Cybercrime Supply Chain 2023

Measurements and Assessments of Cyber Attack Resources and Where Criminals Acquire Them

David Piscitello, Interisle Consulting Group
Dr. Colin Strutt, Interisle Consulting Group

23 October 2023

APWG CAUCE Interisle Consulting Group M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

Study Sponsors

The following organizations provided financial support and peer review for this study.

Anti-Phishing Working Group (APWG) is an international coalition of counter-cybercrime responders, forensic investigators, law enforcement agencies, technology companies, financial services firms, university researchers, NGOs, and multilateral treaty organizations operating as a non-profit organization. Its directors, managers, and research fellows advise national and sub-national governments as well as the United Nations (Office on Drugs and Crime) as recognized experts (as defined by the Doha Declaration of 2010 and Salvador Declaration of 2015) as well as multilateral bodies and organizations. https://apwg.org/

Coalition Against Unsolicited Commercial Email (CAUCE) is an all-volunteer Internet end-user trust and safety advocacy organization. The CAUCE Board of Directors provides Internet advocacy and consultation with governments, NGOs, law enforcement agencies, and trade associations. The mission of CAUCE is to defend the privacy rights of Internet users and support anti-abuse work in all its forms. CAUCE focuses on messaging security: email, direct message, text, or social media discourse. CAUCE provides instruction and professional development to law enforcement agents and security researchers in developing nations, in-person or remotely, by demonstrating the latest tools and techniques in cyber-investigations. CAUCE provides input to governmental and international policy, regulation, and law, and supports published research projects that advance its stated goals. https://www.cauce.org/

Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) provides a collaborative global trusted forum that brings industry together to help fight and prevent Internet online abuse. Working with members, industry groups, and global partners, M3AAWG will continue its efforts to help prevent online abuse, focusing on protecting communications, data privacy and security, and the supply chain. https://www.m3aawg.org/

Executive Summary

Three cybercrimes – malware, spam, and phishing – are a collective plague on society and economies worldwide. Malware can infect any device connected to a network. Malware attacks are criminal or nation-state activities that cost governments, corporations, and individuals hundreds of billions of dollars every year. Malware (“bots”) send spam messages, operating from cloud or hosting service accounts or compromised devices. These bots provide delivery methods for messages that contain lures to phishing pages or malware download sites. Modern day spam is rarely benign: as a delivery system, spam is almost always a component of a subsequent cybercriminal activity. Phishing attacks lure victims to web sites that appear to be run by a trusted entity but are in fact controlled by a criminal, defrauding millions of Internet users every year.

Taken together, these cybercrimes have global impact. Cybercriminals routinely exploit Internet resources to launch these attacks, affecting consumers, businesses, and economies globally. They are pervasive and contribute to a lack of consumer trust in online services, which in turn creates a drag on economic opportunity.

Criminals who perpetrate these cybercrimes enjoy an enormous economic advantage over defenders and responders. They can acquire resources from an online *cybercrime supply chain* where everything from phishing kits and malicious software, email lists and mobile numbers, domain names and Internet addresses, and places to host attacks are all readily and cheaply available.

Systems warfare is a strategy that attempts to disrupt the operations of an adversary’s functions. This report contends that applying a similar strategy to mitigate cybercrime can be effective. However, to employ such a strategy requires the ability to accurately measure particular elements of the cybercrime supply chain. Measurements collected by Interisle and presented in this report focus attention on the links in the supply chain where disruption can have meaningful impact.

For this study, Interisle collected malware, spam, and phishing reports from eleven publicly and commercially available threat intelligence or reputation services covering a one-year period. From these, we identified the Internet naming, addressing, and hosting resources that criminals use to conduct over 10 million cybercrime attacks and where criminals went to acquire these attack resources. We then ranked Top-Level Domain (TLD) registries, TLD registrars, hosting providers, and subdomain resellers that criminals most frequently exploited to obtain resources, using both raw counts and comparative metrics.

Interisle measured and identified distinct and persistent patterns of exploitation and abuse over a one-year period. While some of these patterns are familiar to cybersecurity practitioners and law enforcement, our data revealed the widespread existence of some less popularly known exploitations of domain registration and hosting services. The findings from this study underscore a previous Interisle finding, that the prevailing uncoordinated and ineffective attempts to curb cybercrime are not working, and that new strategies are required. The recommendations explain how cooperative, pro-active, and cross-sector efforts by governments, private sector, and public policy communities could disrupt the cybercrime supply chain.

Our data show that:

Nearly 5 million domains were reported for serving as a resource for cybercrime

Spam campaigns are the largest consumers of criminal domains: three-quarters of the domain names used in cybercrimes were identified as spam domains.

Cybercriminals often quickly use domain names they register for cybercrimes

47% of phishing domains are reported within 14 days and 54% are reported within 30 days.
28% of spam domains are reported within 14 days and 33% are reported within 30 days.

New gTLDs continue to provide a greenfield opportunity for cybercrime activity

Over 1 million domains were reported for spam activity from September 2022 to August 2023. A handful of the new gTLDs account for most of the cybercrime activity. The five most exploited new gTLDs account for 46% of the cybercrime domains reported across all new gTLDs.

Subdomain reseller services have become even more attractive as free domain registrations from operators like Freenom become scarce

Over 500,000 subdomain hostnames were reported for serving as resources for cybercrime at 229 subdomain resellers.

Criminals exploit bulk registration services to acquire domain names for cybercrimes

Over 1.5 million domain names exhibited characteristics of malicious bulk domain registration behavior. Bulk registrations accounted for one-third of the malicious domain registrations reported for serving as resources for cybercrimes.

Brand infringement is commonplace in domains registered by criminals to perpetrate cybercrimes

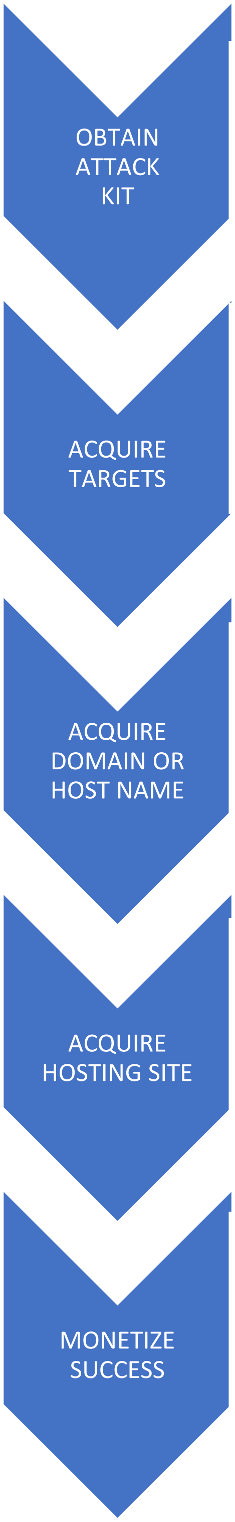
Exact matches of a brand name appeared in 206,040 cybercrime records, 169,835 domain names, and 22,679 subdomain reseller host names.

The United States had the most IPv4 addresses reported for serving as resources for cybercrime activity. China, India, Australia, and Hong Kong rounded out the top 5

China and the United States accounted for 7 of the 10 hosting networks that hosted the most malware. Combining spam, phishing, and malware records in this study, China and the United States accounted for 8 of 10 hosting networks with the highest cybercrime activity.

Background: What is the Cybercrime Supply Chain?

Cybercriminals acquire resources for malware attacks, spam, and phishing campaigns in several ways. The supply chain for a cyberattack typically involves the acquisition of several resources:



- **ATTACK "KIT"**
  For phishing, this is often a set of files and scripts that allows the phisher to impersonate a brand. Many kits include web forms where Internet users are lured to sites impersonating a known organization. Victims are duped into submitting their access credentials or personal data. Such kits can be found on social media sites, public repositories, or found on dark or deep web sites. Spammers similarly acquire kits that include a mail server and the means to compose simple email messages that deliver phishing, scam, or malware URLs or malicious attachments.

- **TARGETS**
  Some cyberattacks cast a wide net. For these, attackers may use markets where mail lists can be purchased or they may use email scraping tools to create their own lists to spam, phish, or bait malware. For sophisticated attacks – spear phishing, network infiltration, data exfiltration, or business email compromise – attackers conduct research to identify highly profitable targets ("whales") or targets with sensitive and highly marketable data

- **DOMAIN OR HOST NAMES**
  Attackers often register domain names for fake web sites, email servers, or file services. They may use the names of web sites where they have gained administrative control or accounts at free or cheap hosting ("subdomain") services where the account name serves as a subdomain of the hosting site's domain name, *e.g.*, `amazonsecuredateupdate.duckdns.org`. Note that certain malware, especially loaders, download additional software components by establishing connections to a computer or device using an IP address, so in this case domain names and name resolution are unnecessary.

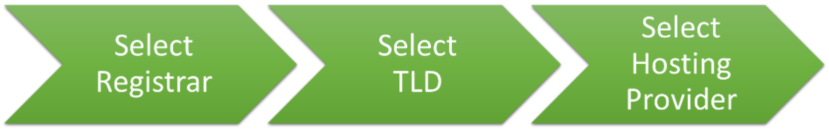
- **HOSTING**
  Attackers have several options for hosting: use compromised cloud accounts, use servers or devices where they've gained administrative control over web or other system services, or use free or cheap hosting or cloud services . For certain hosting, they bind domain names that they register to the IP address of the host. For subdomain services, the user account name typically resolves to the service provider's IP address.

- **BROKERS OR MARKETS**
  Most cybercrimes are for-profit enterprises, so attackers monetize data that they illicitly obtain through secondary fraud services (*e.g.*, mules, cryptocurrencies, or online marketplaces). Some attackers (access brokers) sell credentials or access methods of organizations whose networks they have compromised to other threat actors.

The Focus of This Report

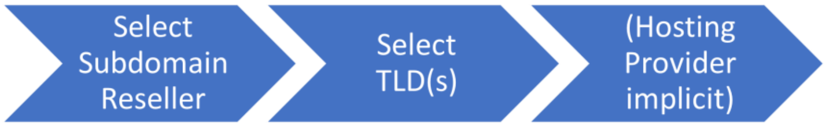
This reports focuses on measurements for the name and addressing resources that criminals employ to conduct illicit acts. Studies of attack kits, target acquisition techniques, and monetization of criminal proceeds are beyond the scope of this study. With respect to names and addresses, criminals can choose from three different supply chains:

Supply chain includes registrars, TLDs, and hosting



Criminals choose domain registrars, register domain names in a TLDs, and upload fake or malicious content to hosting resources of cloud or web hosting providers.

Supply chain includes subdomain resellers and hosting



Criminals create accounts at subdomain resellers, use the account names as host names and upload fake or malicious content to the hosting resources of the reseller.

Hosting

Select Hosting Provider

Criminals do not use domain names or host names but construct hyperlinks for their content using IP addresses that they obtain from their hosting providers (predominantly seen with malware).

This report examines each of these different styles of supply chain in terms of the number of cybercrime records associated with each combination. These measurements show that criminals enjoy supply chain flexibility, and that the means or efforts to disrupt the chains may involve different parties.

Introduction

Three cybercrimes – malware, phishing, and spam– are a collective plague on society and economies worldwide.

Malware (**mal**icious soft**ware**) can infect or compromise any device connected to a network. Malware is an organized criminal or nation-state activity that costs governments, corporations, and individuals hundreds of billions of dollars every year. Criminals use malware to perpetrate identity theft or financial fraud (banking trojans), to steal information or extort funds (ransomware), or to remotely control compromised devices. Criminals or hostile state actors use malware to establish an illegal, persistent network presence for surveillance, data theft or destruction, or to inject malicious content into forums or social media.

Phishing defrauds millions of Internet users every year. Phishing attacks lure victims to web sites that appear to be run by a trusted entity but are in fact controlled by a criminal. The phishing page persuades 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 2022 annual report by the U.S. Federal Bureau of Investigation's Internet Crime Complaint Center says that it received 300,497 phishing complaints reporting losses of $52 million in the U.S. alone.

Spam is a notorious consumer of Internet resources. A DataProt study found that spam emails accounted for more than 56% of all emails sent in 2022. A Statistica survey reported that "*As of January 16, 2023, the country with the highest number of spam emails sent within one day worldwide was the United States, with around eight billion. Ranking second and third were Czechia and the Netherlands, with 7.7 billion, and 7.6 billion, respectively.*" Spam is often wrongly dismissed as unsolicited commercial emails or texts that are benign. But very little spam is truly benign. Spam is commonly transmitted from bots operating from cloud or hosting service accounts of compromised devices that host malware (spambots). Spambots are malware, installed without consent. The bot itself and the thousands of emails each bot emits consume CPU, RAM, bandwidth, and storage from the source of transmission to the spam recipients' devices.

Large organizations typically have expert resources at their disposal to identify and defend against spam, malware, and phishing attacks. Small businesses, community organizations, small municipalities, and average consumers do not. Large organizations and brands are harmed when they are impersonated in cyberattacks, but the average citizen, the Internet end user, suffers from these attacks as well. While large organizations might have resources and knowledge to report incidents of spam, malware, and phishing attacks, the average person has no understanding of how or where to report such incidents, even if they could determine that there were incidents to report. In addition to costs associated with direct victimization, consumers pay higher prices for services when businesses must cover losses stemming from attacks that employ malware, spam, and phishing.

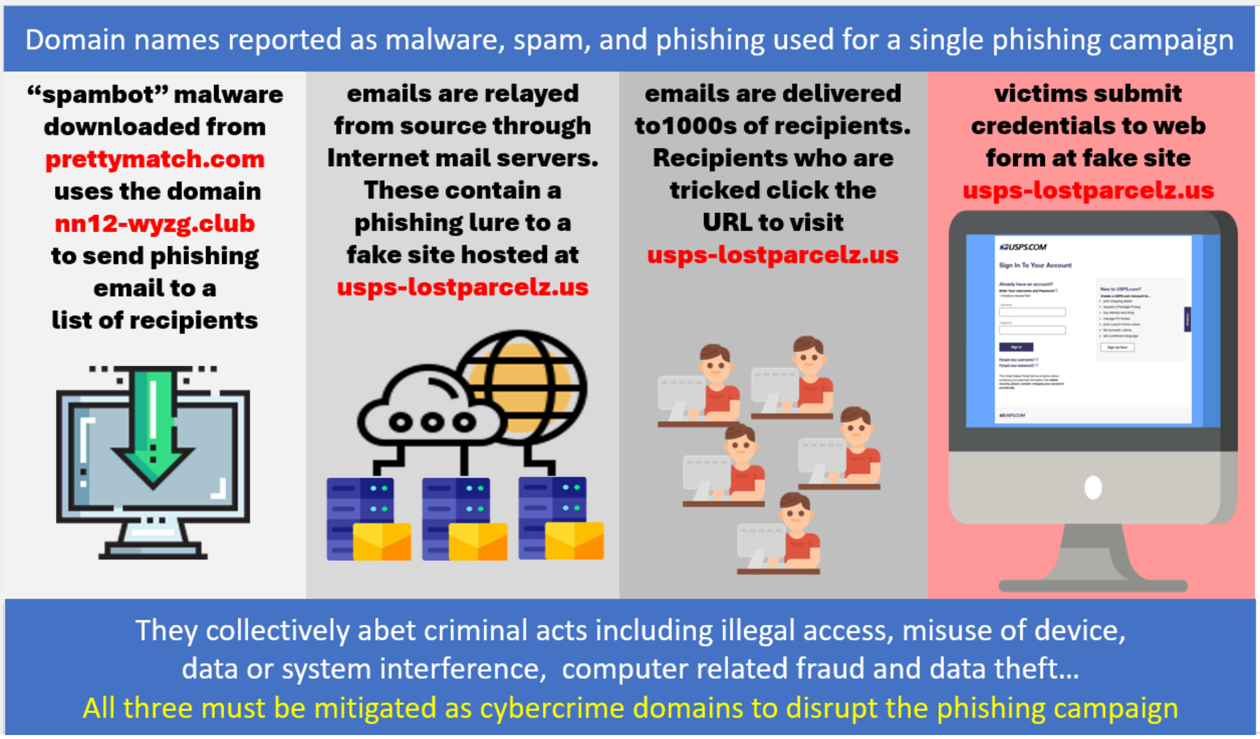
Taken together, these attacks and incidents impact globally; the global economy suffers as well. The routine exploitation of Internet resources used by cybercriminals to launch phishing attacks negatively impacts consumers, businesses, and economies worldwide. Pervasive phishing and other cybercrimes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

Cybercrimes are Highly Intertwined

The relationships among malware, spam, and phishing are numerous and diverse. DataProt reports that "*Scams and fraud comprise only 2.5% of all spam emails; however, phishing statistics indicate that identity theft makes up 73%*". The Emotet banking trojan malware was distributed in Excel attachments using a high-volume email distribution. Phishing now rivals malware as a primary means of illegal access. The 2023 CrowdStrike Global Threat Report notes that 71% of illegal access and persistent presence in victim networks were malware free: attackers are abusing valid credentials more than ever, and they are obtaining these credentials through phishing attacks. The 2022 IBM 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. **Treating any of these cybercrimes as non-objectionable or devoting less attention is akin to leaving untreated cancer cells that a pathologist finds at the edge or** positive margin **of a tissue, which indicate that all of the cancer was not removed.** The analog to cybercrime is simple: if you don't mitigate the spam domains along with domains associated with a phishing or malware attack, then the criminals can resurrect their infrastructure and resume criminal activity.

Interisle has observed these relationships for several years. Interisle has been reporting cybercrime measurements, primarily phishing and malware, for several years. As we continue to learn from the data we collect and the reactions or responses to our Phishing Landscape and Malware Landscape studies, we've observed that many interested parties conclude from our findings that all the domain names and IP addresses associated with a given cyberattack are similarly tagged; for example, parties unfamiliar with reputation blocklists assume that the domain names used to send phishing emails and all those extracted from URLs in the email message body or attachments were reported as phishing domains.

This is not always the case. Typically, several if not thousands of domains or IP addresses are used over the course of a cyberattack life cycle. Investigators or reputation services will report misuse of these names or addresses as spam, malware, phishing, or other abuses or cybercrimes, using the best available intelligence at the time when they detect and identify the nature of an attack. But cyberattacks build or evolve over time. Consider the attack depicted in the following graphic:



Domain names reported as malware, spam, and phishing used for a single phishing campaign

"spambot" malware downloaded from prettymatch.com uses the domain nn12-wyzg.club to send phishing email to a list of recipients

emails are relayed from source through Internet mail servers. These contain a phishing lure to a fake site hosted at usps-lostparcelz.us

emails are delivered to1000s of recipients. Recipients who are tricked click the URL to visit usps-lostparcelz.us

victims submit credentials to web form at fake site usps-lostparcelz.us

They collectively abet criminal acts including illegal access, misuse of device, data or system interference, computer related fraud and data theft...
All three must be mitigated as cybercrime domains to disrupt the phishing campaign

In our example, an Internet user has visited `prettymatch.com` and unintentionally downloaded spambot malware. The domain prettymatch.com was reported as serving malware. Once installed, the spambot used `nn12-wyzg.club` as the sending email server. This domain was reported for serving spam email because the domain appeared in email message headers of the Simple Mail Transfer Protocol, SMTP, which is used ubiquitously to provide email services (*e.g.*, rDNS, HELO, MAIL FROM, From, Reply-To, and Message-ID domains fields). The domain `usps-lostparcelz.us` was extracted from a hyperlink (URL) in the spam message body *e.g.*, `hxxps://usps-lostparcelz.us/signin.html`. This domain was reported as a phishing domain. **Applying our earlier analogy, all these domains fall within the positive margin of the actions necessary to mitigate this cyberattack to the greatest extent possible**.

In our example, the contents of the email message or web page was directly relevant to the phishing attack. In other cases, the spam email content may appear non-objectionable, but the underlying motive is often malicious. . For example, consider an email message with **Subject: Hello** and a message body, "**Hi, let me know if you received this**." Assuming that there is no malicious attachment, it is impossible to know the attacker's motive. It could be benign, but history and field experience have shown that the attacker may be probing for active email account or hoping to evoke a reply. These are typically precursors to subsequent malicious activity; for example, the attacker may subsequently use the email addresses of recipients who reply as targets for a phishing or malware campaign. The important takeaway here is that *the absence of an overt threat from a message received does not make the spam domain less of a threat*. Thus, when mitigating or disrupting any cyberattack, it is important to act uniformly and quickly on all the domains and addresses reported, irrespective of whether a domain or address has been reported for spam, malware, or phishing.

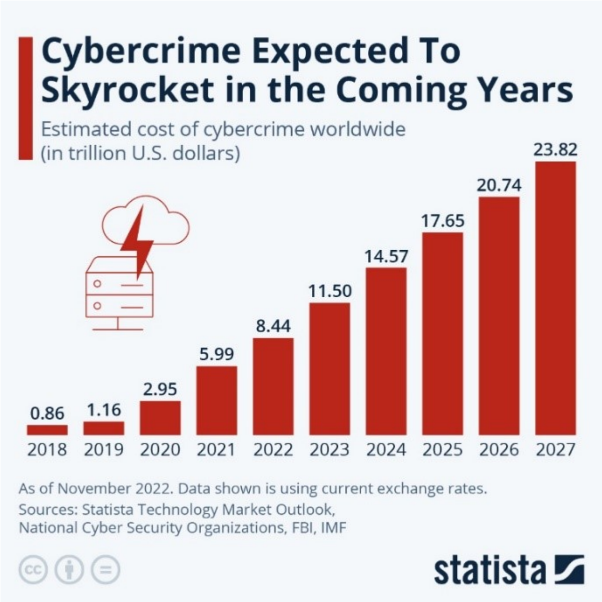
Why This Study, and Why Now?

Interisle's past studies of phishing and malware found that these cybercrimes increase in number, scale, and reach year after year. The World Economic Forum includes the cost of cybercrime among the top 10 most severe global risks. Statistica estimates the global cost of cybercrime exceeded $8 Trillion USD in 2022 and will near $24 Trillion USD by 2027.

Cybercrime is worsening annually. Response is falling further and further behind.

As explained in the section *Background: What is the Cybercrime Supply Chain?* criminals enjoy an enormous economic advantage over defenders and responders. They can acquire resources – from domain names, addresses, hosting space, malicious software, phishing kits, email lists, and mobile numbers to access brokerages and launderers – cheaply and easily from an expansive cybercrime supply chain.

Combating cybercrime is an arms race where the cost to defend, detect, mitigate, and prosecute far exceeds the cost to commit crimes or attack nations.



Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)

As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF

Greater coordination and cooperation are necessary in order to combat cybercrime.

Concerted efforts to disrupt the cybercrime supply chain are needed to complement traditional cybercrime countermeasures (*e.g.*, post hoc mitigation and pursuit of criminal actors). Engagement from private actors, law enforcement, and lawmakers is necessary to effectively disrupt cybercrime supply chains.

Accurate measurements of the elements of the cybercrime supply chain will focus attention to the links in the supply chain where disruption can have meaningful impact

In order to assess the potential benefit of disrupting cybercrime supply chains, Interisle collected spam, malware, and phishing reports from eleven publicly and commercially available threat intelligence or reputation services (see our list of data contributors at the Cybercrime Information Center). From these sources, we created over ten million unique **records** to measure cybercrime attacks: these records reflect the resources that criminals use to conduct their attacks, and by analyzing the resources used, we identified where criminals go to acquire these resources. We then ranked Top-Level Domain (TLD) registries, TLD registrars, hosting providers, and subdomain resellers that represent the greatest amount of cybercrime activity based on raw counts and comparative metrics.

This study uses Interisle's methodology for distinguishing attacks where domain names were purposely (maliciously) registered by criminals from attacks that were hosted on compromised domains or web sites. This distinction is important because it indicates where additional prevention and mitigation efforts could be applied most effectively, and importantly, which operator (registry, registrar, hosting provider, subdomain reseller) is best positioned to implement these. The study also identifies suspicious registration behaviors by exposing large numbers of exact matches of registered brands encoded in domain names and identifying a high incidence of cases where "sets" of domain names that were registered within seconds (in bulk), weaponized, and subsequently reported for use in cybercrime attacks.

The report concludes with sets of recommended policies, legislation, and practices that the domain name industry, governments, and private sector should adopt to disrupt the cybercrime supply chain.

Key Statistics and Trends

Data collected at the Cybercrime Information Center is used for our landscape studies (see FAQ). For this study, there were 10,566,683 unique records covering the one-year period from 1 September 2022 to 31 August 2023. The starting point was threat data contributed from widely used and respected threat data providers: the Anti-Phishing Working Group (APWG), Invaluement , Malware Patrol, MalwareURL, OpenPhish, PhishTank, Spamhaus, SURBL, and URLhaus. Feed data was enriched with domain registration, DNS, passive DNS, routing, geolocation, and other metadata from public services (WHOIS, RDAP) and commercial sources including Domain Tools and ZETAlytics.

The statistics presented in this report include both absolute metrics (for example, the number of domain names registered in a particular TLD that appear on a blocklist) and relative metrics (such as a score, representing the number of those domain names as a proportion of the total number of domains registered in that TLD or as a proportion of the total number of domains registered via a registrar). Attention to this distinction is critical to understanding and properly interpreting our analyses and findings.

Key statistics for this study period appear in the following table:

Cybercrime measurements (September 2022 – August 2023)	
Measurement	**Total for period**
Cybercrime records used for this study	10,566,683
Unique domain names reported for serving as a resource for cybercrime	4,799,546
Maliciously registered domain names reported for serving as a resource for cybercrime	2,577,865
Unique subdomain reseller hostnames reported for hosting cybercrime	550,507
Maliciously acquired subdomain reseller hostnames	356,252
Total number of IP addresses associated with a reported cybercrime	4,676,242
Subdomain resellers with hostnames reported for hosting cybercrimes	251
Top-level domains where cybercrime domains were reported	905
Hosting network ASNs where cybercrime domains were reported	30,708
gTLD registrars where cybercrime domains were reported	2,432
All domain registrars where cybercrime domains were reported	4,382
Countries where IPv4 addresses were reported for hosting cybercrimes	233

Notes on the table:

- ***Cybercrime records*** include unique event data for phishing, malware, and spam attacks.
- ***Unique domains reported for serving as a resource for cybercrime*** includes domain reported in domain blocklists and domain names extracted from URLs reported in URL blocklists.

- In addition to measuring domain names, we also measure ***Unique subdomain reseller host names reported for hosting cybercrime***. This is a measurement of user accounts of frequently exploited subdomain services. Subdomain resellers typically assign a host name from a domain name that the provider owns using a third level domain of the format `subdomain.domainname.tld`. The "subdomain" label is often the user's account name. This gives users their own "host name" in the DNS for web, file, blog, or other content that they publish.
- The DNS is used to resolve domain names reported for cybercrimes to IPv4 addresses on the date reported. To obtain the ***Total number of IP addresses associated with a reported cybercrime,*** the IPv4 addresses extracted from URIBLs was included along with the IPv4 addresses identified using name resolution (DNS).
- IP geolocation data[1] is used to identify ***Countries where IPv4 addresses were reported for hosting cybercrimes***.

Nearly 5 million domains were reported for serving as a resource for cybercrime

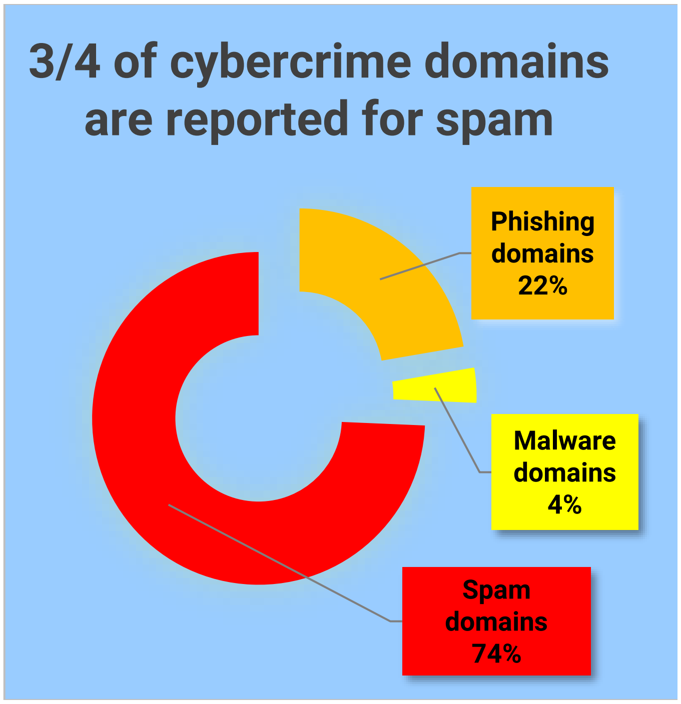
We determine that 54% of the domain names found in cybercrime reports were registered purposely by criminals to abet a criminal act, while 65% of the subdomain reseller host names were acquired with malicious intent.

Trends of Key Statistics

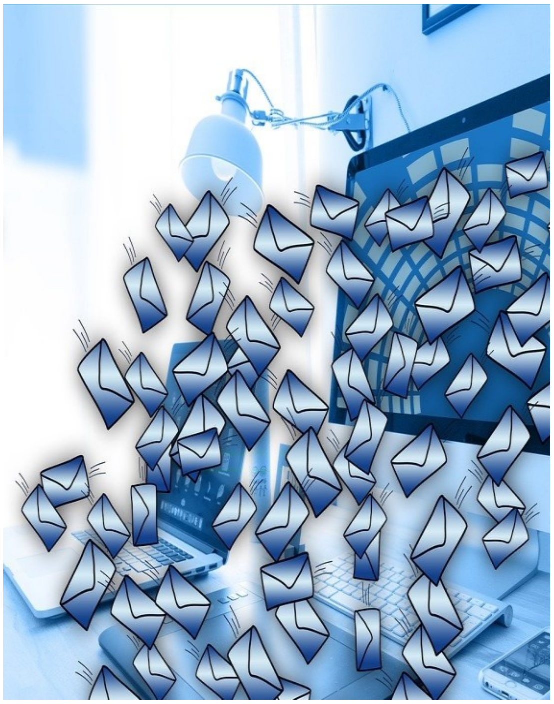
During the study period, we produced approximately 850,000 cybercrime records per month, with a high of nearly 1.3 million records in May 2023. A breakdown by crime activity revealed:

- 1,894,087 records of phishing activity,
- 4,601,073 records of malware activity, and
- 4,071,523 records of spam activity.

[1] Interisle uses RIPEstat geo data (per Maxmind GeoLite) to determine the countries where cybercrime activities were reported. To understand accuracy limitations of geolocation services, read "*How accurate are IP geolocation services?*" at https://blog.apnic.net/2020/09/15/how-accurate-are-ip-geolocation-services/



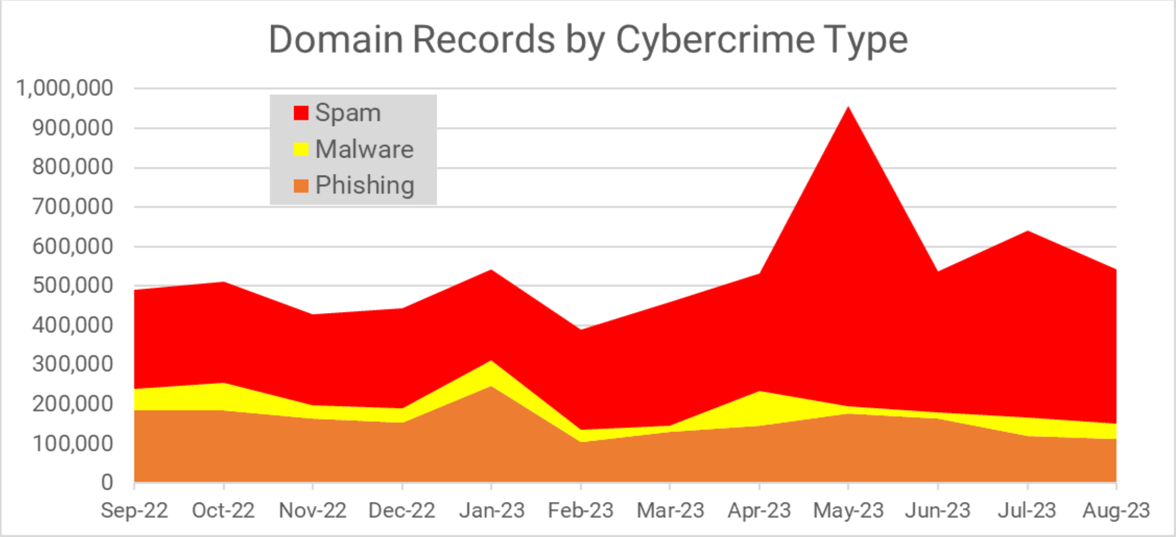
3/4 of cybercrime domains are reported for spam



Domain Reporting

Of the 4,799,546 domain names associated with cybercrime activity, 3,567,649 were associated with spam campaigns, 1,069,644 were associated with phishing attacks and 162,179 were associated with malware hosting or distribution.

Spam campaigns are the largest consumers of criminal domains



Address Reporting

Nearly all the malware threat data ingested report the IPv4 addresses where malware was hosted or distributed. Of the 4,676,242 unique IPv4 addresses associated with cybercrime activity, 682,812 were associated with spam campaigns, 211,2279 were associated with phishing attacks and 3,919,5908 were associated with malware hosting or distribution. 137,447 IPv4 addresses were associated with more than one cybercrime activity.

Cybercrime Activity

One goal of our research is to better understand the methods that criminals use to evade detection. We are also interested in how quickly they use domain names that they register purposely for cybercrimes.

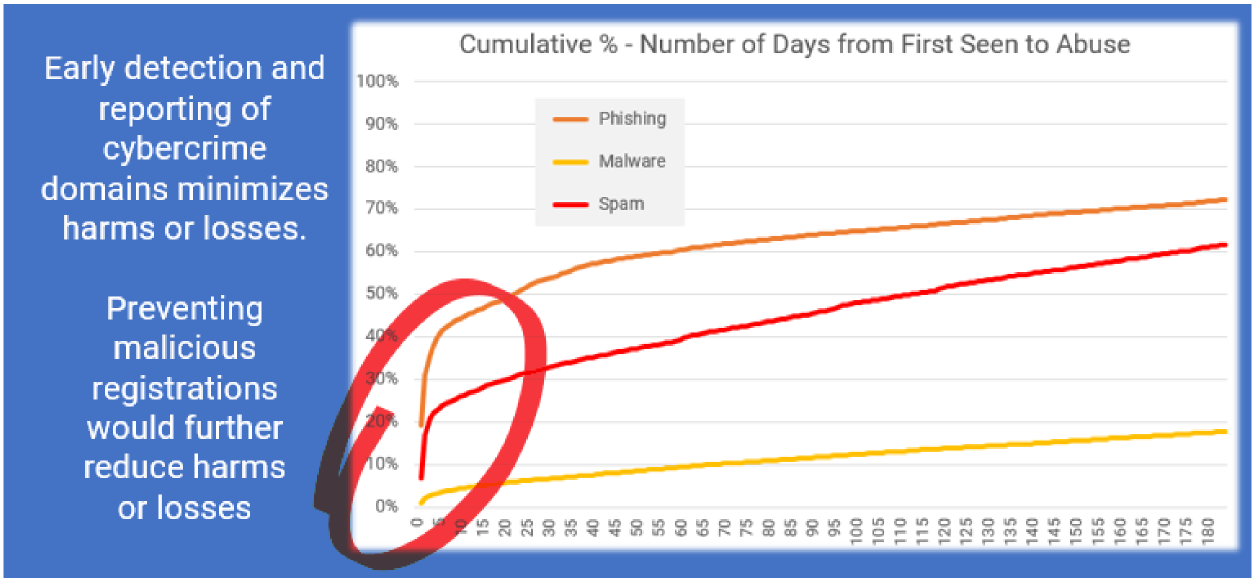
To these ends, we analyzed how many days elapsed from when a domain name was registered or first appeared in the DNS to when that domain was reported for abetting a cybercrime.

Where domain registration dates could not be obtained — for example, contending with domains registered in ccTLDs that do not publish WHOIS data or when rate-limiting or other issues impede our collection of WHOIS data – we used passive DNS data collected by ZETAlytics. Passive DNS (pDNS) shows when a domain name was first seen to resolve in the DNS. This “first appearance” date was used when no registration date is available from WHOIS.

Time Elapsed between Domain Appearance and Cybercrime Reporting

Reporting of phishing and spam domains shows a very fast detection from when a domain is registered or first detected by pDNS to when it is reported for cybercrime. This is also true for hostnames assigned by a subdomain reseller to a user’s account.

Spam and phishing domain reporting occur at about the same percentage. Approximately 84% of phishing domains were reported by the end of one year, which is roughly the same as the 81% observed for spam domains.



Early detection and reporting of cybercrime domains minimizes harms or losses.

Preventing malicious registrations would further reduce harms or losses

47% of phishing domains are detected within 14 days and 54% are detected within 30 days

28% of spam domains are detected within 14 days and 33% are detected within 30 days

11% of the 4,897,331 domains or subdomain reseller hosts for which we could determine a registration date or pDNS-first-seen date, were detected for abuse within the first day. And 21% were reported within the first 48 hours. These findings suggest that proactive or preemptive measures could meaningfully reduce cybercrime activity, for example,

TLD registries or registrars can take proactive measures to disrupt the supply chain. These operators are in the best position to identify and block attempts for spam and phishing domains at the time of registration. In some cases, these measures that are currently employed to blocklist phishing and spam domains can be employed.

Registrars can monitor and investigate bulk registrations, particularly where a single registrant can purchase dozens, hundreds, or thousands of registrations from a single account in a single session in a matter of minutes. This is atypical registration behavior and even an automated examination of the domains the registrant seeks can be used to determine that the registration has a high probability of being used for a cybercrime. With such measures in place, the registrar can **refuse to register domains that are suspiciously composed**, for example, domain names that are suspiciously long, include an excessive number of hyphens or numbers, include brands (or brand similarities), or have observably suspicious composition patterns.

The study data set shows thousands of suspiciously composed domains that are registered in bulk, for example:

Examples of suspiciously composed domains registered in bulk

Reported for phishing within one day of appearance (part of a larger set)	**Reported for spam within one day of appearance** (part of a larger set)	**Reported for malware within one day of appearance** (part of a larger set)
`tools-usps.ink`	`a316tom.com`	`atendimentowl.com`
`tools-usps.cloud`	`a318tom.com`	`atendimentobk.com`
`tools-usps.tech`	`a319tom.com`	`atendimentobs.com`
`tools-usps.chat`	`a320tom.com`	`atendimentopt.com`
`tools-usps.site`	`a321tom.com`	`atendimentosx.net`
`tools-usps.xyz`	`a322tom.com`	`atendimentoht.com`
`tools-usps.icu`	`a323tom.com`	`atendimentokz.com`
`tools-usps.ltd`	`a316tom.com`	`atendimentofb.com`

In the table, the set of domains reported for phishing illustrates that criminals can trivially acquire domain names with exact matches of brands (here, ‘usps’ commonly associated with the United States Postal Service). The spam set illustrates a commonly employed technique where domains names contain sequential patterns. The malware set illustrates a pseudo-random name generation technique. Measures that prevent suspicious compositions of these kinds (or delay registration until an appropriate use is demonstrated), *especially when domain names are registered in volume*, are essential to be able to disrupt the supply chain.

If they can be identified *post hoc* through automation, they can be implemented prior to accepting and processing a domain registration.

Cybercrime Activity Across the Domain Name Space

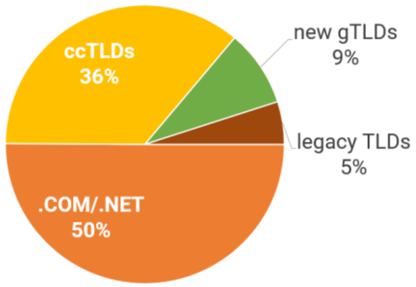
According to Domain Tools, at the end of August 2023, there were over 342 million registered domains in the global domain name space. We identified domains reported for cybercrime activity in 906 of the approximately 1,550 existing TLDs during the current study period.

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

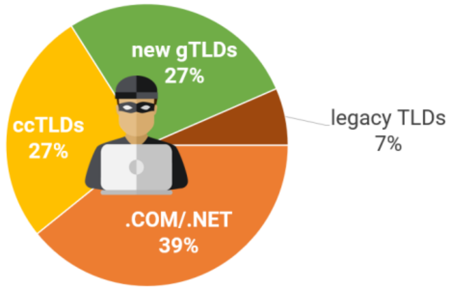
- the .COM and .NET registries, operated by Verisign, representing 50% of the domains in the world,
- the country-code domains (ccTLDs) representing 36% of the domains,
- the legacy generic TLDs – those other than .COM and .NET and introduced before 2013, *e.g.*, .ORG, .BIZ, .INFO – representing 5% of the domains, and
- the new gTLDs introduced from 2014 to the present (*e.g.*, .TOP, .LIVE, .REST, .SUPPORT, .CYOU) representing the remaining 9% of the domains.

We examined the domains reported for cybercrime activity to see how they were distributed across the domain name space. Our data show that cybercrime activity does not track with market share.

All Registered Domains - August 2023



Cybercrime Domains - Sep 2022 to Aug 2023



Legacy TLDs

.COM and .NET represent 50% of the market share, with roughly 171.7 million domains registered per our data set. The 1.9 million domains reported for cybercrime activity in .COM and .NET represent only 39% of cybercrime activity overall. The legacy TLDs (not including .COM and .NET) have a slightly higher percentage of domains reported for cybercrime activity than their market share.

ccTLDs

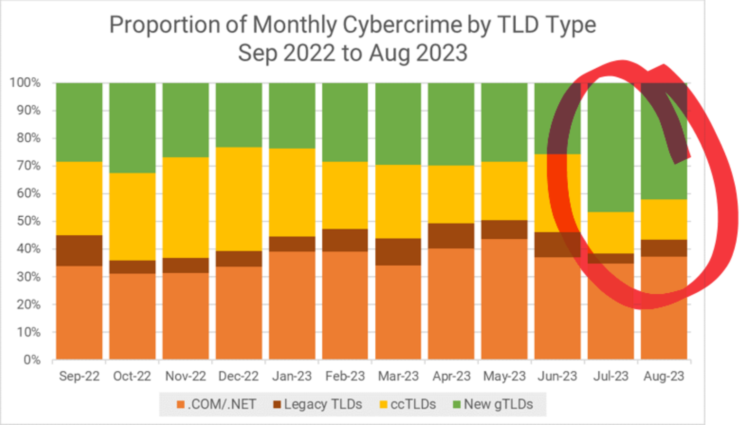
The ccTLD space has 36% market share, with roughly 123.5 million domains registered per our data set. With nearly 1.3 million domains reported for cybercrime activity, about 1% of the ccTLD space is associated with cybercrime, representing 27% of the overall reported domains.

For the 231 ccTLDs for which we have cybercrime records, only 107 had a minimum of 25,000 registered domains and at least 25 cybercrime domains. In this set,

- the top 5 account for 45% of the cybercrime domains in ccTLDs,
- the top 10 account for 65%,
- the top 25 account for 86%, and
- the top 58 account for 95%.

Freenom’s five commercialized ccTLDs (.TK, .ML,.GA, .CF, .GQ), which ceased offering free domain name registrations in 1Q2023, *still* accounted for 29% of the cybercrime domains reported in the ccTLD name space for the yearly study period.

As Freenom’s influence in ccTLD criminal domain numbers diminished, cybercrime domains reported in the new TLDs increased



New gTLDs

The new gTLDs continue to provide a greenfield opportunity for cybercrime activity. The measurements speak to how attractive new gTLDs remain:

- 9% of the market share but three times that share of cybercrime domains reported.
- More domains reported for cybercrime (1.32 million) than the entire ccTLD space (1.29 million).
- Over 1 million domains reported for spam activity.

A relatively small number of the new TLDs account for most of the cybercrime activity

We identified 554 new gTLDs in our study data. Only 117 of the 554 new gTLDs have a minimum of 25,000 registered domains and at least 25 cybercrime domains. In this set,

- the top 5 account for 46% of the cybercrime domains in new gTLDs,
- the top 10 account for 64%,
- the top 20 account for 80%, and
- the top 50 account for 95%.

Nearly all the cybercrime activity reported in the new gTLD name space was found in gTLDs that are listed as having a Non-Sponsored agreement type with ICANN (source: ICANN Registry Agreements). The 117 new gTLDs for which we obtained a minimum of 25,000 registered domains and at least 25 cybercrime domains included two IDN gTLDs (xn--p1ai, Russia and xn--fiqs8s, China), two Community agreement gTLDs (.CAT, .OVH); there were no Brand gTLD agreements registry operators (*e.g.*, .AAA, .CITI, .YAHOO). The rest of the gTLDs are Non-Sponsored, Base agreements registry operators (which include three cities, .TOKYO, .NYC, .LONDON).

The new gTLD program was intended to increase consumer choice, but the addition of so many Non-Sponsored new gTLDs also expanded the registration field for cybercriminals

Some new gTLD registry operators have sought to compete by offering cheap and sometimes free registrations. These operators have consistently attracted cybercriminals, who wish to avoid detection or spend as little of their own money as possible. Some registry operators and registrars who have competed on price appear to operate less than-effective anti-abuse programs, as those programs cost money and effort. Inexperienced registry management may also be a factor that contributes to high cybercrime activity in a new gTLD.

Malicious Domain Registrations Across the Domain Name Space

We measured the number of unique domains reported for cybercrime activity across a total of 906 TLDs. For our studies, we classify a domain reported for cybercrime activity as being either a domain registered purposely to carry out a malicious or criminal act (maliciously registered domain) or a domain registered for legitimate purposes but co-opted ("compromised") by criminals through a cyberattack.

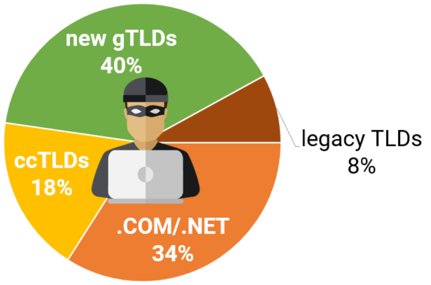
This distinction often helps investigators identify the operator who can best assist with mitigation of a criminal activity. Investigators should seek assistance from a domain name registrar, a TLD operator, or the operator that provides DNS if the domain is determined to be maliciously registered. The registrar is well positioned to suspend the domain name registration or name resolution. The investigator may also contact a 3rd party DNS provider to suspend name resolution, or a web hosting provider to remove content associated with cybercrime.

Investigators are typically sensitive to suspending a compromised domain because the action can harm the domain's legitimate registrant by bringing down the legitimate site's web site and email. Here, investigators should contact the hosting provider to have the malicious content removed.

We use a set of criteria to discriminate malicious domains from compromised domains including the time elapsed from domain creation date or first appearance of the domain to its being reported for cybercrime activity. We also look for characteristics of suspicious label composition; for example, we look for atypically long labels, labels containing exact matches of over 2000 brands that we track, labels containing brand similarities, and labels containing suspicious numbers of digits or hyphens in the label. We also use the metadata provided by the cybercrime feeds which can identify a brand target associated with a cybercrime report. We also look for registration behaviors that are characteristic of bulk registration.

The percentage of malicious registrations in the new TLD space exceeds four times its market share

Maliciously Registered Cybercrime Domain
Sep 2022 to Aug 2023



Ranking of TLDs by Criminal Domains Reported

Our study data show that criminals took advantage of much of the global name space, registering domains primarily in the top-level domains that offered open registrations. Some TLD registrations, for reasons of pricing, operating practices, or business processes, appear to be more attractive to cybercrimes than others.

In the rankings that follow, we include TLDs with a minimum of 30,000 domains and 25 cybercrime domains.

Ranking of All TLDs by Cybercrime Domains Reported

For the September 2022 to August 2023 study period, a ranking of all TLDs by Cybercrime Domains included three **legacy TLDs**, 5 **new gTLDs**, and 2 **ccTLDs**.

Rank	TLD	Total Cybercrime Domains Reported ▼	Yearly Cybercrime Domain Score	Cybercrime Domains as a Percent of All TLD Domains
1	COM	1,742,619	109.7	1%
2	CN	290,070	393.3	4%
3	TOP	206,512	897.7	9%
4	INFO	179,747	479.6	5%
5	NET	139,194	109.0	1%
6	LIVE	112,349	1,798.9	18%
7	TK	111,695	259.9	3%
8	ONLINE	105,794	417.3	4%
9	SITE	100,977	739.5	7%
10	SHOP	93,725	530.1	5%

The Yearly Cybercrime Domain Score is a metric to measure the prevalence of cybercrime activity in TLDs. The calculation for the metric is:

Yearly TLD Phishing Domain Score =

*(number of unique phishing domains reported in a TLD across the year / number of domains delegated from a TLD) * 10,000*

The three legacy TLDs – .COM, .INFO, and .NET – have large numbers of registrations compared to other TLDs in this ranking. We can use the scoring metric to compare whether a TLD has a higher or lower incidence of domains reported for cybercrime relative to others. The cybercrime domain scores of .COM, and .NET are significantly lower than the other TLDs in the Top 10.

Ranking of ccTLDs by Cybercrime Domains Reported

For the September 2022 to August 2023 study period, the ranking of the Top 10 ccTLDs by Cybercrime Domains included three of the five commercialized ccTLDs operated by Freenom (.TK, .CF, .GQ).

Rank	ccTLD	Total Cybercrime Domains Reported ▼	Yearly Cybercrime Domain Score
1	CN	**290,070**	393.3
2	TK	**111,695**	259.9
3	US	**65,909**	331.7
4	CF	**64,286**	489.9
5	GQ	**62,112**	587.3
6	RU	**53,190**	107.3
7	UK	**53,131**	51.6
8	ME	**46,443**	401.0
9	CO	**43,486**	125.5
10	IN	**35,641**	120.7

Even though Freenom has stopped accepting registrations, three of its ccTLDs continue to influence the rankings because they were so persistently used by cybercriminals. Since April 2023, a mere handful of cybercrime domains were reported in the .GA and .ML ccTLDs. .TK, .CF and .GQ all have had decidedly fewer domains reported for cybercrime activity. These were perhaps registered prior to April 2023 and stockpiled for later use.

Ranking of New gTLDs by Cybercrime Domains Reported

The Top 10 new gTLDs, ranked by cybercrime domains reported, are all non-sponsored TLDs.

Rank	New gTLD	Total Cybercrime Domains ▼	Yearly Cybercrime Domain Score
1	TOP	**206,512**	897.7
2	LIVE	**112,349**	1,798.9
3	ONLINE	**105,794**	417.3
4	SITE	**100,977**	739.5
5	SHOP	**93,725**	530.1
6	XYZ	**89,959**	273.1
7	CLICK	**50,779**	940.9
8	CYOU	**49,490**	1,877.9
9	CFD	**34,879**	452.3
10	LINK	**25,828**	1,123.8

High yearly cybercrime domain scores are prevalent among new TLDs

While .COM is always the highest ranked by reported cybercrime domains, 30 new gTLDs had yearly cybercrime domain scores that were 5-25 times that of .COM. The top 5 of these were:

New gTLDs with Highest Cybercrime Domain Scores	Yearly Cybercrime Domain Score ▼	.COM score: 109.7 .NET score: 109.1
BEAUTY	2,834.8	
REST	2,542.2	
CYOU	1,877.9	
MONSTER	1,873.1	
LIVE	1,798.9	

An Internet user is more likely to encounter a dangerous domain when they click on a hyperlink in an email or text message or visit a web site address that contains a domain name registered in a TLD with a high yearly cybercrime score. If a risk-averse organization determines that there is a high likelihood of exposing a user to attack, that organization is likely to blocklist an entire TLD to mitigate that threat.

Ranking of TLDs by Malicious Domain Registrations

The ten TLDs with most domains reported for serving as a resource for cybercrime activity included three **legacy TLDs** (.COM, .INFO, .NET), two **ccTLDs** (.CN, .ML) and five **new gTLDs** (.TOP, .SHOP, .LIVE,

.SITE, .ONLINE). Among these, the TLDs had the highest percentages of reported domains that we determined to be malicious registrations.

Rank	TLD	Cybercrime domains reported ▼	Domains Determined to be Malicious Registrations	Malicious Domains Percentage
1	COM	**1,742,618**	819,146	47.0%
2	TOP	**206,512**	189,592	91.8%
3	INFO	**179,747**	126,874	70.6%
4	CN	**290,070**	93,953	32.4%
5	SHOP	**93,725**	89,792	95.8%
6	LIVE	**112,349**	89,217	79.4%
7	SITE	**100,977**	86,485	85.6%
8	ONLINE	**105,794**	81,696	77.2%
9	ML	**118,717**	76,949	64.8%
10	NET	**139,194**	58,180	41.8%

Abuse of Subdomain Resellers for Cybercrime

Subdomain resellers offer hosting and DNS services on a domain name that the provider owns. Users create an account and are assigned a hostname of the format `subdomain.domainname.tld`. Some of these providers offer website-building services. Others offer a third-level domain with free DNS management; in these cases, the user can redirect the assigned subdomain "name" to content at other hosting services, or they can register a "vanity" domain at any registrar and use this (for example, the domain `securityskeptic.com` is a vanity name for `securityskeptic.typepad.com`, a TypePad blog).

Over 500,000 subdomain hostnames serve as resources for cybercrime at 229 subdomain resellers

The ten subdomain resellers with the largest numbers of hostnames reported were:

Rank	Subdomain Reseller	Total Cybercrime Host Names Reported ▼	Count of Reseller's Unique Domains Reported
1	Google	177,622	72
2	DuckDNS	120,258	1
3	CentralNIC	70,017	15
4	Weebly	28,610	2
5	Cloudflare	20,269	2
6	Hostinger	19,102	6
7	Replit	16,508	1
8	ChangeIP	13,463	140
9	Wix	9,794	3
10	Square	7,561	1

Our 2023 Phishing Landscape study revealed that cyber attackers are increasingly turning to these services to host phishing pages. The data here suggests that they are becoming popular for purposes other than phishing (*e.g.*, malware hosting or ad landing pages) as well.

Cyber-attacks hosted at these services are hard to mitigate. The subdomain resellers are responsible for the naming, addressing, and content hosting, so only they can respond to abuse complaints and mitigate attacks. But subdomain resellers often lack effective, proactive measures to keep criminals from creating accounts and abusing their services. Many providers simply can't respond to complaints that request customer contact information. Since many offer free services and often only collect an email address, or permit anonymous registration, they simply do not know customer identities.

Subdomain reseller services have become even more attractive as free domain registrations from operators like Freenom become scarce

Cybercriminals have learned how to create accounts in bulk at some of these services, and so it is imperative that the providers implement strong anti-abuse measures.

Cybercrime Activity Across All TLD Registrars

Many criminals register domain names purposely for the perpetration of cybercrime. They also use the domains of innocent registrants by breaking into their hosting or domain management services. While they purchase and manage domain names through many registrars, some registrar services, pricing, or practices appear to be more attractive to cybercriminals than others.

We ranked all Domain Registrars by Cybercrime Domains for the September 2022 to August 2023 study period. This included all cybercrime domains reported for which we were able to identify the registrar. This includes gTLD and ccTLD registrations for registrars. The table shows the number of cybercrime domains for each registrar along with the top 5 TLDs in which those registrar's domains were registered.

Rank	TLD Registrar	Total Cybercrime Domains Reported ▼	Largest Counts of Cybercrime Domains in
1	NameCheap	704,901	.COM, .ONLINE, .SITE, .NET, .INFO
2	Freenom	401,634	.ML, .TK, .CF, .GA, .GQ
3	NameSilo	297,975	.COM, .INFO, .TOP, .LIVE, .US
4	GoDaddy	293,733	.COM, .LIVE, .INFO, .IN, .ORG
5	GMO d/b/a Onamae	268,887	.COM, .CLICK, .CFD, .NET, .INFO
6	Alibaba Cloud Computing	172,623	.CN, .COM, .TOP, .ASIA, .XYZ
7	PublicDomainRegistry	161,815	.COM, .ONLINE, .NET, .INFO, .ORG
8	Gname	90,713	.COM, .NET, .ICU, .CYOU, .VIP
9	Registrar.eu	75,905	.INFO, .COM, .LINK, .CLUB, .ME
10	eNom	59,297	.LIVE, .COM, .FYI, .NET, .ZONE

Some registrar services, pricing, or practices appear to be more attractive to cybercriminals than others

Both NameCheap and NameSilo have extraordinarily large numbers of cybercrime domains reported yet both have significantly smaller numbers of domains under management than GoDaddy, the largest domain registrar. GMO, d/b/a Onamae, has nearly as many domains under management as GoDaddy but is much smaller. These findings suggest that a study of service features, pricing or accessibility is needed. (Since Freenom has been forced through litigation to shut down operations, its presence in the top 5 is short-lived.)

Malicious Domain Name Registrations and gTLD Registrars

Counts of cybercrime domains help us to identify where domain names reported for cybercrime were registered. By identifying characteristics of maliciously registered domain names and distinguishing these from compromised domains, we can identify which parties – TLD operators, registrars, or hosting providers – are best positioned to act to prevent cybercrime.

For example, investigators may first seek assistance from hosting providers to mitigate cybercrime attacks, by having the cybercrime page and related content removed from a compromised web site. For domains that were purposely registered as a resource for a spam campaign or malware hosting, a registrar is often best positioned to assist in mitigation. A registrar can suspend a domain registration or name resolution for a domain while it reviews the registrant's contact data to assess the legitimacy of the registration. Ten TLD registrars with the most maliciously registered domains reported for serving as resources for cybercrime activity were:

Rank	gTLD and ccTLD Registrars	IANA ID	Cybercrime Domains Reported	Domains Determined to be Malicious Registrations ▼	Percentage of Malicious Domains
1	NameCheap	1068	704,901	326,632	46.3%
2	NameSilo	1479	297,975	173,225	58.1%
3	GMO d/b/a Onamae	49	268,887	171,751	63.9%
4	Freenom	n/a	401,634	171,502	42.7%
5	GoDaddy	146	293,733	136,776	46.6%
6	Alibaba Cloud Computing	1599	213,967	94,444	44.1%
7	PublicDomainRegistry	303	172,623	79,016	45.8%
8	Gname	1923	90,713	47,426	52.3%
9	Registrar.eu	1647	75,905	46,051	60.7%
10	Sav.com	609	54,644	39,613	72.5%

The following table shows those registrars with at least 50,000 cybercrime domains during the September 2022 to August 2023 study period ranked by the highest percentage of those domains that were registered purposely to abet cybercrime.

Rank	gTLD and ccTLD Registrars	Cybercrime Domains Reported	Domains Determined to be Malicious Registrations	Percentage of Malicious Domains ▼
1	Sav.com	54,644	39,613	72.5%
2	eNom	59,297	39,562	66.7%
3	GMO d/b/a Onamae	268,887	171,751	63.9%
4	Registrar.eu	75,905	46,051	60.7%
5	NameSilo	86,075	51,091	59.4%
6	Gname	297,975	173,225	58.1%
7	GoDaddy	90,713	47,426	52.3%

Rank	gTLD and ccTLD Registrars	Cybercrime Domains Reported	Domains Determined to be Malicious Registrations	Percentage of Malicious Domains ▼
8	NameCheap	293,733	136,776	46.6%
9	PublicDomainRegistry	704,901	326,632	46.3%
10	Alibaba Cloud Computing	213,967	94,444	44.1%

The high percentages of malicious domain registrations illustrate why efforts to identify suspicious registration behavior and prevent criminals from registering suspicious domains are necessary to disrupt the cybercrime supply chain.

89 registrars had at least 60% of their cybercrime domains registered maliciously

The top ten represent just the tip of an iceberg: from our data, considering registrars with at least 25 cybercrime domains, we determined that 60% or more of the cybercrime domains reported were malicious registrations in 89 registrars.

Cybercrime Activity Across Hosting Networks (ASNs)

We studied where cybercrime activity was hosted and where unsolicited messaging associated with cybercrime originated, to identify hosting providers that criminals find attractive or exploit. We collected the IP addresses (DNS A records) to which cybercrime records were resolving, including IP addresses that were used explicitly in cybercrime URLs. We then looked up the Autonomous System Number (ASN) containing each IP address. This provides insight into the hosting network where the cybercrime activity was hosted. IPv6 addresses were not reported in our cybercrime feeds: the following sections consider cybercrime activity that was hosted on IPv4 addresses only.

Ranking of Hosting Networks (ASNs) by Number of Unique Cybercrime Addresses

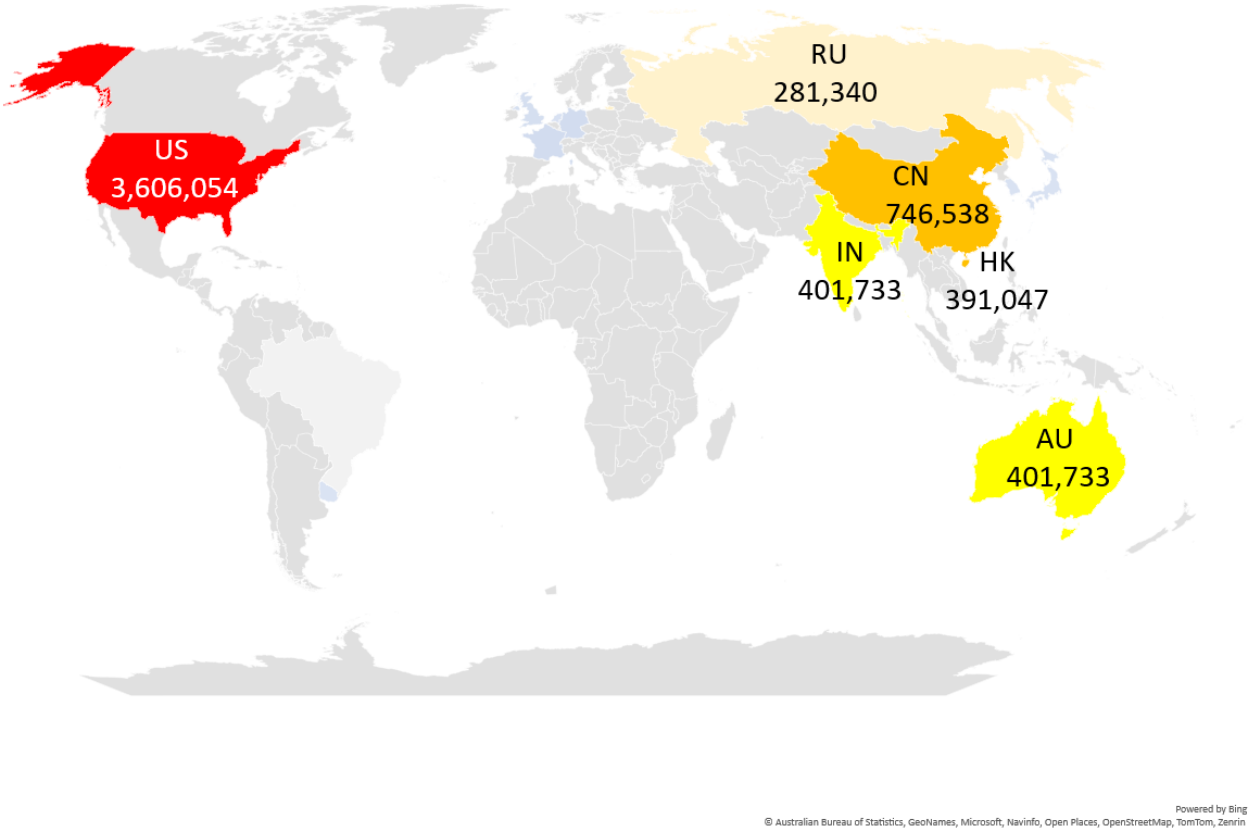
We found cybercrime activity in 30,708 hosting networks. Ten of the top hosting providers accounted for 28% of the 3,864,207 IPv4 addresses for which an ASN could be determined. We used RIPEstat geo data (per Maxmind GeoLite) to identify the 233 countries where IP addresses reported for hosting cybercrimes for each of ASN had the most IPv4 cybercrime addresses reported.

Hosting networks in the China and US were hives for cybercrime activity

Rank	Hosting Provider	ASN Number	Country	Unique IPv4 Addresses Reported ▼
1	No.31,Jin-rong St.	4134	China	**362,403**
2	China169 Backbone	4837	China	**233,924**
3	Bharat Sanchar Nigam	9829	India	**179,952**
4	DigitalOcean	14061	United States	**128,365**
5	Chunghwa Telecom	3462	China	**95,042**
6	Cloudflare	13335	United States	**66,896**
7	Amazon	14618	United States	**64,955**
8	Clayer	137951	China	**62,707**
9	Amazon	16509	United States	**61,353**
10	TE-AS	8452	Egypt	**56,381**

Our 2023 Phishing Landscape study data showed that the five hosting networks that most attracted phishers were in the United States. Our 2023 Malware Landscape study showed that China and the United States accounted for 7 of the 10 hosting networks that hosted the most malware. When we combined spam, phishing, and malware records in this study, China and the United States accounted for 8 of 10 hosting networks with the highest cybercrime activity.

Worldwide, the United States had the most IPv4 addresses reported for serving as resources for cybercrime activity. China, India, Australia, and Hong Kong rounded out the top 5. Russian Federation, Great Britain, and three European countries (France, Germany, and Brazil) complete the top 10.


RU
281,340
US
3,606,054
CN
746,538
IN
401,733
HK
391,047
AU
401,733
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

These findings, persistent irrespective of the cybercrime reported, should raise questions in the United States and China, two nations that are arguably the most technologically advanced in the world. Both may need to consider proposals for regulations that require Internet as a Service operators to collect and maintain accurate contact information, or that oblige domain registrars or registries to “lock and suspend” a hosting or registration service while a cybercrime investigation is conducted.

Impersonated Brands

Criminals often register legitimate-looking domain names for cybercrimes as part of the impersonation or deception that facilitates the perpetration of a fraud. They don't hesitate to register such names because they know from experience that most TLDs and registrars have no policy or legal obligation to screen for well-established brand names at the time of domain name registration.

Some make no effort to create deceptively similar names but include the exact brand in the composition of domain names that they register for cybercrime campaigns (*e.g.*, `applesupport.cf`, `apple-verification.xyz`, `amazonpaymentservlce.ga`). Criminals also use exact brand matches when they create accounts at subdomain resellers (*e.g.*, `barclays-online-support.web.app` and `barclays-helpdesk.web.app`).

In past studies, we noted that the number of brands being targeted by cybercrimes has increased since we began reporting in 2020. For this study, we wanted to determine which brands were most frequently impersonated in name resources for cybercrime activity more broadly. We searched for exact brand matches in the domain names, in URLs containing domain names, and in subdomain service hostnames reported for abetting cybercrime activity.

We found that nearly 170,000 domain names, and nearly 23,000 subdomain reseller host names, contained an exact match for a brand in their name. Here are the top 10 brands found in registered domain names and in subdomain reseller host names.

Rank	Brands Found in Registered Domain Names	Number of Matches ▼
1	Apple	23,018
2	Amazon	10,946
3	United States Postal Service	9,242
4	Chase	4,571
5	Google	4,395
6	Steam	4,185
7	Netflix	4,005
8	Coinbase	3,632
9	EPOS Card	3,418
10	Ally Bank	3,409

"exact match" domains victimize the most vulnerable users…

these are the elderly or least technically savvy members of society

Exact match of a brand name appeared in
206,040 cybercrime records
169,835 domain names
22,679 subdomain reseller host names

People often read what they want to see, *NOT* what is displayed in a text or hyperlink

Cybercriminals exploit this

Rank	Brands found in Subdomain Reseller Hostnames	Number of Matches ▼
1	SQUARE ENIX	5,367
2	GoDaddy	4,664
3	Amazon	1,805
4	Yahoo!	1,273
5	Microsoft	1,163
6	Cloudflare	1,016
7	Facebook	790
8	Rogers	610
9	Hotmail	553
10	Webmail	519

Preventing registration of domain names containing exact matches of brands would remove one form of deception from the cybercriminal's supply chain. It is also one of the simplest ways to insulate Internet users and organizations from the harms or losses resulting from phishing, scams, counterfeiting, and other crimes. A preventative program can begin with searches for, and preventing (or delaying) registration of, trademarks, especially when a registrant attempts to acquire volumes of domains in matters of minutes (*e.g.*, "in bulk"). This one measure won't prevent cybercrimes, but it removes from the supply chain the names that take advantage of the most vulnerable users.

Users can also learn from these findings:

- Read the entire URL.
- Read what is displayed, not what you expect to be displayed.
- Resist the temptation to stop reading once you've encountered a brand or familiar string of characters in URLs and only use this to conclude the URL is safe.

Users are encouraged to visit the website Stop. Think. Connect. Website for additional online safety awareness resources for all ages, in many languages and formats.

Bulk Registration of Domain Name Resources for Cybercrime

Cybercriminals rely upon domain names that can be rapidly acquired, used in an attack, and abandoned before they can be traced. Spam and ransomware campaigns, and criminal infrastructure operations – botnets and Ransomware or Phishing as a Service (RAAS, PhAAS) – particularly benefit from the ability to use bulk registration services offered by domain name registrars.

In an October 2019 study, Criminal Abuse of Domain Names, Interisle observed extraordinary daily spikes in domain names added to reputation blocklists. We investigated these spikes by studying the creation dates, sponsoring registrar, and registrant contact data that was published in WHOIS prior to May 2018. Close examination of what initially appeared to be daily spikes revealed that certain cybercriminals *repeatedly* registered hundreds or thousands of domain names in a matter of minutes. These were subsequently used to support snowshoe spam campaigns, phishing, or ransomware attacks.

For this study, we again searched for characteristics of bulk registration behavior. Because registrant contact data is now widely unavailable, we look for occurrences where sets of ten or more domain names were registered via the same registrar within 10 minutes of each other. These sets were treated as bulk domain registrations. We then counted the number of such sets as well as the total number of domains in each set. We do not have contact data to confirm that these sets were registered by a single registrant, but it seems unlikely that several unrelated (or non-conspiring) registrants would register domain names with the exact label composition characteristics, at the same time, in volume.

We only examine domain names that have already been identified as resources for cybercrimes, so any suggested or supposed reason for a legitimate person or legal entity to register tens, hundreds, or thousands of domains in a matter of minutes falls outside the scope of this report.

Over 1.5 million domains exhibited characteristics of malicious bulk domain registration behavior

The domain name system was never intended to supply criminals with thousands of domains in a matter of minutes and do so year after year. However, we associated 1,529,677 domains with bulk domain registration behavior. These occurred in 29,561 sets. We found occurrences of bulk domain registration of domains in 292 registrars.

The table below shows some of the largest occurrences of bulk domain registration behavior.

Registration Time Span (UTC)	Number of Bulk Domain Registrations	Registrar	Sample Cybercrime Domains
13:45 - 14:05 12/25/2022	15,058	Alibaba Cloud Computing Co., Ltd. (Wanwang)	jklzqgx.cn oyuotkk. zpggyl.cn nuagmyf.cn tzrppvu.cn qiwfuls.cn mimipnw.cn meqqdss.cn
15:56 - 16:45 12/22/2022	11,932	Alibaba Cloud Computing Co., Ltd. (Wanwang)	bttslad.cn uvxgzma.cn npzmblz.cn xbhfsol.cn sskrock.cn aqnpyhr.cn tugimgh.cn ktiwsqq.cn
18:49 - 19:45 12/13/2022	11,771	Alibaba Cloud Computing Co., Ltd. (Wanwang)	ggflxiw.cn jtvtrmj.cn jcdpsfc.cn doznubt.cn grjvaje.cn cdruonx.cn ogtqdgl.cn uhnumfp.cn
16:42 - 17:29 11/20/2022	10,245	Alibaba Cloud Computing Co., Ltd. (Wanwang)	fnfqnvz.cn dabxmmp.cn pwfrmij.cn porhqas.cn fxxdfxm.cn qekvtbq.cn gnzcrea.cn twpakis.cn
08:48 - 09.40 2/24/2023	9,515	GoDaddy	bandao101.com bandao102.com ... bandao2048.com bandao2050.com
17:10 - 17:43 12/2/2022	8,086	Alibaba Cloud Computing Co., Ltd. (Wanwang)	rbtqadz.cn uqvtbxq.cn pqbldtl.cn nxdrfsw.cn udvdaux.cn pxddsbe.cn qesqigj.cn
07:22 - 10:50 8/26/2023	7,938	Xin Net Technology Corporation	jxcpay.com jxfyqy.com jxgysjds.com jxcxdjx.com jxgzph.com jzcjspjx.com jzjflzz.com jzlenovo.com
23:20 - 23:33 on 11/112022	6,441	Alibaba Cloud Computing Co., Ltd. (Wanwang)	ggflxiw.cn jtvtrmj.cn jcdpsfc.cn doznubt.cn grjvaje.cn cdruonx.cn ogtqdgl.cn uhnumfp.cn
12:31 - 15:11 4/13/2023	6,211	GMO Internet Group d/b/a Onamae.com	tbdswo.cfd feuosj.cfd qylpns.cfd albprm.cfd feqkpg.cfd gdhmjx.cfd mstpgo.cfd qufvzm.cfd
03:15 - 04:23 11/6/2022	5,800	Alibaba Cloud Computing Co., Ltd. (Wanwang)	nantonggupiao.cn nantonggupiaozhishi.cn nantonggupiaogongsi.cn nantonggupiaoxuexi.cn nantonggupiaozixun.cn nantonggupiaoapp.cn

The examples from the sets show that domain names containing pseudo randomly or otherwise autogenerated strings are common in bulk registrations. We only examine domain names reported for serving as resources for cybercrimes, but it is worth asking whether there are any legitimate purposes for domain names composed in this manner. However, just as they can composed by automation, so can they be identified prior to processing a domain registration through automation. And they would be readily identified or confirmed by human inspection as suspicious.

We also found evidence of bulk registration of exact brand matches in bulk registrations:

Registration Time Span (UTC)	Registrar	Sample Domains

04:42 - 04:43
6/15/2022
	Alibaba Cloud Computing Ltd. d/b/a HiChina	`usps-team.fun`
		`usps-manage.ren`
		`usps-team.top`
		`usps-manage.xyz`
		`usps-team.xyz`

00:17 - 00:28
2/26/2022
	Chengdu West Dimension Digital Technology	`amazontechnicalaccademy.com`
		`amazontechnicalacedamy.com`
		`amazontechnicalacadeny.com`
		`amazontechnicalacadmy.com`
		`amazonntechnicalacademy.com`

22:45 -22:45
12/18/2022
	Alibaba Cloud Computing Ltd. d/b/a HiChina	`microsoft-outlook-mniyu.website`
		`microsoft-outlook-sfuzc.website`
		`microsoft-outlook-hcvmc.website`
		`microsoft-outlook-jtztx.website`
		`microsoft-outlook-huyhy.website`

These examples underscore how important it is to remove one form of deception from the cybercriminal's supply chain so that Internet users won't fall victim to attacks that use domain names containing exact matches of brands.

Bulk registrations accounted for one third of the malicious domains reported for serving as resources for cybercrimes

We identified ten registrars where over 60% of the domains reported as resources for cybercrime activity were associated with a bulk registration:

Rank	Registrar	IANA ID	Domains Associated with Bulk Registration Behavior	Percent Cybercrime Domains Reported ▼
1	Domainipr	3222	605	90%
2	Metaregistrar	2288	3,338	89%
3	Xin Net Technology	120	24,563	80%
4	West263 International	1915	10,573	80%
5	Chengdu West Dimension	1556	30,431	79%
6	Xiamen 35.Com Technology	1316	5,184	73%
7	Aceville	3858	8,213	70%

Rank	Registrar	IANA ID	Domains Associated with Bulk Registration Behavior	Percent Cybercrime Domains Reported ▼
8	Spaceship	3862	2,074	66%
9	NameCheap	1068	447,544	65%
10	Hong Kong Juming	3855	14,424	64%

Ten registrars with the highest number of domains associated with bulk registration behavior were:

Rank	gTLD Registrar	IANA ID	Domains Associated with Bulk Registration Behavior ▼	Cybercrime Domains Reported
1	NameCheap	1068	447,544	690,267
2	Onamae.com	49	158,376	268,644
3	NameSilo	1479	145,156	291,137
4	GoDaddy	146	108,117	356,881
5	PublicDomainRegistry	303	45,878	184,700
6	Gname	1923	44,271	90,713
7	Chengdu West Dimension	1556	30,431	38,718
8	Dynadot	472	29,011	77,393
9	HiChina	1599	27,086	50,940
10	Xin Net Technology	120	24,563	30,553

Weaponizing Domain Names

The term ‘weaponize’ refers to the act of adapting something nominally benign – an off the shelf medicine, fertilizer, or even space – to serve as a tool in the pursuit of some malignant (criminal) activity. The broader context is that adapting these everyday items creates security threats, including national security threats to the well-being or lives of residents, visitors, and citizens.

For example, when terrorists misuse farm performance products (*e.g.*, fertilizers) to construct improvised explosive devices, they ***weaponize*** ammonium nitrate. Readers may find the video, *Weaponizing Domain Names,* helpful.

When the illegal drug industry diverts pseudoephedrine to the manufacture of methamphetamine, they ***weaponize*** a medication intended to relieve suffering.

> ***When cybercriminals acquire and employ thousands of internet domain names to distribute spam or to host illicit content, they are weaponizing domain names to cause financial loss or harm***

In the extreme cases of ransomware attacks against healthcare or emergency systems or critical infrastructures, the potential harms include loss of life.

An Obligation to Protect the Public from Harm

Other industries have a regulatory obligation to protect the public from criminal misuse of potentially dangerous products through mandatory or recommended validation regimes. U.S. pharmacies, for example, require valid proof of identity from any party that attempts to purchase quantities of pseudoephedrine that exceed well-defined limits. Tracking regulations apply to sellers of ammonium nitrate in the USA. These exist to protect the public against the construction of improvised explosive devices.

Legitimate businesses comply with these and like-minded regulations in the interest of public safety. Legislators should consider whether the domain name industry should have a similar obligation to verify registrant contact data and registrant payment methods as part of the validation process; for example, registrars could decline transactions in which the registrant contact data does not match the authorized credit card user.

Putting it all Together: The Cybercrime Supply Chain

This report has examined the contributions of each portion of the name and addressing resources that cybercriminals employ: TLDs, Subdomain Resellers, TLD Registrars, and Hosting Providers. Earlier, we explained that criminals have choices when they seek to acquire names and addresses. Here, we examine these choices separately to show how malicious domain names or malicious subdomain reseller host names are acquired.

Supply Chain: Registrars, TLDs, Hosting

The following table shows the top 10 combinations of Registrar, TLD, and Hosting Provider where more than 5,000 maliciously registered cybercrime domains were identified. This supply chain is commonly found in the study's phishing and spam data sets.

Rank	Registrar	TLD	Hosting Provider	Cybercrime Records ▼	Maliciously Registered Cybercrime Domains
1	eNom	live	Cloudflare, Inc.	25,895	14,193
2	GoDaddy	com	BGP Consultancy	24,713	21,732
3	Freenom	ml	A2 Hosting	24,594	24,173
4	Xin Net Technology	com	Clayer	22,443	22,406
5	PublicDomainRegistry	com	M247	20,727	17,638
6	GoDaddy	com	HONG KONG Megalayer	15,049	14,907
7	DNSPod	com	Clayer	13,225	13,068
8	Freenom	tk	Cloudflare	12,869	6,628
9	Freenom	ml	Interserver	11,847	11,381
10	Freenom	ml	Microsoft Corporation	10,076	9,437

Supply Chain: Subdomain Resellers, Hosting

The following table shows the top 10 combinations of Subdomain Reseller and Hosting Provider where criminals created user accounts and used the hostnames assigned by the reseller for criminal activities. This supply chain has become increasingly present in our phishing and spam data sets.

Rank	Subdomain Reseller	TLD	Hosting Provider	Cybercrime Records ▼	Maliciously Acquired Cybercrime Hostnames
1	DuckDNS	org	LG DACOM	42,768	42,758
2	DuckDNS	org	Netminders Server Hosting	24,641	24,546
3	Weebly	com	Weebly	19,512	19,462
4	DuckDNS	org	DediPath	18,618	18,467

Rank	Subdomain Reseller	TLD	Hosting Provider	Cybercrime Records ▼	Maliciously Acquired Cybercrime Hostnames
5	Google	app	Fastly	16,653	16,061
6	Hostinger	com	Hostinger International	14,426	14,261
7	Google	com	Fastly	13,045	12,772
8	Google	com	Google	10,911	10,859
9	Replit	co	Google	9,963	9,744
10	Square	site	Weebly	7,559	7,390

Supply Chain: Hosting

The following table shows the top 10 Hosting Providers for cybercrimes that employ only IP addresses. This abbreviated supply chain was most evident in the study's malware data.

Rank	Hosting Provider	Cybercrime Records ▼	Cybercrime Addresses
1	No.31,Jin-rong Street	388,302	361,679
2	China169 Backbone	304,773	233,520
3	Bharat Sanchar Nigam	210,985	179,938
4	DigitalOcean	113,816	112,339
5	Amazon	106,513	105,938
6	Chunghwa Telecom	95,528	94,745
7	TE-AS	56,411	56,366
8	Google	52,000	51,775
9	PJSC Rostelecom	47,739	47,248
10	TELEFONICA BRASIL	44,042	43,767

Building a Better Future: Policies, Practices, and Legislation

Our study has measured and identified distinct and persistent patterns of the name and address resources criminals acquire to perpetrate cybercrimes. The patterns show that:

- Spam, malware, and phishing activities are intertwined.
- Phishing and malware are criminal acts that rely on name and address resources for successful perpetration.
- Spam, whether email, messaging, or social media, is a predicate act that provides resources for serious crimes, *e.g.*, phishing or malware.

Our 2023 Phishing Landscape and 2023 Malware Landscape studies showed that mitigation of phishing and malware isn't working. Their attack surfaces expand year after year, as do the victim counts and losses.

Post hoc responses – triage, mitigation, and incident recovery – are necessary but insufficient actions. Interisle believes that adopting a coordinated strategy that disrupts supply chains can be effective in mitigating cybercrime. Efforts to starve criminals of Internet resources they need to execute cybercrimes are long overdue. The global domain and web hosting industries, governments, and parties most adversely affected by cybercrime have roles to play.

We must strategically starve criminals of easy access to resources for cybercrimes

Actions for Effective Change

We identified nearly 5 million domains used as resources for cybercrime activity and an equally large number of addresses where cybercrime resources for malware, spam, or hosted. These figures clearly illustrate that criminals can trivially acquire the resources they need to perpetrate cybercrimes. Proactive or preventative measures are required to disrupt cybercrime supply chains.

Coordination, cooperation, and consistent action across a broad range of stakeholders and actors in the cybercrime supply chain is the most, if not the only, effective way of creating change

Specific recommendations follow for the domain industry, cross-industry collaboration, government action, and litigation.

Actions for Effective Change: Domain Industry

The domain name industry must adopt policies and practices that can deprive criminals of the DNS resources and disrupt their ability to conduct cyberattacks**.** The ICANN organization and the domain name community generally should consider the following improvements in industry policies and practices.

Registry and Registrar Agreement Modifications

ICANN has negotiated new contractual obligations 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:

- **Treat spam with the serious concern it merits.** Industry advocacies including M3AAWG and CAUCE define spam as "bulk unsolicited email" (which is generally illegal to send in most countries). **Three-quarters of the nearly five million domains that Interisle studied were reported as spam domains. No one is investing in resources at this scale to send benign content except as a precursor to a subsequent crime.** 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*.
  Our study demonstrates that **spam is almost never non-objectionable or benign but is nearly always a criminal (abusive) act itself or a predicate act to other serious crimes**. This is norm, and ICANN policy should address the norm not the exception, and ensure that registrars respond to spam reports, irrespective of abuses the message or content delivered.
- **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.*"
  This language does nothing to address the very serious exact-match brand registration or bulk registration problems that we identified in our study. ICANN should review the practice of bulk registration and develop a policy to prevent abuse. A know-your-customer model that validates the identities of registrants who acquire domain names in volume, obliges the registrant to a strict anti-abuse AUP, establishes them as legal entities, and publishes registrant data is recommended.
- **The new contracts do not impose any obligations to suspend domains that are maliciously registered**. Our study identified millions of domains where a customer had registered domains to perform criminal acts. Most of these domains – particularly domains registered by the thousands in matters of minutes – can be detected and blocked at time of registration. They should be suspended expeditiously by the registrar or registry operator pending investigation. **For the overwhelming number of domains that exhibit suspicious composition or rapid-fire registration patterns, the disrupting effect of domain suspensions will only affect criminals.**

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, which does not adequately acknowledge that it is a predicate act to cybercrime.
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. Our study data shows that cybercrimes generally run their course or affect the most victims within 24 hours of the onset of the attack. Malware, spam and phishing complaints should be investigated within 24 hours.
5) ICANN should create ways in which gTLD registry operators can stop doing business with a registrar that exhibits a high incidence of abusive and especially bulk registrations. These are often cases in which criminals make malicious registrations repeatedly. A registrar is essentially a supply chain business. The domain industry should follow examples of the pharmaceutical and farm performance industries 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 in the short period of time before they are weaponized for cybercrimes.** 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. Some registrars, *e.g.*, NameCheap, now limit the registration of domain names containing notable brand names and phrases, apparently as a way of preventing cybercrime. While voluntary efforts are welcome, an industry-wide policy and process is needed, or criminals will turn to registrars that do not adopt domain screening measures for their supply of domains.

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 identified in complaints or when their investigations identify active cybercrime activity on the domains. Criminals who register large batches of domain names can thus move attacks to domains that have yet to be reported. Registrars and registry operators are the only parties who can identify the full set of a registrant's domains and policy should direct them to suspend entire domain portfolios controlled by demonstrated malefactors.

R**egistrars should refrain from offering forms of bulk registration** except in circumstances where the customer acknowledges that they are a legal entity, provides credentials to corroborate their legal entity status, and provides a legitimate purpose (*e.g.*, protection of registered trademark or a legitimate service offering). This will effectively starve criminals of a resource that is consumed in volume.

The ICANN community should consider policies that protect Internet users from deceptive domain registrations. For example, registrars should make a pre-registration effort to prevent exact-match brand registrations by any party other than the recognized brand owner. Since the uniform dispute resolution process (UDRP) is out of reach of all but the largest organizations, ICANN should adopt some policy to allow businesses other than these some means to protect users from abuse of their names and services. Removing domain names that contain recognized brand strings from the supply chain eliminates a form of impersonation that criminals use to exploit the most vulnerable Internet users.

Implementation of these tools and techniques should be adopted across the domain name registration industry.

Investments, Incentives, and Enforcement

In previous reports, Interisle has stated that, to be effective, anti-abuse policies and practices must be developed, practically implemented, and enforceable. We recognize that industry players will incur a level of cost to implement anti-abuse practices and we again 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 cybercrime.** Registries and registrars should be incentivized to experiment with the many tools and techniques applied post registration by blocklist operators or researchers. Financial incentives for implementation and adoption of such automated tools, *e.g.*, a transaction fee reduction, 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 particularly.

c) **Monetary penalties**. A disincentive program could be implemented by ICANN (and by ccTLD registries), where a registrar with an excessive cybercrime yearly score would pay increased fees. Disincentive fees could be used to fund mitigation and awareness programs.

d) **Registrars should know or verify their customers**. Criminals often use false identities and stolen credentials to register domain names. Registrars should be encouraged or obliged to employ identity verification services to screen customers.

e) **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.*"

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**

and spam activity have 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 has a responsibility to ensure that additional new TLDs do not result in a more abundant supply chain.**

Address Cybercrime Mitigation Beyond ICANN

ccTLD and gTLD policies and policymaking are developed separately from the ICANN organization, and often independently by country. The domain name space needs a **cooperative effort from ccTLDs and gTLDs to develop policies to disrupt the supply of domain names to criminals across the name space**, so that any party seeking assistance when responding to cybercrimes where domain names serve as resources can rely upon some baseline of cooperation and action worldwide.

Actions for Effective Change: Cross-Industry Collaboration

Cybercriminals exploit name and address resources outside the domain name space. Our study data shows that the same abuses that plague the domain industry are present in the hosting industry. Hosting and subdomain resellers must cooperate more closely with domain industry players and stakeholders within to disrupt supply chains more effectively.

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

Effective cooperation programs can benefit an operator. They reduce the costs of removing illegal (phishing or malware) content or unauthorized software (*e.g.*, email or attackware) and thus eliminate costs in customer support and personnel 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. These should specifically identify spam, phishing, and malware.
- Uniform and timely action for the removal of content or unauthorized software that serve resources for cyberattacks.
- Adoption of recommended (best) content management practices that can reduce customer web vulnerability or other service (*e.g.*, email) attack surfaces.
- Uniform and timely cooperation with law enforcement, 3rd party brand protection services, and private sector cyber investigators.

Actions for Effective Change: Government Action

Industry self-regulation and existing domain policies can fail to adequately mitigate cybercrime in a ccTLD; for example, see *Nothing is Free: The Collapse of Freenom* on page 21 of Interisle's 2023 Phishing Landscape study. Governments should consider taking a more prominent role to ensure that criminals are less likely to use their namespace to supply domains for cybercrimes.

Some ccTLD policies are more successful than others in mitigating cybercrime threats. For example, most ccTLDs that have higher prices than gTLDs have little, or no cybercrime. Some ccTLDs have adopted policies requiring that registrants have a verifiable connection (nexus) to the country, such as proof of residence or evidence of incorporation, as a pre-requisite for domain registration These **ccTLDs 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 cybercrimes 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. In our comment, Interisle proposed record-keeping obligations for domain name registries. Similar obligations could help mitigate abuse of subdomain resellers or hosting services.

The U.S. 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 cybercrimes generally as they do 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 ccTLD. 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 typo squatting.

The UK Department for Science, Innovation and Technology's (DSTI) recent issued a consultation, Powers in Relation to UK-Related Domain Name Registries, which seeks input on policies for mitigating domain name abuse and misuse in UK-related top-level domains (TLDs). The Interisle contribution to UK DSTI explains that effective policies and procedures must aim at preventing criminals from maliciously registering names in the first place, not just cleaning up after abuse has already occurred. Our input also discusses the benefits in using the Council of Europe's Convention on Cybercrime's descriptions of harmful activities as a basis for defining prohibited uses of domain names, including facilitating multi-jurisdictional abuse mitigation and enforcement.

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. 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*”.

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.

Actions for Effective Change: Litigation

In our 2023 Phishing Landscape study, we noted that, **in the absence of more effective mitigation measures and broader cooperation, litigation has shown to be an effective tool in stemming abuse**. Interisle views litigation as a last resort. It is expensive, slow and success does not assure uniform improvement or change. However, it may become more frequent unless more efforts are made to disrupt the cybercrime supply chain.

Conclusion

The findings from this study underscore a previous Interisle finding, that the prevailing uncoordinated and ineffective attempts to curb cybercrime are not working, and that new strategies are required. The recommendations explain how cooperative, pro-active, and cross-sector efforts by governments, private sector, and public policy communities could disrupt the cybercrime supply chain.

Cybercriminals routinely exploit Internet resources to launch malware, spam, and phishing attacks. Our study findings show that the criminals who perpetrate these cybercrimes benefit from an expansive cybercrime supply chain and enjoy an enormous economic advantage over defenders and responders. These attacks negatively impact consumers, businesses, and economies globally.

The problem is worsening — domain registrars and domain registries in the gTLD and ccTLD name spaces along with hosting providers and subdomain resellers – have not kept pace with preventative measures to reduce cybercrime. Unless better supply chain disruption strategies are put into place, it’s inevitable that regulation and litigation will increase.

About the Authors and Contributors

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).

The authors would also like to acknowledge the peer review efforts of:

John Levine is an author, consultant, and speaker. John is the primary author of the well-known Internet for Dummies and many other books, and has been running e-mail systems since the 1970s. He is the President of CAUCE North America, the leading grass roots anti-spam advocacy organization. Levine is a Senior Adviser to the Messaging Anti-abuse Working Group (M3AAWG), has been a board member of the Internet Society, and is a member of the ICANN Security and Stability Advisory Committee (SSAC). John contributes to the Cybercrime Information Center as a developer and threat intelligence data subject matter expert.

Laurin B. Weissinger is a Senior Security Consultant at Fresenius Digital Technology and teaches Information and IT Security at the Department of Computer Science, Tufts University. He is also a visiting fellow at Yale Law School. Laurin serves as a Research Fellow at APWG and an Expert Advisor to M3AAWG, while being a member the "Digital Trust" group at ISACA Germany and the FIRST Human Factors SIG. Laurin has completed his DPhil (PhD) at the University of Oxford, and holds degrees from the Universities of Cambridge, Oxford, and Birmingham, along various industry certifications.

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, visit: www.interisle.net

Acknowledgments

The authors extend thanks to APWG, CAUCE, and M3AAWG for financial support. We also wish to acknowledge contributions of data and access to services that are instrumental to the types of studies and analyses that we conduct:

- Anti-Phishing Working Group (APWG), Invaluement, Malware Patrol, MalwareURL, OpenPhish, PhishTank, Spamhaus, SURBL, and URLhaus 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.