plummeted, from its historical range of 40% to 70% down to just 4.6%. This emphasizes

the exceptionally low quality of the registration base during the period in question.



Associating domains was straightforward because so many .LOAN domains had been blocklisted, and because:

1. 4,418 .LOAN domains were attributed to FUNNULL by the FBI, and another 5,447 were attributed to FUNNULL by Infoblox. These "seed" domains were interspersed through long sequences of clearly related domain registrations.
2. The domains fell into distinct patterns. For example:
   A. Just over 100,000 of the domains (75% of the TLD) were composed of numerals only. Such domains were not intended to host businesses or personal sites, but were algorithmically generated to be used and discarded.
   B. Much of the sequence *00001.loan* through *99999.loan* was registered, including many of the FUNNULL domains the FBI and Infoblox identified. Six-digit domains were also registered, with gaps between them.
   C. The gaps apparently exist because FUNNULL was registering numbers *across TLDs*, scattering registrations across time and the domain space. For example, the FBI observed the FUNNULL domains *12529.loan* and *12538.loans* (plural, a different TLD), which were registered at different registrars 27 days apart. And the FBI logged FUNNULL registrations including *27271.one*, *27272.loan*, *272722.me*, *272777.cn*, and *272788.loan*.
3. FUNNULL's domains were limited to a small number of registrars and nameserver pairs. U.S. registrar Dynadot had 84,449 total domains (blocklisted plus associated), some delegated to nameservers in China. NameCheap and NameSilo had more than 6,000 each.

4. There were smaller sets of malicious registrations apparently made by other actors. For example a set of 86 domains was used for a "toll road" phishing campaign. (e.g., *http://e-zpass.com-etcww.loan/*) There were other blocklisted domains in clear alphabetical sequences, such as *chipca.loan* and *chipcb.loan* through *chipcz.loan*.

After the U.S. sanctions on FUNNULL were imposed on 29 May 2025, most of FUNNULL's .LOAN domains remained in the zone file; they were not suspended via clientHold or serverHold. And FUNNULL registered thousands more .LOAN domains after the sanctions went into effect, including large sets at U.S.-based registrars.

Of the 76,892 blocklisted domains, about 5,541 (7.2%) were removed from the zone before their one-year anniversaries. Some, such as the batch of 86 phishing domains above, had been suspended by the registrars. Other blocklisted domains were placed on serverHold status, suspended by the registry operator.

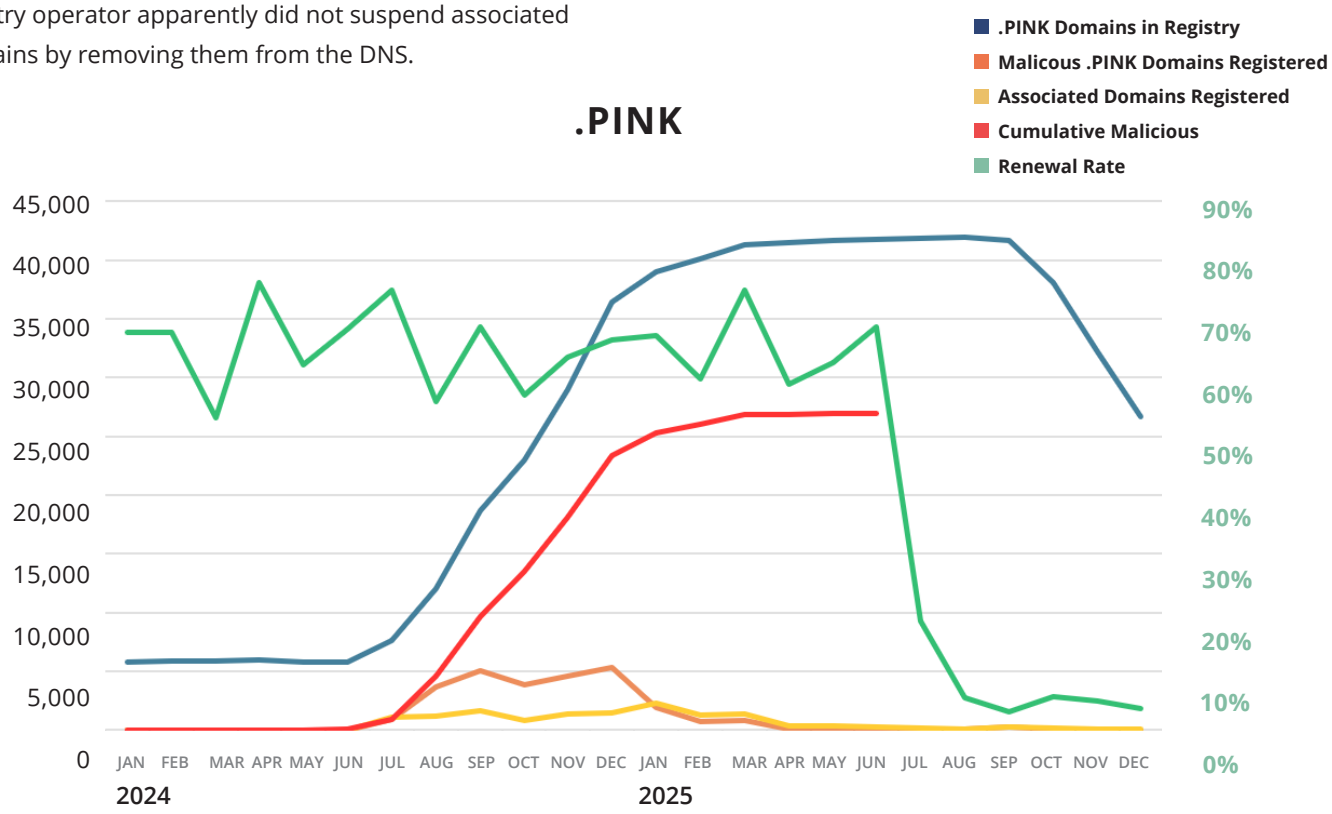
Of the 31,774 domains we found via expansion analysis, all were still in the zone in September 2025–i.e. none had been suspended. Although there had been significant blocklistings, and the registrar and registry operator had apparently responded to some complaints about thesedomains and their registrant(s), the registrars and registry operator apparently did not suspend associated domains by removing them from the DNS.

Case Study: .PINK

We chose to examine .PINK because it displayed rapid growth. In June 2024 it contained only 5,800 domains, but by March 2025 it had grown by a factor of seven, to almost 42,000 domains. .PINK was launched as a generic and open TLD.[41] It is operated by Identity Digital, a major registry operator based in the United States.

Like .LOAN, .PINK's growth was attributable to bad actors. 22,987 .PINK domains registered in 2024 and 2025 were blocklisted. Our expansion analysis found an additional 8,798 .PINK domains that were closely associated with the blocklisted domains, and that the RBLs had not listed. This was a 38% expansion beyond the 22,987 blocklisted domains. **After expansion analysis, it appears that in September 2025, 76.3% of the domains in the .PINK TLD were associated with abusive actors.**

The following chart shows that a surge in malicious registration drove .PINK's fast growth. A year after the malicious registrations, .PINK's renewal rate plummeted, from its historical average of 60% to 70% down to just 3.1% in December 2025. This emphasizes the exceptionally low legitimate use of the TLD during the period in question.



The abusive domains were mainly associated with FUNNULL, following some of the same patterns and registration tactics that we found in .LOAN. The FBI documented 1,839 .PINK domains registered by FUNNULL, and Infobox documented 571 more. Many of those domains were in the sequence *00001.pink* through *99999.pink*.

Funnull registered .PINK names in a numerical sequence, with gaps between numbers. Some of the domains were identified by security observers, and some were not identified or blocklisted at all:

	Detected by
22238.pink	Infoblox, SURBL
22253.pink	no source; associated domain
22261.pink	no source; associated domain
22274.pink	Spamhaus
22277.pink	FBI
22290.pink	FBI
22291.pink	no source; associated domain
22301.pink	Infoblox, Spamhaus
22302.pink	no source; associated domain
22314.pink	no source; associated domain
22317.pink	no source; associated domain
22319.pink	Spamhaus
22320.pink	Spamhaus
22322.pink	no source; associated domain

FUNNULL's .PINK domains were registered across registrars, and the bad actor mixed up blocks of related domains in order to evade detection. For example:

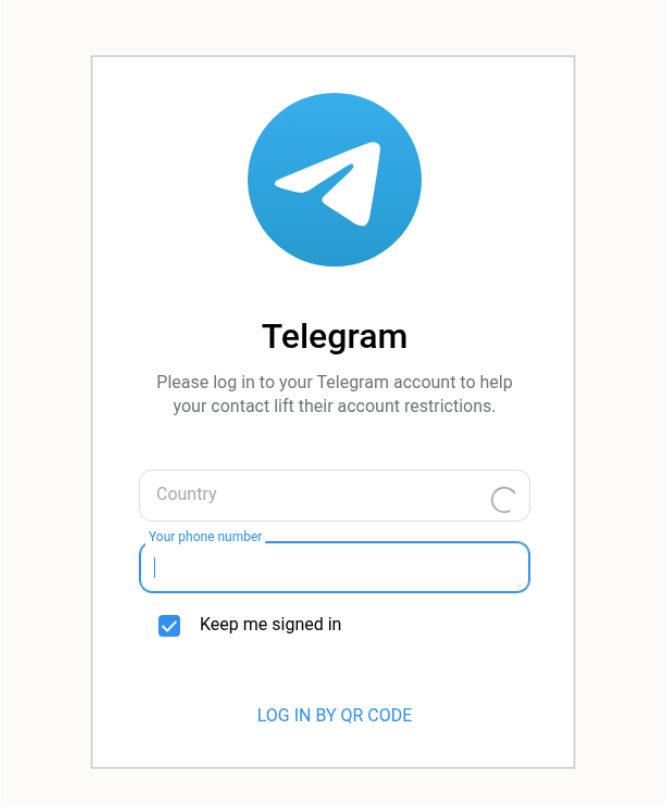
- 00035.pink through 00043.pink were registered at Sav.com from 9 to 11 September 2024.
- 00044.pink through 00099.pink were registered on 28 September 2024, across three registrars: Dynadot, Sav.com, and Domain International Services Limited.
- Then domains falling in the numerical sequence before those – 00030.pink through 00034.pink – were registered at Domain International Services Limited also on 28 September 2024.
- Later FUNNULL shifted to a pattern of five random letters.

Many of the nameserver pairs were not the registrars' default nameservers that they assign automatically when registrants do not designate their own nameservers. For example, FUNNULL registered .PINK domains at U.S. registrars including Dynadot and GoDaddy, but placed the domains on nameservers n1.xundns.com and n2.xundns.com, which are operated by Chinese hosting provider DNS.LA. After a few days of being created, others were switched to China-based nameservers such as ns1.1233dns.com and ns2.951dns.com.

After the U.S. sanctions of FUNNULL were imposed on 29 May 2025, most of FUNNULL's .PINK domains continued to resolve, and FUNNULL registered more more .PINK domains, some at U.S. registrars.

Of 19,419 domains blocklisted by September 2025, 3,156 (16.3%) had been removed from the zone by that time. Of the 8,795 domains we found via expansion analysis, all were still in the zone in September 2025 –i.e. *none had been suspended by the registrars or the registry*. Although there had been significant blocklistings (and sanctions), the registrars and registry operator had suspended a distinct minority of the blocklisted domains, and none of the associated domains.

There were also .PINK domains registered by other threat actors. Four hundred and forty-two .PINK domains following the pattern *teleg[4 random letters].pink* were registered at registrar Chengdu West. They were used to phish Telegram users, and some were blocked by Google Safe Browsing. Only 77 of them had been blocklisted by our sources; we found another 364 by association. After several months, only 34 of the 442 domains had been suspended.



Above: phishing page at telegbftc.pink, 5 May 2025. Source: urlscan.io[42]

A different set of .PINK domains registered at Chengdu West was also used to phish Telegram users. That set was composed of thirteen random letters. Only six were ever blocklisted, and we found 176 more by association.

Case Study: .BOND

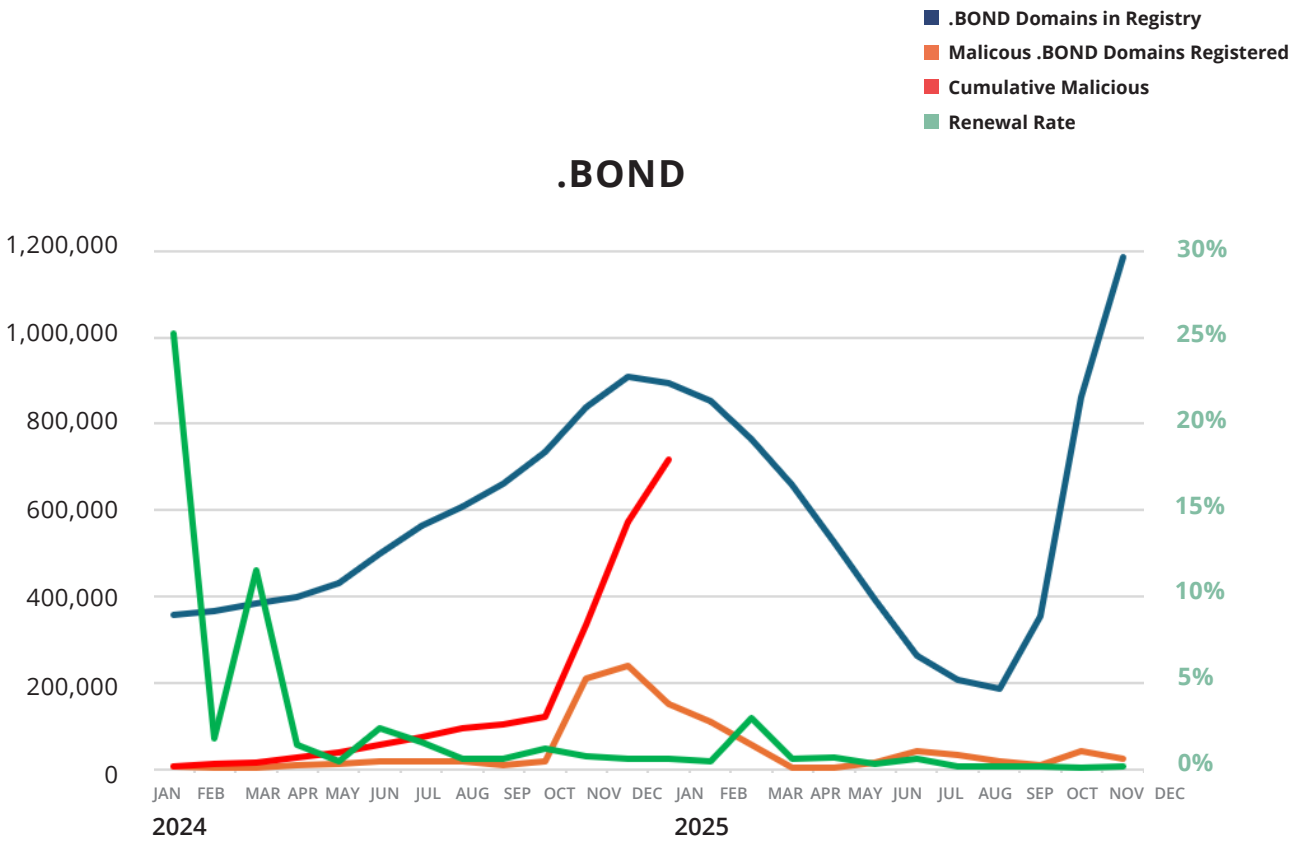
We chose to study .BOND because of its anomalously low renewal rate, and because the number of domains in the TLD fluctuated radically. .BOND is an open gTLD operated by Shortdot SA in Luxembourg. .BOND contained interesting sets of associated domains.

770,000 .BOND domains registered between November 2024 and March 2025 became blocklisted. From January through October 2025, a registrant Infobox called "Revolver Rabbit" registered at least 350,000 .BOND domains at registrar Key-Systems.[43] Evidently the registrations were for an advertising network, and other unrelated parties abused the network to distribute information-stealing malware. [44, 45, 46] The domains followed a recognizable format: hyphen-separated words followed by a five-digit number, such as *security-apps-25597.bond, work-abroad-18297.bond*, and *cremation-services-37263.bond*. At the time, Key-Systems was promoting .BOND as a domain that would help establish registrants with a "professional image as a trusted financial entity."[47]

.BOND also contained clusters of domains registered to phish government sites, such as Italy's postal service (poste-italiano.bond), the U.K. Royal Mail (lonsecpb.bond, lonsecpc.bond, lonsecpm.bond, lonsecpn.bond), and a cluster of 800 domains designed to spoof and phish other U.K .government sites (uk-subsidy.bond, uk-dwpc.bond, uk-tra.bond, uk-trb.bond, uk-trc.bond, etc.).[48]

As a result of this activity, .BOND has had abysmal renewal rates over the last two years. .BOND's overall renewal rate for 2025 was 0.5%. Only about one in two hundred .BOND domains renewed in 2025, underlining the abuse problems and low longer-term use of domains in the TLD.

In November and December 2025, Japanese registrar GMO Internet Group registered more than one million .BOND domains, accounting for almost all of the 1.18 million domains in the .BOND registry. GMO offered .BOND domains for an extremely low price: ¥114 or US$0.75 each. This massive influx consists almost entirely of algorithmically generated domains, consisting letters and numerals. (*3gx2q1.bond*, *3gxcmq.bond*, *decadetjfkgc.bond*, *decadeuohbqe.bond*, etc.) Blocklisting of these domains started accelerating in late March 2026, and we will not be surprised if they mount significantly as 2026 continues.



Case Study: .GIFT

For our fourth case study, we randomly selected .GIFT from among a list of small, open gTLDs that have not been historically associated with abuse. The .GIFT registry is sponsored and operated by Uniregistry.

In September 2025, .GIFT had 5,977 domains in the registry. Of the .GIFT domains created in 2024 and 2025, 528 had been blocklisted. Several of those domains were known to have been registered by FUNNULL in July 2024.[49] It appears that at least 400 of the blocklisted .GIFT domains were associated with FUNNULL, which registered them into January 2025. These domains were all composed of five random letters, and were registered at just two registrars (Dynadot and NameSilo).

Our expansion analysis found an additional 332 .GIFT domains that were closely associated with the others, and that the RBLs had not listed. **This was a 63% expansion beyond the original 528 blocklisted domains.** The additional domains also appear to be associated with FUNNULL, following the same five-letter pattern.[50] After expansion analysis, it appears that 15% of the .GIFT registry was associated with abusive actors.[51]

Of the 528 blocklisted domains, only 49 (9%) had been removed from the zone by September 2025. Of the 332 domains we found via expansion analysis, all were still in the zone in September 2025. This indicates that although there had been blocklisting, the registrars and registry operator had suspended very few of the domains, and suspended no associated domains.

In 2025, .GIFT had a relatively high 61.3% renewal rate, reflecting the TLD's lower abuse rate, and indicating a higher-quality set of registrants.

Renewal Rates

Low renewal rates can provide corroborating evidence of large-scale abusive registration activity.

Registries and registrars must continually register new

GTLDS WITH LOWEST RENEWAL RATES, 2025

RANK	TLD	DEC 2025 DUM (MINIMUM 250,000)	DUM GROWTH 2025	GROWTH % 2025	MALICIOUS REGISTRATIONS CREATED IN 2025	% OF 2025 REGISTRATIONS BLOCKLISTED	2025 RENEWAL RATE
1	.BOND	1,185,926	275,709	30.3%	514,197	30.2%	**0.5%**
2	.SBS	1,343,850	420,248	45.5%	144,403	11.3%	**0.9%**
3	.CYOU	452,569	135,081	42.5%	116,812	30.1%	**2.4%**
4	.CFD	556,460	187,441	50.8%	124,386	25.3%	**3.0%**
5	.LOL	269,965	-452,939	-62.7%	12,384	6.2%	**3.8%**
6	.AUTOS	275,315	194,252	239.6%	13,001	5.4%	**5.3%**
7	.ICU	642,413	199,853	45.2%	149,861	28.5%	**6.0%**
8	.TODAY	352,811	-200,835	-36.3%	24,050	13.7%	**8.2%**
9	.CLICK	792,683	239,934	43.4%	89,413	14.7%	**9.4%**
10	.SHOP	4,309,485	389,065	9.9%	243,660	7.1	**11.4%**

domains in order to replace expiring domains, and must register even more in order to grow. Renewal rates are therefore a key indicator of business quality.

The benchmark .COM/.NET registry traditionally has a renewal rate of 74% to 75%, enjoying a stable base of domains that renew year after year. The well-known .ORG TLD has an even higher renewal rate, at over 80% yearly. The overall renewal rate for all gTLD domains in 2025 was 67%,[52] (heavily influenced by the high renewal rate in the large .COM TLD). The median renewal rate for individual gTLDs was 63%, and 122 gTLDs had renewal rates below 50%. Those are overall renewal rates, for all domains in a TLD. While older domains tend to renew, the renewal rates for newly registered domains are lower.[53]

Spamhaus considers that a new domain creation rate that is 10% to 20% higher than usual is "unusually high… This behavior suggests a large volume of domain churn, with domains being registered and cancelled quickly."[54]

Of gTLDs with at least 250,000 domains in them, some had overall renewal rates of less than 10% in 2025. Most of these TLDs actually grew during 2025, attracting significant numbers of malicious registrations that filled losses due to non-renewal and made growth possible.

Bulk Registrations, Sales Programs, and Market Incentives

Bad actors tend to register sets of domains, and some consume large numbers of domains over time. These domains also tend to be low-priced, a reflection of aggressive price competition in the gTLD market and sales strategy choices made by registrars and registry operators.

Bulk Registrations

Of the 8.3 million gTLD domains registered in 2025 and were blocklisted through 30 April 2025, we estimate that 7.3 million of them (88%) were "bulk registrations." Prior research has documented that malicious name registration campaigns often involve registrars that offer bulk registration options.[55, 56, 57, 58]

Under our methodology, domains are "bulk registered" if they were all blocklisted, and at least ten domains were registered through the same registrar with no more than ten minutes between consecutive registrations. Domains within these sets usually share lexical/string characteristics and the same nameserver set (i.e., the same per registrar-nameserver combination). The domains in a bulk set are often in the same gTLD, but sometimes bad actors register related domains across several TLDs at the same time. When examined, the domains in batches tend to be obviously related to each other. Our method under-counts the size and occurrence of bulk registrations, because it counts only domains that were blocklisted. As expansion analyses show, there are often more registered domains in the bulk set that were not listed by blocklist providers. Our method also fails to capture smaller (lower volume) batch registrations, and those spaced out over longer time periods.

The largest set we found consisted of 10,848 blocklisted domains created by registrar GMO Internet Group, Inc. (IANA ID 49) from 18:02:02 to 23:20:38 UTC on 25 November 2025 – a sustained registration rate of 106 domains per minute for more than five hours. These were all algorithmically generated .BOND domains, consisting of meaningless strings of letters and numbers.

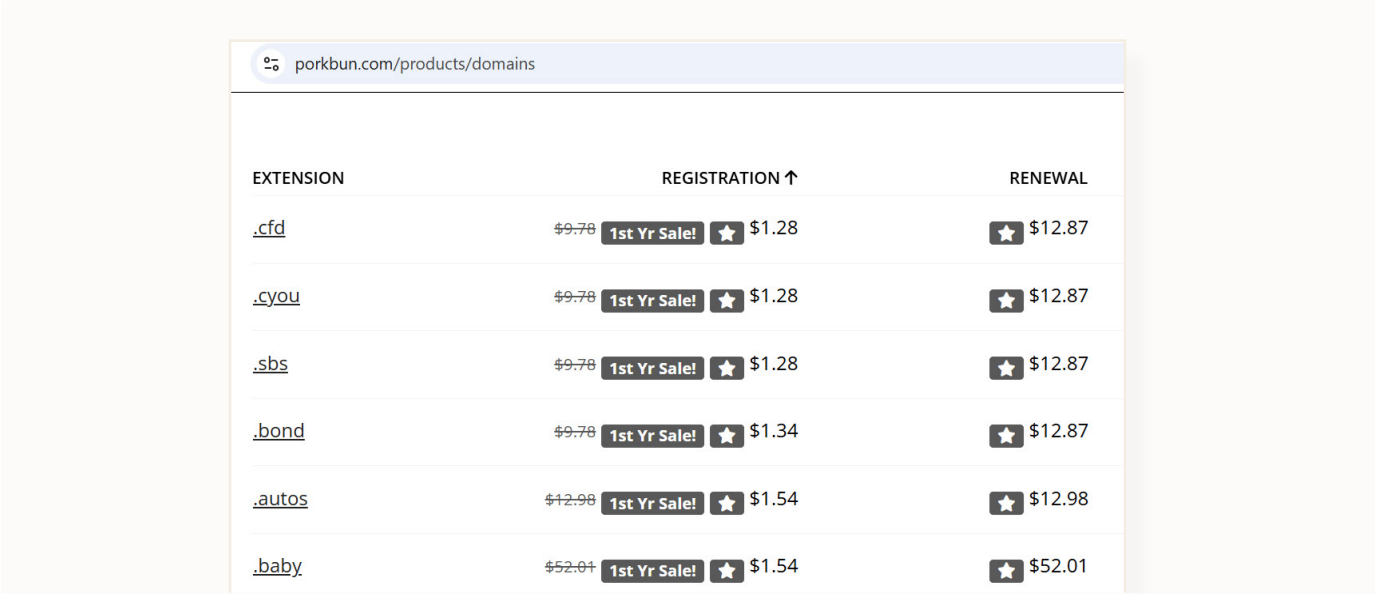
Twelve registrars accounted for more than 80% of the bulk-registered domains. The gTLD registrar with the most bulk registered domains was Gname.com Pte. Ltd. (IANA ID 1923), which registered 881,225 subsequently blocklisted domains in 4,221 batches.

Sales Programs & Market Incentives

Volume-based discount programs and high-volume, low-margin sales strategies create strong commercial incentives for repeat bulk sales. Cybercriminals, who purchase domains in large quantities and rarely renew them, represent a large and reliable source of precisely this kind of demand.

The gTLD market is intensely competitive. The introduction of hundreds of "generic," open TLDs by ICANN in 2001 and 2012 created an increased supply of domains. The operators of new gTLDs have often competed on the basis of price, offering cheap domains in order to establish market share. Those strategies have regularly (but not always) attracted abusive registrations, and the relationship between low pricing and abuse is well documented,[59, 60, 61] A recent ICANN-sponsored study found that each dollar reduction in registration fees corresponds to a 49% increase in malicious domains.[62] The .UK registry operator, Nominet, recently acknowledged this issue when launching a new growth initiative: "Mindful of trust in the .UK domain, and experience of registries elsewhere, we do not want to support unsustainable registrations that spike initially but then fall away or fuel domain abuse."[63]

The market will become even more competitive when ICANN introduces more open new gTLDs in 2027 and beyond.[64] All else equal, the increase in domain supply and



Above: discounted first-year retail prices at registrar Porkbun.com. Some are discounted 90% off the stated retail price.

the entry of additional competitors can be expected to intensify price competition, particularly in segments where buyers are price-sensitive and view products as largely interchangeable, as criminals do.

A variety of open gTLDs have been available at retail prices below US$2.00, due to registry wholesale promotions, registrar-funded discounts, or other deep-discount pricing strategies. Some domains are sold for as little as US$0.49.

How are these low prices offered? Registry operators typically drive sales by offering discounts on the wholesale price they charge registrars for new registrations (domain creates), or by offering rebates when a registrar meets sales or growth targets. Registrars may then pass those savings to registrants through lower retail prices. Registries and registrars often implement such programs by discounting the first year of a domain registration. Then, when the domain comes due for renewal at the end of its first year, it renews at a higher price. The business logic is that a low introductory price can expand the customer base, and that some percentage of the domains will renew at a higher price, creating repeatable revenue in the future.

For example, after several years of relatively flat sales in .COM, Verisign pursued growth in 2025 by offering a discount program, which saw some registrars sell .COM domains to customers at retail for less than half of .COM's usual $10.26 *wholesale* price. Verisign saw evidence of "registrars shifting towards customer acquisition" and "more registrar engagement" with its marketing programs.[65]

As a result, .COM grew by 4.5 million domains in 2025, .COM's most significant growth in several years. Most of the growth in the gTLD market came from the open new gTLD sector, which grew by 11 million domains in 2025.

Some registrars routinely keep their prices low and sell at low margins as a customer acquisition strategy. Sometimes registrars may sell domains for below the wholesale price they pay the registry by cross-subsidizing the low price with sales of other products. A cheap domain name can function as a "loss leader" that entices customers to buy a broader set of higher-margin services from the registrar, such as web hosting and email accounts.

While low retail prices are apparent on registrars' web sites, the details and terms of the sales and marketing programs behind those prices are generally not made public. Registries offer them to their registrar distribution channels privately and sometimes under terms of business confidentiality. Companies sometimes negotiate special deals between themselves, such as to place a registry's gTLD high up in a registrar's web site display and search results. Some registrars offer bulk discounts, which may or may not be advertised, and may give special prices to certain resellers and end customers who buy large numbers of domains.[66] It is therefore difficult for outside observers to understand exactly what incentives are being offered and subsidized by whom.

These low-margin pricing volume discount strategies can be commercially rational, but they also create risk

and can distort incentives. Cybercriminals treat domain names as disposable commodities: they buy them cheaply and do not renew them.

When selling domains to bad actors, the registrar and registry operator will never realize revenue from renewals, making criminals perhaps the lowest-margin customers in the market. However, because cybercriminals require a continuous supply of new domains and purchase them in large volumes, they represent a large and reliable source of repeat demand.

The high volumes or high proportions of abusive registrations associated with certain registry and registrar operators suggests that some of them may be deriving commercial benefit from sales to criminals. Even when abusive registrations generate little or no profit or other direct commercial benefit, registries and registrars may still have an economic incentive to tolerate them. As long as the cost of carrying these domains remains low or commercially neutral, and deterring them is more costly or risks losing higher-margin legitimate customers, tolerating them can still be commercially rational.

While cybercriminals and certain registrars and registry operators may benefit, the costs of cybercrime facilitated by abusive registrations fall on victims, businesses, and society at large. In economic terms this is a classic *negative externality*, where the parties who benefit from the transaction do not bear the full costs they create.

The persistence and scale of bulk registrations made by bad actors suggest the following:

1. **Some registrars are apparently benefitting commercially by selling large numbers of very low-priced domains to abusive registrants.** If those sales consistently produced losses, rational providers would adjust their pricing and sales strategy to limit their commercial exposure.

2. **Many bad actors appear to be using acceptable, payment instruments to pay for their registrations, rather than stolen credit cards.** If cybercriminals were mostly paying for domains with stolen credit cards, registrars would adjust their practices to prevent losses and credit card charge-backs. Registrars would also delete many more domains in the Add Grace Period (AGP), which allows them to get refunds from the registries and from ICANN. However, the numbers of domains deleted in AGP appear to be far below the limits that set off excess deletion penalties under ICANN policy. Payments made by cryptocurrency or gift cards may pass muster. In any case, it appears that registrars are often receiving real funds from cybercriminals.

How cybercriminals pay for their domains, and when and how those payments are passing fraud checks,are areas that deserve further study.

Discussion and Conclusion

The data presented in this report makes clear that a significant portion of the domain name market is driven by registrations made by malicious actors. Malicious registrations accounted for at least 10 percent—and possibly 20 percent—of new sales in the gTLD market in 2025. The number of blocklisted registrations even eclipsed net gTLD market growth in the months of January, February, and May 2025.

While abuse was widespread, abusive registrations were notably concentrated at a small number of registrars. Just five registrars were responsible for half of all blocklisted domains created in 2025. Thirteen gTLDs saw more than half of their new registrations flagged for abuse.

The case studies of .LOAN, .PINK, .BOND, and .GIFT illustrate how professional criminal organizations exploited the market. These actors registered domains in massive batches—totaling hundreds of thousands of domains—across multiple registrars and TLDs, using them for phishing, malware distribution, and large-scale fraud. The exceptionally low renewal rates that followed confirm that these domains were not renewed often due to low legitimate usage. In contrast, some TLDs and registrars grew without attracting outsized abuse, showing that the choices that providers make do matter.

How cybercriminals pay for their domains, and when and how payments are passing fraud checks, are areas that deserve further study.

Bulk registrations, low prices, and minimal deterrents make domains easily exploitable tools for cybercriminals. While sales and incentive programs are intended to drive growth and market share, they can also incentivize sales to high-volume, repeat customers such as cybercriminals. Some registrars and registries appear to derive commercial value from criminal demand, even when selling at deeply discounted prices.

In economic terms, this is a sign of a market out of equilibrium with distorted incentives. It is also evidence of a classic *negative externality*: a situation in which a party benefits from an activity, but imposes costs on unrelated third parties. Here cybercriminals and certain registrars and registry operators benefit, while the costs are imposed on victims of cybercrime and the public in general, who suffer financial losses, business and personal disruptions, and an erosion of public trust.

Importantly, however, abuse on this scale is not inevitable. Associated domain name check studies show that abuse detection and mitigation can be made more efficient and effective. Sales strategies, provider practices, and abuse-mitigation choices can materially affect whether growth is driven by legitimate demand or by cybercriminal registrations. Better contractually binding and enforceable policies are needed.

Sponsors

We gratefully acknowledge the sponsors of this project who contributed threat intelligence data, financial support, or in-kind assistance. All aspects of the study, including the methodology and analysis, were conducted independently by Interisle. The findings and conclusions presented in this report are those of Interisle alone and were not influenced by the sponsors.

The Anti-Phishing Working Group (APWG)

Coalition for Online Accountability (COA)

DomainTools

Meta

Spamhaus

SURBL

A list of organizations that support Interisle's data collection activities, which we use for this and other projects can be found at:
https://www.cybercrimeinfocenter.org/contributors

Acknowledgements

The authors wish to thank the following:

- Renée Burton and Zach Edwards of Infoblox, for their insights about FUNNULL.
- April Lorenzen and Zetalytics, for access to passive DNS data.
- Rod Rasmussen, Lyman Chapin, and Dave Piscitello, for their constructive comments as the report was in draft.
- The teams at Spamhaus and SURBL, for their insights about blocklists.
- Pete Strutt at Common Co., for design services.
- The researchers whose work is cited in this report, and to the security professionals and members of law enforcement who fight cybercrime.

About Interisle Consulting Group

Interisle's principal consultants are experienced practitioners with extensive track records in industry and academia and world-class expertise in business and technology strategy, Internet technologies and governance, financial industry applications, and software design. For more about Interisle, please visit: www.interisle.net

About the Authors

Greg Aaron is an internationally recognized authority on the use of domain names for cybercrime, and is an expert on DNS policy, domain registry operations, and related intellectual property issues. He has performed complex investigations and due diligence projects with industry, law enforcement, law firms, and security researchers to address phishing, intellectual property violations, malware, spam, and botnet cases, and has advised governments and online commerce providers. Mr. Aaron is Senior Research Fellow for the Anti-Phishing Working Group, and is a member of M3AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group. As a member of ICANN's Security and Stability Advisory Committee (SSAC), he advises the international community regarding the domain name and numbering system that makes the Internet function. He has participated in numerous ICANN working groups, including several devoted to anti-abuse and privacy topics such as the EU's General Data Protection Regulation (GDPR). He was the senior industry expert on a team that evaluated the policy and technical qualifications of more than one thousand new gTLD applications to ICANN in 2012-2013. He has created products and services used by organizations to discover and track Internet-based threats, and has managed large top-level domains, including .INFO, .ME, and .IN. Mr. Aaron is a magna cum laude graduate of the University of Pennsylvania.

Karen Rose is an internationally recognized expert in Internet policy, technology, and development with over 25 years of experience in the field. Since 2017, she has consulted on a range of Internet policy and digital economy issues. Ms. Rose was previously a senior executive at the Internet Society (ISOC) where she led the organization's work to expand Internet infrastructure and related policy capacity around the world, as well as research on emerging Internet issues. Prior to that, she served at the U.S. Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). While in government, she was co-author of the U.S. policy statement and related agreements that globalized management of the Internet's Domain Name System (DNS) and led to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN). Ms. Rose served on the board of Netnod, one of Europe's most recognized Internet exchange point operators, and on the .US domain stakeholder advisory committee. She currently serves on the advisory panel for AfChix, an African organization dedicated to advancing women in tech.

Dr. Colin Strutt has published and spoken extensively on networking technology, name collisions, enterprise management, eBusiness, and scenario planning, and has represented the interests of DEC, Compaq, and the Financial Services Technology Consortium in national and international industry standards bodies. He holds six patents on enterprise management technology, and has more than forty years of direct experience with information technology as a developer, architect, and consultant; his recent work includes the design and operation of a regional public safety network, providing technical expertise relating to patents, and analysis of world-wide Internet use. Most recently, he has been involved in the cybercrime data analysis for the Cybercrime Information Center and the related Interisle reports. Dr. Strutt holds a B.A. (with First Class Honours) and a Ph.D. in Computer Science from Essex University (UK).

Methodology

All aspects of the study, including the methodology and analysis, were conducted independently by Interisle. The findings and conclusions presented in this report are those of Interisle alone and were not influenced by the sponsors.

How does Interisle identify abusive domain names?

We begin with data from prominent Reputation Block Lists (RBLs). These contain domain names and/or the URLs of known phishing pages, malware, and web pages that host dangerous or unwanted content. The RBLs we use are provided by professional security threat-reporting sources, and are used to protect billions of user accounts across the world. These providers continually add and remove domains and URLs from these lists, according to their own criteria.

RBLs are widely used as a defense measure. Internet service providers, email providers, Web browser providers, DNS resolvers, and other organizations use these RBLs to block access to (and traffic and email from) these domains and URLs, protecting their users from online threats. Pretty much every user of the Internet is protected by RBLs, including the users of corporate and university networks, ISPs, and public wifi networks and DNS resolvers. Web browsers such as Chrome, Safari, and Edge use reputation blocklists to prevent users from visiting malicious sites. Most e-mail providers use blocklists to protect email accounts.

This data provides a practical measurement of what is happening in the "real world," the Internet ecosystem that uses the DNS. It shows what domain names are being blocked—the domains that professional anti-abuse sources have identified as harmful, and what domains are being blocked by security administrators at private and public networks and services around the world. Interisle uses this data to identify abusive domain registration and usage trends, such as what hosting providers, registrars, and services are most heavily used and exploited by cybercriminals.

ICANN takes a similar approach with its Metrica abuse measurement system. ICANN notes: "We believe that it is beneficial to collect the same DNS abuse data that is reported to industry and Internet users. Security systems such as anti-spam or anti-malware gateways or firewalls that protect billions of users incorporate these data into their DNS abuse mitigation measures. Domain Metrica thus reflects how the users and network operations communities see the domain name ecosystem through the lens of reported DNS abuse data."[67]

What blocklists does Interisle use?

The APWG phishing feed (phishing; high-confidence only), OpenPhish (phishing), PhishTank (phishing; confirmed phishing only), Spamhaus DBL (malware, phishing, spam/malicious domains; "abused-legit" not counted), SURBL (malware, phishing, and Abuse domains), URLHaus (malware), Invaluement, and Malware Patrol (malware). See below for the details. Each provider describes the general details of their processes.

For this study we also included domains registered in 2025 for use in notable cybercriminal campaigns. Most of these domains were blocklisted by the RBLs we monitor, but some were not and we added them to our list of maliciously registered domains. The sources are:

- Funnull phishing and cryptocurrency scam campaign: list provided by the U.S. Federal Bureau of Investigation (FBI): https://www.ic3.gov/CSA/2025/Complete_List_of_Domains_Attributed_to_Funnull.zip
- LabHost "Phishing-as-a-Service" (PhaaS) case: list provided by the U.S. Federal Bureau of Investigation (FBI): https://www.ic3.gov/CSA/2025/LabHost_Domains.csv

- Lumma malware case: domains seized as a result of Microsoft's filings in U.S. federal court cases 1:25-cv-06493-MHC (injunction 12 December 2025) and 1:25-cv-02695-MHC (injunction 12 June 2025), and https://www.cisa.gov/sites/default/files/2025-05/AA25-141B.stix_.xml
- Lighthouse "Phishing-as-a-Service" (PhaaS) case: domains seized as a result of Google's filings in U.S. federal court case 1:25-cv-09421-LAK (injunction December 1, 2025)
- RaccoonO365 "Phishing-as-a-Service" (PhaaS) case: domains seized as a result of Microsoft's filings in U.S. federal court cases 1:25-cv-07111-JSR (injunction 16 September 2025)
- Toll road phishing campaign: list provided by Netcraft. https://github.com/netcraftcom/public-iocs/blob/main/state-tax-road-toll-smishing-IOCs.csv
- PDF phishing campaign: list provided by Zimperium and Netcraft. https://github.com/Zimperium/IOC/blob/master/2025-01-PDF-Phishing/urls.csv
- Hotel phishing campaign: list provided by Netcraft: https://www.netcraft.com/blog/thousands-of-domains-target-hotel-guests-in-massive-phishing-campaign and https://github.com/netcraftcom/public-iocs/blob/main/2025-11%20hotel%20phishing%20IOCs.csv
- Cryptocurrency scam: list provided by Silent Push
- Hiragana IDN phishing campaign: List provided by Netcraft: https://github.com/netcraftcom/public-iocs/blob/main/hiragana-%E3%82%93-IOCs.csv

Infoblox provided Interisle with data about some FUNNULL domain names. These were used to aid our case study analyses, but were not added to our blocklist counts.

How does Interisle choose what blocklists to use?

The blocklist providers we use meet important criteria including very low false-positive rates, coverage of relevant kinds of abuse, and wide adoption by companies, governments, and academia. Each RBL also provides a review or appeal process and the ability to redress false-positives. Academic literature and the extent of commercial use indicate that the false-positive rates are quite low among the lists we have chosen.

Our choices of blocklists, and how we use them, follow the considerations described in the "RBL Evaluation Methodology" paper by ICANN's Office of the CTO, which is a useful guide.

We use more blocklists than some other organizations do. There is usually only a small overlap between the domains that one blocklistlist finds versus another. By using more feeds, we gain a better, more comprehensive understanding of what's happening out on the Internet. For more about this, see below.

Does Interisle's system find all instances of abuse?

No. The blocklist providers we use do not claim to detect or list all the abusive activity happening on the Internet. The data we have is only a subset of the abuse problem. Our numbers are a floor, and the number of domain names being used for abusive purposes is higher. We have found that our data provides reliable indicators of trends, and of where abuse is concentrated.

What other data does Interisle collect?

We gather data that gives context to blocklist data, and helps us understand where abuse is taking place. All of this data is publicly available. Among other things, we collect:

- DNS query data. This tells us things such as what IP address a domain is on, and what nameservers a domain name is using.
- Domain registration data. This is the authoritative information about when a domain name was registered, the name of the registrar and its IANA ID number, the domain's contact data, and more. We collect it from domain registries and registrars using RDAP and WHOIS.

- gTLD zone files
- Passive DNS to find the "first observed " dates of domains.
- Feed-specific metadata. Some of our feeds provide additional information, such as the type of abuse a domain or IP address is associated with, the brand that is impersonated in a phishing attack, or a malware family or type.

How does Interisle process and count the data?

Blocklist providers continually add and remove domains and URLs from their lists, according to their own criteria. Our collection system collects updated data from each blocklist provider several times per day, and de-duplicates domain names (both within a list and across lists) as part of processing.

Some blocklists provide URLs. We only count a domain name once, irrespective of how many host names or URLs have been reported on that domain name.

A domain name that we extract from any blocklist will cause the domain name to be counted only once when we calculate unique domain abuse totals. If a domain is listed for two or more types of abuse, that domain will be counted (again, once) in each relevant abuse category. For example, if one blocklist identifies a domain name as a malware domain and a second identifies that domain as a phishing domain, and that domain was not listed before, then:

- The total unique domain count is increased by one,
- The cumulative abuse count is increased by one,
- The malware domain count is increased by one, and
- The phishing domain count is increased by one.

Only unique domains are counted toward the total reported DNS abuse counts in a TLD or registrar portfolio.

Subdomain providers offer third-level domains, such as *example.web.app*, and many such third-level domains are used for phishing and other malicious activities. However, we count only the second level domain (*web.app*), and once only, when reporting domain totals for a TLD or registrar portfolio.

Some RBL providers add a domain to the blocklist and then remove it from the blocklist after a certain time, sometimes because the domain was suspended. In this report, Interisle counts how many and which domains were added to the lists, i.e. how many domains were identified as problems.

How does Interisle determine the number of domains in a TLD or at a registrar?

We determine the numbers in each gTLD, and sponsored by each registrar, using domain counts from ICANN's official registry reports. Interisle uses registrar IANA ID numbers to distinguish registrars.

ICANN and the NetBeacon Institute (services provided by KOR Labs) use the number of domain names found in zone files. Zone files always contain fewer domains than the registry itself, sometimes by 6% or more, because expired domains pending deletion are removed from the zone file. Domains suspended for abuse by registrars and registries (via ClientHold and ServerHold) are also removed from the zone file. This can increase the difference between domains-in-registry and domains-in-zone.

Verisign tends to report the number of domains in the .COM and .NET registries, which it operates. Otherwise Verisign uses zone file size to calculate gTLD renewal rates for the other TLD publishes in its Domain Name Industry Brief reports and gTLD registration and renewal trend dashboards.

The above differences can affect the numbers reported by various organizations, and can affect domain abuse scoring of registrars and TLDs. For example, for December 2025, Verisign reported 161 million domains in .COM in its industry brief, but 164.6 million in its ICANN registry report.

How does Interisle calculate renewal rates?

We use the registration numbers in the official monthly ICANN registry reports to calculate renewal rates. Those reports contain:

- the number of domains in each gTLD registry at the end of each month, and
- how many domains were sponsored (DUM, or "domains under management"), registered (created), renewed, and deleted by each registrar in each gTLD each month.

We use industry-standard methods to calculate the following:

- **New Registrations:** The number of domain names added (Created) in a gTLD during a selected period. In the ICANN reports these are called *net-adds*. This includes domains created for more than a one-year term. We do not count domains added and then deleted in the Add Grace Period.
- **Renewals:** The number of domain names in a selected period that were renewed (for any length of time). In the ICANN reports these are called *net-renews*.
- **Renewal rate:** The percentage of domain names renewed during the selected time period. This is calculated as the number of domain names that are renewed divided by the number of domains that were eligible for renewal (which is the number of domains created one year prior (net-adds), plus the number of domains renewed one year prior). Rates are calculated with the simplifying assumption that all domain names expire and are eligible to renew each year. Multi-year registrations can cause the renewal percentage to be very slightly overstated. The number of Restored domains is negligible, and so we have ignored that effect.

Two other factors can make our renewal rate calculations vary slightly from those published by other sources:

1. Renewal rates are not fully measurable until 45 days after the end of a reporting period, and that factor is not reflected specifically in the ICANN reports. (Registries have the detailed information about exactly which domains were deleted in the 45-day Autorenew Grace Period.) This factor may make our renewal rate calculations turn out slightly lower than what a registry later reports publicly.
2. Instead of domains in the registry (which is what the ICANN reports contain), some parties use zone file size as a proxy for the size of the TLD. As noted above, zone files always contain fewer domains than the registry contains.

How does Interisle determine if a domain has been "maliciously registered?"

A malicious registration is a domain name that we determined was registered by a bad actor, for the purpose of carrying out malicious activity. A compromised domain is owned by a legitimate registrant, but a criminal has taken control of it by hacking or account compromise in order to carry out malicious activity. Distinguishing between the two is important. By identifying malicious registrations, we can see where and how criminals purchase domain names. Also, malicious registrations can be safely suspended by a domain name registry operator or registrar – the suspension will not harm anyone but the criminal. In contrast, suspending a compromised domain can harm legitimate users, preventing the innocent registrant's web site and email from functioning. Those cases should be reported to the hosting provider and the registrant, who can secure the account and remove the harmful activity at the source.

We use multiple criteria to determine if a domain flagged by a blocklist has been maliciously registered. The most important are:

1. Domain age. We look at the number of days between the domain's registration date and the time the domain was blocklisted. (Or if registration date is not available via RDAP or WHOIS, the time between the domain was first observed in a passive DNS query and when the domain is blocklisted.) We consider

domains blocklisted within 90 days of registration to be malicious. Studies indicate that such domains are usually too new to have been compromised, and that a high percentage of maliciously registered phishing domains tend to be used within days of registration. This method excludes some maliciously registered domains that are "aged" by bad actors (by not using them for more than 90 days) in an attempt to improve domain reputation. Other researchers have considered domains as malicious if they were blocklisted within a longer 150-day period after registration.

2. The composition of the domain name. We search listed domains for tell-tale strings that indicate malicious use. These include strings designed to mislead users (login, security, etc.), and brand names that are the targets of phishing attacks (citibank, whatsapp, etc.). We also search for close misspellings and variations of these terms, which criminals often register to evade simple matching measures. Our tell-tale strings lists include strings that we have "observed in the wild," i.e. seen used in confirmed attacks.

3. We look for clear evidence of common control and usage, such as batches of domains registered at the same time at the same registrar, delegated to the same nameserver pair, and for algorithmically generated domain names that follow patterns, such as sequences of numbers and letters. (See "bulk registrations" below.)

These methods share similarities with those used by other researchers, such as the COMAR and MalCom methods used by KOR Labs, the service provider to the NetBeacon Institute. Their and our calculations for malicious phishing registrations have historically been within a few percentage points of each other.

How does Interisle define malicious "bulk registrations"?

We define a set of domains to be bulk registered if the domains were blocklisted and at least ten domains were registered through the same registrar with no more than ten minutes between consecutive registrations. Domains within these sets usually share lexical/string characteristics, and the same nameserver set (registrar-nameserver combination), and we confirm the presence of those features for large batches. The domains in a bulk set are usually in the same gTLD, but sometimes bad actors register domains across several TLDs at the same time.

Our method under-counts the size and occurrence of bulk registrations, because it counts only domains that were blocklisted. There may have been more registered domains in the bulk set, but the blocklist providers did not list them all. Our method also fails to capture smaller (lower volume) batch registrations, and those spaced out over longer time periods.

Note that *bulk registrations* and the concept of *associated domain checks* under policy-making consideration at ICANN are two related concepts. The domains in a bulk registration set are by definition related to each other and were presumably registered by the same party. A competently performed associated domain check by the registrar should uncover all the domains in a bulk set we identified, plus perhaps others.

In research about malicious bulk registrations and associated domain discovery, researchers in ICANN's Office of the CTO found that "batch registrations are prevalent, significantly predict overall abuse rates, and are useful for pivoting and expanding from known malicious 'seed' domain sets."

What kinds of abuse are counted in this study?

We counted a domain if it was included on a blocklist, and was a unique second-level gTLD domain.

Some blocklists are dedicated to listing only domains and URLs about a specific category of abuse. (For example, PhishTank tracks phishing exclusively). Other blocklists will list domains associated with several kinds of abuse, and will tag specific domains to certain abuse types.

Some domains appear on those blocklists without being specifically tagged with an abuse type by the blocklist provider. These categorization gaps are often the result of the large amount of abuse and domains being processed in real-time by blocklist providers, and the multiplicity of

signals used in their reputation scoring systems. Some domains may be tagged by a blocklist provider for a specific type of abuse such as phishing. Conversely, some domains used for phishing or malware are not tagged as such by blocklist providers such as SURBL and Spamhaus.

All gTLD domain name registrars state in their terms of service that domains cannot be used for illegal activities. Some registrars suspend domains that are outside of ICANN's definition.

Why are some domains blocklisted without a specific abuse type? What is a "spam" domain?

RBLs such SURBL and Spamhaus list domains that are used for a variety of abusive purposes. These domains get listed because the RBL provider finds them risky and worthy of blocking. Some of the domains on these RBLs are not tagged with a specific abuse type, as explained above. Since some of those undifferentiated domains were found in spam messages, and since that RBL may be used to filter email, some people colloquially call these "spam domains."

However, "spam domains" is an often inapt term, and doesn't explain *why* some domains are a problem and why they get blocklisted. Some of these "spam domains" are actually ***scam and fraud domains***.

Spam has been traditionally defined as "bulk, unsolicited email messages." With a few exceptions, the sending of bulk, unsolicited email messages violates the law in many countries. However, there are two even bigger problems.

First, most spam messages are sent via criminal and duplicitous means: via botnets, via hijacked IP space, and using fictitious (forged) business names and identities to obtain hosting and sending resources. Reputable senders follow best practices, do not send unsolicited messages, do not have their domains blocklisted, and do not advertise harmful content.

Second, domains that are advertised in unsolicited bulk email are used for various criminal purposes. Blocklist providers such as SURBL and Spamhaus find some malicious domain names by examining what is advertised in the body of spam messages. These are the destinations that spammers want potential victims to go to. Here spam is a delivery method, not the abuse being advertised. "Spam" therefore does not always describe why these domains are problems and get blocklisted. The Budapest Convention on Cybercrime (the major international treaty designed to address Internet crime) produced a guide to illustrate the multi-functional criminal use of spam.

It is a misconception that blocklist providers such as Spamhaus and SURBL focus entirely on spam, either as the primary detection method, or that they curate their lists to be used for email filtering exclusively. Rather, they focus on whether a domain may be malicious or risky, and their lists are used in a variety of protective systems. When describing whether to list a domain, Spamhaus uses this general methodology.

Some domains found by scanning spam messages are used to perpetrate ***scams and frauds*** – investment and cryptocurrency scams, romance and "pig butchering" scams, fake shops, scam casinos, advance fee fraud, and more. These types of frauds and scams resulted in the majority of cybercrime financial losses suffered in 2025. Other blocklisted domains are used to operate other types of fraud, such as illegal pharmaceutical sites and counterfeit product sales. These various scam, fraud, and abuse domains are detected by various methods in addition to email scanning.

Blocklist providers presently do not tag domain listings with specific "fraud and scam" abuse types, due to a lack of an industry-standard taxonomy, because of the diversity and wide-ranging nature of scams and frauds, and because of the challenges of making such classifications on the fly while processing large volumes of detections.

In the end, blocklist providers do not list all the domains they find in bulk unsolicited email. They list only those domains that they judge to be unacceptable risks to Internet users.

Interisle therefore counts domains as phishing or malware when a list is devoted exclusively to such an abuse type, or when a multi-abuse list such as SURBL or Spamhaus specifically tags domains for those abuse types. When looking at the overall use of domain names in this report, Interisle counts all of the domains that Spamhaus and SURBL list, such as when Interisle reports how many domains were blocklisted in a TLD for all kinds of abuse.

How do Interisle's methods differ from those used by ICANN Metrica and the NetBeacon Institute?

The main differences are that:

- Interisle uses more sources, consumes more data, and therefore becomes aware of more blocklisted domain names.
- The organizations count and report some things differently.

These differences are important to understand, because different conclusions can be gained (or obscured) depending upon how the data is selected and presented.

All three organizations do some of the basics similarly. All three place an emphasis on feed trustworthiness and reliability, all three gather a range of associated data such as domain registration records, and all de-duplicate their lists to report about unique second-level domain names. They use some similar methods to determine which domains were maliciously registered versus compromised. To learn about their methodologies, please see: ICANN Metrica FAQ and the NetBeacon Institute methodology (provided by KOR Labs).

Here are the data sources that each organization uses, and how many domains each source listed over the course of a year:

DATA SOURCES	ABUSE TYPES REPORTED	NUMBER OF UNIQUE DOMAINS LISTED BY THIS SOURCE IN 2025	INTERISLE	ICANN METRICA	NETBEACON INSTITUTE
APWG	phishing	207,812	✓	✓	✓
OpenPhish	phishing	95,412	✓		✓
PhishTank	phishing	100,097	✓	✓	✓
WMC Global PhishFeed	phishing	*(unknown)*		✓	
Spamhaus DBL	malware, phishing, botnet C&C, spam/malicious domains	9,773,569	✓	✓	
SURBL	malware, phishing, and other Abuse/spam domains	6,536,604	✓	✓	
URLHaus*	malware	11,503	✓	✓	✓
Invaluement	Risky domains found in bodies of spam messages	183,107	✓		
Malware Patrol	Malware, botnet C&C	17,042	✓		
Total number of sources			**8**	**6**	**4**
Total number of unique domains listed in 2025 by sources used			**14,855,456**	**< 9,831,489****	**375,311**

** URLhaus data is now also incorporated into the Spamhaus DBL*

*** See below about use of SURBL and Spamhaus*

There is some overlap in the domains that the above sources list. And each RBL lists some domains that are not found on any of the others.

Differences in Total Domains Identified

As illustrated above, NetBeacon uses far fewer sources than Interisle, and those sources list far fewer total domains than Interisle's data sources. Interisle's study set contains almost forty times as many domains as NetBeacon's.

Interisle and ICANN Metrica use multiple sources to learn about each type of abuse. In contrast, NetBeacon uses three sources of phishing data, and only one source of malware data. Because NetBeacon uses fewer sources that detect far fewer domains, NetBeacon's TLD and registrar domain counts and scores are significantly lower than Interisle's and ICANN Metrica's.

For example, for the November 2025 time period:

NetBeacon found 28,076 phishing domains, while Interisle found 299,369 – more than ten times as many.

NetBeacon reported that the .ICU TLD had 554 newly observed malicious domains (phishing + malware). Interisle found that .ICU had 8,683 new phishing domains alone in that period—more than 15 times what NetBeacon observed—plus additional domains flagged for malware and other problems.

Redactions and Transparency

NetBeacon redacts the names of some registrars and TLDs that have high levels of abuse. NetBeacon describes this choice as "a concept of consistency": a TLD or registrar will only be listed if they appear in the top ten "for 4 or more of the last 6 months, otherwise they will be redacted."

Interisle believes that such redactions are incompatible with studying the nature of domain abuse. It is common for spikes of abuse to occur when bad actors register domains in certain places, and for abuse to move between TLDs and registrars. As many researchers have documented, these spikes and movements often last less than four months, and some registrars display evidence of malicious batch registrations over short time periods only, as bad actors carry out malicious campaigns. Interisle therefore publishes unredacted statistics as a matter of transparency, and to reflect what happened where.

Differences Counting Abuse

ICANN Metrica subscribes to the SURBL and Spamhaus lists, but only counts a subset of the domains on those lists. Metrica counts only those domains that SURBL and Spamhaus specifically tag for phishing, malware, and botnet C&C. Metrica does not count domains that SURBL and Spamhaus do not specifically attribute to those abuse types. ICANN Metrica does not count those domains because ICANN's contractual definition of DNS just encompasses malware, botnets, phishing, and domains used to send email advertising those, and the last category is not tagged or differentiated in the feeds.

When Interisle studies particular abuse types, Interisle counts domains as phishing or malware when SURBL or Spamhaus specifically tag domains for those abuse types. In this report, Interisle counts all of the domains that Spamhaus and SURBL list because the domains have been blocklisted as risky, and the destinations and delivery mechanisms are often interrelated and problematic.

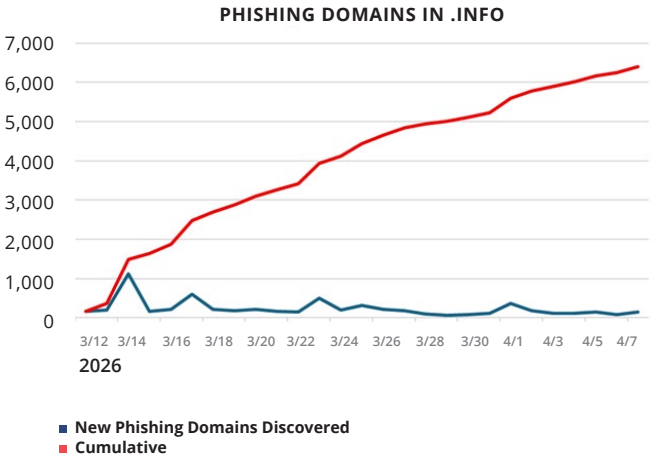
Differences in Choices of What to Display

ICANN Metrica provides the number of domains *that are currently on the blocklists* that ICANN monitors, *minus domains that are on the blocklists but do not appear in the zone file*. This is meant to represent how many domains may be active threats on a given day.

Domains are being added to and removed from the blocklists each day. Metrica's method tends to obscure that "churn" and does not give a picture of how many domains total are being listed over time. Also, certain providers

keep domains on their blocklists for longer periods of time than others. ICANN Metrica can therefore tend to emphasize the effects of those blocklists, and can tend to show that abuse is in a steady state:

In contrast, Interisle might display the number of domains that are *added to the blocklists* in a given time period. This reveals spikes and lulls, and the cumulative number found over time. Here's a chart for the same TLD (.info) and same time period as above.



We believe that the number of domains being listed for abuse is a useful indicator for the amount of criminal activity in a particular place, and it can be an interesting rough proxy for the amount of damage that is being done.

Endnotes

1. Federal Bureau of Investigations Internet Crime Complaint Center (ic3). Internet Crime Report 2025. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

2. With the country-code TLDs, or ccTLDs, being the other 37%. Verisign Domain Name Industry Brief Q1 2026. https://www.dnib.com/articles/the-domain-name-industry-brief-q1-2026

3. Interisle monitoring of blocklists.

4. ICANN monthly registry reports: https://www.icann.org/resources/pages/registry-reports

5. https://www.icann.org/octo-ssr/metrica/faqs-en

6. Nosyk, Korczyński, Maroofi, Bayuer, et al: "INFERMAL: Inferential Analysis of Maliciously Registered Domains." 2025. https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

7. ICANN Office of the Chief Technology Officer: "Insights and Clarifications on the INFERMAL Study." 10 June 2025. https://www.icann.org/en/system/files/files/insights-clarifications-infermal-study-10jun25-en.pdf

8. Lim, Sommese, Jonker, Mok, claffy, and Kim: "Registration, Detection, and Deregistration: Analyzing DNS Abuse for Phishing Attacks." 17 April 2025. https://arxiv.org/pdf/2502.09549

9. Korczyński, Wullink, Tajalizadehkhoob, Moura, and Hesselman. "Statistical Analysis of DNS Abuse in gTLDs Final Report" (SADAG). 9 August 2017. https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

10. Interisle Consulting Group (Aaron, Piscitello, Rose, and Strutt): "Phishing Landscape 2025: A Study of the Scope and Distribution of Phishing." https://interisle.net/insights/phishing-landscape-2025-an-annual-study-of-the-scope-and-distribution-of-phishing

11. Interisle Consulting Group (Piscitello, Rose, Strutt, and Wade): "Cybercrime Supply Chain 2025: Measurements and Assessments of Cyber Attack Resources and Where Criminals Acquire Them." https://interisle.net/insights/cybercrimesupplychain2025

12. Nosyk, Korczyński, Gañán, Maroofi, Bayer, Odgerel, Tajalizadehkhoo, and Duda: "Exposing the Roots of DNS Abuse: A Data-Driven Analysis of Key Factors Behind Phishing Domain Registrations." CCS '25: Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security. 2025. https://korlabs.io/documents/6/ccs2025-infermal.pdf

13. Cheadle, Gañán, Lloyd, and Tajalizadehkhoob: Security, Stability, and Resiliency Research, Office of the CTO, ICANN. "Detecting Malicious Domain Registration Batches: Patterns, Prevalence, and Security Implications." December 2025. IEEE: 2025 APWG Symposium on Electronic Crime Research (eCrime). https://www.icann.org/en/system/files/files/detecting-malicious-domain-registration-batches-13feb26-en.pdf

14. For additional breakdowns, see the Verisign Domain Name Industry Brief reports at: https://www.dnib.com/listing/report

15. Verisign "Q4 and Full Year 2025 Earnings Conference Call" presentation: https://investor.verisign.com/static-files/c1fa29cb-a44d-4c32-824d-3d53e0e7c923

16. The .COM and .NET TLDs make up 70% of the gTLD space. In 2025 .COM grew by 4.6 million domains, up 2.9%, while .NET shrank 2.2%. The new gTLD sector grew by 11 million domains, up 29.9%. The other older legacy gTLDs grew by 2.4 million domain name registrations, or 13.7%--most of that growth came from .INFO (which grew by 1.5 million domains) and .ORG (which grew by 519,000 domains). For quarterly Domain Name Industry Brief market reports, see https://www.dnib.com

17. Palo Alto Networks, "Strategically Aged Domain Detection." December 29, 2021. https://unit42.paloaltonetworks.com/strategically-aged-domain-detection/

18. Chiba, Nakano, and Koide, "DomainDynamics: Lifecycle-Aware Risk Timeline Construction for Domain Names." Computers & Security, 2025. https://doi.org/10.1016/j.cose.2025.104366

19. Cheadle, Gañán, Lloyd, and Tajalizadehkhoob: Security, Stability, and Resiliency Research, Office of the CTO, ICANN. "Detecting Malicious Domain Registration Batches: Patterns, Prevalence, and Security Implications." December 2025. IEEE: 2025 APWG Symposium on Electronic Crime Research (eCrime). https://www.icann.org/en/system/files/files/detecting-malicious-domain-registration-batches-13feb26-en.pdf

20. Infoblox 2025 DNS Threat Landscape Report, page 6. These included both gTLD and ccTLD domains. https://insights.infoblox.com/resources-reports/infoblox-2025-dns-threat-landscape-report/

21. https://www.iana.org/assignments/registrar-ids/registrar-ids.xhtml

22. https://www.iana.org/domains/root/db

23 See ICANN Registrar Accreditation Agreement (RAA), paragraphs 1.3, 1.4, 1.5, and 3.11.

24. Namecheap press release: https://www.namecheap.com/about/press-releases/24-04-16/the-new-domain-registration-web-services-platform-spaceship-wants-to-help-shape-the-unseen-future-internet/

25. Wise, Glaska, and Rocha, Infoblox. "Uncovering Actor TTP Patterns and the Role of DNS in Investment Scams." 28 April 2025. https://www.infoblox.com/blog/threat-intelligence/uncovering-actor-ttp-patterns-and-the-role-of-dns-in-investment-scams/

26. Interisle Consulting Group (Aaron, Piscitello, Rose, and Strutt): "Phishing Landscape 2025: An Annual Study of the Scope and Distribution of Phishing." September 2025. https://interisle.net/insights/phishing-landscape-2025-an-annual-study-of-the-scope-and-distribution-of-phishing

27. Cheadle, Gañán, Lloyd, and Tajalizadehkhoob: Security, Stability, and Resiliency Research, Office of the CTO, ICANN. "Detecting Malicious Domain Registration Batches: Patterns, Prevalence, and Security Implications." December 2025. IEEE: 2025 APWG Symposium on Electronic Crime Research (eCrime). https://www.icann.org/en/system/files/files/detecting-malicious-domain-registration-batches-13feb26-en.pdf

28. U.S. Department of the Treasury, "Treasure Takes Action Against Major Cyber Scam Facilitator." 29 May 2025. https://home.treasury.gov/news/press-releases/sb0149

29. Eduard Kovaks, SecurityWeek, "Polyfill Supply Chain Attack Impacting 100k Sites Linked to North Korea." 12 March 2026. https://www.securityweek.com/polyfill-supply-chain-attack-impacting-100k-sites-linked-to-north-korea/

30. Silent Push, "Infrastructure Laundering: Silent Push Exposes Cloudy Behavior Around FUNNULL CDN Renting IPs from Big Tech." 30 January 2025. https://www.silentpush.com/blog/infrastructure-laundering/

31. Silent Push, "Unveiling Triad Nexus: How FUNNULL CDN Facilitates Widespread Cyber Threats." 22 October 2024. https://www.silentpush.com/blog/triad-nexus-funnull/

32. Brian Krebs, Krebs on Security. "Infrastructure Laundering: Blending in with the Cloud." 30 January 2025. https://krebsonsecurity.com/2025/01/infrastructure-laundering-blending-in-with-the-cloud/

33. Quad9, "Trends H2 2024: Cyber Insights." 11 February 2025. https://quad9.net/news/blog/trends-h2-2024-cyber-insights/

34. Silent Push, "Post-Sanction Persistence: Triad Nexus' Operations Infrastructure Reborn as Threat Actor Distances Activity from FUNNULL CDN." 14 April 2026. https://www.silentpush.com/blog/triad-nexus-funnull-2026/

35. The Daily Tech Feed, "Funnull Unleashes RingH23 to Hijack CDN and MacCMS, Redirects Millions to Malicious Sites."https://thedailytechfeed.com/funnull-unleashes-ringh23-to-hijack-cdn-and-maccms-redirects-millions-to-malicious-sites/ and https://blog.xlab.qianxin.com/funnull-resurfaces-exposing-ringh23-arsenal-and-maccms-supply-chain-attacks/

36. U.S. Department of the Treasury, "Treasure Takes Action Against Major Cyber Scam Faclitator." 29 May 2025. https://home.treasury.gov/news/press-releases/sb014

37. See https://www.ic3.gov/CSA/2025/250529.pdf and https://www.ic3.gov/CSA/2025/Complete_List_of_Domains_Attributed_to_Funnull.zip

38. https://domainincite.com/23302-i-was-wrong-famous-four-bosses-were-kicked-out

39. Supreme Court of Gibraltar, including but not limited to case citation numbers 2025/GSC/022, 2023/GSC/044, 2021/GSC/17, 2019 Comp No 03, 2016 Comp Nos 09-11.

40. https://www.iana.org/domains/root/db/loan.html

41. https://circleid.com/posts/20140417_general_availability_period_for_new_pink_top_level_domain_opens

42. https://urlscan.io/result/0196a199-f77a-72ab-a963-b28cdca76177/

43. Per WHOIS and RDAP records, blocklistings from URLHaus, and other records.

44. Barnett, James, Infoblox Threat Intel: "RDGAs: The Next Chapter in Domain Generation Algorithms." 24 July 2024. https://www.infoblox.com/blog/threat-intelligence/rdgas-the-next-chapter-in-domain-generation-algorithms. For comment on associated domains, see "Barnett, David. "An Unnatural .Bond: A Study of a 'Megacluster' of Malware Domains." CircleID, 23 July 2024. https://circleid.com/posts/20240723-an-unnatural-dot-bond-a-study-of-a-megacluster-of-malware-domains#fn8

45. For how malware has been spread via advertising networks and domain parking platforms, see Infoblox, "Parked Domains Become Weapons with Direct Search Advertising, https://www.infoblox.com/blog/threat-intelligence/parked-domains-become-weapons-with-direct-search-advertising/ and "The Hidden Dangers of Malicious Adtech," https://www.infoblox.com/blog/threat-intelligence/the-hidden-dangers-of-malicious-adtech

46. For more about the malware and examples of its association to this series of .BOND domains, see for example: https://www.joesandbox.com/analysis/1705331/0/html and https://www.joesandbox.com/analysis/1488516/0/html

47. "How to Stand Out in Finance: Building Credibility in a Competitive Market." https://www.domaindiscount24.com/en/blog/how-to-stand-out-in-finance-building-credibility-in-a-competitive-market

48. Regarding this phishing technique, see KOR Labs, "Bulletin: DNS Abuse Campaign Exploiting "Subdomain Cloaking", https://korlabs.io/blog/bulletin-dns-abuse-campaign-exploiting-subdomain-cloaking/

49. .GIFT domains were included in the FUNNULL list published by the U.S. Federal Bureau of Investigation (FBI). See https://www.ic3.gov/CSA/2025/250529.pdf and https://www.ic3.gov/CSA/2025/Complete_List_of_Domains_Attributed_to_Funnull.zip

50. The clusters of associated domains we found displayed functional characteristics of FUNNULL, such as malicious advertising and redirection to yet more suspicious domains. An example is mzvzq.gift. This domain redirected, offered a suspicious APK download (see https://urlscan.io/result/9ca11650-c0d1-4109-ab42-bc76ea9ca944/), and was associated with 203.210.16.175 – an IP address blocklisted by Spamhaus. At one point mzvzq.gift redirected to suspicious destinations on other related domains such as such as bcnkvs.top (see https://www.virustotal.com/gui/url/1a7152589e957bc46cdfde458e7961b5db3939e805b0ca114ced65aa1fd3f910/details0)

51. We did not chart .GIFT's performance because of unexplained DUM anomalies in one of its reports to ICANN. https://www.icann.org/sites/default/files/mrr/gift/gift-transactions-202510-en.csv

52. Verisign DNIB, https://www.dnib.com/dashboards/gtld-registration-and-renewal-trends

53. Of the .ORG domains that came up for their first-year renewal in 2024, only 52.4% renewed. PIR Annual Impact Report 2024. https://pir.org/annual-impact-report-2024/

54. Spamhaus Domain Reputation Update, October 2025 – March 2026. https://content.spamhaus.org/4d83c22f-84c5-4f82-95ab-4e6b39f73db5.pdf

55. Affinito, Sommese, Akiwate, Savage, Claffy, Voelker, Botta, and Jonker. "Domain Name Lifetimes: Baseline and Threats." In TMA, pages 1–9, Austria, 2022. https://www.sysnet.ucsd.edu/~voelker/pubs/domain-lifetimes-tma22.pdf

56. Cheadle, Gañán, Lloyd, and Tajalizadehkhoob: Security, Stability, and Resiliency Research, Office of the CTO, ICANN. "Detecting Malicious Domain Registration Batches: Patterns, Prevalence, and Security Implications." December 2025. IEEE: 2025 APWG Symposium on Electronic Crime Research (eCrime). https://www.icann.org/en/system/files/files/detecting-malicious-domain-registration-batches-13feb26-en.pdf

57. Nosyk, Korczyński, Maroofi, Bayuer, et al: "INFERMAL: Inferential Analysis of Maliciously Registered Domains." 2025. https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

58. Interisle Consulting Group (Piscitello, Rose, Strutt, and Wade): "Cybercrime Supply Chain 2025: Measurements and Assessments of Cyber Attack Resources and Where Criminals Acquire Them." https://interisle.net/insights/cybercrimesupplychain2025

59. Lim, Sommese, Jonker, Mok, claffy, and Kim: "Registration, Detection, and Deregistration: Analyzing DNS Abuse for Phishing Attacks." 17 April 2025. https://arxiv.org/pdf/2502.09549. This comprehensive analysis of phishing domains focused on maliciously registered domains, DNS behaviors, and detection timelines, finding that attackers favored low-cost TLDs.

60. Affinito, Sommese, Akiwate, Savage, Claffy, Voelker, Botta, and Jonker. "Domain Name Lifetimes: Baseline and Threats." In TMA, pages 1–9, Austria, 2022. https://www.sysnet.ucsd.edu/~voelker/pubs/domain-lifetimes-tma22.pdf

61. Examples of how low price enabled abuse at scale include when new gTLD .INFO attracted significant malicious domain name registration as a result of "two-for-one" and registrar rebate programs in the early 2000s, (https://web.archive.org/web/20090215123646/https://www.prweb.com/releases/2008/11/prweb1580134.htm), when

.CN reduced prices in 2007 (https://docs.apwg.org/reports/APWG_GlobalPhishingSurvey2007.pdf), and into the new gTLDs from the 2012 round, when registrars and registries completed on price in a newly crowded market. ("Spamhaus Presents: The World's Worst Top Level Domains." 2016. "https://www.spamhaus.org/resource-hub/domain-reputation/spamhaus-presents-the-worlds-worst-top-level-domains/#introduction)

62. Nosyk, Korczyński, Maroofi, Bayuer, et al: "INFERMAL: Inferential Analysis of Maliciously Registered Domains." 2025. https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

63. https://nominet.uk/blog/growing-uk/

64. https://newgtldprogram.icann.org/en

65. ".com is Back as Verisign Discounts Bear Fruit." DomainIncite.com, 24 April 2025. https://domainincite.com/31007-com-is-back-as-verisign-discounts-bear-fruit

66. For example: https://web.archive.org/web/20260521152940/https://realtimeregister.com/solutions/domains/domain-promotions/specialpromotions

67. https://www.icann.org/octo-ssr/metrica/faqs-en