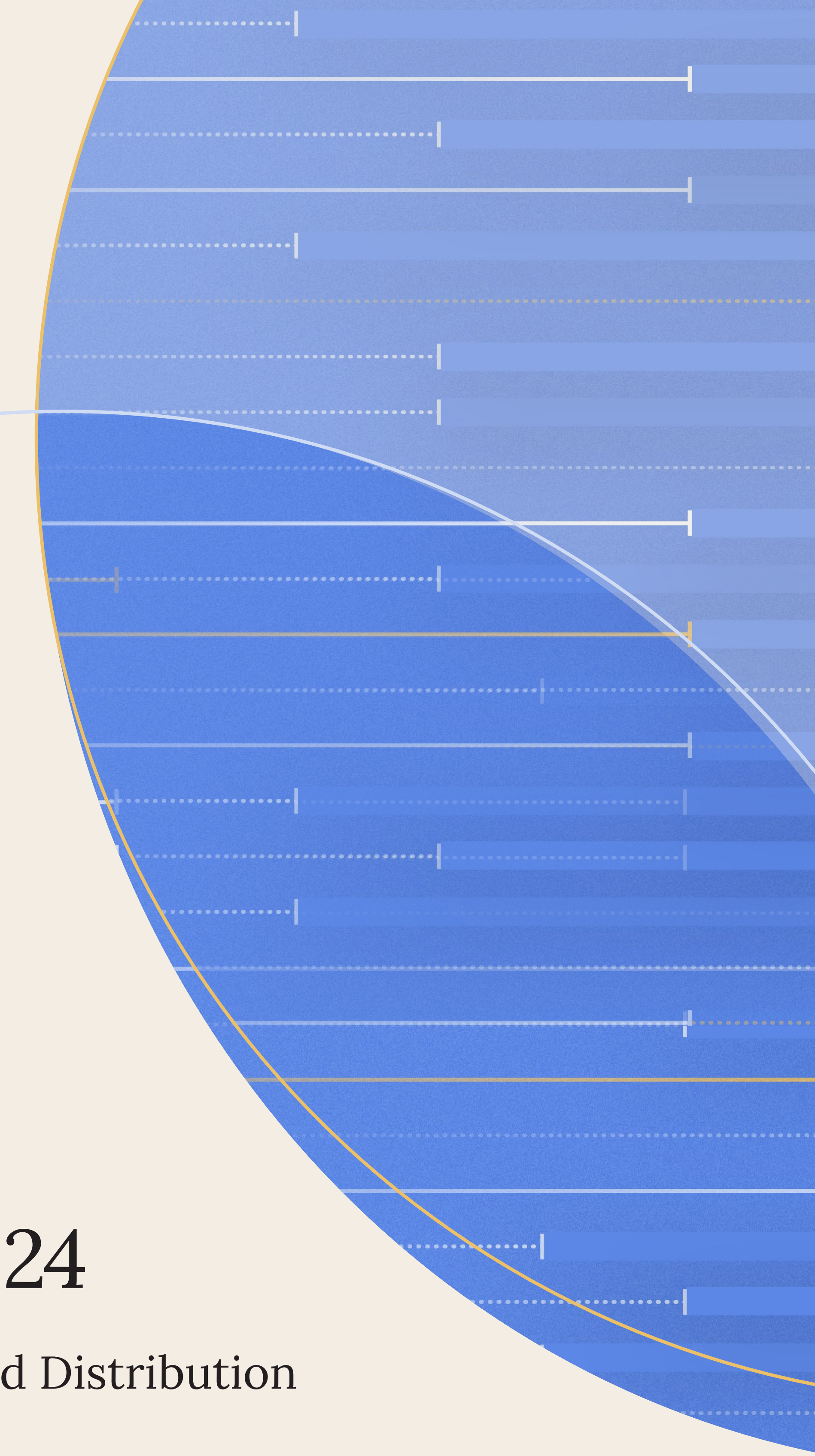
Interisle

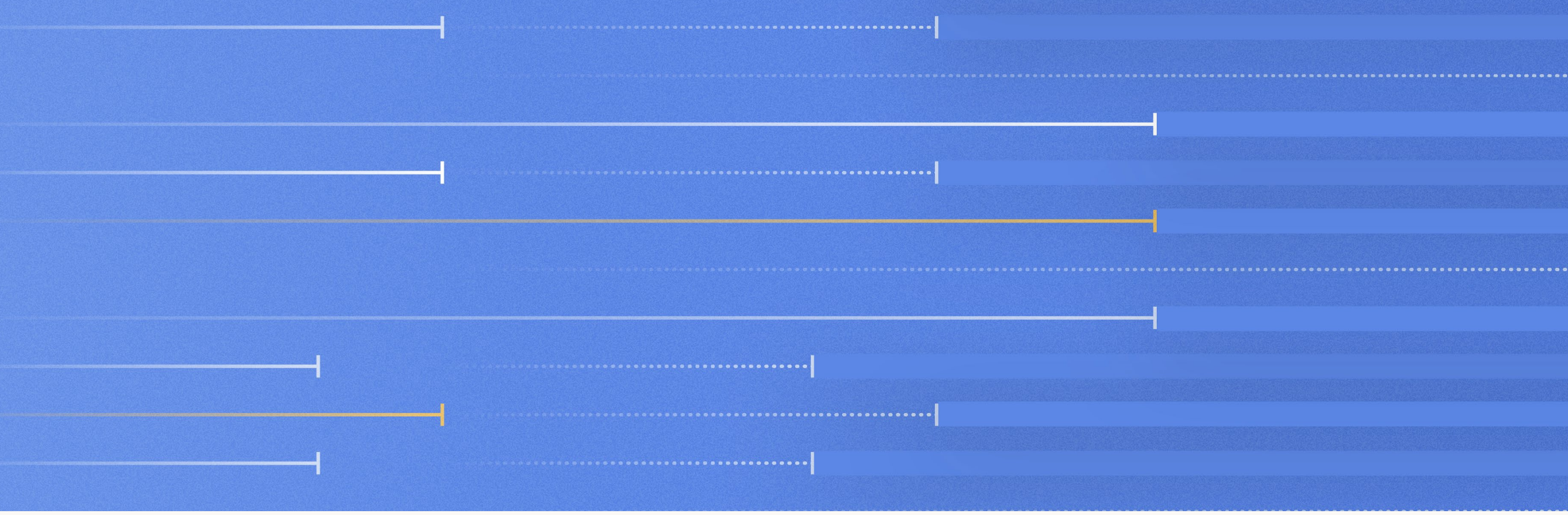


Phishing Landscape 2024

A Study of the Scope and Distribution of Phishing

INTERISLE CONSULTING GROUP 23 JULY 2024

CONTENTS



EXECUTIVE SUMMARY

Phishing defrauds millions of Internet users every year.

Cybercrime and its devastating impacts continue to grow at an alarming rate. This past year the United States experienced a record number of both cybercrime complaints (over 880,000) and estimated direct monetary losses (US$12.5 billion) according to the Federal Bureau of Investigation. The swelling number and severity of attacks has led the World Economic Forum to rank cyberthreats among the top five biggest risks to short-term global security and economic stability.

Phishing, the practice of using messages and fraudulent websites to pose as a trusted party in order to deceive victims into providing sensitive information, is the most commonly used tactic in the perpetration of these cybercrimes. Understanding how phishers obtain and deploy their resources – and implementing strategies to starve their access to them – is critical to the overall fight against cyberthreats.

This report is Interisle's fourth annual analysis of data and key trends in this critical area. For this study we analyzed 3.9 million phishing reports collected over a year (May 2023 to April 2024). We then used data from our previous studies (available at the Cybercrime Information Center) to create year-over-year comparative measurements, an analysis based on over 15 million phishing reports.

Our analysis shows that:

The total number of phishing attacks grew by nearly 50,000 attacks compared to last year, to just under 1.9 million incidents worldwide.

Cybercriminals evolved their tactics to use new resources. While the number of unique domain names reported for phishing held relatively steady at just over 1.1 million, phishing attacks hosted at subdomain providers skyrocketed in the past year. Commercial subdomain use was up 51% to over 450,000 reported names, representing 24% of all phishing attacks. The use of the decentralized InterPlanetary File System (IPFS) to host and launch phishing attacks also increased remarkably – up 1,300% to some 19,000 reported phishing sites.

After the demise of the phish-friendly domain registry Freenom, cybercriminals moved to using inexpensive domain names in new gTLDs, in addition to subdomain services. 42% of all domains reported for phishing were registered in new gTLDs, compared to 25% last year.

The registration of high volumes of domain names at one time (bulk registration) is a practice highly exploited by phishers. At least 27% of all domain names used in phishing attacks were found to be registered in bulk.

Four of the top five hosting providers used by phishers to host phishing attacks were based in the United States. One U.S. company accounted for over one-third of all phishing attacks.

Domain name registration policies significantly affect the level of phishing in a TLD. We studied ccTLD pricing and policies in Europe and the Asia-Pacific region showing that more robust customer verification requirements correlate with lower levels of phishing activity.

Disturbingly, our study shows that clear and known patterns of resource abuse continue (e.g., use of bulk registration, high levels of abuse in new gTLDs) while the exploitation of alternative resources is on the rise (e.g., subdomain providers, IPFS). Yet, it also demonstrates that market changes and policies can have a significant impact.

Based on our findings, we recommend the implementation of a series of measures to curb the criminal abuse of resources and more effectively remediate phishing problems when they are found.

Our recommendations include:

Implement robust identify verification / certification requirements for parties wishing to bulk register domain names and limit the number of accounts and subdomains a customer can register at subdomain providers.

Strengthen verification of customers and submitted registration information across the domain name, subdomain, and hosting industries, including implementing automated tools to screen for bogus registration data and fraudulent payment information.

Expand the deployment of automated systems to screen for suspicious patterns of domain name and subdomain registrations, including algorithmically generated names and names deceptively similar to known brands.

Implement more effective, proactive procedures to identify the use of hosting resources for cybercrime, including measures to suspend suspicious accounts in a timely way.

Create “Trusted Reporter” programs across industry to facilitate swift suspension of phishing resources identified by recognized and trusted cybercrime monitors.

More effective, outcome-oriented, cross-sector collaborations aimed at preventing and more quickly mitigating criminal access to phishing resources.

Introduction

Cybercrime continues to grow at an alarming rate worldwide, and the impacts on consumers, businesses, and institutions are devastating. Cybercrime incidents and related monetary losses reached record highs in 2023. The U.S. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3), for example, conservatively estimated over $12.5 billion in direct losses in the US alone, a 10% in cybercrime complaints and a 22% increase in financial losses compared to 2022.

Statista expects the global cost of cybercrime to surge in the next four years, rising from $9.22 trillion in 2024 to $13.82 trillion by 2028. The World Economic Forum (WEF) ranks cyberthreats as one of the most severe risks to global economic and social stability in the near-to-mid future.

Phishing, the practice of impersonating a trusted party to dupe an online victim into revealing sensitive information, continues to be the most pervasive cybercrime “gateway” tactic. Phishing attacks are effective because they take advantage of the trust people have in known parties, e.g., brands or their employers. A targeted consumer or company employee is simply more likely to click on a phony email link or provide sensitive credentials to a criminal if it appears the request is originating from a trusted source.

The prevalence of phishing and cybercrime are the leading cause of user mistrust in the Internet worldwide, curbing online use and engagement in the overall digital economy. Phishing wields devastating damage on the primary victims of their attacks, which range from everyday people to large companies and institutions. In addition, phishing also levies collateral damage on the brands and entities being impersonated. These harms are various and wide-ranging, including diminished brand trust, increased costs from customer service calls and complaints, and direct loss of business, among others.

Cybercriminals use phishing as a gateway for consequent illegal and malicious activities, including fraud, ransomware, malware, and distributed denial of service (DDoS) attacks, and to steal corporate or national security information. By understanding how phishers acquire and deploy the resources they need to launch attacks, more effective solutions can be developed to close this gateway,

Phishing attacks are effective because they take advantage of the trust people have in known parties, *e.g.*, brands or their employers. A targeted consumer or company employee is simply more likely to click on a phony email link or provide sensitive credentials to a criminal if it appears the request is originating from a trusted source.

curb online criminal activity, and reduce victimization.

This is our fourth annual Phishing Landscape Report. For this report, we collected and analyzed nearly 3.9 million phishing reports from four widely respected threat data providers (Anti-Phishing Working Group (APWG), OpenPhish, PhishTank, and Spamhaus). From this data we identified 1.9 million distinct phishing attacks perpetrated worldwide during our study period of May 2023 to April 2024. We used the data from our 2021-2023 studies to create year-over-year comparative measurements.

Building on our previous work, we then analyzed phishing activity at points along the cybercrime supply chain to understand how phishers perpetrate attacks and where these criminals go to acquire the resources needed to conduct them.

Specifically, we investigated in detail where and how cybercriminals acquire the resources needed to conduct their attacks and how they deploy these resources, specifically where they obtain domain names and subdomains, and hosting.

We additionally analyzed and identified the top hosting suppliers exploited by phishers and trends in the vbrands most impersonated in phishing attacks. Finally, based on the data and analysis we provide recommendations on how phishing prevention and mitigation efforts can be aimed at key points along the supply chain to disrupt phishing.

Phishing takes many forms.

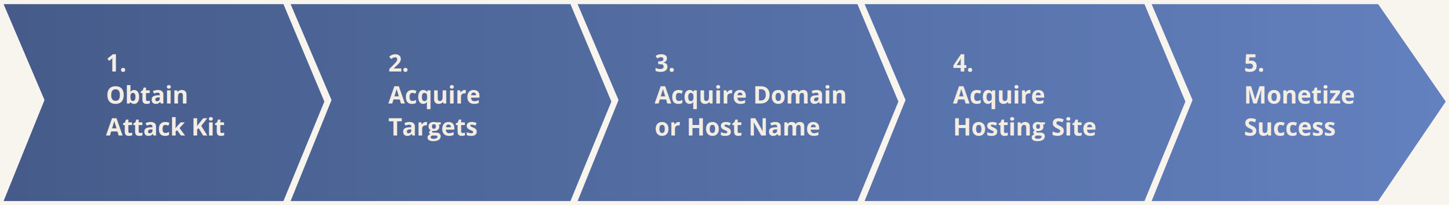
A phishing attack is a perpetration of fraud that begins with an attempt to lure a party to a fake web site where a convincing impersonation of a merchant, brand, or product causes the party to submit or reveal personal data, a user account, or credit/financial information to the criminal attacker.

In most cases, the lure is a URL. A user who clicks on the URL is like a fish that takes the bait, not realizing that there's a barbed hook within. However, just as fishers adapt to water conditions by using hand lines, rods, or nets to fish, criminals are quick to adopt any delivery method(s) that promise to reach more potential victims.

Historically, the means of delivering the phishing lure to a user has been electronic mail. Today, delivery mechanisms include text or messaging apps (a.k.a., "smishing"), voice messaging ("vishing"), and social media posts, messaging, or comments. Phishers now also include QR codes in YouTube videos or posted notices.

Bottom line: phishers will do whatever it takes to put a malicious URL in front of the largest potential victim pool.

The Cybercrime Supply Chain



1. Obtain Attack Kit

2. Acquire Targets

3. Acquire Domain or Host Name

4. Acquire Hosting Site

5. Monetize Success

Cybercrime is a business. Like any other business, cybercriminals need access to a range of resources and supplies to ply their trade. We call the assemblage of these resources the "Cybercrime Supply Chain." This framework allows cybercrime to be analyzed and understood like any other business, and it reveals opportunities to disrupt and starve criminals of the resources needed for attacks.

The cybercrime supply chain framework consists of five key elements. Deeper descriptions and an analysis of each element can be found in our report Cybercrime Supply Chain 2023.

In our reports, we focus our attention most closely on two of the five elements, Acquire Domains or Hostnames and Acquire Hosting, since our current access to data sets provide an opportunity delve deeply and uniquely into these key supply chain elements.

Key Results

MEASUREMENT	MAY 2022 TO APRIL 2023	MAY 2023 TO APRIL 2024	% CHANGE
Total number of phishing attacks	1,850,392	1,897,952	+ 3%
Number of phishing attacks associated with malicious domain registrations	1,049,389	1,053,735	+ 0.4%
Unique domain names reported for phishing	1,124,679	1,117,670	− 1%
Number of maliciously registered phishing domains	**725,520**	**878,111**	**+ 21%**
Top-level domains where phishing domains were reported	699	720	+ 3%
gTLD registrars with domains under management reported for phishing	**1,200**	**1,951**	**+ 63%**
All registrars with domains under management reported for phishing	2,394	3,047	+ 27%
Hosting networks where phishing web sites were reported	4,382	4,284	− 2%
Number of phishing attacks using a subdomain provider	**302,086**	**454,948**	**+ 51%**

The number of phishing attacks continues to rise. We observed an increase of 47,560 reported phishing attacks over the 2022-2023 study period, the smallest increase since we began measuring phishing attacks in May 2020.

We define a phishing attack as a phishing site that targets a specific brand or entity. Phishing attacks measure 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. A measure of how much phishing activity is being observed is in our opinion the most accurate indicator of positive or negative change over time.

Note: We cannot determine the reason(s) for the smaller increase in phishing attacks from the data that we collect. Changes in phisher behavior, suspension of registry operations (e.g., Freenom), successful disruption of phishing infrastructures by law enforcement, or changes in the reporting behavior of contributors to our phishing feeds may have played a role. The attacks reported by our sources are a fraction of all the attacks that took place worldwide. Consequently, we believe that the phishing problem is much greater than our data indicates.

Phishing is a gateway crime.

More than 90% of cyberattacks begin with phishing
Source: CISA

More than 90 % of organizations in the United Kingdom, Spain, and the United States were targeted by phishing in 2023.
Sources: Proofpoint, Inacom

More than one million unique domain names reported for the second year in a row.

Domain names are essential resources for phishers. Users are accustomed to seeing domain names in URLs and suspicious should they see Internet addresses. Phishers often impersonate brands or companies by including near- or exact matches of these names in their domain names or web site host names.

The notable drop in February 2023 shows the effect of the closure of ccTLD registry Freenom, which had been used by phishers to register large numbers of domain names. By January 2024, phishers appear to have recovered from the loss of this significant domain name supplier. We examine how phishers responded to losing Freenom in the section *Phishing in the Post-Freenom Era*. We observed significantly increased phishing activity hosted on subdomain providers (*e.g.*, free website operators). We examine this later, in the section *Subdomain Providers*.

Malicious phishing domain name registrations increased by 21%.

While unique domains reported for phishing decreased slightly, **we saw a marked increase (21%) in the number of phishing domains that were maliciously registered** compared to our previous report. There was a 14% increase in the percent of unique domains that were determined to be maliciously registered (from 65% to 79%).

Recovery from Phishing attacks is costly.

Average business recovery cost of a single phishing-related data breach estimated at $4.5 million.
Source: IBM

$3 billion lost in the U.S. in 2022 through business email compromise phishing attacks alone.
Source: FBI

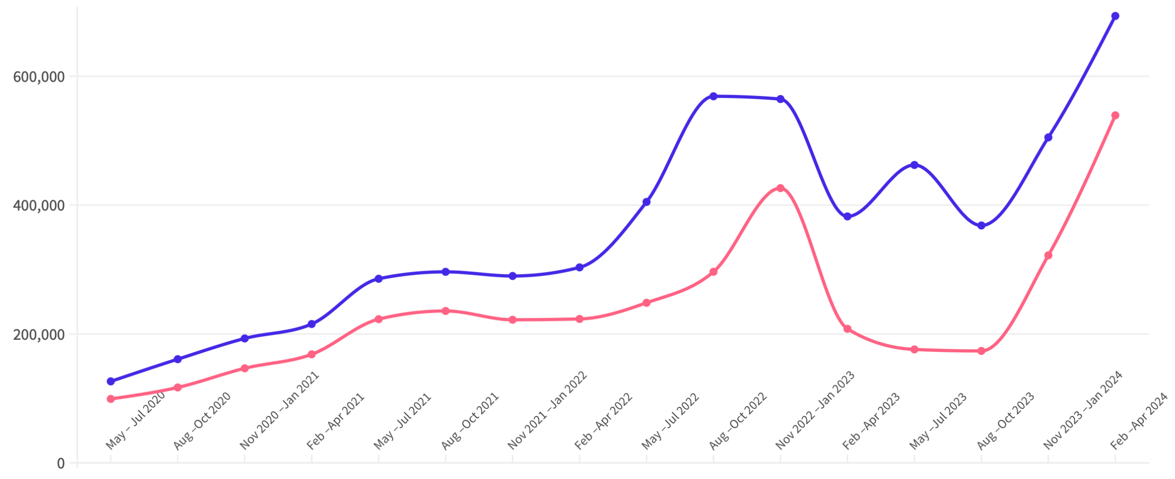
At least 27% of the domains used for phishing in our study data were registered in bulk.

Cybercriminals may register and use hundreds or in some cases thousands of registered domain names for a single phishing campaign. Registration of malicious domains in volume (bulk registrations) is one of the most common domain acquisition tactics in the phishing space.

Phishing attacks hosted at subdomain provider services increased 51% over the prior study period.

Subdomain providers give customers services on a domain name that the provider owns. Users receive their own DNS space, using a third level domain of the

Phishing Attacks and Phishing Domains



The FBI received nearly 300,000 complains in 2023, the most reported cybercrime for the past 5 years. Source: FBI

form: *subdomain.domainname.tld*. Many of these services provide web hosting or offer website-building services on the subdomain, and the services are almost always free. Phishers exploit these services to build and maintain phishing sites, for no cost. The 51% rise in the use of subdomains shows how quickly phishers can move to exploit alternative supply chain resources when they are cheap and have few acquisition barriers.

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).

The number of *maliciously registered domain names* is based on our determination that a domain name was purposely registered by a phisher to perpetrate a phishing attack.

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. For more information about how we process phishing reported through our feeds, see the Terminology and FAQ pages at the Cybercrime Information Center.

Phishers prey on vulnerable parties

Online fraud, often initiated through phishing, disproportionally victimizes some of the most vulnerable individuals and groups in society. The US FBI received nearly 300,000 complaints in 2023, placing phishing as the most reported cybercrime over the past 5 years. In 2023 U.S. senior citizens 60+ suffered financial losses of nearly $3.4 billion in 2023, three times more than adults 30-39 ($1.2 billion) and more than two times more than adults 40-49 and 50-59 ($1.2 and $1.7 billion respectively).

Source: FBI

Phishers are successful even when ISPs and service operators provide URL or ad blocking services. Google's Safe Browsing service currently lists more than 1.8 million phishing sites and sends more than 3 million warnings to users every day, but our data suggest that they are misunderstood or ignored.

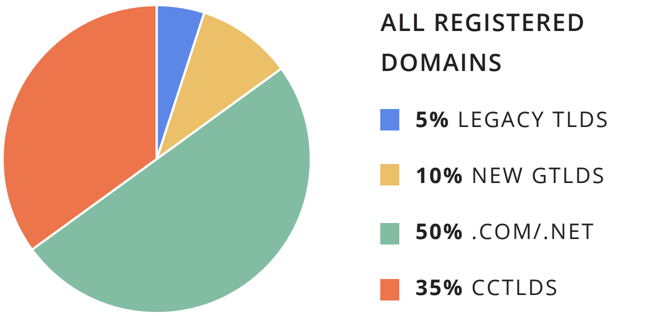
Source: Google

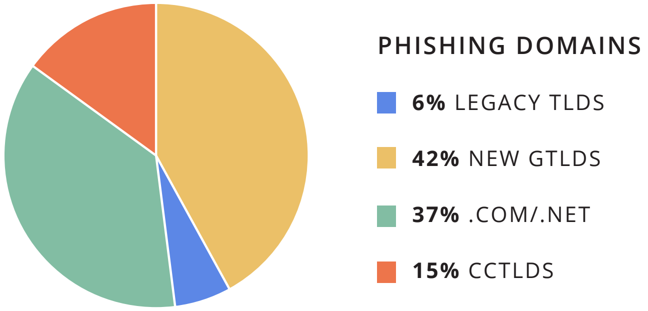
Top Level Domains

According to Domain Tools, at the end of April 2024, there were over 340 million registered domains in the global domain name space. We observed phishing in 720 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:

- .COM and .NET
- Country-code domains (ccTLDs)
- Legacy gTLDs other than .COM and .NET delegated before 2013 (*e.g.*, .ORG, .BIZ, .INFO)
- New gTLDs delegated from 2014 to the present (*e.g.*, .LOL, .SBS, .SHOP, .TOP)

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





In addition to having the lowest percentage of phishing domains reported by namespace category, we found that **ccTLDs have the lowest combined phishing attack and combined phishing domain scores in the namespace market.**

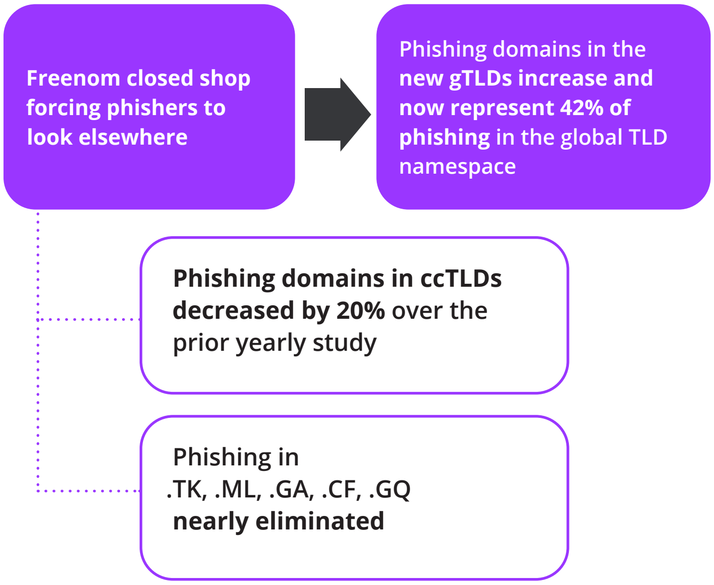
COMBINED PHISHING SCORES	CCTLD SCORES	.COM/.NET SCORES	LEGACY GTLDS SCORES	NEW GTLDS SCORES
Phishing Attack Score	34.8	36.5	77.6	223.4
Phishing Domain Score	14.4	24.2	38.0	151.0

Phishing in the .COM and .NET gTLDs and in the legacy gTLDs remained relatively unchanged.

New TLDs attracted the most phishing activity. 42% of the phishing domains reported during this study period were in the new gTLDs, which have the smallest share of the market (10%). This is a marked increase over our 2023 study findings, where new gTLDs held an 8% market share and 25% of the phishing domains.

Phishing in the Post-Freenom Era

We attribute part of the increase in new gTLD phishing activity and much of the decrease in ccTLD phishing activity to phishers migrating from Freenom's commercialized ccTLDs to the least expensive alternatives in the gTLD name space. The topic of phishing employing Freenom's ccTLDs was described in detail in our 2023 Phishing Landscape Report. Phishing activity subdomain providers also increased. See the *Subdomain Providers* section for our analysis of this phishing activity.

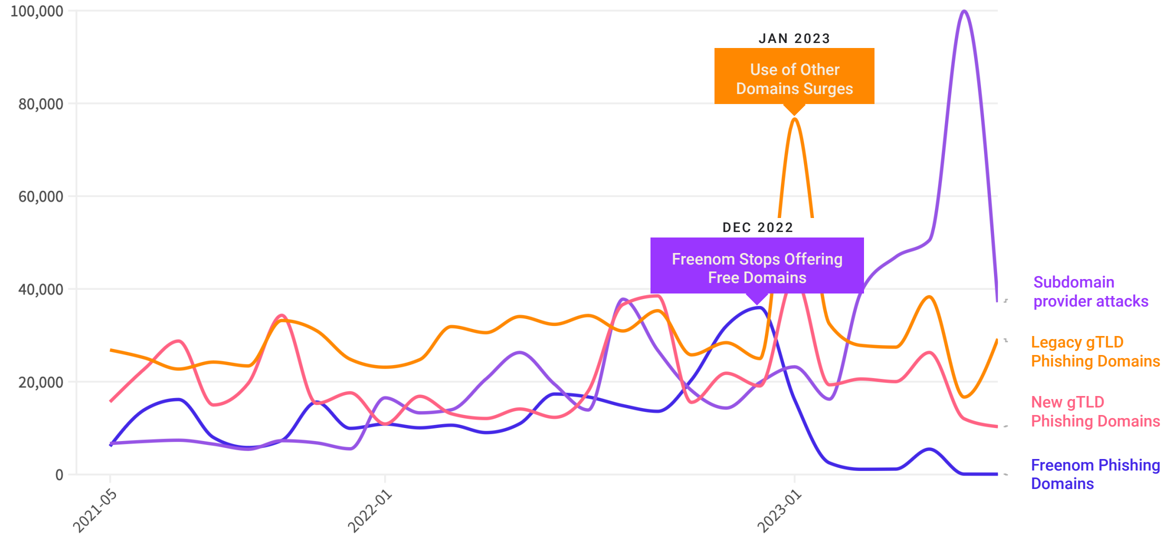


Freenom closed shop forcing phishers to look elsewhere

Phishing domains in the new gTLDs increase and now represent 42% of phishing in the global TLD namespace

Phishing domains in ccTLDs decreased by 20% over the prior yearly study

Phishing in .TK, .ML, .GA, .CF, .GQ **nearly eliminated**



Ranking of TLDs by Phishing Domains Reported

Some TLDs' pricing, operating practices, or business processes were more attractive to phishers than others. Our 2024 study data showed that criminals most often registered domains the top-level domains that offered registrations to anyone without restrictions.

2024 RANK	TLD	REGISTRY OPERATOR	2024 DOMAINS IN TLD	PHISHING DOMAINS REPORTED
1	com	Verisign	156,670,775	**379,669**
2	top	Jiangsu Bangning	2,768,147	**117,014**
3	xyz	XYZ.COM LLC	3,371,694	**67,348**
4	cn	CNNIC	8,172,577	**55,627**
5	info	Identity Digital	3,589,133	**31,734**

TLD rankings for this yearly study period are posted at the Cybercrime Information Center.

Notably for the 2024 study period,

- Two TLDs, .XYZ, and .INFO, replaced Freenom's .ML and .TK commercialized ccTLDs in the top 5 ranking by phishing domains reported.
- 13 of the new gTLDs were ranked in our Top-level Domains Year over Year Comparison: May 1, 2023 - April 30, 2024. With Freenom out of the picture, only three ccTLDs joined the top 20 (.CN, .CC, .RU).
- .COM had the highest number of domains reported for phishing. However, the 156M .COM domains under management represent 46% of the domain marketplace, so the raw count is less meaningful than the phishing score, discussed below. By comparison, .TOP had fewer than 3 million domains under management but over 100K phishing domains reported.

In the section *Domain Registration Policies Matter*, we look at domain registration policies to understand what, if any, influence these have on where phishers register domain names. In the section *Phishers Like Cheap*, we also look at

4–YEAR COMPARISON OF TLDS WITH MOST PHISHING DOMAINS REPORTED			
2021 Study	**2022 Study**	**2023 Study**	**2024 Study**
1. COM	1. COM	1. COM	1. COM
2. TK	2. CN	2. CN	2. TOP
3. XYZ	3. SHOP	3. ML	3. XYZ
4. ML	4. XYZ	4. TOP	4. CN
5. GA	5. TK	5. TK	5. INFO

pricing data to understand the affect that low prices have on attracting phishers.

Ranking of TLDs by Scoring Metrics

The more phishing domains in a name space or TLD, 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. The metric Phishing Score allows for comparisons between TLDs of different sizes; here, we use *Phishing Domains per 10,000* to show whether a TLD has a higher or lower incidence of phishing relative to others.

2024 RANK	TLD	DOMAINS IN TLD	PHISHING DOMAIN SCORE
1	lol	347,972	**577.5**
2	bond	271,107	**472.1**
3	support	36,274	**434.8**
4	top	2,768,147	**422.7**
5	sbs	605,035	**363.0**

The Top five gTLDs with the highest phishing domain scores are new gTLDs. Compared to .COM's phishing domain score of 24.2, these are catastrophically, terrifyingly, high.

Phishing score is an important metric for several reasons.

High scores represent a threat vector for users and organizations. 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.

High scores are a liability for registry operators. High yearly phishing domain scores erode the reputation of a TLD. Legitimate registrants have learned to avoid TLDs that have poor reputations. Risk-averse organizations have resorted to blocklisting entire TLDs, and some blocklist providers and security companies assign increased risk scores to TLDs with poor reputations.

Malicious Domain Registrations Across the Domain Name Space

We measured the number of unique phishing domains reported across a total of 720 TLDs. For our studies, we classify a phishing domain as being:

maliciously registered – purposely registered to carry out a malicious or criminal act. or

compromised – domain names that were registered for legitimate purposes but co-opted by criminals. For example, a criminal may hijack a legitimate user's domain registrar account and alter the corresponding DNS entry to resolve a name or URL to a host that the attacker controls.

This distinction is important because it determines how the phishing site should be mitigated:

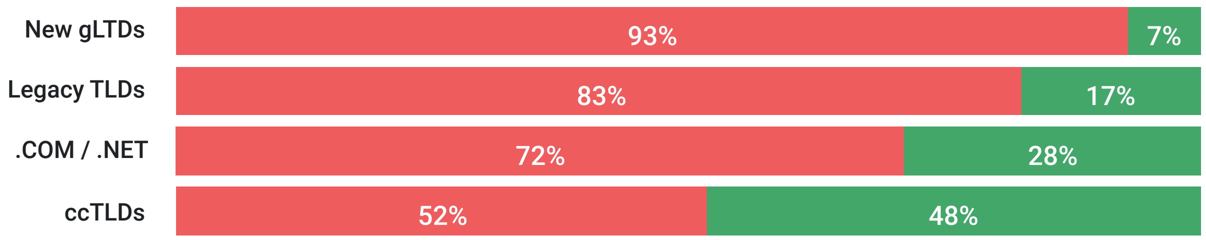
- If the domain is maliciously registered, the domain can be suspended, so it no longer resolves. The registrar, TLD operator, the DNS operator for the domain, and/or the web hosting provider can all take action to stop the malicious activity.
- Compromised domains should not be suspended. Doing so can harm a domain's legitimate registrant by bringing down their web site and email. The hosting provider should be asked to remove the phishing site.

Malicious domain registrations represent the most phishing domains, but exceptionally so in the new gTLDs.

Phishing in the new gTLDs almost always occurs on a maliciously registered domain. Over four years of studies, it is evident that registration processes, policies, and/or pricing in the new gTLDs attract far more phishing than other categories in the global domain name space.

The new gTLDs remain a fertile source for acquiring phishing domains. Four years of studies show that phishers have tended to exploit new gTLDs for intense periods, and then move on to other new gTLDs. Cheap

Maliciously Registered vs. Compromised Phishing Domains



registration fees are frequently available for domains in new gTLDs in the table below and other new gTLDs. We observed that phishers particularly exploited .CFD, and .SBS in the fourth quarter of 2023.

Based on our methodology for distinguishing malicious registrations from compromised domains, the domains reported for phishing in these gTLDs were highly likely to have been registered by criminals for phishing.

GTLD	PHISHING DOMAINS	MALICIOUS PHISHING DOMAIN REGISTRATIONS	% PHISHING DOMAINS MALICIOUSLY REGISTERED
shop	31,179	31,129	**100%**
bond	12,800	12,716	**99%**
lol	20,096	19,933	**99%**
sbs	21,962	21,683	**99%**
top	117,014	115,247	**98%**
cfd	13,960	13,428	**96%**
club	13,260	12,749	**96%**
xyz	67,348	62,439	**93%**

We found that about one-half of the domains reported for phishing in ccTLDs are maliciously registered. Several ccTLDs had high percentages of malicious phishing registrations:

CCTLD	PHISHING DOMAINS	MALICIOUS PHISHING DOMAIN REGISTRATIONS	% PHISHING DOMAINS MALICIOUSLY REGISTERED
cc	11,583	9,878	**85%**
pl	5,718	4,860	**85%**
ru	20,186	16,054	**80%**
co	6,537	4,669	**71%**
id	5,292	3,028	**57%**
us	7,521	4,006	**53%**

Malicious registrations in .RU now represent 80% of phishing domains reported in that ccTLD versus 62% from our 2023 study. Notably, .US was ranked #2 in 2023 and has dropped to #6. Further, malicious registrations now represent just over one-half (53%) of phishing domains reported in .US versus 62% from 2023. We observed that the decrease is the result of phishers migrating away from .US to other sources for phishing domains (as phishers often do) following a spike in malicious registrations in January 2023.

We cannot determine from our data why phishers no longer misuse .US as much as they did in January 2023. It is possible that phishers found .US particularly attractive for specific attack campaign or were testing their ability to exploit the TLD at volume. It does not appear, however, that the reduction was due to any changes in domain name registration processing or other procedures to combat malicious use. When we visited .US registrars in May 2024 and attempted to register .US domains, we did not observe any changes in nexus obligation processing or other procedures compared to our testing in 2023. While the reduction in exploitation from 2023 levels is positive for .US, it still remains among the most exploited ccTLDs for malicious registrations and will likely remain attractive to cybercriminals and vulnerable to high-level of misuse if no changes are made.

Domain Registration Policies Matter

Many ccTLDs impose requirements on domain registration. Such requirements include individuals (natural persons), proof of residency, citizenship, or real connection to the country and for businesses, a commercial registration, commercial presence (*e.g.*, headquarters) in country. Many countries request proof of identity, *e.g.*, a state personal identification number, passport, VAT number, and/or address in country. A recent study investigated whether the data accuracy practices of European Union (EU) country code Top Level Domain (ccTLD) registries contribute to those low levels of malicious domain names within EU ccTLDs.

To determine whether data accuracy or more stringent registration requirements generally, affected malicious domain registration levels, we studied two sample sets of ccTLDs – 26 countries in the European Union, and a like number in the Asia-Pacific region for which we had phishing data – to investigate whether there is a correlation between conditions imposed upon domain registrations and low phishing numbers or scores. We also collected a sample set of gTLDs for comparison purposes.

For ccTLDs, we collected the registration requirements for these from the country's network information centers (NICs) and domain registrars authorized to process registrations for the country.

We grouped the EU ccTLD set into three categories:

REGISTRATION REQUIREMENTS IN EU CCTLD SET	COMPOSITE PHISHING DOMAIN SCORE OF CCTLDS IN CATEGORY	COMPOSITE MALICIOUS PHISHING DOMAIN SCORE OF CCTLDS IN CATEGORY
NONE Any individual or legal entity, irrespective of their nationality, place of residence, area of operations	6.9	5.2
OPEN with requirements Any individual or legal entity, irrespective of their nationality, place of residence, area of operations BUT subject to some form of identity verification	3.3	1.5
RESTRICTED, strict requirements Proof of residency or business presence in country or EU	3.1	0.9

The ccTLDs in the EU have a very low combined phishing score (4.1) and malicious phishing score (2.1). When we look at the categories, we observed that **imposing verification requirements on domain registrations correlates with lower phishing and malicious registrations in the EU ccTLDs. The stricter the requirements, the lower this phishing score.**

We next examined ccTLDs of Asian countries. Here, we grouped the Asia TLDs into four categories.

REGISTRATION REQUIREMENTS IN ASIA CCTLD SET	COMPOSITE PHISHING DOMAIN SCORE OF CCTLDS IN CATEGORY	COMPOSITE MALICIOUS PHISHING DOMAIN SCORE OF CCTLDS IN CATEGORY
NONE Any individual or legal entity, irrespective of their nationality, place of residence, area of operations	33.7	18.8
OPEN with requirements Any individual or legal entity, irrespective of their nationality, place of residence, area of operations BUT subject to some form of identity verification	46.8	21.8
RESTRICTED, strict requirements Proof of residency or business presence in country.No Asia ccTLDs impose strict requirements	0	0
SUSPENDED Four registries have suspended domain registrations	-	-

In the Asia region, the findings are different. Here, .CN and .ID has very high scores relative to other ccTLDs in the "OPEN, with requirements" category in both the EU and Asia ccTLD sets.

The .ID ccTLD has no registration requirements and had the highest phishing score among the Asia ccTLD set. Despite having registration requirements, the .CN ccTLD had a phishing domain score of 68.1 and a malicious phishing domain score of 32.25. If we treat .CN as an outlier, the remaining Asia ccTLDs in the "OPEN, with requirements" category have a phishing domain score of 4.4 and composite malicious phishing domain score of 1.0, which are similar (nearly the same as the EU subset of ccTLDs in this category). Given this, we find that like the EU ccTLDs, stricter requirements in the Asia ccTLD set correlate with lower incidents of phishing.

For comparison purposes, we identified the 25 new gTLDs with the highest phishing domain scores and to this set we added 10 legacy gTLDs: .INFO, .PRO, .ASIA, .COM, .NET, .TEL, .ORG, .BIZ, .NAME and .MOBI. All these gTLDs met our 30,000 domains under management, or 25 phishing domains reported criteria. Any individual or legal entity, irrespective of their nationality, place of residence, area of operations can register domains in these gTLDs.

We then compared the scores for this gTLD set against those for the Asia and EU ccTLDs for which there were no registration requirements.

EU ccTLD registries have the lowest composite phishing scores, and this holds true even when they impose no registration requirements. This suggests that operational or business practices – selection of registrars, pricing, suspicious registration activity monitoring, or other – also influence how likely phishers are to misuse a registry. The significantly higher phishing scores of the new gTLDs suggest that some or all of these practices are absent and sorely needed.

Phishers Like Cheap

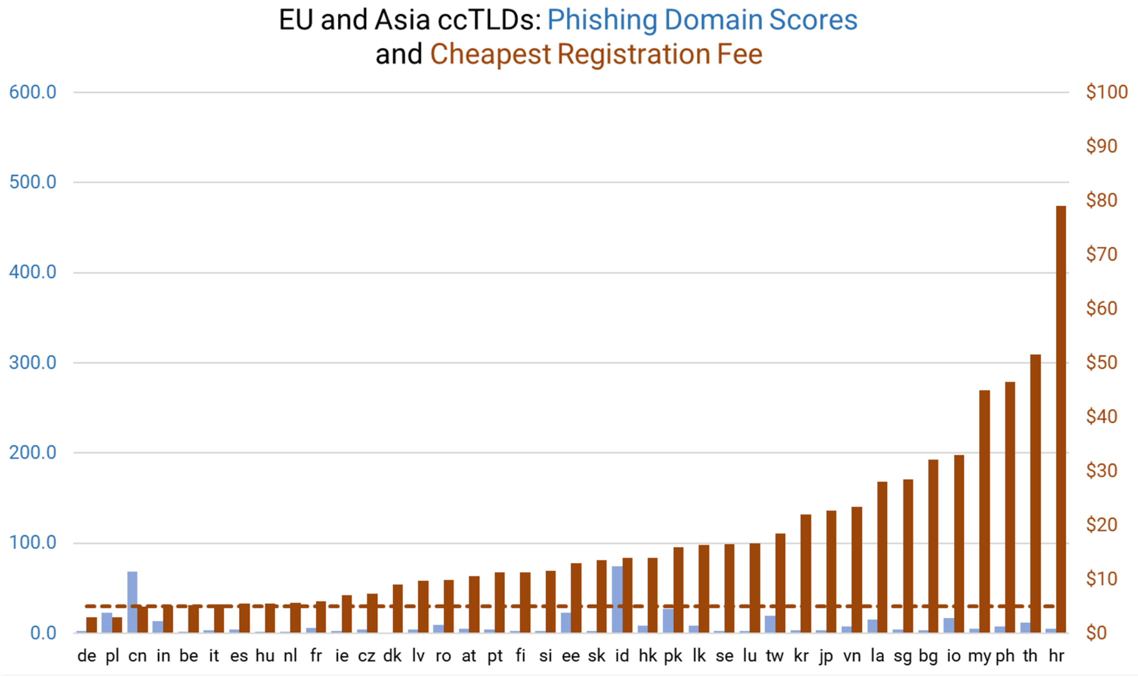
Freenom's exit from the domain registration industry alone does not account for the increase in phishing domains delegated from new gTLDs. Some registry operators continue to compete by offering cheap and sometimes free registrations.

COMPARISON OF TLD SETS WITH NO REGISTRATION REQUIREMENTS	COMPOSITE PHISHING DOMAIN SCORE	COMPOSITE MALICIOUS PHISHING DOMAIN SCORE
EU ccTLDs	6.9	5.2
ccTLDs (Asia and EU ccTLDs studied)	14.0	6.8
Legacy gTLDs	25.5	18.8
Asia ccTLDs	33.7	18.8
Legacy and hew gTLDs combined	40.2	33.3
New TLDs	273.7	262.2

Our data from May 2020 to April 2024 support the widely held view that phishers use cheap domain names because they can spend less and obtain more resources. Our data also show that cheap ccTLD domains are attractive as well.

We used comparative pricing data published by TLD-list.com and complemented these data with fees published by ccTLD registries that process registrations directly. We used TLD-lists.com's Cheapest Price History chart for each TLD to confirm that the fees have been offered frequently during our yearly study period. We omitted .BT, .CY, .MT, .MN, .TL, .MO, .BD from the chart because these did not meet our 30,000 domains under management, or 25 phishing domains reported criteria.

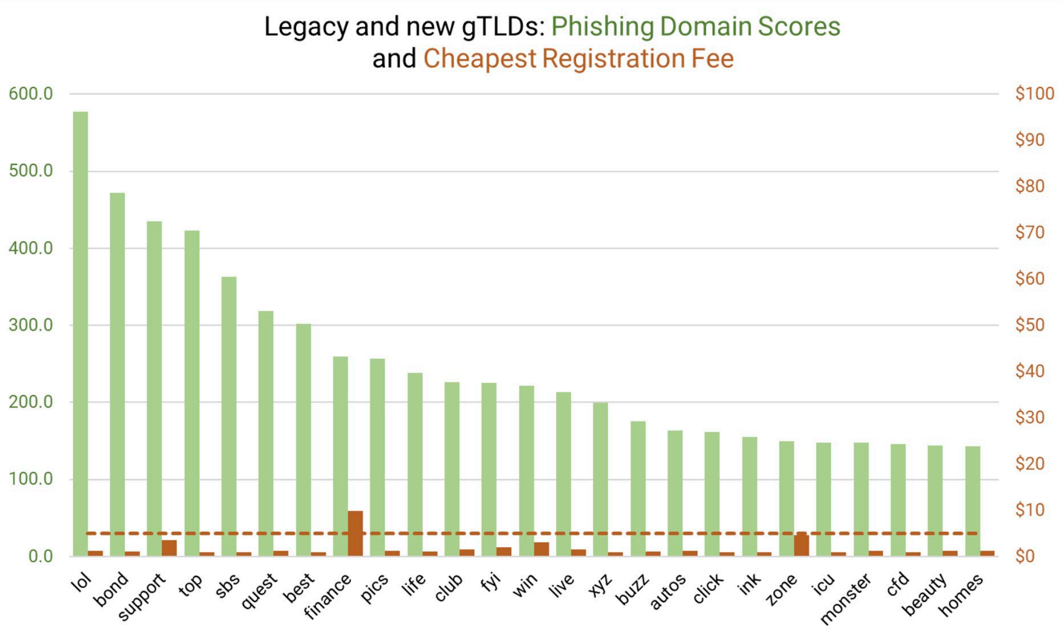
We observed that the ccTLDs with the most expensive domain registrations have the lowest phishing scores. While ccTLD registrations are generally higher than those of gTLDs, the three ccTLDs with the highest phishing domain scores – .CN, .IN, and .PL – were available for ~US$5.00. However, seven other ccTLDs offered registration fees under US$6.00 and these all had very low phishing domain scores, suggesting that EU and Asia ccTLD phishing scores appear to be affected by operational or registration requirements as well as pricing.



When we compared the ccTLD score-versus-pricing data to that of the gTLD data, we observed that all but three of the 35 gTLDs with the highest phishing domain scores were available for under US$5.00. Ten were available for under US$1.00, and 27 for under US$2.00. We also note that the phishing domain scores were generally much higher than those of the ccTLDs. The combination of cheap registration fees and a no registration restriction policy – cheap and easy – make the gTLD space generally, and the new gTLDs in particular, more attractive.

Our research over the past four years has demonstrated persistently, exceptionally high levels of domain abuse in new gTLDs. The attraction of gTLDs to phishers is unlikely to change unless pro-active, preventative measures are adopted for current or future new gTLDs.

Phishers who use fraudulently obtained payment methods can register many domains and their purchases will remain below payment fraud-detection. Registry operators and registrars who compete on price may run less than effective anti-abuse programs, as those programs cost money and effort.



Subdomain Providers

Our analysis reveals that **24% of all phishing attacks took place using resources at subdomain providers. More than half of these attacks use Google's services.** This is a growing vector for attacks. These phishing attacks are difficult to mitigate and pose persistent problems for phishing targets.

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

subdomain.domainname.tld

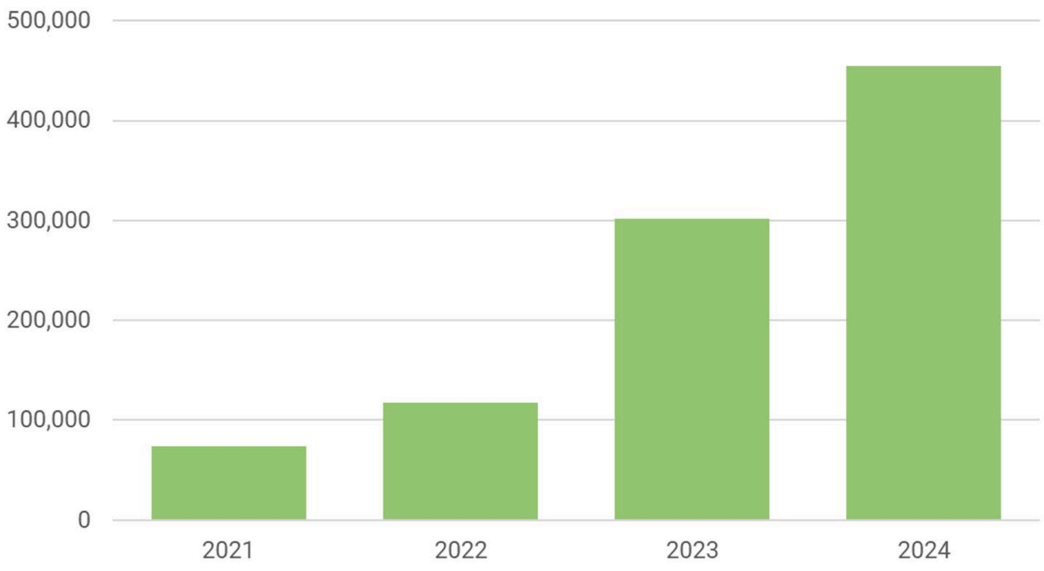
Some of these providers offer website building or hosting services. Others offer free DNS management so the customer can point the hostname to other hosting. Most of these services are free, offering free accounts. Phishers use the services to build and maintain phishing sites

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. Subdomain providers often lack effective, proactive measures to keep criminals from creating accounts and abusing their services, and some pay little attention to complaints. (Some don't even validate the user's email address when they create an account.) Finally, only the subdomain providers can effectively mitigate these phishing attacks.

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 and to scale.

We identified 454,948 phishing attacks created on 750 second-level domains operated by subdomain providers. This is up from just 74,315 attacks in our 2021 report. While the gross numbers are up, these attacks are also a growing percentage of all phishing. They were 24% of all attacks in our 2024 data set, up from 16.3% in our 2023 report, 12.8% in our 2022 report, and 10.7% in our 2021 report.

Phishing Attacks Using Subdomain Providers



Of those 454,948 attacks, 54% used Google's subdomain and hosting services. And **90% of the attacks (410,300) occurred on domains operated by just ten companies.** The top ten providers were:

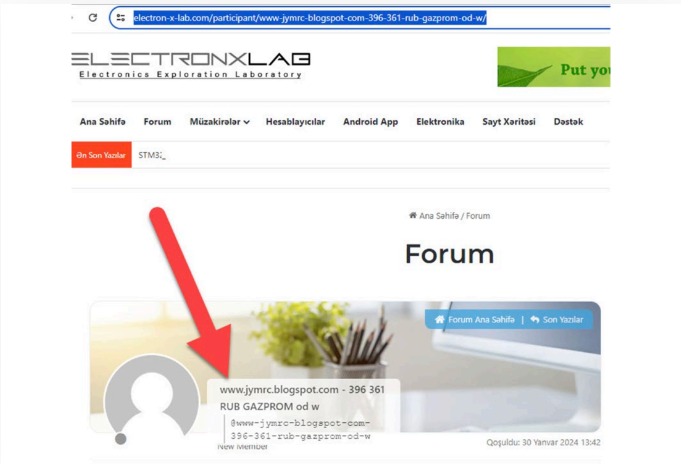
2024 RANK	PROVIDER	DOMAINS	2023 PHISHING ATTACKS	2024 PHISHING ATTACKS	% CHANGE
1	Google	blogspot.com and blogspot.xx on 100+ ccTLDs. web.app, firebaseapp.com, page.link, googleapis.com, appspot.com, doubleclick.net, business.site	77,580	**247,582**	**+219%**
2	DuckDNS	duckdns.org	77,667	**60,913**	**−22%**
3	Weebly	weeblysite.com, weebly.com	19,035	**24,736**	**+30%**
4	Cloudflare	**pages.dev, workers.dev, trycloudflare.com**	7,585	**17,740**	**+134%**
5	CentralNIC	**za.com, sa.com, ru.com, com.de, us.com, uk.com, de.com, br.com, jp.net, eu.com, cn.com, gb.net, uk.net, kr.com, jpn.com, ae.org**	13,636	**12,563**	**−8%**
6	Hostinger	000webhostapp.com, **preview-domain.com, 96.lt**	22,781	**12,464**	**−45%**
7	Github	github.io	3,613	**11,485**	**+218%**
8	Wix	wixsite.com, filesusr.com, usrfiles.com	4,337	**8,281**	**+91%**
9	ChangeIP	**126 different domains**	3,110	**7,521**	**+142%**
10	Replit	**repl.co**	16,256	**7,015**	**−57%**

Services of this type are increasingly being abused to perpetrate significant damage. Subdomain providers must have preventative, proactive ways to prevent the mass exploitation of their services, and to provide quick anti-abuse monitoring and takedown capabilities.

Case Study

Google's Blogger Service and the Gazprom Attacks

Phishers used Google's Blogger service to launch a large, sustained phishing campaign against Gazprom, the state-owned Russian gas and petroleum company. Our sources began reporting the attacks on December 13, 2023, with waves of URLs reported through April 3, 2024. The campaign used at least 44,461 subdomains on Blogspot's domain names across various TLDs, using 6,715 unique hostnames, and at least 271 .SHOP domains and 40 .TOP domains. The attacks were advertised using forum spam – the phishers posted URLs on sites powered by Shopify and other sites across the globe that allowed automated account creations and postings. For example, phishers advertised the domain *JYMRC.BLOGSPOT.COM* on January 30, 2024, in the forum of this Azerbaijani engineering site:



electron-x-lab.com/participant/www-jymrc-blogspot-com-396-361-rub-gazprom-od-w/

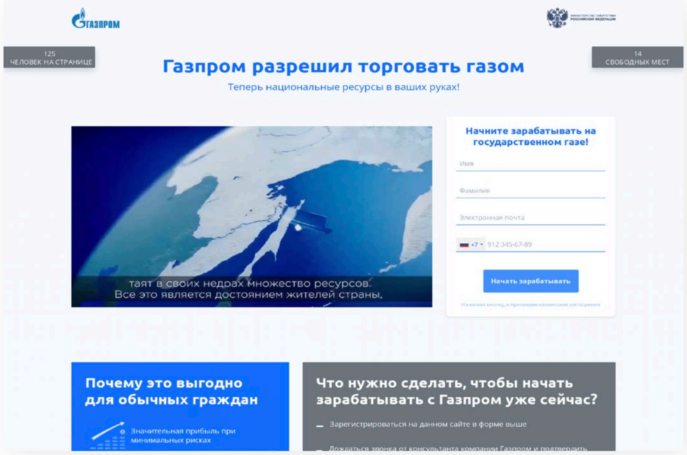
www.jymrc.blogspot.com - 396 361 RUB GAZPROM od w

@www-jymrc-blogspot-com-396-361-rub-gazprom-od-w

New Member

Qoşuldu: 30 Yanvar 2024 13:42

That phishing link led to the Gazprom phishing site on a .SHOP domain purchased by the phishers:



125 ЧЕЛОВЕК НА СТРАНИЦЕ

14 СВОБОДНЫХ МЕСТ

Газпром разрешил торговать газом

Теперь национальные ресурсы в ваших руках!

таят в своих недрах множество ресурсов.
Все это является достоянием жителей страны,

Начните зарабатывать на государственном газе!

Имя

Фамилия

Электронная почта

+7 912 345-67-89

Начать зарабатывать

Нажимая кнопку, я принимаю клиентское соглашение

Почему это выгодно для обычных граждан

Значительная прибыль при минимальных рисках

Что нужно сделать, чтобы начать зарабатывать с Газпром уже сейчас?

- Зарегистрироваться на данном сайте в форме выше
- Дождаться звонка от консультанта компании Газпром и подтвердить

Above: Gazprom phishing site at G2KPM.SHOP, captured January 30, 2024

Nearly all these attacks were hosted on a single IPv4 address (81.91.178.100) operated by a Seychelles-based company called Online Data Servers in ASN 204601 (Zombro B.V).

Phishing activity observed targeting Gazprom was uniquely high during this study period. In fact, our research showed Gazprom to be the second most phished brand behind Facebook (see the *Targeted Brands* section). This is the first time Gazprom has appeared on our top brands list. We cannot directly ascertain why the brand made such a sudden appearance. However, it is possible that recent world events have made this brand an attractive target for cyberattackers. Regardless of the motivation or underlying cause, it is clear that criminals found easy access to resources to conduct their attacks using subdomain hosting services.

Phishers Exploit a New Attack Resource: The InterPlanetary File System

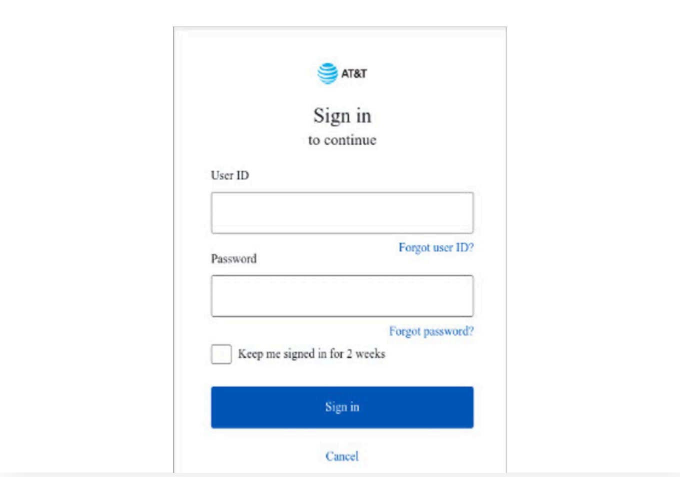
Phishing using the InterPlanetary File System (IPFS) has exploded in the last year and was used to host 19,387 phishing sites in our 2023–2024 data. In our 2022–2023 report data, it was used to launch only 1,475 attacks – a 1,314% increase.

The InterPlanetary File System (IPFS) is a decentralized data storage and delivery network based on peer-to-peer (P2P) networking. It's an example of "Web3" technologies, which are generally based on the concept of decentralization and often incorporate blockchain technology. Instead of having a central server that holds and distributes a Web site or data file, IPFS is a decentralized system of user-operators who hold copies of data. Any user in the network can serve a file by its content address, and other peers in the network can find and request that content from any node that has it.

Major web browsers do not currently support the IPFS protocol, so providers operate "gateways" to help people access IPFS content. A gateway is an IPFS peer that accepts HTTP requests for IPFS content IDs, allowing users to use their default browsers to access the IPFS content on a standard domain name. An example of one of these IPFS content IDs represented as a URLs is:

*https://bafybeieebriagjcprrliv2cod6j7f7 6ayoatuxfnswg 33dz2y2ao3p73m.ipfs.**infura-ipfs.io***

That URL was used to make this mobile-optimized phishing site accessible through web browsers:



Sign in
to continue

User ID

Forgot user ID?

Password

Forgot password?

□ Keep me signed in for 2 weeks

Sign in

Cancel

Site Attacking AT&T Users
Source: urlscan.io

Phishing first appeared on IPFS gateway URLs in 2022, and cybersecurity company Trend Micro became concerned about IPFS's use for phishing in 2023.

In our latest data set, most of the IPFS-hosted phishing was routed through gateways operated by just five companies:

2024 RANK	PROVIDER	DOMAINS	2023 PHISHING ATTACKS	2024 PHISHING ATTACKS
1	IPFS Foundation	dweb.link and ipfs.io	264	**8,743**
2	Cloudflare	cf-ipfs.com and cloudflare-ipfs.com	552	**4,351**
3	NFT.Storage Ltd.	nftstorage.link	0	**2,405**
4	Consensys	infura-ipfs.io	394	**2,381**
5	Fleek	fleek.co and fleek.cool	48	**847**

Cloudflare is currently phasing out its own gateways to use those operated by the IPFS Foundation and its spinoff Interplanetary Shipyard, creating further consolidation at the top of the list.

While IPFS is sometimes touted as a technology that is "permissionless, trustless, censorship resistant, and free of centralized gatekeepers," a phishing site hosted on IPFS can be effectively neutralized if a gateway operator simply stops making the URL resolve on its standard DNS domain.

To make that happen, some gateway providers are using the Bad Bits Denylist. This is a blocklist of IPFS IDs that IPFS gateway operators can refuse to serve, if they choose to. The Denylist is used to curb phishing, malware distribution, copyright violations, and other abuses, and is operated by Protocol Labs, which invented the IPFS protocol and also operates two popular gateways. The Bad Bits Denylist has drawbacks: it is a reactive listing system based on abuse complaints, the IPFS Foundation does not always process abuse reports in a timely fashion, and some gateway providers do not use the Denylist. (Some operate their own, and accept abuse complaints on their web sites.) One prominent gateway operator, NFT.Storage, admits that "malicious actors can generate this content faster than security-minded users can flag them."

We believe that phishers will continue to ramp up their use of IPFS gateways – they will abuse these free, handy services just as they have abused third-level domains providers, URL shorteners, and dynamic DNS providers. Gateway providers, especially the IPFS Foundation and Interplanetary Shipyard, will need to process abuse complaints quickly and must learn to keep criminals from weaponizing these services. We advise them to adopt proactive measures to identify bad actors wherever possible.

Domain Registrars

Of the domain names used to host phishing attacks, most are registered by phishers, to perpetrate phishing. Phishers sometimes use the domains of innocent registrants by breaking into their hosting or domain management services. Some gTLD registrars tend to have more phishing domains because they offer low prices, do not effectively keep phishers from becoming customers, and/or do not respond effectively to abuse reports, inviting repeat registrations.

The registrars with the most gTLD domains used for phishing attacks were:

2024 RANK	REGISTRAR	REGISTRAR IANA_ID	gTLD DOMAINS UNDER MANAGEMENT	PHISHING DOMAINS
1	NameSilo	1479	4,629,000	**93,131**
2	GoDaddy	146	65,960,522	**69,007**
3	GMO d/b/a Onamae	49	5,246,759	**59,792**
4	PublicDomainRegistry	303	4,298,842	**56,845**
5	NameCheap	1068	16,562,932	**52,415**

4–YEAR COMPARISON OF REGISTRARS WITH MOST PHISHING DOMAINS REPORTED

2021 Study	2022 Study	2023 Study	2024 Study
1. NameCheap	1. NameCheap	1. NameSilo	1. NameSilo
2. NameSilo	2. GoDaddy	2. PDR	2. GoDaddy
3. GoDaddy	3. NameSilo	3. NameCheap	3. Onamae
4. PDR	4. DNSpod	4. GoDaddy	4. PDR
5. Tucows	5. ALIBABA	5. Sav.com	5. NameCheap

Registrar rankings for this yearly study period are posted at the Cybercrime Information Center.

Below we compare whether a gTLD registrar (with at least 30,000 domains under management) had 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 score are:

2024 RANK	REGISTRAR	REGISTRAR IANA_ID	gTLD DOMAINS	PHISHING DOMAINS	PHISHING DOMAIN SCORE
1	NICENIC	3765	100,732	45,238	**4,490.90**
2	URL Solutions	1449	229,113	43,877	**1,915.10**
3	Aceville	3858	189,118	13,538	**715.9**
4	WebNic	460	685,443	19,007	**277.3**
5	OwnRegistrar	1250	513,858	13,420	**261.2**

The highest-scoring registrar was NiceNIC International, a registrar in Hong Kong. *NiceNIC had 45% of its entire gTLD portfolio reported for phishing*. Almost all of these domains were maliciously registered, with the reports coming within three days of registration. The domains were registered in batches throughout the year study period. They were mostly hosted at just a few places, including more than 5,000 hosted at a Russian ISP called Prospero (AS200593). The domains were used to attack a wide variety of prominent companies around the world – suggesting that many parties were constantly contacting NiceNIC with takedown requests. NiceNIC also ranked #1 in our 2023 study, when 26% of its gTLD portfolio was used for phishing.

Bulk Registrations

Bulk registrations are one of the most common domain acquisition tactics in the phishing space: at least 27% of the domains used for phishing in our study data were registered in bulk.

Legitimate, law-abiding domain name registrants rarely need to register more than a few domain names at a time. (A few that do are trademark owners, who sometimes register domains names defensively, to protect their brand names.) In contrast, cybercriminals are among the few categories of people who register domains in bulk. Criminals regularly register hundreds to thousands of domains at a time, which they use to run large phishing and spamming campaigns. Yet some registrars tout their bulk registration tools — because bulk registrations provide revenue.

We consider a set of domains to be bulk registered if at least ten domains in our data set were registered through the same registrar, and there was less than ten minutes between consecutive domain registrations. We found 9,081 sets of such bulk registrations, registered at 97 different registrars. These domains are almost always generated by a script and have no meaning — they usually consist of random characters, or two random dictionary words jammed together.

The registrars associated with the highest number of bulk domains were:

Registrar	IANA ID	Total bulk-registered domains	Sets	Largest set (# of domains)
GMO d/b/a Onamae	49	**43,884**	337	17,562
NameSilo	1479	**40,983**	1,621	676
URL Solutions	1449	**37,583**	435	2,241
Gname	1923	**25,589**	714	288
GoDaddy	146	**25,529**	904	494
NICENIC	3765	**16,152**	796	158
PublicDomainRegistry	303	**14,782**	723	169
NameCheap	1068	**14,340**	659	164
WebNic.cc	460	**9,308**	185	1552
Aceville	3858	**7,767**	322	143

The number of sets, and the number of domains registered in these sets, is under-counted. Our data set consists of only domain names that were reported for phishing. Many more domain names were involved in these bulk sets than we know about – certainly many were registered in these sets and used for phishing, but they were not detected and reported. And our data set does not include domains registered for (illegal) spamming campaigns.

Note also that some (criminal) registrants register smallish sets of domains — sometimes 20 at a time — but register sets regularly, sometimes every day over a period of days, or every week, and thereby consume large numbers of domains over time. Seemingly dissociated sets are sometimes the work of one threat actor, which can sometimes be revealed by analysis of the hosting, domain patterns, and other telltale signs. In the past, investigators could associate, and aggregate sets based on registrant contact data. Contact data is now rarely available mainly because of ICANN's policies. and this makes it hard to identify and quickly mitigate phishing campaigns.

The registrars who sponsored the largest single sets of bulk domain registrations are:

REGISTRAR	IANA ID	TOTAL BULK REGISTERED DOMAINS	SETS	LARGEST SET (# OF DOMAINS)
GMO d/b/a Onamae	49	43,884	337	**17,562**
URL Solutions	1449	37,583	435	**2,241**
WebNic	460	9,308	185	**1,552**
Amazon	468	807	5	**748**
NameSilo	1479	40,983	1,621	**676**

Case Study

GMO Bulk Registrations

The largest set included at least 17,562 domains, registered at GMO on 19 February 2024. The phisher registered an average of 38 domain names per minute over an eight-hour period. The domains were all composed of eight random letters, such as *gzraxywl.lol* and *htcjkpzb.lol*. These bulk registrations made at GMO were used to attack a variety of targets, including users of Swiss Post, Facebook, Telegram, Booking.com, and AEON Financial.

Hosting Networks

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.

We found phishing in 4,284 hosting networks. We show results for phishing hosted on IPv4 addresses only. We do not see IPv6 addresses reported for phishing in our feeds.

Ten of the top hosting providers accounted for one-half of the 1,897,952 phishing attacks for which an ASN could be determined. ASNs delegated to Cloudflare accounted for one-third (minimum 50,000 attacks).

2024 RANK	HOSTING PROVIDER	AS NUMBER	# ROUTED IPV4 ADDRESSES	PHISHING ATTACKS
1	Cloudflare	13335	2,600,448	**437,108**
2	Google	15169	11,261,184	**183,454**
3	Amazon	16509	46,800,128	**65,981**
4	Fastly	54113	1,127,056	**49,641**
5	IQWeb	59692	7,936	**47,319**

4-YEAR COMPARISON OF HOSTING NETWORKS WITH MOST PHISHING DOMAINS

2021 Study	2022 Study	2023 Study	2024 Study
1. NameCheap	1. Cloudflare	1. Cloudflare	1. Cloudflare
2. Cloudflare	2. UnifiedLayer	2. Quadranet	2. Google
3. UnifiedLayer	3. Microsoft	3. ColoCrossing	3. Amazon
4. Google	4. NameCheap	4. Google	4. Fastly
5. Digital Ocean	5. Google	5. UnifiedLayer	5. IQWeb

ASN rankings for this yearly study period are posted at the Cybercrime Information Center.

Cloudflare's AS13335 had the most phishing attacks reported for the third year in a row. The San Francisco based operator 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. Phishers continue to take advantage of this to hide the hosting locations of phishing pages from security responders. Cloudflare also provides subdomain services and hosting that were used by phishers.

Google is one of the largest network providers. AS15169 is delegated to Google. While Cloudflare's 437,108 phishing attacks were hosted at 48,798 unique IPv4 addresses in its ASN 13335, Google's 183,454 phishing attacks were hosted at a mere 596 addresses. 168,615 of these were hosted on IPv4 addresses in CIDR prefixes used to host Blogger accounts.

IQweb (United Arab Emirates) has the smallest address allocation of the top five. The hosting operator has 7,680 IPv4 addresses and approximately 100,000 hosted domains but the operator's infrastructure hosted a startling 47,319 phishing attacks.

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, 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:

2024 RANK	AS NAME	AS NUMBER	# ROUTED IPV4 ADDRESSES	PHISHING ATTACKS	PHISHING ATTACK SCORE
1	Zomro	204601	57,856	45,385	**7844.5**
2	BGP Consultancy	64050	97,024	38,898	**4009.1**
3	Dimension Network & Communication	59371	53,760	13,769	**2561.2**
4	Nocix	33387	69,376	14,793	**2132.3**
5	Cloudflare	13335	2,600,448	437,108	**1680.9**

Zomro: Phishing attacks against Gazprom largely accounted for Zomro's extraordinarily high phishing score (see the *Ranking of TLDs by Scoring Metrics* section).

BGP Consultancy and Dimension Networks: More than10,000 of the phishing attacks reported as hosted in BGP Consultancy's AS64050 occurred on domain names sponsored by registrar Gname.com. 8,533 of these domains were registered in .CLUB, .COM, and .ORG. The creation dates and domain string patterns of nearly all these domain names are characteristic of bulk registration behavior (see the *Bulk Registrations* section). We found "all numeric" domain strings, again registered via Gname.com, and mostly delegated from .CC, .CLUB, .COM in Dimension Networks & Communications AS59371.

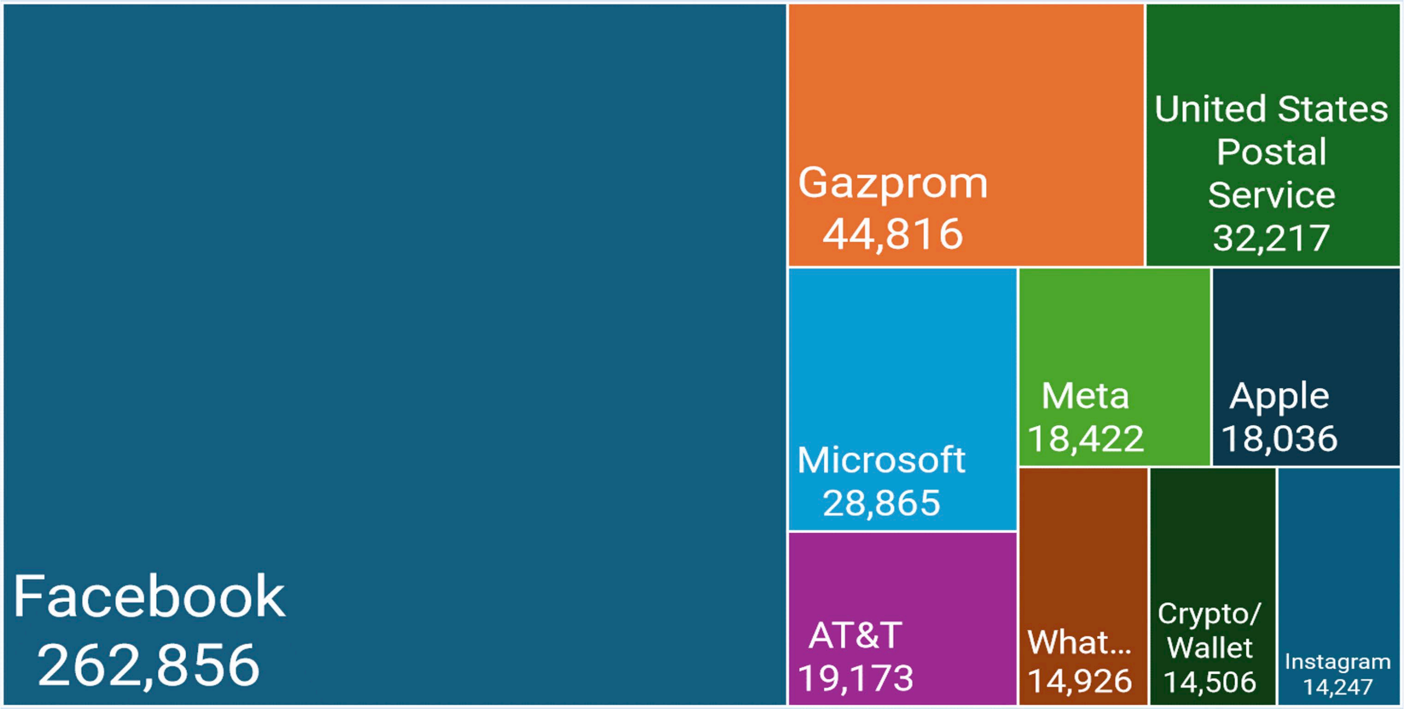
.TOP was Toxic to Nocix. There were 14,793 phishing attacks hosted at Nocix's AS33387, of which 13,650 were from domains registered in .TOP. From May 2023 to October 2023, there were an average of 1,500 phishing attacks per month from .TOP domains hosted at Nocix. As of May 2024, .TOP domains could be registered for ¥12 Chinese (US$1.66) at Chengdu West or for US$1.05 at Spaceship. Lacking academic research or an independent 3rd party pricing study and analysis of registration fees paid for maliciously registered domain names, we cannot say with certainty that cheap fees attract phishers.

Targeted Brands

Facebook was the brand most often used in phishing attacks.

Meta's Facebook was the most attacked brand in our 2023-2024 study data, and Meta's other brands – Instagram, WhatsApp and the Meta brand itself – also appear in our list of the most-impersonated brands. Collectively, impersonation of Meta Platforms' brands increased 126% over the prior year.

Top Phished Brands May 2023 — April 2024



Gazprom, a multinational energy corporation with a majority Russian state-ownership, was the second-most attacked and impersonated brand.

The United States Postal Service ("USPS") remained in the top ten for a second year.

Any organization, service, or brand can be used as a lure in phishing attacks at any time, as phishers appear to constantly look for companies that have potentially lucrative user information, are newly popular, or do not have the resources or familiarity with phishing defenses to respond quickly and adequately.

Using Brand Names in Phishing Domain and Phishing URLs

Phishers continue to use company, service, and product name in phishing URLs to deceive victims.

It is rare that phishers register domain names that contain the brand name they are attacking. Out of the 1.1 million domains names used for phishing, only about 53,000 contained a match for the brand keyword – less than 5%. (We counted domains such as *amazon-login.click* and *securexfinity.com*.) Additional domains contained misspellings of brand keywords. Many phishers know that brand owners are scanning zone files for matches, and so avoid registering them to evade detection.

Instead, phishers continue to embed the names of brands elsewhere in the URLs, where users may see them and mistake them as legitimate. Some are found in the URL path, such as:

https://encontrardispositivos.info/*apple*-eng.php

Some are found in subdomains, such as:

https://login-*apple*.com--verify.info/expire/

Subdomain providers such as Google's Blogger service were used to create many of the brand-in-subdomain attacks, such as:

https://*facebook*-recover-com.blogspot.com/

Case Study: Attacks Involving Meta Brands

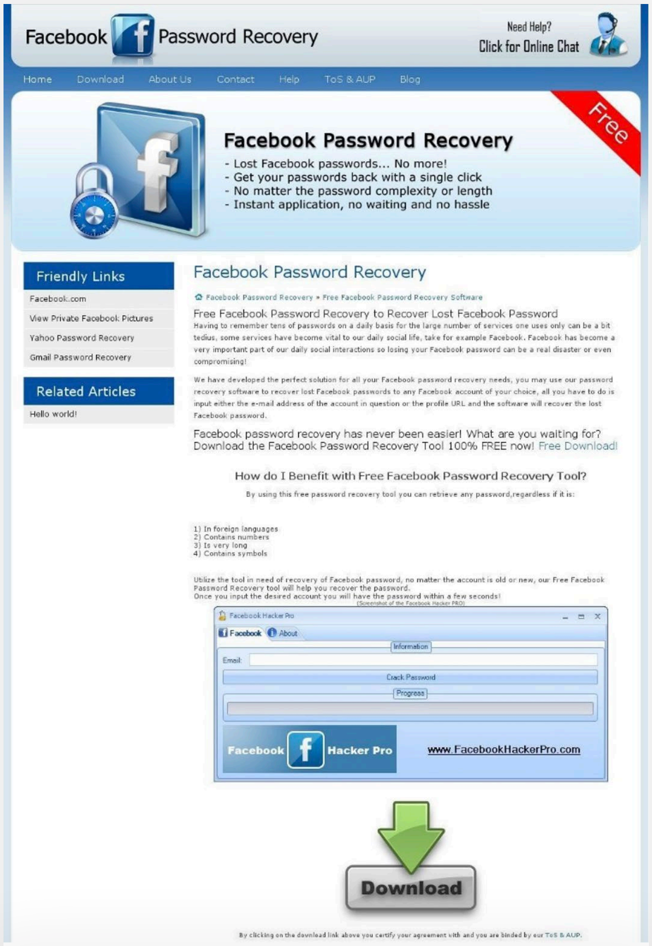
310,508 phishing attacks attempted to lure victims to fake Meta, Facebook, Instagram, and WhatsApp web pages. These attacks were used only 32,811 domain names. Most of the attacks used misspellings or similarities of Meta brands somewhere in the URL, *e.g.*, the hostname or the path, but **8,410 of these attacks incorporated an exact match of a Meta brand in the host name element of the URL.**

More than two-thirds of phishing attacks involving Meta brands were launched using subdomain providers (*e.g.*, free web sites), where phishers create accounts for free using an email address and password and receive DNS service for their phishing host name. 5,693 of these attacks incorporated an exact match of a Meta brand in the user account. 186,703 used subdomains provided by Google. 165,441 of these were on domains operated on Google's Blogger service.

Case Study: Attacks Involving USPS Brand

Phishers used different deception tactics to phish the United States Postal Service (USPS).

Of the 12,068 attacks that were identified as phishing attacks on the United States Postal Service, the string "usps" was present in domain name part of the URL in 11,885 of those attacks. This is a very different behavior from phishing involving Facebook, where phishers flocked to free web hosting because fewer than 200 of the attacks against USPS were hosted at subdomain providers.



Facebook Password Recovery

- Lost Facebook passwords... No more!
- Get your passwords back with a single click
- No matter the password complexity or length
- Instant application, no waiting and no hassle

Facebook Password Recovery

Facebook Password Recovery » Free Facebook Password Recovery Software

Free Facebook Password Recovery to Recover Lost Facebook Password

Having to remember tens of passwords on a daily basis for the large number of services one uses only can be a bit tedius, some services have become vital to our daily social life, take for example Facebook. Facebook has become a very important part of our daily social interactions so losing your Facebook password can be a real disaster or even compromising!

We have developed the perfect solution for all your Facebook password recovery needs, you may use our password recovery software to recover lost Facebook passwords to any Facebook account of your choice, all you have to do is input either the e-mail address of the account in question or the profile URL and the software will recover the lost Facebook password.

Facebook password recovery has never been easier! What are you waiting for? Download the Facebook Password Recovery Tool 100% FREE now! Free Download!

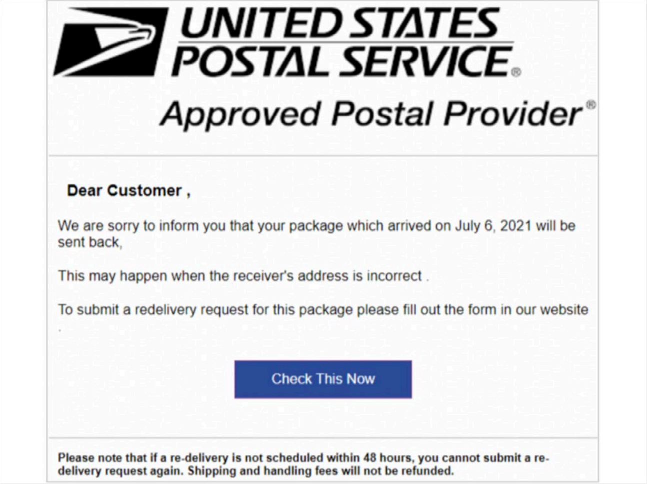
How do I Benefit with Free Facebook Password Recovery Tool?

By using this free password recovery tool you can retrieve any password,regardless if it is:

1) In foreign languages
2) Contains numbers
3) Is very long
4) Contains symbols

Utilize the tool in need of recovery of Facebook password, no matter the account is old or new, our Free Facebook Password Recovery tool will help you recover the password.
Once you input the desired account you will have the password within a few seconds!
(Screenshot of the Facebook Hacker PRO)

By clicking on the dovnload link above you certify your agreement with and you are binded by our ToS & AUP.



Dear Customer ,

We are sorry to inform you that your package which arrived on July 6, 2021 will be sent back,

This may happen when the receiver's address is incorrect .

To submit a redelivery request for this package please fill out the form in our website .

Please note that if a re-delivery is not scheduled within 48 hours, you cannot submit a re-delivery request again. Shipping and handling fees will not be refunded.

EXACT MATCH IN STRING	TLD
usps-delivery	.XYZ, .COOL, .ASIA
delivery-usps	.COOL, .TECH, .PRO, .ASIA
usps-manage	.TECH, .WORK

Recommendations for Reducing Phishing and Criminal Access to Resources

Phishing is the primary attack vector for 90% of cyberattacks.

For the fourth year running, our study has measured and identified distinct and persistent patterns in the exploitation of key Internet resources used in the perpetration of phishing attacks. With the benefit of longitudinal data, we have also demonstrated how and where cybercriminals are adapting to exploit new resources, such as the InterPlanetary File System.

Despite exhaustive global awareness of the threats and impacts of cybercrime, our research, along with the research of a multitude of other organizations and firms, shows that cyberattacks continue to grow unabated. While initiated in cyberspace, these attacks wield concrete and devastating impacts in the real world. As we've noted in this report and previously, the result is billions of dollars of direct losses to consumers, businesses, and institutions, increased costs of commerce, trillions lost in the broader the global economy, and ultimately the disruption of human lives.

It is well past time to implement the strategies and solutions needed to disrupt the cybercrime supply chain and starve cybercriminals of the resources they use to perpetrate crime.

We advocate for balanced policies that will make it harder for criminals to obtain and use domain names, while keeping it easy for law-abiding, legitimate registrants to get the resources they need.

Based on our research, we recommend the following actions.

1. Implement Bulk Domain Name Registration Requirements

Our findings demonstrate that bulk registration is one of the most egregious domain acquisition techniques used by criminals.

Registrants requiring bulk registration should be required to apply and undergo enhanced identity and verification checks before accessing high volume registration services. Such bulk registration "certification" could conceivably be implemented in a variety of ways, for example on a registrar-by-registrar basis or through a credential recognized industry-wide, or by other means.

Registrars and registries should also monitor and scrutinize high-volume transactions for suspicious registration behavior. They should look for domain names closely matching famous and well-known brands, names deceptively similar to brands, and algorithmically generated names, among other suspicious behavior. Effective systems exist to do this, such as the Abuse Prevention and Early Warning System (APEWS) created by EURid. The implementation of such systems can make monitoring easy and cost-effective across the industry.

2. Limit High Volume Subdomain Account Creation

The use of subdomain providers by criminals for phishing attacks (e.g., <subdomain>.blogspot.com) has grown steadily since we began our research in 2021. This year, subdomain services accounted for a remarkable 24% of all phishing attacks. Many of these services allow the creation of large numbers of accounts at one time, which is highly exploited by criminals.

Subdomain providers should limit the number of subdomains (user accounts) a customer can create at one time and suspend automated, high-volume automated account sign-ups – especially using free services.

3. Strengthen Verification of Customers and Submitted Registration Information

Cybercriminals often use false contact information to register resources. The domain name industry, subdomain providers, and hosting companies should strengthen and implement more effective measures to enhance verification of customers and the information provided during registration.

At a minimum, these industries should implement basic automated address verification tools, or otherwise screen for bogus registration data and fraudulent payment information. Digital identity verification platforms or 3rd party services can be used to screen customers for pennies per transaction.

Customer contact data should also be made more readily accessible for legitimate law enforcement, public safety, and private sector cyberattack mitigation purposes. ICANN should also require that the contact information of companies (legal persons) be published in Registration Data Directory Services (RDDS). The European Union recently required this in its NIS 2 directive, and it should be implemented on an industry-wide basis.

As we describe in our study, ccTLDs in Europe and Asia that impose stricter requirements for domain registrations, including identity verification requirements, have lower incidents of phishing and malicious registrations. Adoption of identity verification requirements currently in use by ccTLDs with few or no phishing domains should be considered.

The United States U.S. Department of Commerce recently issued a Notice of Proposed Rulemaking entitled "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities." The proposed rule would require U.S. Infrastructure as a Service (IaaS) providers to verify the identity of their foreign customers and authorize special measures to deter foreign malicious cyber actors' use of U.S. IaaS products. Interisle provided comments on the proposed rule.

Enhanced verification requirements could help deter the use of U.S. hosting services by foreign phishers. Such measures could be more effective, however, if applied to all hosting customers and not just to foreign customers.

4. Expand Deployment of Automated Systems to Screen for Suspicious Registration and Use Patterns.

Phishers often engage in identifiable patterns of suspicious registration behavior, such as registering large batches of algorithmically generated names and names that are confusingly similar to known brands.

Domain name and subdomain providers should monitor and scrutinize transactions for such behavior. They should look for names matching known brands, names that are deceptively similar to known brands, and algorithmically generated names, among other suspicious patterns. If a string is suspiciously composed, the registration request should be delayed until it can be investigated further.

The industry should be encouraged to further develop automated monitoring technology (such as the EURid APEWS) that can be easily and cheaply implemented across the sector. Publicly or commercially available trademark lists could be used as the basis for systems to monitor for brand matches.

Domain name registrars and registry operators should make use of one or more phishing reporting services or data sources to determine what phishing domains have been registered by their customers and to check for other suspicious domains their customers may have registered. Registrars and registry operators should suspend the entire portfolio of domains of newly discovered phishers and their associated accounts. Implementing such proactive measures may also reduce the registrar's future expenses for abuse complaint processing and increase their market reputation.

Similarly, hosting companies should adopt more effective, proactive procedures that identify use of hosting resources for cybercrime, including measures to suspend suspicious accounts in a timely way. IPFS gateway operators also need to prevent criminals from weaponizing their services. We recommend they adopt proactive measures to identify bad actors wherever possible and suspend malicious URLs when they are identified.

5. Offer Trusted Reporter Programs

“Trusted reporters” or “trusted flaggers” are companies or organizations that are skilled at finding and documenting abuse and have proven that they have low false-positive rates. Internet providers offer a way for trusted reporters to send in abuse reports. Some providers check the incoming abuse reports in priority fashion, while others automatically suspend the domains or URLs that are reported. The latter approach has been found to be very effective at deterring abuse, cutting phishing uptimes, and reducing the profits of cybercriminals.

A variety of companies operate trusted reporter programs to address a range of abuses, including some of the large hosting and cloud providers, and online safety authorities. The European Union’s Digital Services Act and NIS 2 Directive created trusted flagger programs. Under these laws, Internet providers can be fined if they do not promptly process reports from trusted flaggers.

Trusted reporter programs that facilitate the swift suspension of phishing resources identified by recognized and trusted cybercrime monitors should be created and/or strengthened across the domain name, subdomain, and hosting industries. Customer contact data should also be made readily accessible to law enforcement, public safety, and trusted private sector cyberattack responders.

6. Require Corrective Action

Every quarter we measure and analyze the amount of phishing activity taking place across domain name registries and registrars. Year after year, our research finds a high level of consistency in the registries and registrars that are most commonly used by criminals to perpetrate phishing.

ICANN should adopt policies that require consistently poor performers to improve business practices and reduce use by criminals or face penalties for failure to do so, including increased fees, suspended or reduced ability to process gTLD domain registrations, and possible deaccreditation.

Disincentive fees could be used to fund phishing prevention research and to develop open-source anti-abuse technical solutions or subsidize anti-abuse services that can be adopted broadly across industry.

7. Adopt Preventative Anti-Abuse Measures Prior to New gTLD Launch

Our research has demonstrated exceptionally high levels of domain abuse in new gTLDs, that continue to own the smallest fraction of the market (10%) while accounting for the largest proportion of phishing attacks (42%). We are concerned that unless pro-active, preventative measures are adopted for current or future new gTLDs, this problem will be exacerbated.

Enhanced, preventative anti-abuse procedures, such as we recommend in this section, should be adopted and applied on an industry-wide basis to existing gTLDs.

8. Enhance outcome-oriented, cross-sector collaboration

Phishing is a multi-sector, multi-industry concern. Coordination, cooperation, and most importantly, consistent action, across a range of actors will be the only effective way to create change. Furthermore, in addition to formal processes such ICANN and voluntary industry efforts, action by government may be needed to foster effective solutions.

Industry would benefit from the development and promulgation of broader industry best practices, including polices, operational practices, and technical solutions to promote:

- Effective enforcement of acceptable use policies that prohibit fraudulent, illegal, or deceptive practices, including phishing.
- Adoption of industry-wide commitments for taking down phishing pages.
- Recommended (best) content management practices that can reduce vulnerable attack surfaces.

- Uniform and timely cooperation with law enforcement, phishing and brand protection services, and private-sector cyber investigators within hours, rather than days or weeks, of identification.
- Development of solutions to facilitate effective and timely data sharing within and across industries for the purpose of identifying and reducing cybercrime.

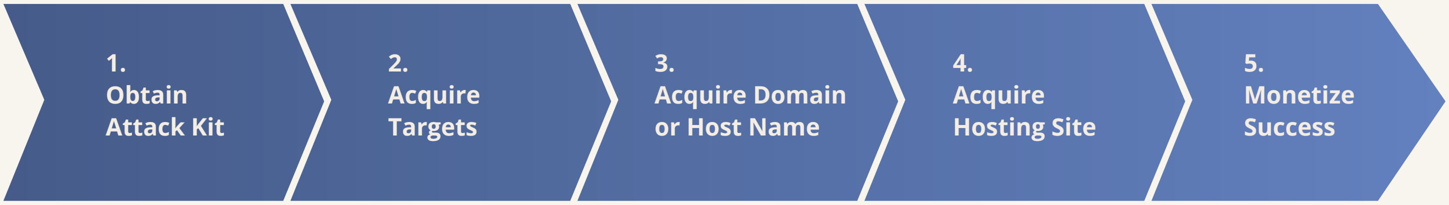
In an effort to promote cross-sector dialogue and development of new solutions, Interisle contributed to the organization of a phishing prevention symposium hosted in Washington, DC by the U.S. Chamber of Commerce and American University.

The event brought new insights into how a broad range of actors have a stake in and could be part of solutions to starve phishers access to cybercrime supply chain resources.

While this type of dialogue is encouraging, beneficial change will only occur if a broad range of stakeholders (including governments, where necessary) step-up and implement real-world solutions to combat phishing. Beneficial action would include:

- Greater involvement by consumer groups in anti-phishing and anti-cybercrime advocacy, including greater involvement and participation in relevant industry fora, advocating for the adoption of anti-abuse measures, communicating the real-world impact of cybercrime on consumers, and representing consumers in cybercrime litigation.
- More active involvement by subdomain, hosting, and gateway providers in phishing resource anti-abuse discussions, solution development, and implementation, as they represent critical and exploited links in the chain.
- Collaboration with the banking and payments industries to combat fraudulent use of credit cards and other payment platforms in the registration of resources. There is also great potential in collaboration programs that would allow these kinds of players to share data and coordinate anti-phishing programs.
- Collaboration amongst industry to directly engage peers and industry-adjacent players that are sources of resource abuse.

The Cybercrime Supply Chain



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.

Karen Rose is an internationally recognized expert in Internet policy, technology, and development with over 25 years in the field. Since 2017, she has consulted on a range of Internet policy, digital economy, and new technology issues for clients including international organizations, corporations, and government. From 2006 to 2016, Karen was a senior executive at the Internet Society (ISOC) where she led the organization's work to expand Internet access, infrastructure, and related policy capacity around the world, as well as the organization's research on emerging Internet issues. Earlier in her career, Ms. Rose served at the U.S. Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). While in government, she was co-author of the U.S. policy statement and related agreements that globalized management of the Internet Domain Name System (DNS) and lead to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN) to coordinate unique Internet identifiers. Ms. Rose previously served on the board of Netnod, one of Europe's most recognized Internet exchange point operators, and on the .us domain stakeholder advisory committee. She currently serves on the international advisory panel for AfChix, an African organization dedicated to advancing women in tech.

Dr. Colin Strutt has published and spoken extensively on networking technology, name collisions, enterprise management, eBusiness, and scenario planning, and has represented the interests of 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).

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.
- All the security personnel who fight phishing.

About Interisle Consulting Group

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