Phishing Landscape 2023

A Study of the Scope and Distribution of Phishing

Interisle Consulting Group, LLC

9 August 2023

Interisle
Consulting Group

Executive Summary

Phishing defrauds millions of Internet users every year. Phishing attacks deceive victims with web sites that appear to be run by a trusted entity, such as a bank or a merchant, but are in fact controlled by a criminal. The phishing page is designed to persuade a victim to provide information that the phisher can use to steal money directly or obtain credentials that can be sold to other criminals.

The role of our Phishing Landscape studies is to collect and analyze reliable and longitudinally consistent data that companies and policymakers can use to mitigate the threat of phishing. We publish these data regularly at the Cybercrime Information Center.

For this study we collected six million phishing reports from 1 May 2022 to 30 April 2023 from four widely used and respected threat intelligence providers: the Anti-Phishing Working Group (APWG), OpenPhish, PhishTank, and Spamhaus. From that data we identified more than 1.8 million unique phishing attacks. We also analyzed more than 11 million phishing reports collected over a three-year period, from 1 May 2020 to 30 April 2023. We added triennial measurements and analyses so that we could consider questions such as: "How has phishing evolved over a three-year period?" and "Are phishers doing business at the same registry, registrar, or web hosting services year after year?"

Phishing leverages Internet resources, exploits vulnerable technologies, and takes advantage of policy and legislative regimes that are siloed and often ineffective. Our study has measured and identified distinct and persistent patterns of exploitation and abuse over a three-year period, and stakeholders have known what is happening for a long time. But far from improving, the phishing landscape is worsening each year. Reviewing the data we have collected since 2020, we conclude that the prevailing uncoordinated and ineffective attempts to curb phishing are simply not working, and that a new strategy is required. In the report, we examine how policy regimes could fight phishing more pro-actively; how governments might encourage effective anti-phishing strategies; and how legal action against the individual organizations that provide resources to phishers could (and recently did) interrupt their criminal supply chain.

Our data show that:

The number of phishing attacks has tripled since May 2020

In addition, phishing attacks during this annual study period from May 2022 to April 2023 increased 65% over the previous study period (May 2021 to April 2022).

The number of unique domain names reported for phishing continues to increase

More than one million unique domain names were reported for phishing during the current period, the most we have observed since we began our observations in May 2020.

New gTLDs host a disproportionate and growing share of phishing domains

New gTLDs represent only 8% of registered domain names worldwide but 25% of domains used for phishing. Year after year, just 25 new gTLDs account for 90% of all new gTLD phishing domains.

Two-thirds of domain names reported for phishing across all TLDs were registered specifically to carry out phishing

Malicious domain name registrations are the most common way that phishers carry out their attacks. Preventing the registration of these domains, and taking them down quicky, should be a priority for the domain name industry.

Phishing that used subdomain providers more than doubled

More than 16% of all phishing attacks were launched from phishing pages hosted at subdomain service providers. 80% of those attacks were perpetrated using just eight subdomain service providers, illustrating how a service of this type can be used to create significant amounts of harm.

Freenom's demise redefined the phishing landscape

Phishing in the Freenom ccTLDs (.TK, .ML, .GA, .CF, and .GQ) was extensive for many years, because the domain names were free and Freenom anti-abuse measures were ineffective. In past years Freenom domains were used for 14% of all phishing attacks worldwide, and Freenom was responsible for 60% of the phishing domains reported in all the ccTLDs in November 2022. Freenom stopped offering registrations in January 2023, and its ccTLDs ceased to be a resource for new phishing domains.

Phishers prefer to host their web sites in the US

42% of all phishing attacks were concentrated in just five US-based hosting networks.

Criminals too easily acquire the resources they need for phishing

The current phishing mitigation strategy is not working. Stemming the persistent and growing tide of abuse will require effective mitigation measures and incentives for the organizations that — wittingly or not — facilitate cybercriminal activity. Coordination, cooperation, and consistent action across a broad range of stakeholders and actors in the phishing supply chain is the only effective way to make a significant impact on phishing.

Introduction

Phishing activities extract a heavy cost on society. Its victims often include multinational companies. IBM's 2022 data breach report estimated that the average recovery cost from a data breach where phishing was the initial attack vector, was nearly $4.45 million. The 2022 annual report by the U.S. Federal Bureau of Investigation's Internet Crime Complaint Center says that phishing is by far the most prevalent type of cybercrime complaint, with 300,497 victims reporting losses of $52 million in the U.S. alone. The report estimates another $2 billion in losses from a form of targeted phishing called business email compromise (BEC).

These figures vastly underestimate the damage. They are self-reported by individual victims, and most victims do not make reports to the FBI. Further, companies (such as banks) do not include the numbers of phishing victims or dollar losses for these reports. Finally, the numbers do not include estimates of lost business, time, credit report damage, or any third-party remediation services acquired by a victim.

While many large entities have expert resources at their disposal to identify and defend against attacks, small businesses, community organizations, small municipalities, and average consumers do not. Policy and industry discussions about phishing often focus on the challenges faced by large corporations and law enforcement, which are significant and legitimate. However, it is ultimately the average citizen, the Internet end user, that suffers from these attacks. In addition to costs associated with direct victimization, consumers pay higher prices for services when businesses must cover losses stemming from phishing.

The global economy suffers as well. The routine exploitation of Internet resources used by cybercriminals to launch phishing attacks negatively impacts consumers, businesses, and economies worldwide. Pervasive phishing and other cybercrimes contribute to a lack of consumer trust in online services, which in turn creates a drag on economic opportunity.

For this Phishing Landscape 2023 study we analyzed nearly 6 million phishing reports from phishing data feeds. These reports identified 1.8 million distinct phishing attacks. We examined phishing activity during the period from May 2022 to April 2023.

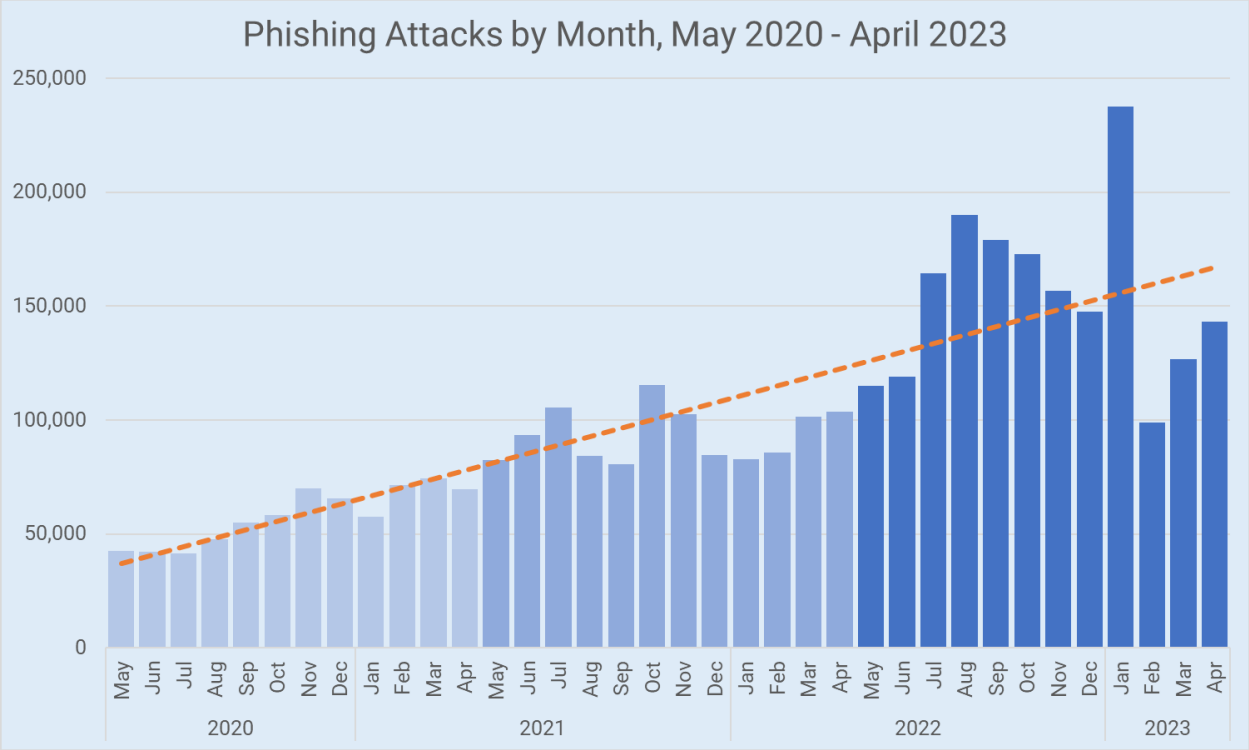
We looked at phishing activity from a variety of perspectives to understand how phishers perpetrate attacks, and specifically, where these criminals go to acquire the resources that they need to conduct phishing. We distinguish phishing attacks where domain names were registered by phishers from phishing attacks that were hosted on compromised domains or web sites. This distinction is important because it indicates where additional phishing prevention and mitigation efforts could be applied most effectively, and importantly, which operator (registry, registrar, hosting provider, subdomain provider) is best positioned to implement these.

To this end, we examined where phishing activity occurred among Top-Level Domain (TLD) registries, gTLD registrars, hosting providers, and subdomain resellers. We ranked these operators according to raw counts and comparative metrics. We concluded this study by reporting on brands most targeted by phishers.

From the study data:

- We observed a 65% growth in phishing attacks during the latest study period (May 2022 to April 2023) over the previous study period (May 2021 to April 2022) — this compares to the 61% growth that we had reported in our 2022 Landscape study.
- We observed noteworthy spikes in July and August 2022 and in January 2023.
- In the most recent months, the number of phishing attacks per month is nearly three times greater than in May 2020.

Monthly phishing attacks reported has tripled since 1 May 2020 and continues to trend upwards



Throughout the study, we provide year-over-year comparisons of phishing activity. By examining phishing behavior over a 36-month period, from May 2020 to April 2023, we identified domain name registration or hosting patterns that persist over time. From the longitudinal analyses afforded by a multi-year data set, we were able to illustrate (through trendlines) prevailing directions of various phishing metrics.

Monthly phishing attacks have tripled since May 2020

Our data show that the **largely independent efforts by the domain name and hosting industries, governments, and private sector organizations have done little to slow the growth of phishing** and the damage it causes to Internet users around the world. In the section *Building a Better Future: Policies,*

Practices, and Legislation on page 40 we review our findings in the context of measures that these parties should consider to effect change.

In this report, we show key statistics and trends to illustrate how phishing has evolved over a three-year period.

We investigate how phishers exploit the global domain name space (Top-level Domains, TLDs) and which domain name registrars they most often frequent to register domains purposely (maliciously) for phishing attacks. We review the effect on phishing when ccTLD operator Freenom, a perennial phishing haven, ceased offering domain registrations at five ccTLDs.

We also explain how criminals create user accounts to host phishing websites through subdomain service providers and which brands are most targeted by phishing attacks.

We closely examine malicious domain registrations, *i.e.*, how phishers register domain names purposely for phishing.

We look at the addresses where phishing web sites are hosted, the hosting providers (ASNs) that are most frequently misused to facilitate phishing attacks, and where these providers are geo-located.

We conclude our report with sets of recommended policies, legislation, and practices that the domain name industry, governments, and private sector should adopt to disrupt the phishing supply chain.

Key Statistics and Trends

We use data collected at the Cybercrime Information Center for our landscape studies (see FAQ). For this study, we collected over 1.8 million phishing reports over a one-year period, from 1 May 2022 through 30 April 2023. We use data from four widely used and respected threat data providers: the Anti-Phishing Working Group (APWG), OpenPhish, PhishTank, and Spamhaus. We augmented this data set with the data we used for our 2021 and 2022 studies to present year-over-year (comparative) measurements.

The statistics that we present in this report include both absolute metrics (*e.g.,* the number of domain names registered in a particular TLD that appear on a blocklist) and relative metrics (*e.g.,* a phishing score, representing the number of those domain names as a proportion of the total number of domains registered in that TLD). Attention to this distinction is critical to understanding and properly interpreting our analyses and findings.

Key statistics for this study period (May 2022 to April 2023) are compared with the corresponding statistics from the previous study period (May 2021 to April 2022) in the following table:

Phishing measurements all show increases over the prior period

Measurement	May 2021 to April 2022	May 2022 to April 2023	Change
Total number of phishing attacks	1,122,579	1,850,392	**+727,813**
Unique domain names reported for phishing	853,987	1,124,679	**+270,692**
Maliciously registered phishing domains	588,321	725,520	**+137,199**
Top-level domains where phishing domains were reported	660	699	**+39**
Registrars with domains under management reported for phishing	1,523	2,394	**+871**
Hosting networks where phishing web sites were reported	4,159	4,382	**+223**

Phishing attacks increased 65% (year over year) and showed a two-year increase of 166%. A phishing attack is a phishing site that targets a specific brand or entity. We determine if multiple phishing reports and URLs refer to the same phishing site and eliminate duplicates to yield the number of unique phishing sites. For more information about how we identify a phishing attack, visit the terminology page at the Cybercrime Information Center.

More than 1 million unique domain names were reported for phishing during the current period, the most we have observed in any period since May 2020

Unique domain names reported for phishing increased by 72% (year over year). This finding is based on our determination of "the first occurrence of a domain name in a phishing report". We use this number to account for domains which appeared in multiple phishing attacks in multiple quarters during the yearly period.

Two-thirds of domain names reported for phishing were maliciously registered. This finding is based on our determination that a domain name was purposely registered by a phisher to perpetrate a phishing attack. For more information about how we determine if a registration was malicious, visit the terminology page at the Cybercrime Information Center.

We obtained the numbers of TLDs, gTLD registrars, and hosting networks where we observed phishing by counting each operator that appeared in the yearly study data. The quarterly key statistics are:

Key statistics for each 3-month period				
Measurement (by Quarter)	**May 2022 – July 2022**	**August 2022 – October 2022**	**November 2022 – January 2023**	**February 2023 – April 2023**
Total number of phishing attacks	404,914	568,856	564,592	382,422
Phishing attacks associated with malicious domain registrations	227,457	364,800	370,195	185,828
Unique domain names reported for phishing	248,414	296,540	426,364	208,031
Malicious registered phishing domains	163,157	207,889	308,467	140,041
Top-level domains where phishing domains were reported	561	567	567	534
gTLD registrars with domains under management reported for phishing	502	576	661	713
All registrars with domains under management reported for phishing	1,163	1,309	1,302	1,320
Hosting networks where phishing web sites were reported	2,483	2,675	2,666	2,167

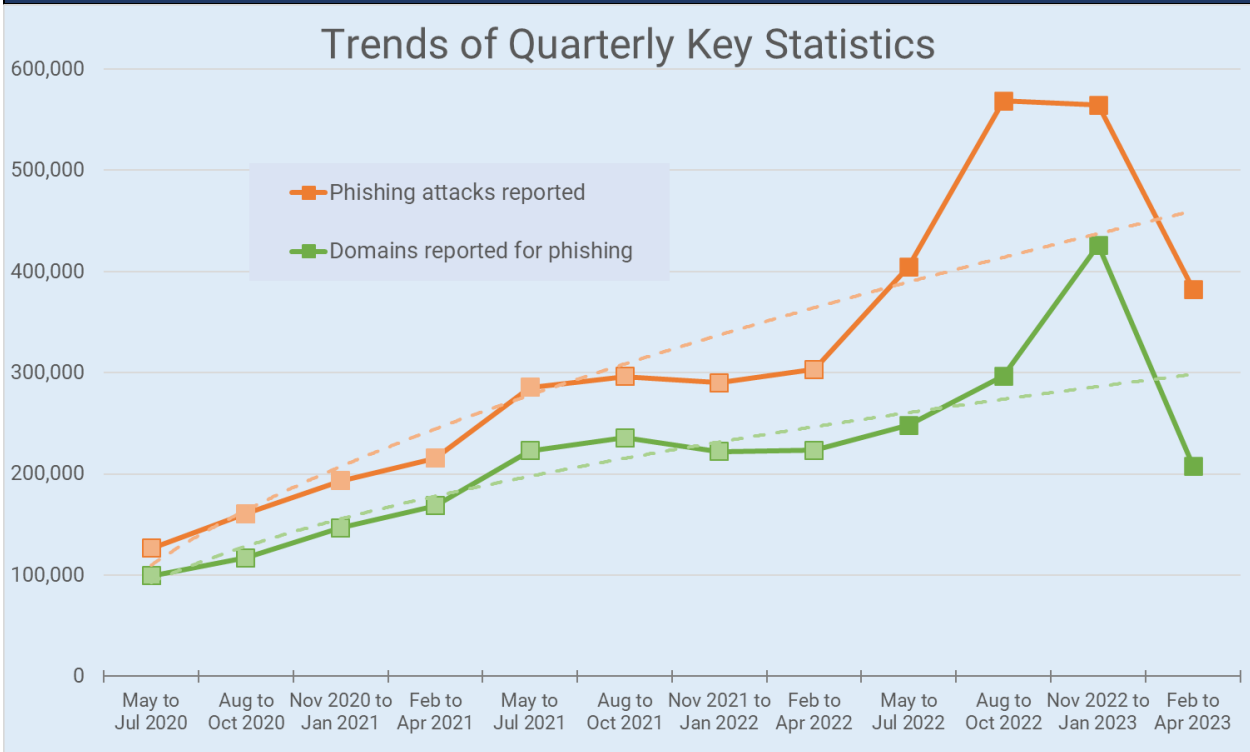
To obtain yearly measurements for TLDs or gTLD registrars, we performed a de-duplication of domain names and URLs that appeared in more than one quarter. As a result, the sum of the four quarterly numbers in the table below will not be the same as the cumulative numbers in the table on page 6.

Trends of Key Statistics

Phishing attacks and unique domains reported for phishing all trended up over the three-year period. The number of phishing attacks and unique domains grew steadily until a notable drop in February 2023. Much of that decline may be attributed to the collapse of the commercial ccTLD operator Freenom. We examine Freenom in some detail in the section entitled, *Nothing is Free: The Collapse of Freenom* on page 21.

We continued to observe a meaningful increase in phishing attacks hosted on subdomain service providers. We examine this later, in the section *Abuse of Subdomain Service Providers* on page 23.

3 years of data show that phishing remains a significant problem



The notable decrease in phishing in early 2023 is partly attributable to the collapse of Freenom. Freenom provided 14% of all phishing domains worldwide in 2022 but stopped offering registrations in January 2023. The number of its domains used for phishing then fell to virtually nothing by April 2023. Readers should not rush to make too much of the phishing decrease in early 2023. For more, see the section *Nothing is Free: The Collapse of Freenom* on page 21. Even with Freenom's contribution removed, **our three-year data show that phishing has without question increased significantly over time.**

We do continue to observe that a steeper decline in the number of unique domain names reported than the number of phishing attacks. This, combined with our observed increase in the use of subdomain

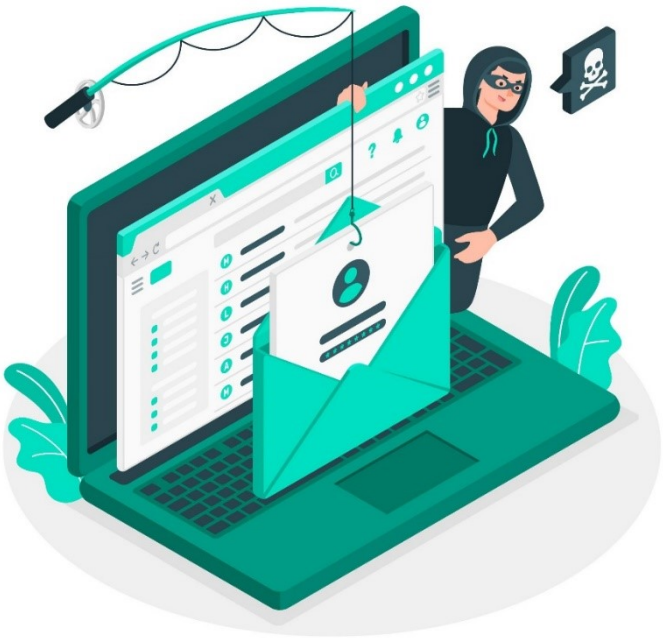
reseller services and other campaigns where multiple phishing websites are hosted on one domain, may signal a shift in phisher behavior.

Phishing *attacks* remain the most relevant metric, because it measures the number of phishing sites launched, and therefore the scope of phishing activity and the number of sites that are being used to victimize target organizations and their users. Other measurements — domain names, URLs, addresses, networks — identify the resources that phishers employ. Efforts to reduce criminal use of domain names are important and beneficial. But when these efforts are applied without complementary efforts to mitigate phishing on cloud services or web hosting, criminals still have numerous alternative resources to phish. The lamentable state of phishing indicates that more collaboration across the operators whose resources are used is necessary.

Phishing Activity

We define a phishing attack as a phishing site that targets a specific brand or entity. This is a basic measure of how much phishing activity is being observed, and in our opinion, the most accurate indicator of positive or negative change over time. By measuring phishing attacks, we can determine if multiple phishing reports (or more than one URL) refer to the same phishing site. When we do find this kind of activity, we eliminate duplicates to yield a count of distinct (unique) phishing attacks.

In past studies, we observed that phishing activity had been highest in the Monday through Wednesday period, and that blocklisting peaked around Wednesdays. Phishers advertise their attacks via spam mail at what they believe to be an optimal time, *i.e.*, when people check their work and personal email on returning to work or after the weekend is over. We also note that there is a delay between when an attack begins and when it is blocklisted — essentially, attacks do peak a bit earlier than reported.



In our May 2022 to April 2023 study period, we saw a slight shift in this pattern. The number of phishing attacks reported on Monday to Friday were reasonably consistent but were lower by about 20% on Saturday and Sunday. We are unable to ascertain whether this is a result of a change in phisher behavior or a change in reporting behavior.

Time Elapsed between Domain Appearance and Phishing

In previous Phishing Landscape studies, we analyzed how many days elapsed between when a domain name was registered and when that domain was associated with a phishing attack. This tells us about how phishers try to evade detection, and how they use domain names they register.

Sometimes we cannot obtain domain registration dates — such as for ccTLDs that do not publish WHOIS or from gTLDs where rate-limiting or other issues impede our collection system. To compensate, we have incorporated passive DNS data collected by ZETAlytics. Passive DNS shows when a domain name was first seen to resolve in the DNS. We use this "first appearance" date when no registration date is available from WHOIS.

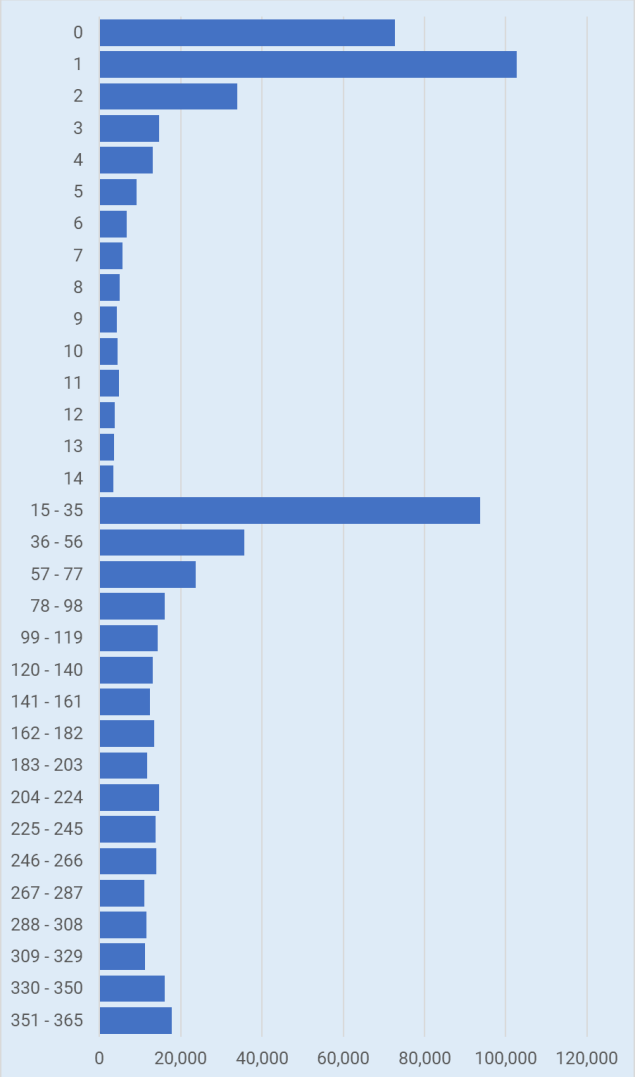
We consider any domain used for a phishing attack within 14 days of domain appearance to be maliciously registered. During the current study period **34% of gTLD domains reported for phishing were used within 48 hours following *domain appearance* and 46% were reported within 14 days**.

46% of gTLD domains reported for phishing were used within 14 days following domain appearance

This finding makes a case for gTLD registries or registrars to identify and preemptively block suspicious registration attempts. Registries and Registrars can leverage field experience and research that are currently employed to blocklist phishing domains. For example, registrars could monitor and investigate bulk registrations, where a party can register dozens, hundreds, or thousands of registrations from a single account in a very short time frame. Here, registrars could apply recommendations from academic research.[1, 2] As an alternative to accepting a registration that has a high probability of being used for phishing, the registrar can decline attempts to register domains that are suspiciously long, include an excessive number of hyphens or numbers, include brands (or brand similarities), or have observably suspicious composition patterns (*e.g.*, bandao###.com, bd#####.com, bdty###.com, ###bdty.com, bdvip###.com) .

[1] Malicious Domain Detection Using Machine Learning On Domain Name Features, Host-Based Features and Web-Based Features
https://www.sciencedirect.com/science/article/pii/S1877050920310383
[2] Understanding the Domain Registration Behavior of Spammers
http://conferences.sigcomm.org/imc/2013/papers/imc247-haoA.pdf

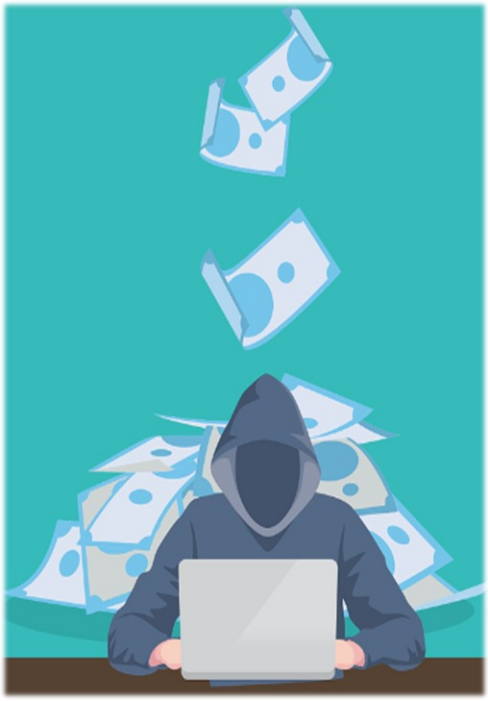
Number of days from first appearance of a domain to first report of phishing activity



For both gTLDs and ccTLDs, **85% of domain names associated with a phishing attack were reported within the first year of registration.**

With the inclusion of passive DNS data, we were able to perform this measurement for nearly one-half of the ccTLD domains.

We see a different elapsed time behavior from ccTLDs: 13% of the ccTLD domains reported for phishing were used within 48 hours following *domain appearance* and 20% used within 14 days.



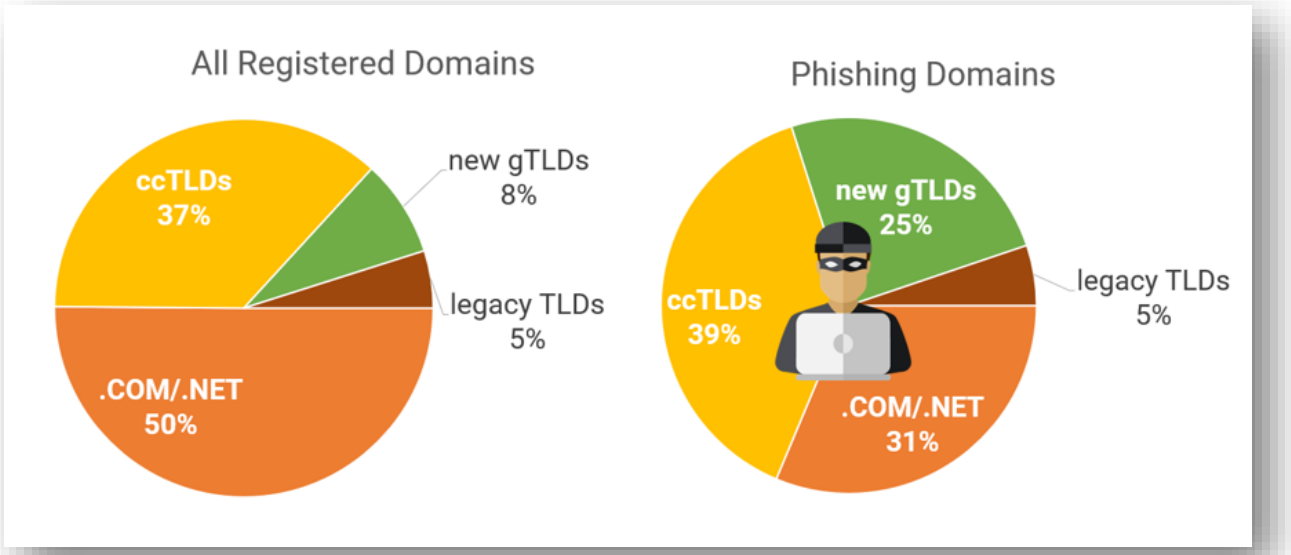
Phishing Distribution Across the Domain Name Space

According to Domain Tools, at the end of April 2023, there were over 344 million registered domains in the global domain name space. We observed phishing in 699 of the approximately 1,500 existing TLDs during the current study period.

For our studies, we divided the overall domain name space into four categories:

- the .COM and .NET registries, operated by Verisign, representing 50% of the domains in the world,
- the country-code domains (ccTLDs) representing 37% of the domains,
- the legacy generic TLDs – those other than .COM and .NET and introduced before 2013, *e.g.,* .ORG, .BIZ, .INFO – representing 5% of the domains, and
- the new gTLDs introduced from 2014 to the present (*e.g.,* .TOP, .LIVE, .REST, .SUPPORT, .CYOU) representing the remaining 8% of the domains.

We analyzed the phishing domains and attacks to see how they were distributed across the domain name space.



31% of all domains reported for phishing were in .COM and .NET, a slight decrease from 34% in the previous period. This percentage is significantly smaller than the combined market share (50%) of those TLDs, which increased slightly from 48% in the previous period. 5% of phishing was in legacy TLDs other than .COM and .NET, which is in line with their market share.

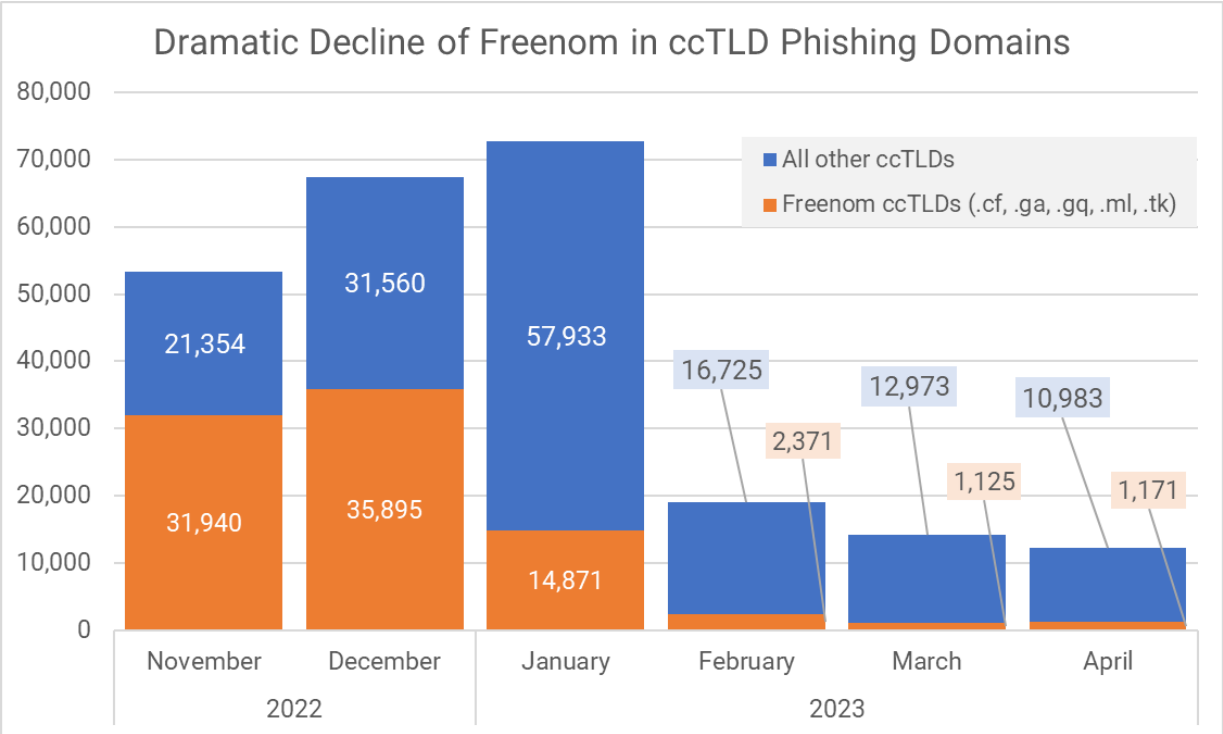
New gTLDs continued to attract phishers

Phishing activity continues to be a problem for the new gTLDs. In April 2020, new gTLDs represented 9% of domain names in the world but accounted for 18% of domains used for phishing. By April 2023, the new gTLDs' market share declined to 8% but their share of phishing domains grew to 25%. Our data show that, consistently, 90% of the phishing domains in new gTLDs are found in just 25 new gTLDs.

39% of domain names used for phishing were registered in ccTLDs. This is roughly in line with the market share represented by ccTLDs. Until early 2023, phishing in the ccTLD category was swollen by phishing domains reported in five commercialized ccTLDs run by Freenom (.TK, .ML, .GA, .CF, .GQ), which offered free domain name registrations. Our data revealed that Freenom's TLDs represented 19% of the ccTLD-registered domain names during the 2023 study period but represented 40% of all ccTLD phishing domains reported. Overall, Freenom's TLDs represented 8% of all registered domains yet accounted for 14% of phishing domains reported across all TLDs.

Freenom was responsible for over 60% of phishing domains reported in ccTLDs in November 2022, but that percentage dropped to under 15% by the end of April 2023

We observed a significant decline in phishing domains reported in the Freenom ccTLDs in 2023. The decline, while not entirely coincident with the cybersquatting and infringement complaint filed against Freenom, had an immediate impact. Freenom stopped processing new registrations: responsible for over 60% of phishing domains reported in ccTLDs in November 2022, Freenom's percentage has dropped to under 15% by the end of April 2023.



For more about the effect of Freenom on phishing in ccTLDs, please see the section *Nothing is Free: The Collapse of Freenom* on page 21.

Malicious Domain Registrations Across the Domain Name Space

We measured the number of unique phishing domains reported across a total of 699 TLDs. For our studies, we classify a phishing domain as being:

maliciously registered, for example, *registered to carry out a malicious or criminal act*. For example, a criminal often creates a domain registration account at one or more domain registrars, and uses these to register domains, singly or in quantity (bulk), using the same services as a legitimate user.

or

compromised, which we define as *domain names that were registered for legitimate purposes but co-opted by criminals* through some form of compromise. For example, a criminal may hijack a legitimate user's domain registrar account, alter the corresponding DNS entry to resolve a name or URL to a host that the attacker controls; here, the domain and DNS are compromised. An attacker may also exploit a vulnerability at a legitimate domain's web hosting and upload fake or malicious content to the web site; in this case, the web server is compromised.

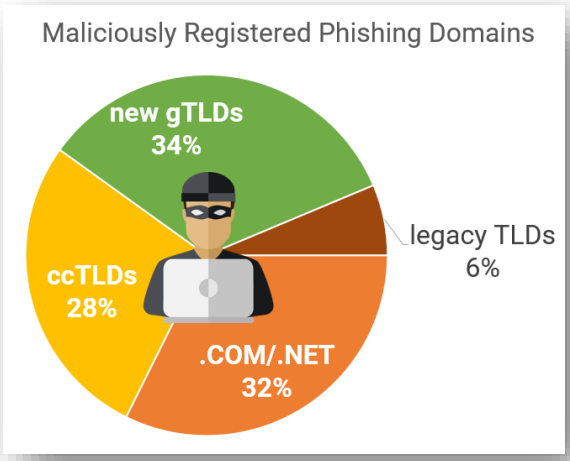
This distinction is important because it often identifies where investigators should go for assistance with mitigation of the criminal activity:

- If the domain is maliciously registered, an investigator will seek assistance from a domain name registrar, a TLD operator, or the operator that provides DNS for the malicious domain to suspend the domain name registration or name resolution. The investigator may also contact the web hosting provider.
- Suspending a compromised domain would harm the domain's legitimate registrant by bringing down the legitimate site's web site and email. Investigators will contact the hosting provider to have the malicious content removed.

Note that parties that discover phishing pages will do their best to blocklist URLs that identify malicious content to avoid further victimization, whereas they may block maliciously registered domain names (and thus all hostnames and URLs created using this name) to contain the pervasive malicious activity.

Visit the Cybercrime Information Center for details regarding our methodology for determining maliciously registered domain names.

When we studied where phishers registered domains purposely for phishing, we saw some meaningful differences in percentages from where phishing domains were reported.



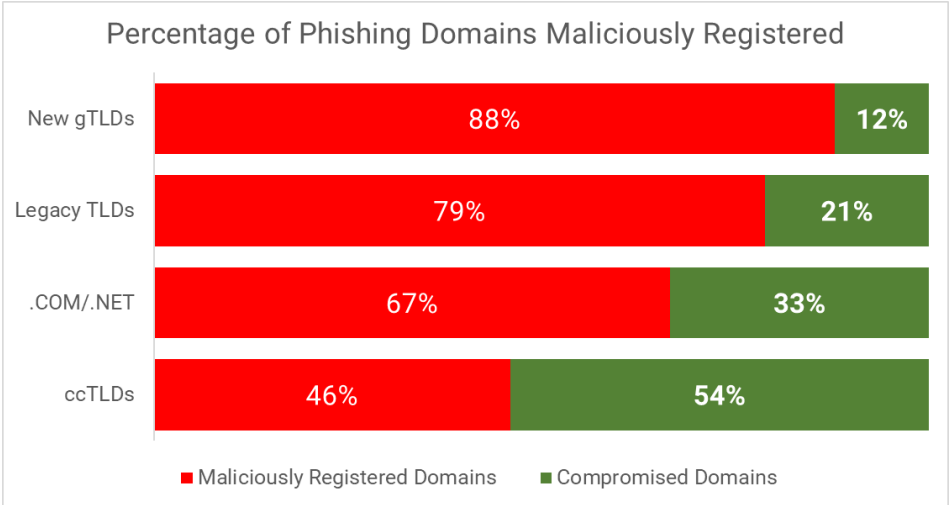
Together, .COM and .NET represent half of the domain name space overall. We determined that 40% of reported phishing domains in .COM and .NET were purposely (maliciously) registered for phishing. The remaining 60% were likely victims of some form of compromise by phishers.

New gTLDs continued to present attractive registration opportunities for phishers. We determined that 34% of all the maliciously registered phishing domains were in new gTLDs. This is more than four times the segment's market share and is consistent with our 2021 and 2022 study findings.

While the new gTLD program was intended to increase consumer choice, it also expanded the registration field for phishers. As competition among TLDs increased, some registry operators have sought to compete by offering low prices—sometimes as cheap as US$0.99, and sometimes even free. These cheap registrations have consistently attracted phishers, who wish to operate below fraud-detection thresholds or spend as little of their own money as possible. Registry operators and registrars who have competed on price have sometimes operated less-than-effective anti-abuse programs, as those programs cost money and effort.

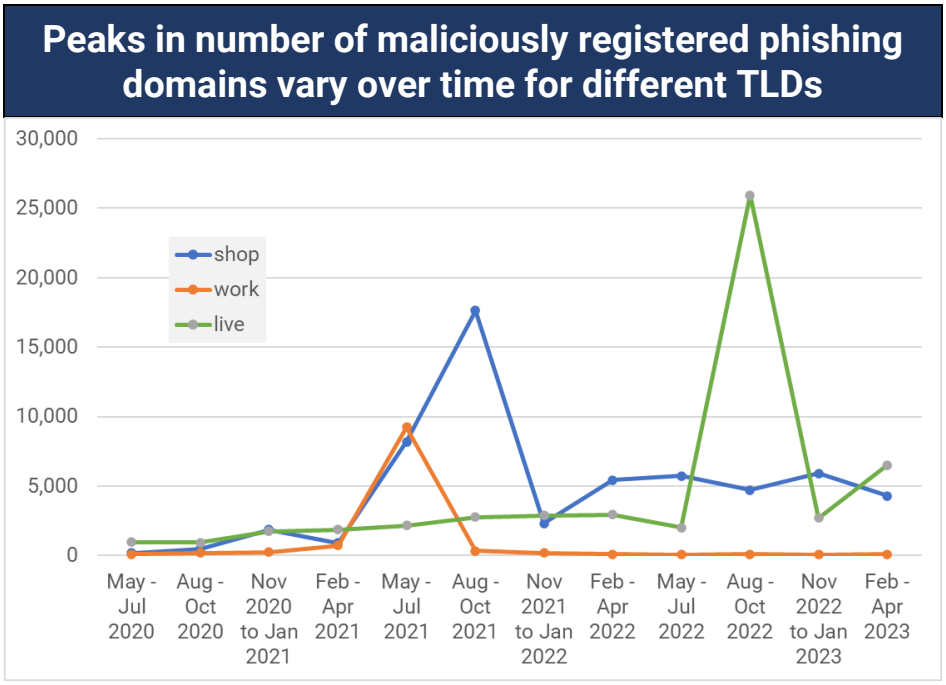
New gTLDs continue to have the highest percentage of maliciously registered phishing domains.

88% of all phishing domains in new gTLDs are maliciously registered



Our data show that phishers tend to exploit new gTLDs for intense periods, and then move on to other gTLDs. For example, one or more phishers appear to have concentrated their attention on the .SHOP TLD in summer 2021, perhaps until the reputation of the TLD faltered and became an impediment to launching an effective attack. They or other phishers then concentrated on another TLD, .LIVE in summer 2022, and exploited it in a similar manner.

Our data also show that phishers don't appear to rely entirely on a single TLD for phishing campaigns. For example, in summer 2021, criminals maliciously registered domain names in both .SHOP and .WORK using registrars DNSPod and NameSilo. Phishing registrations in .WORK dropped to previously low numbers in the fall, but we observed lingering effects in .SHOP for months thereafter. We observed a similar behavior In the fall 2022, when criminals exploited .LIVE using the registrar Sav.com, with a sharp decline to previous phishing numbers in early 2023.



The five ccTLDs operated by Freenom (.CF, .GA, .GQ, .ML, and .TK) accounted for 45% of all the malicious phishing domain registrations in the ccTLDs. The .CN ccTLD accounted for 23% and the .US ccTLD accounted for another 10% of malicious ccTLD phishing domain registrations.

ccTLDs operated by parties other than Freenom and .CN experienced little phishing generally, and relatively few malicious domain registrations particularly, than the gTLDs. We see few or no maliciously registered domains in ccTLDs that restrict registrations, such as .HU, .NZ, and .FI, where a connection to the country, a proof of identity, or evidence of incorporation are required, or .LK, where the acceptable use policy (AUP) includes a "lock and suspend" if domains are reported for suspicious activity. These **ccTLDs make a strong case for validating domain registrants in the interest of public safety**.

In contrast, the .US ccTLD has a "nexus" requirement that theoretically limits registrations to parties with a national connection, but .US had very high numbers of phishing domains. This indicates a possible problem with the administration or application of the nexus requirements. For more about the .US ccTLD, please see *Ranking of TLDs by Scoring Metrics* on page 19.

Ranking of TLDs by Phishing Domains Reported

Our 2023 study data showed that criminals took advantage of much of the global name space, registering domains primarily in the top-level domains that offered open registrations. Phishers also compromised domain registration accounts of unwitting registrants or broke into the hosting services of

web accounts. Some TLDs' registrar services, for reasons of pricing, operating practices, or business processes, appear to be more attractive to phishers than others.

For the 2023 study period, while the number of domains in .COM remained approximately the same from our 2022 study, the number of domains reported for phishing increased by over 55,000.

2023 Rank	TLD	Registry Operator	2023 Domains in TLD	Phishing Domains Reported ▼
1	com	Verisign	159,531,443	**333,158**
2	cn	CNNIC	7,363,700	**117,785**
3	ml	Freenom	1,630,164	**76,715**
4	top	Jiangsu Bangning	1,945,721	**53,286**
5	tk	Freenom	4,729,434	**41,798**

3-year comparison of TLDs with most phishing domains reported

Comparing our 2023 findings to prior studies, we found that:

- .COM continued to have the most unique domain names used for phishing — though that is to be expected due to .COM's great size and ubiquity.
- .CN, the ccTLD of China, had the second largest number of domains used for phishing. Curiously, the number of domains in .CN decreased by over 1.6 million from our 2022 study, but the number of phishing domains reported increased by 14,000. The 2023 and 2022 study numbers are dramatically higher than the 16,000 phishing domains reported in 2021.

- .TOP appeared in the top 10 most phished TLDs in 2021 with 15,000 domains reported for phishing, but dropped from the ranking in 2022. In 2023, .TOP's reported phishing domains increased 353% over the 2021 figure.
- Freenom's five ccTLDs also appeared in the top 20 in our 2021 and 2022 studies. We examine Freenom and its commercialized ccTLDs in detail in the section entitled, *Nothing is Free: The Collapse of Freenom* on page 21.

Ranking of TLDs by Scoring Metrics

The more phishing domains in a name space or portfolio controlled by one company, the greater the opportunity (and need) for that company to take effective anti-abuse measures — including measures to find and suspend malicious phishing registrations early. Scoring metrics allow for comparisons between TLDs of different sizes.

We use scoring metrics to compare whether a TLD has a higher or lower incidence of phishing relative to others. Scoring metrics allow for comparisons between TLDs of different sizes; for example, the metric "Phishing Domains per 10,000" shows whether a TLD has a higher or lower incidence of phishing relative to others. Refer to the Cybercrime Information Center terminology page which describes how we calculate the phishing domain score.

The following table shows the TLDs with the highest yearly phishing domain scores. While .COM is always the highest ranked by phishing domains, these TLDs have yearly phishing scores 20-30 times that of .COM.

Some TLDs have phishing domain scores 20-30 times that of .COM

Rank	TLD	Registry Operator	Domains in TLD	Phishing Domains	Yearly Phishing Domain Score ▼
1	rest	Punto 2012	39,700	2,940	**740.6**
2	live	Identity Digital	649,941	39,714	**611.0**
3	support	Binky Moon	32,705	1,603	**490.1**
4	ml	Freenom	1,630,164	76,715	**470.6**
5	cyou	Shortdot SA	314,942	13,356	**424.1**

High yearly phishing domain scores are problematic for TLDs. A person is more likely to encounter a dangerous domain when they click on a hyperlink in an email message or visit a web site address that contains a domain name registered in a TLD with a high yearly phishing score. When faced with a high likelihood of exposing a user to a maliciously registered phishing domain, risk-averse organizations are likely to blocklist entire TLDs.

The following table shows the gTLDs that had the greatest prevalence of malicious registrations and had more than 10,000 phishing domains over the year. The domains reported for phishing in these TLDs are highly likely to have been registered by criminals for phishing; few were compromised (hacked) domains.

gTLD	Phishing Domains	Malicious Phishing Domain Registrations	% Maliciously Registered ▼
cyou	13,356	13,010	97%
top	53,286	51,459	97%
live	39,714	36,938	93%
shop	22,151	20,211	91%
info	36,346	32,249	89%
online	20,476	16,682	82%
xyz	29,946	24,240	81%

The following table shows the ccTLDs that had the greatest prevalence of malicious registrations and had more than 5,000 phishing domains over the year:

ccTLD	Phishing Domains	Malicious Phishing Domain Registrations	% Maliciously Registered ▼
pw	7,533	5,759	76%
us	29,761	20,312	68%
ml	76,715	51,545	67%
ru	12,271	7,559	62%

Phishing activity in the #2 ranked .US ccTLD is notable. .US is the ccTLD of the United States and had a very large number of its domains used for phishing -- almost 30,000 domains, more than 20,000 of which were registered maliciously by phishers. The National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce administers the contract for .US. The NTIA recently published a proposal that would allow the TLD operator to redact registrant data from WHOIS, making it more difficult to identify phishers and verify registrants' identities and nexus qualifications.

Ironically, at least 109 of the .US domains in our data were used to attack the United States government, specifically the United States Postal Service and its customers. Significant numbers of .US domains were also registered to attack some of the United States' most prominent companies, including Bank of America, Apple, Microsoft, Meta, Amazon, AT&T, Citi, Comcast, and Target. .US domains were also used to attack foreign government operations: six .US domains were used to attack Australian government services, six attacked Great's Britain's Royal Mail, one attacked Canada Post, and one attacked the Denmark Tax Authority.

Nothing is Free: The Collapse of Freenom

For many years, phishers obtained hundreds of thousands of free domain names at a set of five commercialized ccTLDs. This long-standing concentration of abuse suddenly closed in early 2023, creating a dip in global phishing numbers.

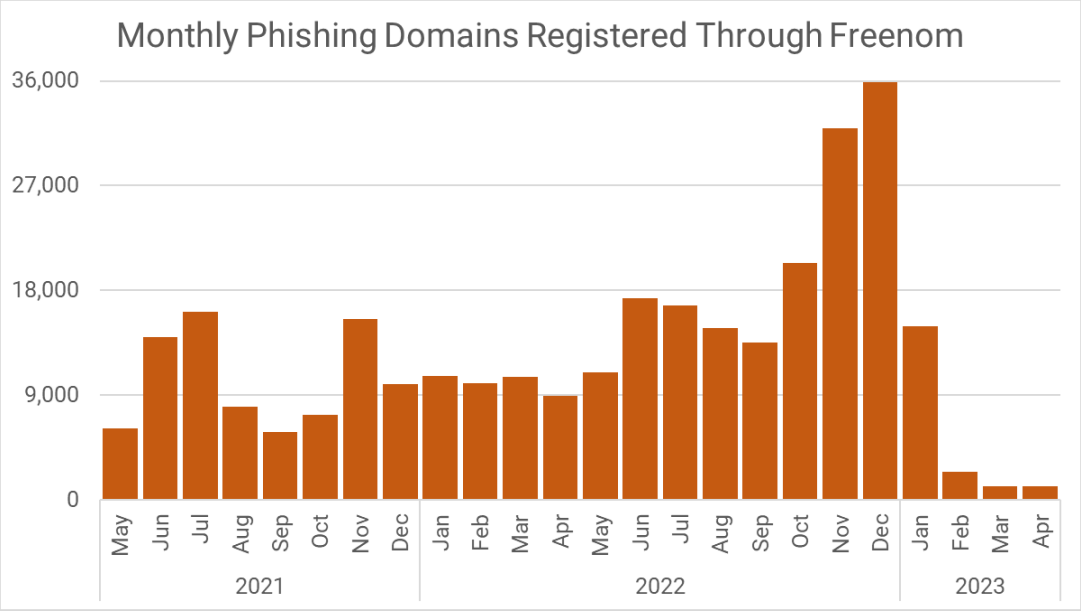
Freenom, a perennial hotspot of phishing, was shut down in early 2023, collapsed by the weight of cybercriminal activity

The ccTLDs — .TK, .ML, .GA, .CF, and .GQ — were operated by a Dutch company called Freenom, which negotiated contracts with the countries' governments. Freenom's business model was to give away the domain names for free, but to monetize the traffic to the expired domains by placing advertising on them. The free domains attracted phishers, and Freenom was criticized for not doing enough to prevent repeat use of its service by criminals.

Phishers used Freenom to register enormous numbers of domains. By 2013, about 28% of the world's malicious domain registrations were made in the Freenom registries. The abuse stayed persistently high over the years.

In our 2022 report, we found that more than 223,000 Freenom domains were used for phishing, accounting for 14% of all phishing domains reported in all TLDs. Freenom's five TLDs were all ranked in the top seven TLDs with the most phishing sites, along with .COM and .XYZ. The Freenom TLDs accounted for 45% of all the malicious phishing registrations in ccTLDs.

But in January 2023, Freenom stopped offering domains names. The number of Freenom domains used for phishing quickly plummeted:

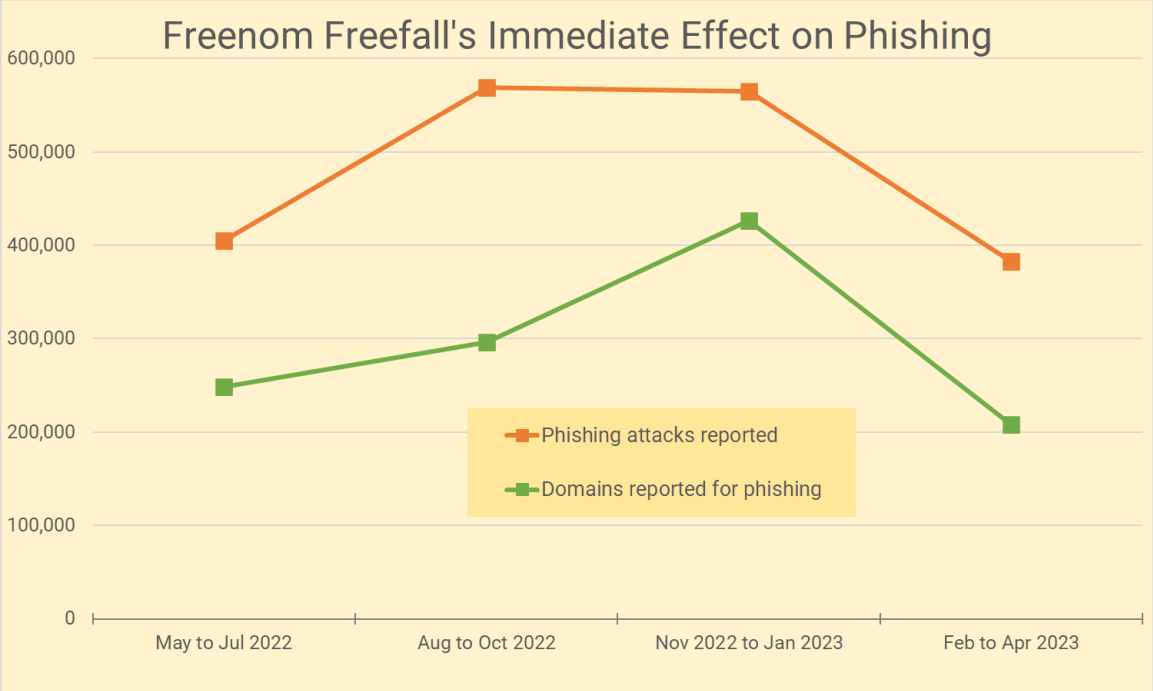


Freenom's closure was evidently prompted by two developments:

- Freenom was taken to court in Amsterdam by one of its investors, which asked the court for an investigation of Freenom's corporate conduct. The court made a decision in October 2022 and published it in late December 2022. The court found that Freenom had repeatedly violated

various reporting rules and obligations and the court appointed a supervisory director to the company's board. The full investigation is apparently underway as of this writing.

- In late 2022, Freenom was sued by Meta, the parent company of Facebook, Instagram, and WhatsApp. Meta alleged cybersquatting, trademark infringement, and violations of California's anti-phishing law, and its claims involved millions of dollars in potential damages. As of this writing, the case is ongoing.



In June 2023, security journalist Brian Krebs cited Interisle's Phishing Landscape studies and data from the Cybercrime Information Center to report that phishing using Freenom domains had dried to a trickle, evidently as phishers used up whatever remaining domain inventories they had.

On June 7, 2023 the Gabonese Republic took back management of .GA "due to the failure of the company Freenom… to provide the Internet community with a satisfactory service." The announcement noted that millions of .GA domains would be deleted because Freenom "has not provided the data that concern them."

On July 17, 2023 Freenom's contract with Mali's government expired, and the government took back control of its .ML ccTLD.

Freenom's free fall is a setback for phishers, but based on our multi-year data phishing is too lucrative to imagine that the setback is more than temporary. While it is possible that phishing attacks may decline in the near future, we believe that it is more likely that phishers will replace Freenom domain registrations, and the attack numbers return to their previous levels.

Abuse of Subdomain Service Providers

Our analysis reveals that 16.3% of all phishing attacks took place using resources at subdomain service providers. This is a growing vector for attacks, up from 12.8% in our 2022 report and 10.7% in our 2021 report.

Subdomain services give customers services on a domain name that the provider owns. This gives users their own DNS space, using a third level domain of the format:

subdomain.domainname.tld

Some of these providers are web hosts or offer website-building services. Some offer just the third-level domain with free DNS management so the domain owner can point it to other hosting. Phishers use the domains and hosting offered by these providers to build and maintain phishing sites.

These phishing attacks are difficult to mitigate and pose persistent problems for phishing targets for several reasons. Many of these companies offer the services for free. Some offer anonymous registration, with little to no identity validation. Some don't even validate the user's email address when they create an account. Finally, only the subdomain service providers can effectively mitigate these phishing attacks.

Subdomain service providers often lack effective, proactive measures to keep criminals from creating accounts and abusing their services, and some pay little attention to complaints. Some phishing kits — software used by phishers to launch and manage their phishing sites — integrate the use of subdomain providers, allowing the phishers to sign up for and use subdomains in an automated fashion. This allows the phishers to launch large numbers of attacks, and to abuse these services repeatedly.

We identified 302,086 phishing attacks created on 671 second-level domains using subdomain service providers. Use of these services for phishing was up 111% from our 2022 report, when we identified 143,506 subdomains on 731 second-level domain names.

Of those 302,086 attacks, 80% of them (240,702) occurred on domains operated by just eight providers. This emphasizes how a service of this type can be used to perpetrate significant amounts of damage, and how important it is for such providers to have proactive and quick anti-abuse monitoring and takedown capabilities. The top providers (with a minimum of 6,000 phishing attacks) were:

Rank	Provider	Domains	Phishing attacks
1	DuckDNS	duckdns.org	**77,667**
2	Google	Blogspot domains, appspot.com, firebaseapp.com, web.app, business.site	**77,580**
3	Hostinger	000webhosapp.com, preview-domain.com	**22,781**
4	Weebly	weebly.com	**19,035**
5	Replit	repl.co	**16,256**
6	CentralNIC	com.de, ae.org, br.com, cn.com, de.com, eu.com, gb.net, jpn.com, ru.com, sa.com, uk.com, uk.net, us.com, za.com	**13,636**
7	Cloudflare	trycloudflare.com, workers.dev	**7,585**
8	Square	square.site	**6,162**

Subdomain Service Providers	Profile	Primary Brands Targeted
DuckDNS	**DuckDNS** offers fee dynamic DNS services, which allow one to access devices from the Internet via a simple-to-remember domain name and can obscure the real location of the hosting. DuckDNS also offers subdomains to users. These services are all attractive to phishers.	Apple Facebook WhatsApp
Google	**Google** had phishers repeatedly take advantage of Google services that offer subdomains and hosting. These included 47,819 phishing sites mounted on Google's Blogspot blog-building service. At least 16,261 phish were launched on Google's web.app, and another 14,094 phishing attacks were mounted on firebaseapp.com; these Google services allow users to "build and deploy your websites and apps without managing any infrastructure."	Facebook Instagram Microsoft
Hostinger	**Hostinger** is a hosting provider that offers free hosting on its 000webhostapp.com domain. This free service has been used prolifically by phishers for years.	Facebook Instagram
Weebly	**Weebly** offers a free website builder service, which is used frequently by phishers. Weebly is a subsidiary of Square, the payment processing company. Combining phishing attacks using Weebly subdomains under Square, would rank Square at #3.	AT&T Yahoo BT Group
Replit	**Replit** provides a range of tools for software development. Among these are features that phishers misuse to create phishing sites: web hosting services, free HTTPS for static websites, and subdomains on Replit's domain replit.co.	Banco Galicia Bancolombia

In 2016, APWG reported subdomain services were used for only 5.3% of phishing attacks. Our data reveal a much higher percentage, 16%, which suggests that these services are becoming more attractive to phishers. Phishers have learned how to create accounts in bulk at some of these services, and so it is imperative that the providers implement better anti-abuse measures.

Phishing Distribution Across gTLD Registrars

Phishers acquire domain names by registering domain names purposely for phishing. They also use the domains of innocent registrants by breaking into their hosting or domain management services. The table below shows that phishers purchase and manage domain names through many gTLD registrars. Some gTLD registrar services, pricing, or practices appear to be more attractive to phishers than others. We consider this phenomenon in the section *Malicious Domain Name Registrations and gTLD Registrars* on page 30.

Ranking of gTLD Registrars by Phishing Domains Reported

The registrars with the most gTLD domains used for phishing attacks (minimum 30,000) were:

Rank	Registrar	Registrar IANA ID	gTLD Domains under Management	gTLD Phishing Domains Reported ▼
1	NameSilo	1479	4,452,651	**73,725**
2	PublicDomainRegistry	303	4,429,499	**68,400**
3	NameCheap	1068	14,666,675	**50,652**
4	GoDaddy	146	65,664,751	**50,339**
5	Sav.com	609	1,633,675	**31,328**

3-year comparison of gTLD registrars with most phishing domains reported

2021 study	2022 study	2023 study
1. NameCheap	1. NameCheap	1. NameSilo
2. NameSilo	2. GoDaddy	2. PublicDomainRegistry
3. GoDaddy	3. NameSilo	3. NameCheap
4. PublicDomainRgistry	4. DNSPod	4. GoDaddy
5. Tucows Domains	5. ALIBABA.COM SINGAPORE	5. SAV.COM

How does this compare with the results in our 2022 Landscape study?

- In 2022 **NameSilo** was #3, with 42,487 domains. NameSilo's phishing problem increased 73% between 2022 and 2023.

- In 2022 **NameCheap** was #1 with 88,643 phishing domains. Since then, NameCheap's phishing problem has decreased by 43%. However, NameCheap's absolute number is still very high.
- In 2022, **PublicDomainRegistry** (PDR) was #6, with 21,948 domains. PDR's phishing problem grew by a staggering 310% from 2022 to 2023.
- **GoDaddy** was #2 in 2022, with 44,160 phishing domains. GoDaddy's number of phishing domains increased 14% from 2022 to 2023.
- **SAV.com**, with 4,230 phishing domains in our 2022 study, experienced a 720% increase in 2023.

Ranking of gTLD Registrars by Scoring Metrics

Gross numbers alone can be biased against registrars that sponsor large numbers of domains, some of which may be compromised and belong to innocent registrants. As we do with TLDs above, we compare whether a gTLD registrar has a higher or lower incidence of phishing relative to others. This is a ratio of the number of domain names used for phishing to the number of registered domain names under management at that gTLD registrar. The highest-scoring gTLD registrars by yearly gTLD registrar phishing score is:

Rank	Registrar	Registrar IANA ID	gTLD Domains under Management	Phishing Domains	Yearly Phishing Domain Score ▼
1	NICENIC INTERNATIONAL	3765	50,833	13,474	**2650.64**
2	TLD Registrar Solutions	1564	71,753	1,675	**233.44**
3	REG.RU	1606	650,515	13,157	**202.26**
4	Sav.com	609	1,633,675	31,328	**191.76**
5	ALIBABA.COM SINGAPORE	3775	693,065	12,539	**180.92**

gTLD Registrar	Profile	Largest counts of Phishing Domains in…
NiceNIC	NiceNIC is located in Hong Kong. A full 26% of its domain portfolio was used for phishing.	.COM
TLD Registrar Solutions	TLD Registrar Solutions is a subsidiary of registry operator CentralNIC, and is based in the U.K.	.DEV, .ONLINE, .FINANCIAL, .APP
Reg.RU	Reg.RU *(a.k.a.* Registrar of Domain Names Reg.ru) is located in Russia. Its phishing domains were roughly half in the legacy TLDs and the rest in new gTLDs.	.COM, .ORG, .INFO .XYZ, .SITE, .SHOP, .SPACE, .FUN

gTLD Registrar	Profile	Largest counts of Phishing Domains in…
Sav.com	Sav.com offers domain registrations and website-building services and is located in the U.S. Its phishing domains were split among gTLDs and the legacy gTLDs.	.LIVE, .BAR, .BEST, .XYZ .COM, .INFO
Alibaba.com Singapore	Alibaba.com Singapore is an arm of the ecommerce company Alibaba and is located in Singapore. Its phishing domains were primarily in .COM, and across a number of new gTLDs.	.COM .TOP, .CYOU, .ICU, .XYZ

Malicious Domain Name Registrations

In the section *Malicious Domain Registrations Across the Domain Name Space* on page 15, we identified where phishers registered domain names purposedly for phishing in the global domain name space. Here, we take a closer look at the name space to identify TLD operators and registration services (gTLD registrars) where malicious registrations are most prevalent.

Malicious Domain Name Registrations and TLDs

For the study period, we determined that 65% of the domains reported for phishing across all TLDs were registered maliciously by phishers (725,520 of the 1,124,684 domains reported for phishing). This percentage is slightly lower than our findings from our 2022 Phishing Landscape study where we found that 69% were maliciously registered. The remaining 35% were domains that we classified as compromised domains, or domains associated with subdomain services.

65% of phishing domains in all TLDs were maliciously registered

57% of all phishing attacks were hosted on maliciously registered domains

We observed a strong correlation between phishing attacks and maliciously registered domain names. 57% of all phishing attacks were hosted on maliciously registered domains. TLD registries and gTLD registrars could be more proactive to mitigate maliciously registered domains promptly and take preemptive measures against suspiciously composed domains names (*e.g.*, domains that impersonate brands or bulk registrations of randomly composed strings).

We identified 12 TLDs with 1,000 or more malicious phishing domain registrations from 1 May 2022 to 30 April 2023.

2023 Rank	2022 Rank	TLD	Registry Operator	Domains in TLD	2023 Malicious Phishing Domain Registrations ▼
1	n/a *	ml	Freenom	76,373	**51,545**
2	1	com	Verisign	50,469	**28,412**
3	7	live	Digital Identity	21,372	**21,242**
4	n/a *	tk	Freenom	40,978	**18,832**
5	6	info	Digital Identity	15,475	**14,539**
6	n/a *	us	Registry Services	8,582	**8,405**
7	n/r **	cyou	ShortDot SA	5,097	**5,056**
8	5	top	Jiangsu Bangning	5,322	**4,769**
9	2	shop	GMO Registry	5,739	**4,513**
10	3	xyz	XYZ.COM	4,082	**3,423**

2023 Rank	2022 Rank	TLD	Registry Operator	Domains in TLD	2023 Malicious Phishing Domain Registrations ▼
11	11	online	Radix FZC	3,510	**2,668**
12	10	net	Verisign	2,215	**1,144**

* ccTLDs were not ranked in the 2022 study, for lack of ccTLD domain registration data

** was not ranked in the 2022 study

Counts of phishing domains help us to identify where domain names reported for phishing were registered. We use a complementary analysis — one in which we can consider malicious or criminal intent on the part of an unknown subject (registrant) — to identify prevention or mitigation opportunities for individual TLDs. Specifically, we discriminate maliciously registered phishing domains from compromised domains (web sites) to identify the parties that are best positioned to combat phishing.

Experience in the field has demonstrated that:

- Maliciously registered phishing domains can be suspended by the registrar or registry operator; this stops the attacks and will not cause any damage or inconvenience to anyone except the phisher.
- Registries with high numbers of maliciously registered domain names can collaborate with their registrars to adopt phishing identification and prevention measures.
- Hosting network operators are best suited to mitigate vulnerabilities for compromised web sites hosting phishing pages. They are also able to deploy measures to detect compromises and to recommend content management practices that can reduce their customers' web vulnerability attack surfaces.
- Phishers are highly unlikely to remove the phishing pages from a hosting server. The responsibility to remove fraudulent phishing content, disable an unauthorized web server, or suspend accounts of subscribers who are perpetrating phishing falls upon hosting operators. Typically, these are violations of the operator's own acceptable use policy.

gTLDs Where Malicious Domain Registrations Dominate in Phishing Reports

In some gTLDs, malicious phishing domain registrations account for the majority of reported phishing domains for the yearly period. This is particularly the case for new gTLDs with a minimum of 1,500 reported phishing domains. **We observed 96 new gTLDs where over 90% of the reported phishing domains were maliciously registered, and 145 new gTLDs where over 80% of the reported phishing domains were maliciously registered**.

New TLDs have extraordinarily high percentages of malicious registrations intended for phishing

Legacy TLDs with more than 1,500 reported phishing domains had a *lower* percentage (68%) of malicious registrations compared to new gTLDs (89%). In the legacy TLDs, we observed more compromised web sites; in particular, the percent of domain names purposely registered for phishing in

.COM was the same as the 65% we determined for the overall domain name space, and both .NET and .ORG were much lower (59% and 58% respectively).

Malicious registrations dominate phishing domain counts in the new gTLDs:

New gTLD	Malicious Registrations	Compromised web sites	% Malicious ▼
cyou	13,010	346	97%
top	51,459	1,827	97%
live	36,938	2,776	93%
shop	20,211	1,940	91%
site	8,539	1,879	82%
online	16,682	3,794	81%
xyz	24,240	5,706	81%

However, malicious registrations are less prominent in most legacy TLDs:

Legacy TLD	Malicious Registrations	Compromised Web Sites	% Malicious ▼
info	32,249	4,097	89%
com	223,364	109,794	67%
net	11,228	7,847	59%
org	8,962	6,636	57%

Malicious Domain Name Registrations and gTLD Registrars

Counts of phishing domains help us to identify where domain names reported for phishing were registered. Further analysis is needed to understand what acts of prevention or mitigation are appropriate for gTLD registrars. By identifying characteristics of maliciously registered domain names and distinguishing these from compromised domains, we can identify which parties are best positioned to act to prevent phishing.

The classification 'compromised domains' represents the set of domains where the domain name owner who operates a legitimate web site may be a victim. Here, investigators should seek out hosting providers to mitigate phishing attacks (*e.g.*, by having the phishing page and related content removed from the compromised web site).

The classification 'maliciously registered phishing domains' represents the set of domains that were purposely registered for phishing, by an actor with criminal intent (to commit fraud). Here, a gTLD registrar is often well positioned to (proactively) identify a domain as "intended for phishing"; for example, only a gTLD registrar has the means to:

- examine a domain name such as amazongjgasb14sjh21saknx.icu, appleidsupport-us.com, or customersupport-netflix.com during registration,
- detect a trademark or brand within the domain name (*e.g.*, Amazon, Apple, Netflix), and
- suspend the registration while it reviews the registrant's contact data to assess the legitimacy of the registration.

The maliciously registered classification also represents the types of domains where investigators should seek the assistance of gTLD registrars to mitigate phishing attacks (*e.g.*, by suspending the domain name or registrant account). For example, when a phishing investigator determines that a phishing campaign is using dozens or more domain names containing random patterns, only a gTLD registrar can determine during the early hours of a phishing attack whether the contact data for a set of verified phishing domains is the same (an historically reliable indicator of a phisher). The gTLD registrar should review the evidence of phishing presented by a phishing investigator quickly and accommodate requests to reveal the contact data of a registrant once they verify the evidence.

The following table shows gTLD registrars with more than 20,000 malicious phishing domain registrations under management from 1 May 2022 to 30 April 2023.

Rank	Registrar	Registrar IANA ID	Malicious Phishing Domain Registrations May 2022 to April 2023 ▼
1	NameSilo	1479	**63,472**
2	PublicDomainRegistry	303	**40,269**
3	NameCheap	1068	**35,425**
4	GoDaddy	146	**25,437**
5	Sav.com	609	**29,598**

We next compared malicious phishing domain registrations to compromised domains, by gTLD registrars. The raw numbers of maliciously registered domains are important — they indicate where phishers registered the most domains.

Malicious registrations directly influence the reputations of the gTLD registrars that are most targeted by phishers when they register domains purposely for phishing. In some cases, a gTLD registrar's malicious domain registration can also have a disastrous effect on the phishing score of a Top-level Domain and consequently on that TLD's reputation. For some TLDs, one gTLD registrar adversely influences a TLD's reported phishing domain counts month after month.

Which gTLD registrars had an adverse effect on which gTLDs, and to what degree? In the following table, we identify gTLD registrars where the registrar's share of all maliciously registered phishing domains in the TLD was at least 40% and thus had a significant influence on a particular gTLD's phishing domain count.

Registrar	TLD	Registrar's share of maliciously registered phishing domains in TLD (%) ▼
Onamae.com	rest	**90**
Sav.com	live	**68**
HiChina (www.net.cn)	shop	**59**
HiChina (www.net.cn)	icu	**54**
NameSilo	info	**52**

Phishing Attacks by Hosting Networks (Autonomous Systems)

We studied where phishing sites were being hosted, to determine if any hosting providers have outsized phishing problems. We collected the IP addresses (DNS A records) that phishing attacks were resolving to. We then looked up the **Autonomous System Number (ASN)** containing each IP address. This provides insight into the hosting network where the phishing web pages were hosted.

The following sections consider phishing hosted on IPv4 addresses only. We do not see IPv6 addresses reported for phishing in our feeds.

Ranking of Hosting Networks (ASNs) by Phishing Attacks Reported

We found phishing in 4,382 hosting networks, a 5% increase from our 2022 study. Ten of the top hosting providers accounted for 55% of the 1,469,835 phishing attacks for which an ASN could be determined.

Five hosting networks accounted for 42% of those phishing attacks (minimum 50,000 attacks).

2023 Rank	Hosting Provider	AS Number	# Routed IPv4 Addresses	Phishing Attacks ▼
1	Cloudflare	13335	2,531,584	**228,010**
2	QuadraNet Enterprises	8100	2,751,232	**134,460**
3	ColoCrossing	36352	785,920	**130,265**
4	Google	15169	11,992,832	**66,563**
5	Unified Layer	46606	811,520	**52,529**

3-year comparison of Hosting Networks with most phishing domains

2021 study	2022 study	2023 study
1. NAMECHEAP-NET	1. CLOUDFLARENET	1. CLOUDFLARENET
2. CLOUDFLARENET	2. UNIFIEDLAYER	2. QUADRANET
3. UNIFIEDLAYER	3. MICROSOFT	3. COLOCROSSING
4. GOOGLE	4. NAMECHEAP-NET	4. GOOGLE
5. DIGITALOCEAN	5. GOOGLE	5. UNIFIEDLAYER

Our data continued to show that US hosting networks were attractive to phishers. We used RIPEstat geo data (per Maxmind GeoLite) to determine the countries where IP addresses reported for hosting phishing attacks for each of ASNs had the most reported phishing attacks**.**

One third of all phishing attacks were concentrated in five US-based hosting networks

The top ranked hosting networks (ASNs) are operated by US based entities:

Hosting Network	Description
Cloudflare	San Francisco CA based Cloudflare provides a DNS redirection service that protects its customers from denial-of-service attacks. Cloudflare's service also prohibits observers from seeing the real hosting locations behind this defense network, and phishers take advantage of this to hide the hosting locations of phishing pages.
QuadraNet Enterprises	A Los Angeles CA based data center provider, providing colocation, dedicated servers, cluster management, and complex hosting solutions.
ColoCrossing	A US based provider of colocation and cloud services, dedicated servers, data centers, and managed services.
Google	Google is also one of the largest network providers. ASN 15169 is delegated to Google LLC, Mountain View, CA and is aliased as Google, YouTube.
Unified Layer	A San Francisco CA based provider of managed cloud services, secure enterprise-class cloud, co-location, and disaster recovery services.

In the United States, efforts to mandate accurate contact information from Internet as a Service operators,[3] or to oblige web hosting services, DNS services, or domain registration services to "lock and suspend" [4] accounts or domains while they investigate a (criminal) complaint may provide protections against phishing attacks.

Ranking of Hosting Networks (ASNs) by Scoring Metrics

The gross numbers of phishing attacks reported are significant. Here, as with TLDs and gTLD registrars, more phishing attacks means more damage and victimization. A heavily abused ASN can enable many attacks.

Gross numbers influence how one compares operators who have more or fewer IP addresses than each other (numbers bias). In the quarterly phishing activity published at the Cybercrime Information Center,

[3] H.R. 6352: DRUGS Act
https://www.govtrack.us/congress/bills/117/hr6352

[4] Executive Order 13984 of January 19, 2021, Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities
https://www.federalregister.gov/executive-order/13984

the Phishing Attack Score metric "Phishing Attacks per 10,000" is used to compare whether a hosting network (AS) has a higher or lower *incidence* of phishing relative to others.

Rank	AS Name	AS number	# Routed IPv4 Addresses	Phishing attacks	Phishing Attack Score ▼
1	Namecheap	22612	74,432	22,913	**3078.38**
2	A2 Hosting	55293	126,720	33,953	**2679.37**
3	ColoCrossing	36352	785,920	130,265	**1657.48**
4	DediPath	35913	282,624	31,632	**1119.23**
5	Interserver	19318	129,280	12,121	**937.58**

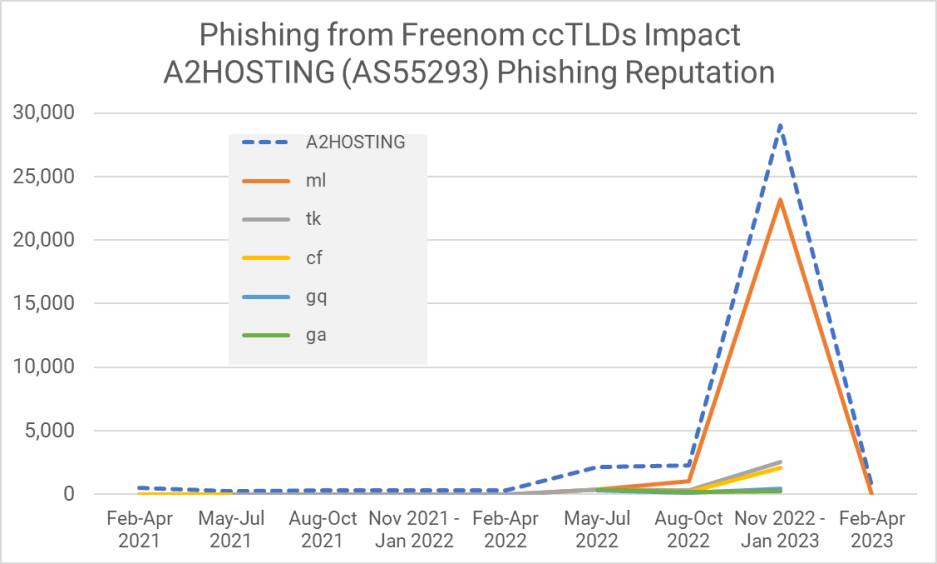
Brands and individuals of victims of phishing attacks are the most obvious harmed parties, other parties such as hosting operators received collateral damage from phishing attacks. We identified three case studies to illustrate these collateral effects.

Fallout from Phishing Attacks — Three Case Studies

While brands and individuals of victims of phishing attacks are the most obvious harmed parties, other parties such as hosting operators received collateral damage from phishing attacks.

Case Study #1: A2 Hosting

A2 Hosting offers a diverse set of hosting solutions. Historically, A2 Hosting typically had very few IPv4 addresses reported for hosting phishing. However, we observed a huge uptick in phishing attacks reported during the November 2022 to January 2023 quarter. Looking at phishing activity reported, we see an uptick in phishing attacks reported in the Freenom ccTLDs in the November 2022 to January 2023 period corresponding to phishing attacks in A2 Hosting.



The chart compares phishing attacks hosted at A2HOSTING to phishing domains registered in the Freenom ccTLDs

Reviewing the phishing data more closely, we found that:

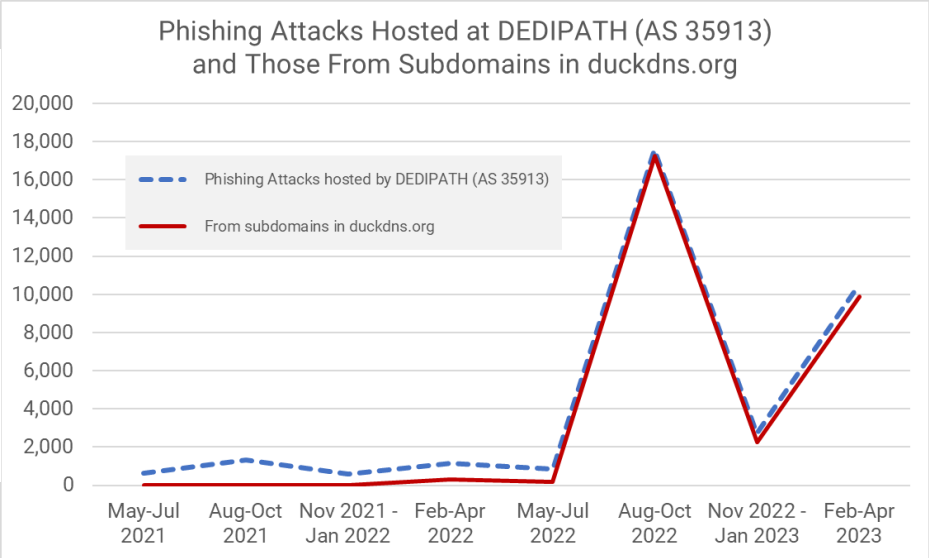
- The domain names that resolved to nearly all of IP addresses reported for phishing in these prefixes were registered in ccTLDs operated by Freenom (.CF, .GQ, .TK but predominantly .ML).
- The domains were pseudo-randomly generated names containing 10 or more numeric characters. Some sets of these domains were entirely composed of numbers, *e.g.*, 10000000000259638[.]ml. In others, English language words or hyphen(s) were prepended to the numeric string, *e.g.*, attention-42423428857201[.]ml.
- Sequentially ascending sets of numeric strings appear in most of the domain name compositions, suggesting that they were registered by the same actor, at the same time. Freenom does not make domain creation dates publicly available, so we were unable to confirm this speculation, but over 20,000 reported phishing domains in our data match these patterns: the domain appearance for over 90% of these domains fell within 15 days of registration.

Given that tens of thousands of pseudo-randomly generated domains were purposely registered in Freenom's commercialized ccTLDs by phishers, for phishing, each hosting a unique attack, and that a tenfold increase in phishing attacks at A2 Hosting coincided with these registrations, it's reasonable to assert that A2 Hosting could be added to the victim count.

Case Study #2: DEDIPATH

Like A2HOSTING, DEDIPATH offers a number of hosting services. We observed a huge uptick in phishing attacks reported at DEDIPATH during the August 2022 – October 2022 period. DEDIPATH typically had very few IPv4 addresses reported for hosting phishing, but phishing attacks launched using the from accounts created at the subdomain service provider, DUCKDNS.ORG vaulted DEDIPATH into our "phishiest" hosting networks in our 2023 study.

The chart compares phishing attacks hosted at DEDIPATH to phishing attacks from duckdns.org subdomains



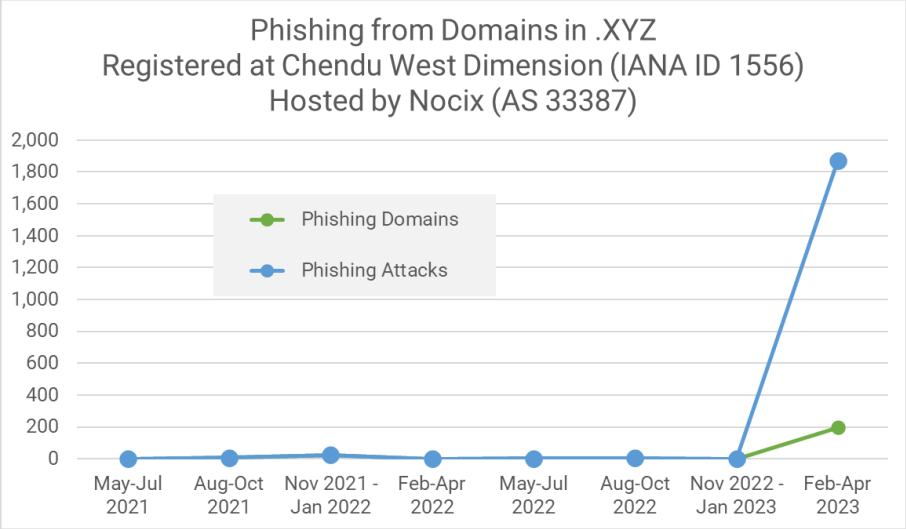
In this case, DEDIPATH or the .ORG TLD could be added to the victim count.

Case Study #3: NOCIX

NOCIX (AS 33387) is a low-cost virtual server and cheap dedicated server provider. We observed an unusual spike in this usually phishing free hosting network of nearly 2000 phishing attacks between 12 March 2023 and 27 April 2023. Reviewing the phishing data, we found that:

- The domain names that resolved to nearly all of IP addresses reported for phishing in these prefixes were registered in the .XYZ TLD through Chengdu West, Ltd. (IANA ID 1556).
- The domains were pseudo-randomly generated names of the form <1 letter><English word><3 random letters>.XYZ (*e.g.*, plovelypya[.]xyz, ljawldi[.]xyz, and junclejqx[.]xyz).

In this case, NOCIX or the .XYZ TLD could be added to the victim count.



The chart compares phishing attacks to phishing domains in .xyz registered through Chendu West Dimension

Managing fallout

In each of these case studies, there was a near 1:1 correspondence between domain name registrations or subdomain account creations and spikes in phishing activity at mostly phishing-free hosting networks.

Coincidence or not, it is likely that all the hosting providers identified in these case studies had to deal with issues that most hosting operator must when confronted with a large-scale phishing event:

- The abuse desk staff must contend with an more complaints than typical of the past.
- The site admins must invest time and manpower to mitigate the phishing content and optimally, identify how the phishers exploited hosting account(s).
- Relationships management staff must request de-listing from multiple blocklist operators.
- Public relations staff must triage the organization's tarnished reputation.
- Customer relations staff must reconcile discontent or frustration of legitimate customers experience harms or losses if the prefixes or perhaps entire ASN of their hosting provider are blocklisted by orgs and ISPs worldwide.

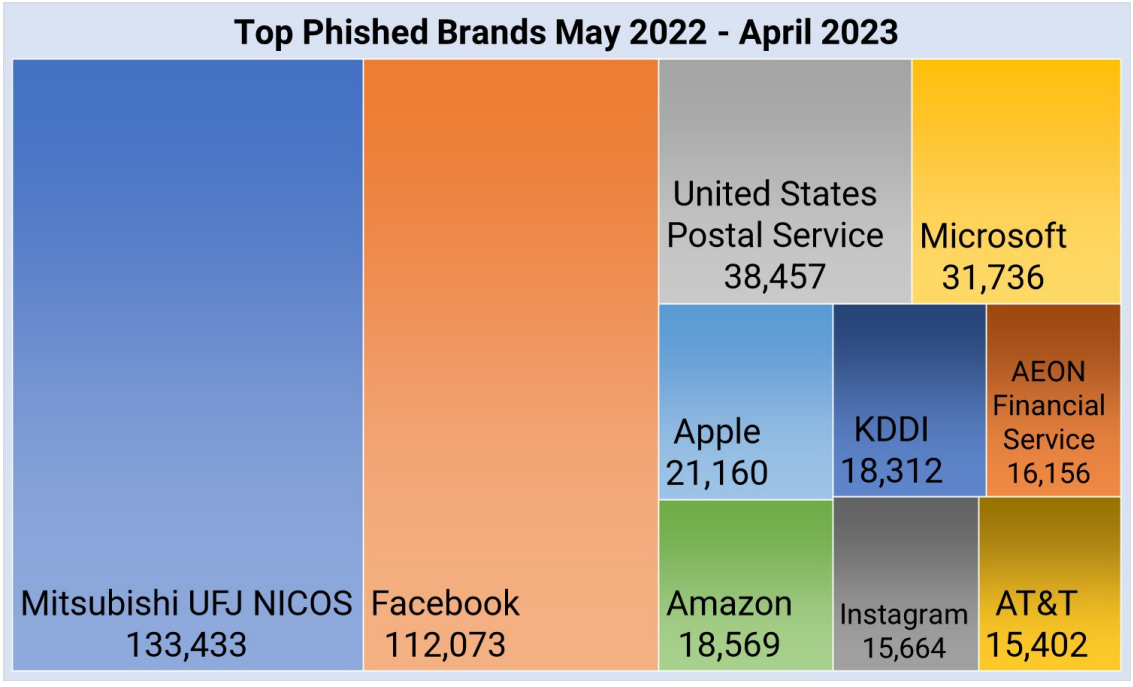
If Freenom, DuckDNS, the .XYZ registry, or Chengdu West Dimension Digital Technology — or generally, any registry, registrar or subdomain service provider — were to have implemented some form of a suspicious registration behaviors program *and* had preemptively blocked the domains or accounts, they would have made a substantial contribution to mitigating phishing attacks and reducing phishing victimization.

Targeted Brands

Phishers cast a wide net during the 1 May 2022 to 30 April 2023 period, targeting nearly 4,200 businesses or organizations, more than doubling the targeted brands we identified in our 2022 Phishing Landscape study.

This behavior tells us that a brand can become a phishing target at any time. Phishers constantly look for companies that have potentially lucrative user information, are newly popular, or are not ready to respond to phishing.

The Cybercrime Information Center terminology page describes how we identify brands.



For the first time since we began reporting, Facebook was not the most targeted individual brand. Japanese credit company Mitsubishi UFJ NICOS Co., Ltd. was the target of over 133,000 phishing attacks during the months of April and May 2022, involving 5,200 unique domains reported for phishing. The very large ratio of phishing attacks versus unique phishing domains illustrates how criminals can weaponize domains for mass phishing attacks.

We determined that 73% of these Mitsubishi phishing domains were maliciously registered. We also identified an interesting nexus in phishing attacks on the Mitsubishi brand:

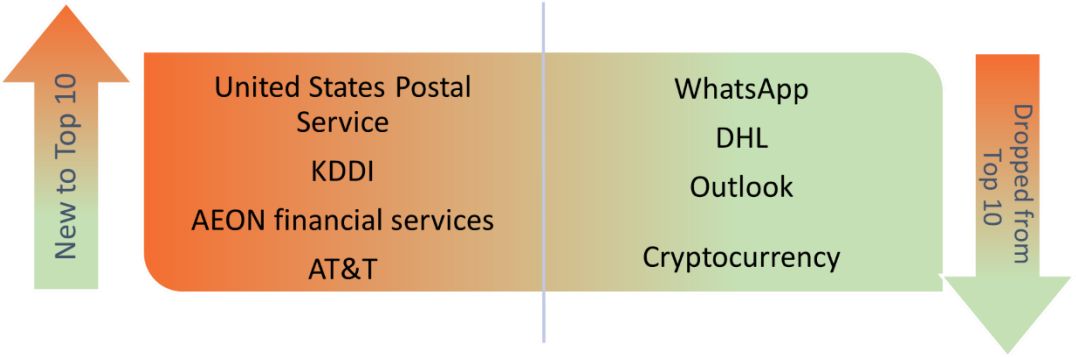
- The .TOP and .CN TLDs had the most unique domains reported for phishing.
- The registrar most frequently used was "Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)".
- 85% of the phishing attacks were hosted in a single ASN, 36352 (AS-COLOCROSSING).

Despite dropping in rank to the second-most-targeted brand, phishing against Meta's Facebook brand more than doubled in volume, from 53,000 attacks reported in our 2022 Phishing Landscape study to more than 112,000 in this latest study. We identified nearly 25,000 unique domains used to phish Facebook; of those, we determined 60% were maliciously registered. Almost all the rest of the attacks, about 38%, occurred at subdomain providers. The TLDs with the most unique domains reported for phishing Facebook were in .COM (with nearly 7,000 domains), .ML, .TK, .ID, .CLICK, .TOP, .CN,.PL, and .GA. We note that the five Freenom ccTLDs (.ML, .TK, .GA, .CF, .GQ) together had nearly 7,000 unique domains reported for phishing Facebook.

Meta's Instagram brand was also among the top ten-most-phished targets. Adding Meta's Facebook, Instagram, and WhatsApp brands together, Meta was the most-targeted company or family of services overall.

We observed other changes in the most targeted brands:

- United States Postal Service, KDDI, AEON financial services, and AT&T joined the top 10.
- DHL and Meta's WhatsApp dropped from the top 10.
- Cryptocurrency/Wallet phishing dropped from the top 10.
- Amazon phishing more than doubled.



Building a Better Future: Policies, Practices, and Legislation

Our study has measured and identified distinct and persistent patterns of exploitation and abuse of Internet resources over a three-year period. Stakeholders have been aware of these patterns for some time. Yet instead of the situation improving, however, our *Key Statistics and Trends* on page 6 show that the situation is worsening each year.

We need a better strategy. We call on the players who are in positions to disrupt the phishing supply chain: the global domain and web hosting industries, governments, and in the extreme, the parties most adversely affected by phishing.

Actions for Effective Change

We should strategically starve phishers and other criminals of easy access to resources. The volume and scale of phishing amply illustrate that criminals can trivially acquire everything they need to phish. We must adopt effective mitigation measures and incentivize the organizations that, wittingly or not, facilitate cybercriminal activity in order to stem the persistent and growing tide of abuse. These companies include hosting providers, domain companies, email providers, and DNS providers. Action by individual industry segments is necessary but has proven insufficient.

Coordination, cooperation, and consistent action across a broad range of stakeholders and actors in the phishing service chain is the most if not the only effective way of creating change. Specific recommendations follow.

Domain Industry

We are in urgent need of domain name industry policies and practices that can stem the tide of DNS resource abuse**.** At a minimum, the following improvements in industry policies and practices are necessary if the ICANN organization and the domain name community are committed to mitigating phishing within their remit.

Registry and Registrar Agreement Modifications

ICANN has just proposed new contractual obligations, which it negotiated with its registries and registrars. ICANN claims that these are designed to be more enforceable. However, the requirements sacrifice a great deal in the interest of "enforceability" and are lacking in several ways:

- ICANN's new proposal apparently narrows the definitions of what registrars and registries must act against. The contracts formerly required the registrars to "investigate and respond appropriately to any forms of abuse," including "illegal activity." **The new contract narrows the list of abuses** to just "malware, botnets, phishing, pharming, and spam." While easy to grasp, this excludes a variety of harmful and related activities, including a wide variety of scams (such as 419 and advance-fee-fraud scams) and child sexual abuse images.
- **ICANN has adopted a new, non-standard, narrow definition of spam.** Industry advocacies including M3AAWG and CAUCE define spam as "bulk unsolicited email" (which is generally illegal to send in most countries). The ICANN contracts will narrow the definition of spam to a subset: only "when spam serves as a delivery mechanism for the other forms of DNS Abuse" — *i.e.*, phishing, malware, etc. This may excuse registrars from responding to most spam reports, since much spam advertises products and scams of other types. It is also very confusing because domain names used for phishing are often *not used to send the email,* but rather are *advertised*

or contained in the body of the email, as the location the victims are asked to go. It is unclear which usage — the former, latter, or hopefully both — that ICANN will require action against.

- **ICANN's new contract language does not require registrars and registry operators to suspend domain names under any circumstances**. Instead, the language may allow them to pass responsibility to other parties entirely. The contracts merely state that the registrar "must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse." A registrar may argue that an "appropriate" action is to refer all problems to the hosting provider. This issue is related to…
- **The new contracts do not impose any obligations to suspend domains that are maliciously registered**. These are domains where a customer has registered domains in order to perform abusive actions. These domains can and should be suspended by the registrar or registry operator, and doing so causes no collateral harm to any other party. **Two-thirds of domain names used for phishing are maliciously registered, so this is a big part of the problem.**

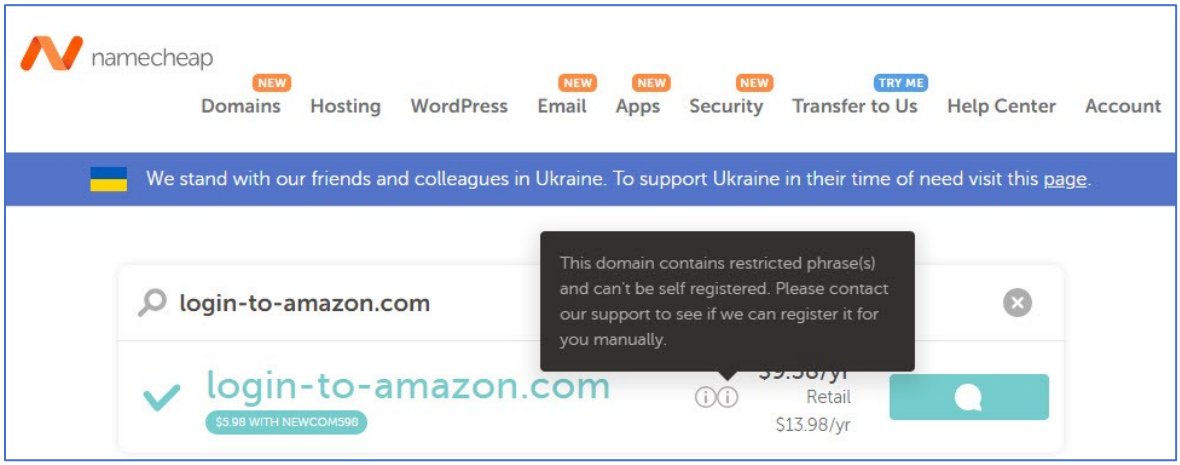
These efforts fall short of what is needed to effectively mitigate DNS abuse generally and phishing specifically. Instead, we recommend that domain name registry and registrar contracts include specific language regarding their obligations to prevent, detect, investigate, and mitigate maliciously and abusively registered domain names. We believe key measures should be adopted swiftly, including:

1) Adoption of widely accepted definitions of cybercrimes, including phishing, malware, botnets, and particularly, spam. The domain industry has advocated a greatly constrained definition of spam. Adopting a definition of spam that is inconsistent with definitions understood by cybersecurity communities, law enforcement, and international cybercrime conventions will cause confusion, create friction, and most importantly, will impede timely and uniform response to domain abuse complaints.
2) Clear prohibition of the use of registered domain names to conduct fraudulent, illegal, or deceptive practices, including phishing.
3) Requirement for the swift suspension or cancellation by registrars and registries of domain names that are identified as maliciously or abusively registered.
4) A duty for domain name registrars and registries to investigate reports of abuse in a timely manner that is clearly defined. Careful research has determined that a phishing attack generally runs its course and has snared all its victims within 24 hours of the onset of the attack. So for phishing at least, only action that takes place in under 24 hours from when the attack begins is efficacious.
5) ICANN should create ways in which gTLD registry operators can stop doing business with a registrar that exhibits a high incidence of abusive registrations. These are often cases in which criminals make malicious registrations repeatedly, or in bulk. A registrar is essentially a supply chain business. The domain industry should follow examples of other industry verticals that have adopted measures to mitigate abuse in their supply chains, including refusal to do business with abusive partners.

Adoption Of Preventative, Proactive Anti-Abuse Techniques

ICANN's new anti-abuse contract provisions focus on mitigating abuse after it has already begun. Registrars and registries are the only parties positioned to preemptively block suspiciously composed domain names before they are weaponized for phishing attacks. Tools and technical methods for

detecting likely abusive registrations have been implemented by some industry players. For example, the .EU registry currently screens registered domains based on lexical features and similarity to known brands. If the string is suspiciously composed, the requested domain name is delayed from delegation by the registry until it can be further investigated. Similarly, the large registrar NameCheap is now limiting the registration of domain names with notable brand names and phrases in them, apparently as a way of preventing phishing:



Registrars and registry operators are also in an excellent position to suspend large batches of domain names registered by misbehaving registrants. Some registrars suspend only the domains that are complained about or have active phishing on them; this allows phishers to simply work their way through large batches of domain names unimpeded. Instead, registrars and registry operators are under no legal obligation to tolerate such behavior and should suspend entire domain portfolios controlled by malefactors. This practice can prevent abuse.

The implementation of such tools and techniques should be widespread across the domain name registration industry.

Investments, Incentives, and Enforcement

To be effective, anti-abuse policies and practices must be developed, practically implemented, and enforceable. Industry players will incur a level of cost to implement anti-abuse practices and so we recommend that a combination of "carrots and sticks" — financial incentives and non-compliance penalties — should be adopted to encourage responsible behavior.

a) **Investments in new or novel methods to mitigate phishing.** Registries and registrars should be incentivized to experiment with the many tools and techniques applied post registration by blocklist operators or researchers. Investments in these or new techniques that could be applied pre-registration or pre-delegation by registrars and registries should be encouraged or rewarded. Further, financial incentives for implementation and adoption of such automated tools could be put in place to encourage adoption.

b) **Adopt additional compliance and enforcement tools**. Historically, ICANN's compliance team has been limited to two mechanisms: suspension of a registrar's ability to create domains or complete removal of a registrar's accreditation. ICANN should identify additional, alternative consequences that are more flexible and can be used against registries or registrars that are not

attending to DNS abuse generally, and cybercriminal activity such as phishing, specifically. The financial disincentive program mentioned below is one example.

c) **Monetary penalties**. A disincentive program could be implemented by ICANN (and by ccTLD registries), where a registrar with an excessive phishing score would pay increased fees (see
d) *Ranking of gTLD Registrars by Scoring* Metrics on page 26). Such disincentive fees could be used to fund phishing mitigation research and to develop open-source mitigation solutions. These programs can be practical because they can be based on documented phishing.
e) **Registrars should know or verify their customers**. Criminals often use false identities and stolen credentials to register domain names. There are inexpensive identity verification services that registrars can use to screen customers, for pennies per transaction.
f) **ICANN should require the publication of more identity data in WHOIS** (registration data publication services). This would allow anti-abuse actors to better identify, report, and block malicious actors. As Interisle documented, ICANN's policy has allowed registrars and registry operators to hide much more contact data than is required by the European General Data Protection Regulation (GDPR) — perhaps five times as much — so that only a fraction of registrant contact data remains available. The European Union has realized how the domain industry over-redacted data, and in its new NIS2 legislation has attempted to correct that by stating that TLD registrars and registries "should be required to make publicly available domain name registration data that fall outside the scope of Union data protection rules, such as data that concern legal persons."
g) **We are wary of financial incentives that give registrars and registry operators money based on low phishing scores**. One reason is that such programs are difficult to administer — they ask the parties to prove a negative. As we saw in our previous reports, much phishing does not make it into reporting lists, which could lead to rewards where they are not deserved. (See "*List Coverage: The Phish That Get Away*" in our 2022 report, page 38.) Second, some registrars have reduced abuse on their own. We are therefore concerned that such financial incentives might not move the needle and could throw money away. Finally, we don't see that other industries are subsidized — by a government or by a regulator such as ICANN — for keeping criminals out of their businesses. The better approach is for registrars and registry operators to build in the cost of running a clean business into their financial and business models.

New gTLD Program Considerations

The expansion of new gTLDs sought to bring consumers greater choice and lower prices, as well as new business opportunities. While consumers and Internet users were the intended beneficiaries of new gTLDs, they have become the subject of increased attacks emanating from these same TLDs. Phishing activity has been particularly acute and problematic in new gTLDs that offer cheap domains. When hundreds of new TLDs went on the market, some operators decided to compete on price, and the low prices attracted abuse. **ICANN should weigh this phenomenon when allowing further top-level domains.** Several organizations and review processes within ICANN have suggested this over the past several years, but no good study has been completed by ICANN.

Address Phishing Mitigation Across the Global Name Space.

The ICANN organization only has remit over the generic TLD name space. ccTLD and gTLD policies and policy-making are developed separately and often independently by country. While ccTLD participation in ICANN is not comprehensive, it is considerable. A common anti-phishing policy-making effort

involving ccTLDs and gTLDs would facilitate "mitigation uniformity" across the name space, at least to the extent that any party seeking assistance when responding to phishing attacks involving domain names can rely upon some baseline of cooperation and action.

Cross-Industry Collaboration

Adopting mitigation measures in the domain name space alone will not fully address the phishing problem

Phishers exploit resources outside the domain name space and ICANN's remit in order to fuel attacks. Hosting and subdomain service providers must cooperate more closely with domain industry players and stakeholders within to identify and respond to attacks and better mitigate exploitation of their resources more effectively. As we discussed in the section *Fallout from Phishing Attacks — Three Case Studies* on page 35, removal of phishing content is a costly activity. Cooperation may reduce phishing content removal and thus eliminate costs in customer support and manpower to mitigate attacks while avoiding damage to business reputation.

Web, DNS, and other Internet services hosting providers would benefit from the development and promulgation of broader industry best practices, including policies, operational practices, and technical solutions that would promote:

- Adoption of an industry-wide acceptable use policy that prohibits fraudulent, illegal, or deceptive practices, including phishing.
- Uniform and timely action for the removal of phishing pages, DNS zone data, or other content that serve as phishing attack resources.
- Recommended (best) content management practices that can reduce customer web vulnerability attack surfaces.
- Phishing awareness campaigns and phishing education landing pages (*e.g.*, APWG).
- Uniform and timely cooperation with law enforcement, phishing (or brand) protection services, and private sector cyber investigators.

Government Action

ccTLDs represent 37% of the marketplace and ICANN's remit does not extend to ccTLDs. Where industry self-regulation and existing domain policies fail to adequately mitigate phishing in a ccTLD (for example, see *Nothing is Free: The Collapse of Freenom* on page 21), governments should consider taking a more prominent role in ensuring such cybercrimes are less likely to emanate from their namespace.

From our data, we see evidence that some ccTLD policies are more successful than others in mitigating phishing threats. For example, most ccTLDs that have little or no phishing have either higher prices than gTLDs or have adopted policies requiring that registrants have a verifiable connection to the country, such as proof of identity or evidence of incorporation are required for domain registration. The same is true for TLDs with a strictly enforced AUP and restricted gTLDs. These TLDs make a strong case for implementing rigorous domain name registrant verification requirements in the interest of public safety.

Emerging legislation in some countries does not include phishing (cybercrime) in their scope but could be adapted to do so. In the U.S., Executive Order 13984 of January 19, 2021, *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*, provides authority to impose record-keeping obligations on users of Infrastructure as a Service (IaaS). In a

comment to the Department of Commerce, Interisle Consulting Group argued that the DNS is as much of a critical infrastructure as the mobile and "hard-wired" networks that comprise the Internet and recommended that U.S. domain name service providers should be classified as U.S. IaaS providers, that U.S. domain name registries should be required to maintain complete and accurate databases of the identity and contact information of all registrants for the domain names that such registries administer, and that U.S. domain name registries and registrars should be required to provide "real time" access to these databases, including contact information, to meet the timeliness of access that first responders need to identify and mitigate threats. The same record-keeping obligations could help mitigate abuse of subdomain service providers or (dynamic) DNS hosting services.

The US H. R. 6352, amendment to the US Federal Food, Drug, and Cosmetic Act which provides "a process to lock and suspend domain names used to facilitate the online sale of drugs illegally, and for other purposes" is representative of this kind of obligation. The mechanics are consistent with how takedowns are commonly, informally conducted and can be applied as effectively to phishing (or cybercrimes generally) as to illegal pharmaceuticals.

In the U.K., the government recently activated a law that gives it the power to appoint a new manager for its .UK TLD. The British government says it will only exercise this power if the registry operator lets DNS abuse or cybersquatting proliferate and fails to follow government orders to fix the situation. Abuse in .UK is relatively low, but the proactive stand shows a government making its expectations about abuse clear, and empowering itself to do something about it.

The U.K. government is also considering legislation relating to its TLDs: .uk, .scot, .wales/.cymru, and .london covering the misuse and unfair use of domain name. Misuse might include malware, botnets, pharming, phishing, and spam emails. Unfair use might include cybersquatting and typosquatting.

Adoption of the European Union's GDPR has demonstrated that government regulation and the risk of violation fines raised the stakes high enough to make parties act to protect privacy.

Broader adoption of the Counsel of Europe's Convention on Cybercrime as model law would be beneficial. Governments (States) can pursue a common criminal policy by adopting legislation and cooperating with other States. The Convention's Articles and Guidelines for fraud, network security, and copyright infringement address phishing, malware, botnets, and spam. Having a common criminal policy to serve as a baseline could facilitate multi-jurisdictional mitigation efforts and would obviate the need for more and fruitless discussions over what constitutes DNS abuse.

The .NL registry (SIDN) is changing its policy to prohibit privacy and proxy services from registering domains in its ccTLD, noting that "registration data for .nl domain names registered to private individuals hasn't been publicly available since 2010".

Litigation

In the absence of more effective mitigation measures and broader cooperation, litigation has shown to be an effective tool in stemming abuse. Litigation is usually viewed as a last resort, as it is expensive and slow. However, it may become more frequent absent effective industry-based mitigation practices.

Most lawsuits with a phishing claim involve cybersquatting. For example, in 2006, Microsoft sued Dyslexic Domain for infringement, and Newtonarch LLC, Partner IV Holdings for cybersquatting. Also in 2006, a French court imposed liability on a registrar, Moniker Online Services Inc, after it had registered

various infringing names. In 2007, Microsoft sued Red Register for illegally profiting from trademarks. In 2008, Verizon won a $31M suit against OnlineNIC for cybersquatting, and Microsoft and Yahoo! Inc. also sued the registrar in 2008 and 2009. And OnlineNIC was again sued yet again by Meta in 2019.

Lawsuits that seek to stem phishing are not just brought on the basis of cybersquatting. In 2020, NameCheap was sued by Meta for claims including false designation of origin and trademark infringement. The complaint also alleged that NameCheap had failed to cooperate in malicious domain investigations and took issue with the way NameCheap operated its proxy service. The two parties settled the case in April 2022. The settlement apparently had its intended effect for Meta: new phishing domains (attacking any target) registered through NameCheap declined more than 50 percent the following quarter. Most recently, Freenom halted domain registrations after being sued for phishing under a California statute and for false designation of origin.

ICANN reported that the number of Uniform Domain Name Dispute Resolution Policy (UDRP) cases has been growing by 6% per year on average since 2013, and UDRP complaints field at the World Intellectual Property Organization (WIPO) rose from 1,823 in 2006 to 5,616 in 2022. In 2019, 16 percent of domain name cases filed with WIPO involved instances of phishing schemes. ICANN reported that the number of Uniform Domain Name Dispute Resolution Policy (UDRP) cases has been growing by 6% per year on average since 2013. In this 2023 study we identified over **4,000 businesses or organizations targeted in phishing attacks – more than twice the number from our 2022 study**.

Domain registrars, domain registries and web hosting services have not kept pace with preventative measures

The problem is worsening — domain registrars, domain registries, and web hosting services have not kept pace with preventative measures to reduce the total amount of phishing. Unless better anti-phishing solutions are put into place, it's reasonable to expect that regulation and litigation will increase.

About the Authors

Greg Aaron is an internationally recognized authority on the use of domain names for cybercrime, and is an expert on domain name registry operations, DNS policy, and related intellectual property issues. Mr. Aaron is Senior Research Fellow for the Anti-Phishing 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 works with industry, researchers, and law enforcement to investigate and mitigate cybercrime, and is also a licensed private detective. He was the Chair of ICANN's Registration Abuse Policy Working Group (RAPWG) and has been a member of ICANN's EPDP Working Group, which created registration data access policies. 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 around the world, including .INFO, .ME, and .IN. He is President of Illumintel, Inc., a consulting company. Mr. Aaron is a *magna cum laude* graduate of the University of Pennsylvania.

Lyman Chapin has contributed to the development of technologies, standards, and policy for the Internet since 1977, and is widely recognized and respected as a leader in the networking industry and the Internet community. Mr. Chapin is a Life Fellow of the IEEE, and has chaired the Internet Architecture Board (IAB), the ACM Special Interest Group on Data Communication (SIGCOMM), and the ANSI and ISO standards groups responsible for Network and Transport layer standards. Mr. Chapin was a founding trustee of the Internet Society and a Director of the Internet Corporation for Assigned Names and Numbers (ICANN). He currently chairs ICANN's Registry Services Technical Evaluation Panel (RSTEP), which is responsible for assessing the impact of new Domain Name System (DNS) registry services on the security and stability of the Internet, and the DNS Stability Panel, which evaluates proposals for new Internationalized Domain Names (IDNs) as country code top-level domains (ccTLDs). He is also a member of ICANN's Security and Stability Advisory Committee (SSAC). He has written many other papers and articles over the past 40 years, including the original specification of the Internet standards process operated by the IETF. Mr. Chapin holds a B.A. in Mathematics from Cornell University.

David Piscitello has been involved in Internet technology and security for more than 40 years. Until July 2018, Mr. Piscitello was Vice President for Security and ICT Coordination at ICANN, where he participated in global collaborative efforts by security, operations, and law enforcement communities to mitigate Domain Name System abuse. He also coordinated ICANN's security capacity-building programs and was an invited participant in the Organisation for Economic Co-operation and Development (OECD) Security Expert Group. Dave is an Associate Fellow of the Geneva Centre for Security Policy. He served on the Boards of Directors at the Anti-Phishing Working Group (APWG) and Consumers Against Unsolicited Commercial Email (CAUCE). He is the recipient of M3AAWG's 2019 Mary Litynski Award, which recognizes the lifetime achievements of individuals who have significantly contributed to making the Internet safer.

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 Digital Equipment, Compaq, and the Financial Services Technology Consortium in national and international industry standards bodies. He holds six patents on enterprise management technology and brings more than forty years of direct experience with information technology, as a developer, architect, and consultant, with recent work including design and operation of a regional public safety network, providing technical expertise relating to patents, and analysis of world-wide Internet use. Dr. Strutt holds a B.A. (with First Class Honours) and Ph.D. in Computer Science from Essex University (UK).

About Interisle Consulting Group, LLC

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

Acknowledgments

The authors extend thanks to:

- Spamhaus and OpenPhish, for their kind contribution of data for this study.
- The PhishTank and the APWG eCrime Exchange communities, for their collaborative efforts to identify phishing.
- Domain Tools, for access to historical and bulk parsed WHOIS and the IRIS investigations platform.
- April Lorenzen and Zetalytics, for access to passive DNS data.
- Saeed Abu-Nimeh for access to the Seclytics Predictive Threat Intelligence platform.
- John Levine, for operational support.
- CAUCE, for financial support.
- All the security personnel who fight phishing.