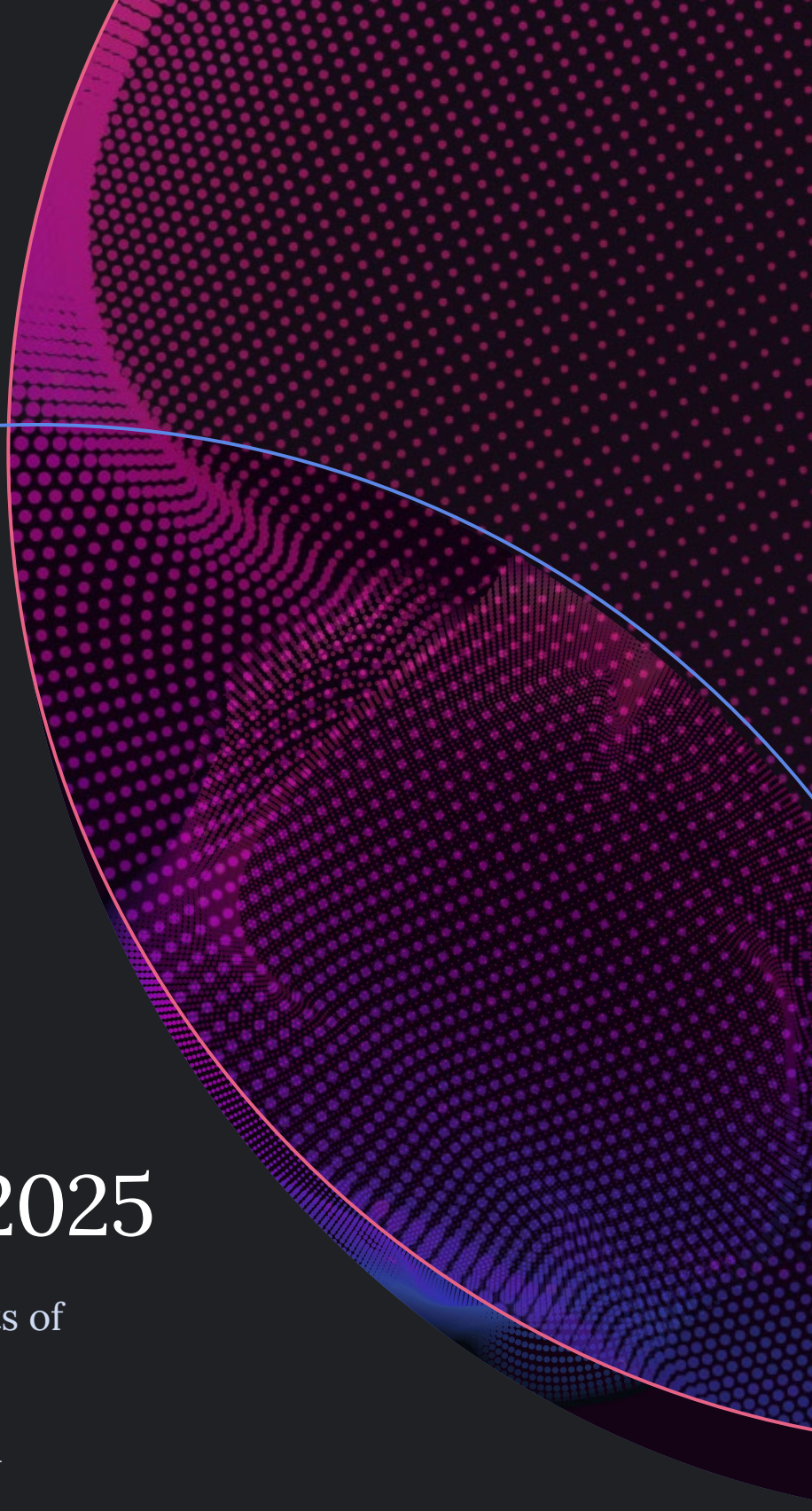
Interisle



Cybercrime Supply Chain 2025

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

INTERISLE CONSULTING GROUP NOVEMBER 2025

CONTENTS

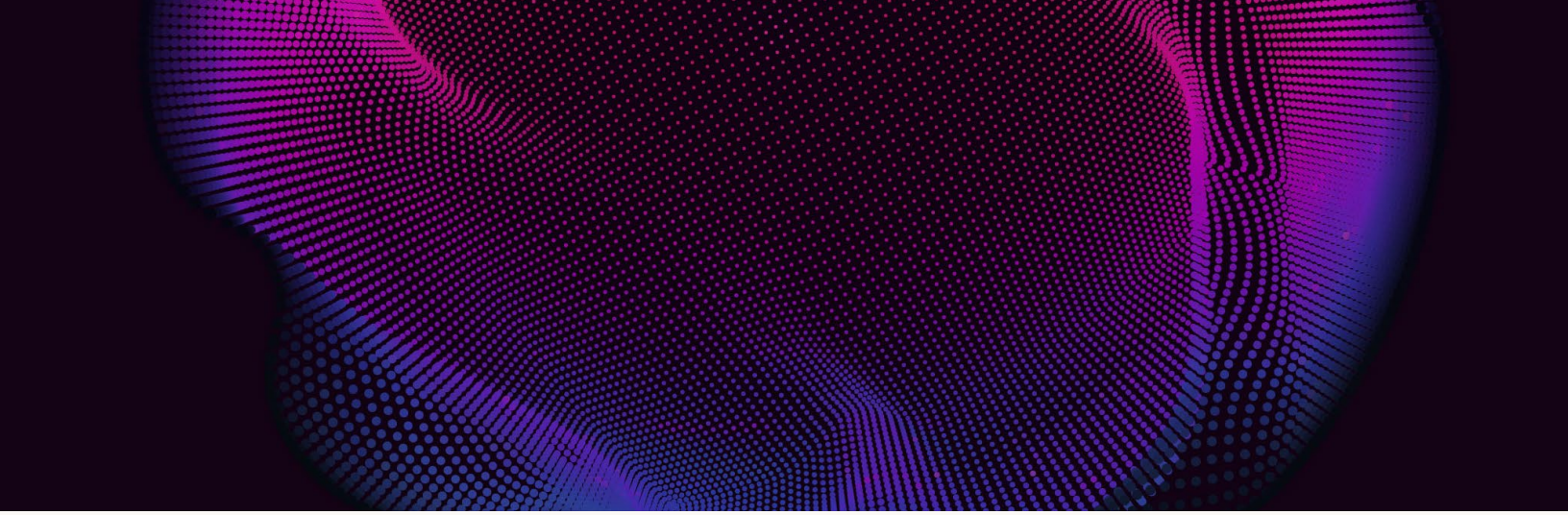
Study Sponsors

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) is a technology-neutral global industry association where both public and private sectors of the internet's economy unite as a working body to advance a safer digital environment for all. Founded in 2004, M3AAWG provides a trusted and collaborative worldwide forum to fight and prevent online abuse and includes more than 250 members worldwide. M3AAWG members and collaborators consist of Internet service providers (ISPs), communications service providers, social networking companies, hosting and cloud services providers, major antivirus vendors and security vendors, email service providers, leading hardware and software vendors and major brands, as well as invited experts, government agencies and related industry groups and partners. Working with these groups and individuals, M3AAWG develops and publishes best practices papers, position statements, training and educational videos, and other resources. M3AAWG's four organizational priorities in the fight against online abuse include: Communications & Content (Securing the Conversation); Platform & Infrastructure (Hardening the Stack); User & Endpoint (Protecting the Edge); and Policy & Regulations (Applying the Expertise).
https://www.m3aawg.org/



EXECUTIVE SUMMARY

Cybercrime has flourished and continues to grow because it is a lucrative endeavor.

Cybercrime has flourished and continues to grow because it is a lucrative endeavor. When compared to the GDP of nation states, cybercrime economy is expected to outperform all countries except China, the United States and India in 2025. The costs inflicted on society by cybercrime are orders of magnitude greater than the earnings pocketed by criminals.

Like any business, cybercriminals need resources and services to conduct their illicit operations. Efforts to make it more difficult and costly for criminals to acquire these resources, as well as the means to monetize their gains, can help reduce the attractiveness and profitability of criminal enterprises and should be part of the overall strategy to mitigate cybercrime.

The Interisle Cybercrime Supply Chain framework provides a means to analyze this criminal resourcing. By assessing cybercrime like any other business, we reveal opportunities to starve criminals of the resources they need for their costly attacks. Our third annual study uses this framework to illustrate and analyze resource use in three of the most common and costly cybercrime attacks and attack vectors: malware, phishing, and spam.

To provide this analysis, we collected malware, phishing, and spam reports from eleven publicly and commercially available threat intelligence or reputation services. We analyzed where cybercriminals obtained the naming and hosting resources used in these attacks and the common tactics used to acquire them. We then ranked Top-Level Domain (TLD) registries, TLD registrars, hosting providers, and free web hosting providers that represent the greatest amount of cybercrime activity based on raw counts and comparative metrics.

Our analysis reveals that:

Malware, phishing, and spam attacks grew by 60%, to over 26 million attacks. While phishing increased by a worrisome 40% from 2024, spam grew at the most alarming rate, more than doubling over 2024 from 8 million to over 17 million unique attacks.

New gTLDs accounted for 47% of cybercrime domains reported while holding only 12% of the total domain name market. The percentage of names registered by criminals for illicit activity in the new TLD space was nearly five times its market share. Country-code TLDs (ccTLDs) and the .COM/.NET TLDs showed meaningful decreases in cybercrime domains reported.

19.5 million unique domains were used in cyberattacks compared to 8.6 million last year – a 126% increase. Cybercriminals sharply increased their registration of cheaply priced and easily registered name resources for cyberattacks. Year over year, these registrations increased by 149%.

Over 7.3 million domains used in cyberattacks were registered in bulk, a 177% increase compared to last year. Cybercriminals took full advantage of buying in bulk – registering high volumes of domain names over short periods of time.

Exact matches of brand names appearing in domain names increased 97% year over year. Neary 500,000 domain names and free web site account names contained exact matches of brands that we track.

Cybercriminals decreased their use of free web site hosting as a key resource for attacks over the past year. While 683,000 subdomain hostnames were found to be used in attacks, this represents a decrease of 42% compared to last year.

The number of IPv4 addresses reported for hosting cybercrime activity decreased 20% year over year. The United States, China, and India had the most IPv4 addresses reported for hosting cybercrime.

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

Among our recommendations:

Implement robust identify verification/certification requirements for parties wishing to register domain names in bulk. Limit the number of accounts that a customer can register at free web hosting providers.

Expand the deployment of automated systems across industries in the cybercrime supply chain to screen suspicious resource registration and use patterns with the aim of preventing criminal resource acquisition and shutting down problematic use more swiftly.

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

Require corrective action by service providers that are shown to consistently and disproportionately supply cybercriminals with the resources used in attacks. Penalize consistently poor performers to reduce misuse of their operations by criminals.

Clear opportunities exist to preemptively disrupt criminal access to resources across the cybercrime supply chain by making it more difficult or costly to acquire them. Yet progress in the adoption of preemptive measures remains frustratingly slow.

Effective, uniform, outcome-oriented, cross-sector collaborations are necessary to prevent or quickly mitigate criminal access to cybercrime resources.

Introduction

Cybercrime is a highly lucrative global endeavor. The Internet Crime Report prepared by the U.S. Federal Bureau of Investigation reported that cybercrime resulted in US$16 billion in direct financial losses for U.S. consumers and businesses alone in 2024 and more than US$50 billion in direct losses over the last five years.

This report focuses on threats that are considered cybercrimes in the Council of Europe's Convention on Cybercrime (the Budapest Convention). The Convention on CyberCrime is an international treaty for crimes that are committed via the Internet and other computer or device networks. The Budapest Convention has a technical amendment specifically for the circumstances where spam is a crime. How we map malware, phishing, and spam onto the Convention Articles is described at the Cybercrime Information Center.

Cybercrime has matured into a professionalized and multinational industry. Criminal enterprises and entrepreneurs now acquire the resources they need from a variety of suppliers, service providers, exchanges, and specialized marketplaces. Their supplies, services, and transactions are sourced from both legitimate and dark economies.

The business management strategies, industry structures, and profit drivers within the cybercrime industry emulate a legitimate economy and would be familiar to any real-world executive. Pay rates and benefit packages sometimes rival that of real-world corporate jobs. Research by Kaspersky, for example, found dark web job postings for IT roles paid as much as US$20,000 per month, with benefits including paid time off and sick leave.

Cybercriminals have achieved a global reach impacting all sectors of society. The costs to societies worldwide are orders of magnitude greater than the direct earnings pocketed by criminals. Cybersecurity Ventures predicts

Over $1.5 Trillion USD

Revenues Earned by Cybercriminals Annually

Source: Prof. Michael McGuire

$12.2 Trillion USD

Estimated total annual cost of Cybercrime on the Global Economy

Source: Cybersecurity Ventures

$2.9 Billion USD

Cost of Business Email Compromise (BEC) scams in 2024

Source: FBI

$1.54 Million USD

Average Ransomware Payment in 2023

Source: Sophos

$4.88 Million USD

Average Phishing-related Breach Cost in 2025

Source: Deepstrike

$1.5 Million USD

Average Cost to Recover from Ransomware Attack in 2025

Source: Sophos

cybercrime will inflict US$12.2 trillion in recovery and direct losses globally in 2025 – a 13% increase over 2024. When compared to the GDP of nation states, global cybercrime is expected to outperform all countries except China, the United States, and India in 2025.

Cybercrime is a complex, systemic problem. Cybercriminals can easily perpetrate attacks across borders, obscure their operations, and establish and disband campaigns quickly. A multi-disciplinary, international effort is needed to disrupt or dismantle cybercriminal infrastructures and prosecute criminal conspirators.

What Purpose Does This Study Serve?

Cybercrime is a highly profitable and formidable problem because it operates in environments where permissive policies or business practices offer convenient and cheap access to resources with little or no risk of punishment that elsewhere serves as a deterrent and enforcement mechanism. If we treat cybercrime like a business, then we can apply business analysis principles to cybercrime to derive fundamentally important insights about the criminal trade economy. That criminal economy relies on the legitimate economy to obtain input resources and realize the outputs of financial gain.

We can ask the following questions to get a better understanding of cybercrime:

- What factors fuel the criminal trade economy and make it lucrative?
- What resources, such as hosting and names, are actors using?
- How can the cost of resource acquisition be increased and the conversion of criminal proceeds into cash made more burdensome?
- In particular, what aspects of the business model are vulnerable to disruption by legitimate actors, and how can these be disrupted?

Making relevant resources more difficult and costly for criminals to acquire will make cybercrime less attractive, and this should be considered as part of the overall strategy to mitigate cybercrime.

> Cybercrime continues to grow because it is a highly profitable business

This is Interisle's third annual Cybercrime Supply Chain report. Consistent with our 2023 and 2024 studies, we focus our analysis on three criminal activities: malware, phishing, and spam. In addition to being individually significant, these three cybercrimes each have roles in attack campaigns. Certain malware, for example, provides the infrastructure to emit spam and these infrastructures are used to distribute phishing. These abuse types are so intertwined that cybercriminals now operate them as "crime as a service" serving a criminal subscriber/affiliate community.

Scope & Focus of this Study

Key opportunities to disrupt the cybercrime business model exist in places where cybercriminals acquire the tools, resources, and services needed to conduct attacks. Interisle refers to the assemblage of these resources as the Cybercrime Supply Chain. This framework allows cybercrime to be analyzed and understood like any other business, and it reveals opportunities to starve criminals of the resources needed for attacks.

For each of the links in our supply chain framework -- Attack Resources, Attack Targets, Naming Resources, Hosting Resources, and Cashing Out – this report provides a narrative overview of how cybercriminals acquire and use the associated resources.

To conduct our quantitative analysis for the Attack Targets, Naming Resources, and Hosting Resources links, we collected malware, phishing, and spam reports from eleven

Cybercrime overall grew by 60% from 16 million to 26 million events year over year

publicly and commercially available threat intelligence or reputation services (see our list of data contributors at the Cybercrime Information Center). Interisle does not have relevant data to provide a comprehensive quantitative analysis of the Attack Resources and Cashing Out links of the supply chain; however, the narrative overviews describe their function and challenges in mitigating criminal access to associated resources.

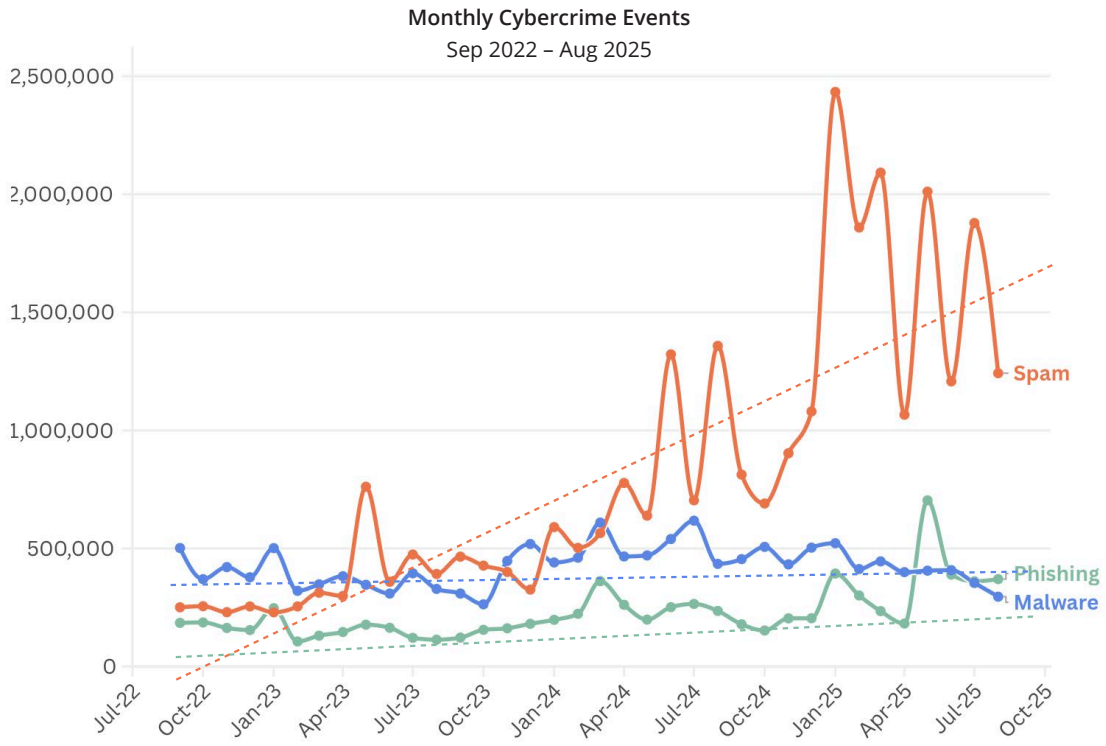
In May 2025, we added an additional phishing feed, SURBL, which we had already been using as a source of spam data. We have consistently noted that we under-report cybercrime numbers. By adding this additional phishing source, our global coverage and accuracy have improved, with the end result that we are now under-reporting less than before.

Phishing activity increased by over 40% from 2.6 million to over 3.7 million events

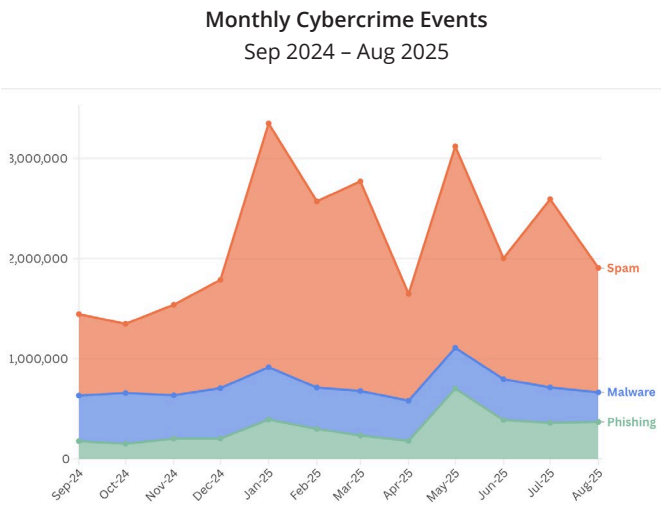
We identified 26 million unique cybercrime events, a 60% growth over last year's study. (3% of those cybercrime events resulted from adding SURBL as a phishing feed.) We then analyzed where cybercriminals obtained the naming and hosting resources used in these attacks and common tactics used to acquire them. We then ranked Top-Level Domain (TLD) registries, TLD registrars, hosting providers, and free web hosting providers that represent the greatest amount of cybercrime activity based on raw counts and comparative metrics.

Spam activity more than doubled again from 8 million to over 17 million events

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, free web hosting provider) is best positioned to implement these. The study also identifies suspicious registration behaviors by exposing large numbers of exact matches of registered brands contained within domain names and identifying a high incidence of cases where "sets" of domain names that registered within seconds (in bulk), weaponized, and were subsequently reported for use in cybercrime attacks.



Key Statistics

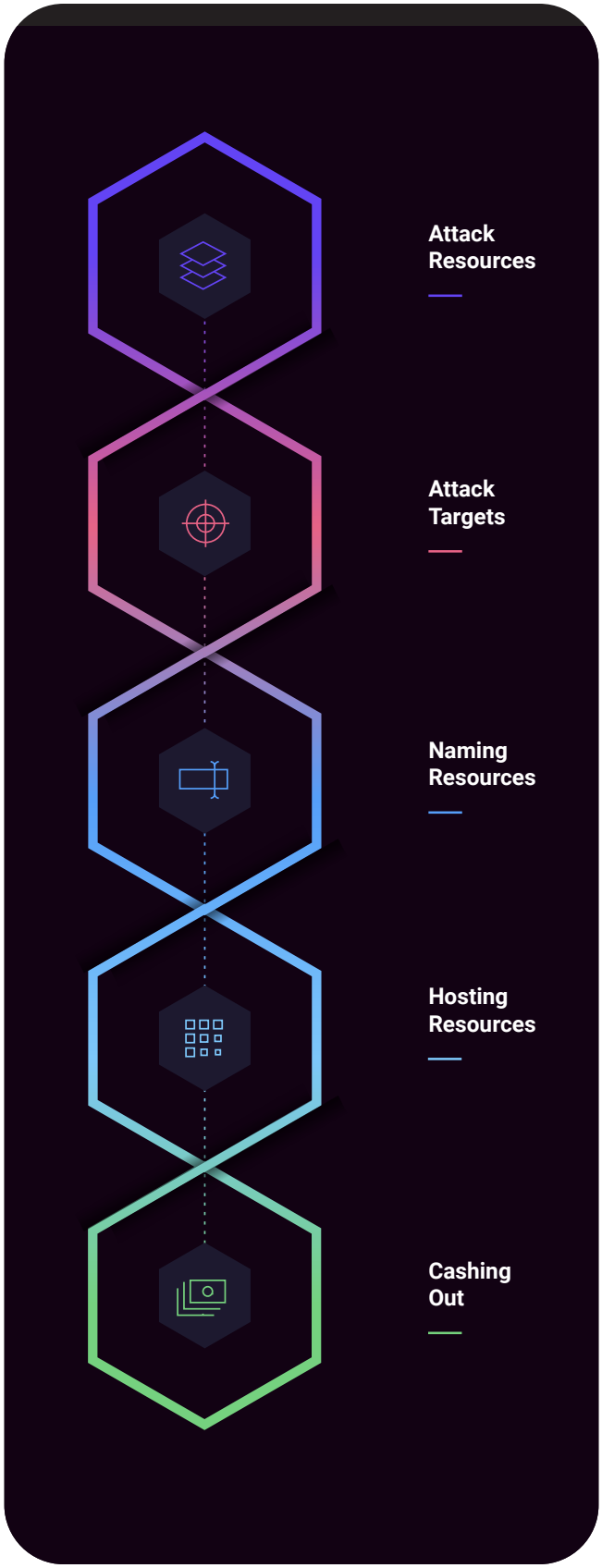


We compared measurements from the previous two Cybercrime Supply Chain studies to the results for this study. Spam has emerged as the highest reported of the three cybercrimes that we tracked. Additionally, the spam growth trajectory is nothing short of alarming.

The Cybercrime Supply Chain

In the physical world, supply chains facilitate the integration of necessary inputs to producers of intermediate and final products and services. For example, smartphones integrate chips, displays, batteries, and other hardware items into a device that users buy and use. However, a physical smartphone by itself has only minimal value. To make smartphones useful, other players supply internet services, cellular networks, applications, cloud services, and storage systems. Similarly, cybercriminals assemble resources and services sourced from the legitimate and dark economies to develop, execute, and profit from attacks.

The Cybercrime Supply Chain framework for our analysis of malware, phishing, and spam consists of five key links. The narrative overviews that follow describe their function and challenges in mitigating criminal access to associated resources.



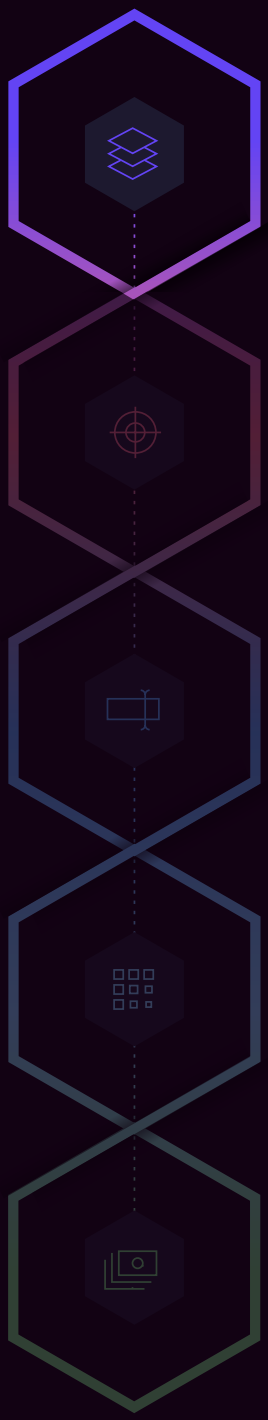
Attack Resources: Cybercriminals used public repositories, the dark web, and social media sites to offer a collection of (malicious) files and scripts that allow even a novice to perpetrate fraud by impersonating a well-known organization or brand. These **attack kits** can be customized for a particular kind of attack, *e.g.,* a fake web site for phishing or a web page that hosts malware. These are veritable "cyberattack in a box" starter kits frequently used by criminals. **Crime as a Service (CaaS)** operators offer all the cybercrime supply chain elements – malware, messaging, fake sites, naming, and hosting – into a commercial service that distributes profit through subscriber or affiliate business models. CaaS offerings make attack resources more accessible and convenient.

Attack Targets: Internet end users are primary targets for cybercrimes. Acquiring targets involves obtaining contact information (*e.g.,* email addresses, mobile numbers) for potential victims as targets of attacks. Attracting or luring users to fall victim to attacks often involves impersonation of well-known brands or a victim's own organization. In these attack scenarios, merchants, manufacturers, governments – virtually any organization with an online presence – are not the direct targets of attacks. But this exploitation adversely affects their business and reputation. In different scenarios – for example, phishing-enabled data breaches, business email compromise, or data-exfiltrating malware – these organizations end up being direct victims of cybercrimes.

Naming Resources: Attackers use the Internet's naming and hyperlink (URL) systems to identify fake web pages and malware hosting sites. These systems are familiar to most users and often do not raise suspicion. Attackers often register cheap domain names to establish fraudulent web sites, email servers, or file services. They may also use the names of web sites where they have gained administrative control, such as by hacking into an existing website or domain name administrative record.

Hosting Resources: Attackers need a place (an address) to host their fake web sites, malware download pages, or spambots. Here they have several options including compromised cloud accounts, systems where they've gained administrative control, or free or cheap hosting or cloud services. Cybercriminals frequently use cheap or free web site services where they create user accounts and use the hostnames assigned by a web hosting or subdomain provider that they then use for criminal activities.

Cashing Out: Cybercriminals must convert what they steal, extort, or defraud from victims into some form of usable currency, asset, or merchandise. Depending on their location, cybercriminals will focus on ways that are not easily traceable by law enforcement. Cashing out refers to the diverse methods and the legitimate or dark economies they use to monetize and launder their proceeds to convert these into tangible assets.



01
Attack Resources

02
Attack Targets

03
Naming Resources

04
Hosting Resources

05
Cashing Out

Attack Resources

In our previous supply chain studies, we explained how cybercriminals used public repositories, the dark web, and social media sites to offer a rollup of (malicious) files and scripts that allowed even a novice to impersonate a well-known organization or brand.

Cybercriminal actors now make access to attack resources more accessible and convenient. **Crime as a Service (CaaS)** operators roll all the cybercrime elements – malware, messaging, fake sites, naming, and hosting – into a commercial service that distributes profit through subscriber or affiliate business models.

In 2025, CaaS has risen to prominence, and we will accordingly discuss this in greater detail.

Attack Kits

Attack kits are typically sets of files and scripts that provide a criminal with tools to conduct an attack quickly and easily, and they are usually specific to certain types of crime.

Exploit kits provide malicious software that takes advantage of software vulnerabilities in a user-attended device (*e.g.,* a mobile phone or laptop), an operating system, or an application (*e.g.,* a browser or document productivity software). Some exploit kits contain a "loader", malware that is designed to deliver additional malware. Once installed, the loader "calls home" for additional payloads: for example, a banking trojan, remote access trojan (RAT), or an executable that can send email (*e.g.,* spambot). Exploit kits such as the RIG exploit include a mail server and the means to compose email messages that deliver phishing lures, scams, or other malicious content.

Phishing kits typically include web pages and forms where Internet users are lured to sites that impersonate a known organization or brand. The kits themselves are typically archived files (*e.g.,* a zip file) that can be obtained from public repositories, the dark web, or social media pages. Phishing kits typically offer an attacker a choice of web page, forms, and brands to impersonate. The attacker merely needs to host the content, generate phishing URLs, and send email or text message "lures" that contain the URL of the phishing page.

Attack kits vary in price, based on factors such as quality, adaptability, notoriety, or popularity.

Crime as a Service (CaaS)

While attack kits remain useful resources for cyber criminals, the business side of cybercrime is rapidly embracing service models. Criminal enterprises are now deploying subscriber or affiliate services for phishing, malware, or ransomware attacks. These services typically use spam infrastructures as delivery systems. The criminal enterprises have been identified as operating worldwide from China, Russia, North Korea, the Middle East (Iran), and Africa (Nigeria).

The "as a service model" is similar to legitimate cloud offerings, *e.g.,* software, platform, infrastructure, containers. The difference is that all the cybercrime supply chain elements – malware, messaging, fake sites, naming, and hosting – are rolled into a "commercial" service that is operated by a criminal enterprise.

These services share several common characteristics. Typically offered in dark web marketplaces, they offer buyers ready-made attack campaigns on a subscription or pay-per-use basis, in many cases providing cash-out payment methods as well. This lowers the barriers to entry for criminal activity and makes the cybercrime business broadly accessible.

In our 2025 Phishing Landscape study, we explained that **Phishing as a Service (PhaaS)** typically includes fake login, a (spam) infrastructure, and automated tools for sending phishing emails, SMS scam texts, stolen data management, domain name registration, and hosting malicious sites. Several PhaaS offerings rose to prominence in 2025, including Lucid, Lighthouse, Darcula, EvilProxy, and W3ll, and Raccoon0365. Alloy and Artists Against 419 (AA419) have observed related **Fraud as a Service (FraaS)** operations.

Malware as a Service (MaaS) offerings provide customers with the ability to conduct surveillance, data exfiltration, adware, financial fraud, or extortion campaigns. AgentTesla

(remote access trojan), Emotet (banking trojan and loader), TrikBot (credential harvester) and Ryuk (ransomware) have all been associated with the LummaC2 MaaS infrastructure that operated successfully until dismantled in early 2025.

Ransomware as a Service (RaaS) is a commercial online extortion business. Some investigators report that some RaaS have evolved into an affiliate business with recruitment, candidate screening and profit sharing. DragonForce and RansomHub have been prominent RaaS operators in what has become an increasingly competitive criminal marketplace.

Spam as a Service (SaaS) offers a commercial, automated email campaign. These services emulate email marketing services. One service, SpamGPT, incorporates generative AI into its feature sets. This gives its subscribers the ability to create convincing, even targeted messages in different styles using correct grammar and spelling. SpamGPT also features SMTP cracking – a means to compromise legit email services – and sophisticated spoofing techniques. Such features exploit the positive sender reputation of the compromised or impersonated email server and can defeat anti-spam measures of targeted organizations.

The criminal enterprise marketplace has advanced well past "emergence" and CaaS has become a major criminal threat, particularly for cryptocurrency investors. Disrupting other links in the supply chain may play an even more important role in mitigating cybercrime in 2026.

Disrupting Access to Attack Kits or CaaS

Disrupting access to hosted attack kits or CaaS poses several challenges:

- While many repositories or file sharing services have acceptable use policies (AUPs), these are not rigorously enforced.
- Providers struggle to keep malicious code off their platforms, and no uniformly enforceable controls are present industry-wide to prevent misuse.
- Authors allege that their kits are published for educational purposes only, post disclaimers that discourage misuse, and deny any responsibility if misused.
- Claims that software is generally protected as free speech create uncertainty regarding how or when to enforce AUPs.

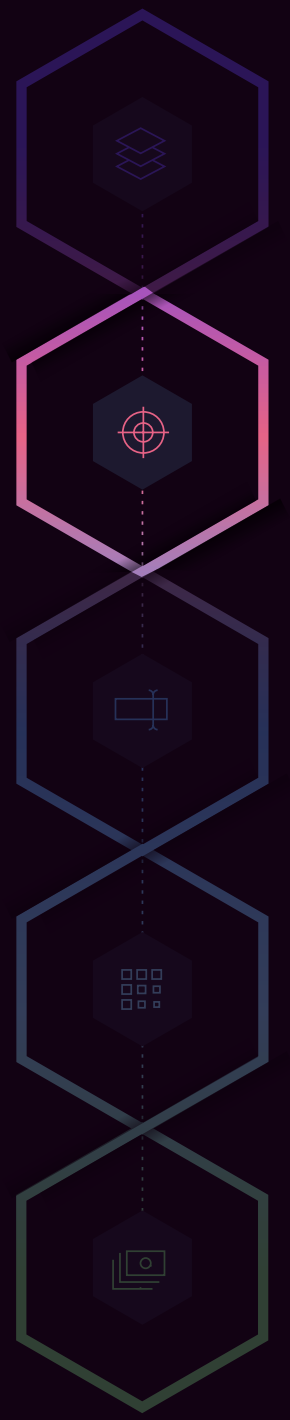
Case law in the United States (*e.g.,* Google v RNC) concluded that blocking harmful content falls within the scope of "Good Samaritan" blocking (see US Code Title 47, § 230, "*Protection for private blocking and screening of offensive material*"). However, these judgments don't apply in all jurisdictions.

Broader adoption of such laws could incentivize repository providers and other hosting services to blocklist attack kit URLs more vigorously but also encourage repository providers, other hosting services, and blocklist providers into identifying and denying access to attack kit URLs more robustly by clarifying and strengthening their legally permissible activities.

Successful takedowns in 2024 and 2025 demonstrate that access to CaaS platforms can be disrupted by law enforcement agencies cooperating with each other. The FBI and Europol were able to disrupt the LummaC2 MaaS network. Europol's Operation Endgame resulted in a dismantling of a loader distribution network, seizure of criminal proceeds, and arrests of "high value targets". Private actors were also able to achieve disruption: Microsoft's Digital Crimes Unit and Health ISAC have co-filed an Emergency Temporary Restraining Order against the Raccoon035 PhaaS alleged conspirators, which hides much of its infrastructure behind Cloudflare's reverse proxy service.

These and earlier actions (*e.g.,* LabHost, BulletProofLink) often require assistance from domain and hosting industry stakeholders. Such global law enforcement operations, like operations to dismantle botnets, can take months or years to complete.

While experience and improved global cooperation have resulted in more successful takedowns recently than a decade ago, any further acceleration may require new or revised legal assistance treaties or broader adoption of cybercrime model law.



01
Attack Resources

02
Attack Targets

03
Naming Resources

04
Hosting Resources

05
Cashing Out

Attack Targets

Attack kits provide the means to perpetrate online crime. Attackers must then identify one or many subjects of their attacks ("targets"). Attackers want to profit from their criminal enterprise, and they'll do so, for example, by convincing unwitting users to share personal, financial, or sensitive data during phishing attacks or scams, or to pay extortion fees after they fall victim to a ransomware attack. Such attacks provide cybercriminals with monetary gains (cryptocurrency or cash) or transactional data (*e.g.,* credit card or bank account details). Similarly, when attackers succeed in causing users to inadvertently install malware, they compromise devices that they will use to send spam, mine cryptocurrency, steal information, or distribute malware across local networks.

Any party who uses the Internet for personal or business purposes is a potential target. Attackers employ many methods to acquire contact information. They can purchase mobile phone or email lists from legitimate and dark online markets. Criminals can also create their own lists by using scraping tools that crawl websites and online directories to extract email addresses, mobile phone numbers, or social media handles.

For attacks against Internet users, criminals often impersonate brands. In such cases, the impersonated brand or organization is primarily a lure but they are also a victim; for example, merchants lose revenue when their products or services are used to lure users to counterfeit goods sites and may see their reputation being affected. Brands, or generally any organization, are also routinely directly targeted by phishers. Business email compromise attacks identify high value targets who fall victim to convincing, highly personalized messages and inadvertently authorize a bogus financial transaction. Attackers also fake intra-organizational correspondence to convince users to download data-exfiltrating malware from a URL in the message.

Impersonation plays an important role in end-user focused cybercrime, as tricking the end-user is usually part of the cybercriminal modus operandi. Successful attacks replicate email or text correspondence that users expect or anticipate from a merchant, bank, or organization. In many cases, they use the exact images and logos of brands and (nearly) the same language that the legitimate organization uses for product announcements, issues with payments, or even fraud warnings.

To complement to this convincing correspondence, cybercriminals may register legitimate-looking domain names for cybercrimes to facilitate the perpetration of fraud. Most registrations of this sort are easy to acquire, and doing so is virtually without risk: most TLDs and registrars have no policy or legal obligation to follow "know your customer" procedures or screen for well-established brand names at the time of domain name registration.

Internet end users are primary targets for cybercrimes

Any person or organization with an online presence is a potential cybercrime target

Impersonated Brands

For this study, we wanted to determine which brands were most frequently impersonated for phishing, spam, and malware attacks. We searched for exact brand matches in the domain names, in URLs containing domain names, and in subdomain provider hostnames reported for abetting cybercrime activity.

We found an exact match of a brand name we track in 432,974 domain names and in 43,074 host names of free web hosting providers. Cybercriminals also use visually similar strings (*e.g.,* faceb00k, pa1pal) so these figures represent a low estimate of brand misuse in domain name or subdomain hostname composition.

We observed a 97% increase in brand names appearing in domain names year over year. While there was a 4% decrease in brand names appearing in host names of free web hosting providers, that goes against the backdrop of a 42% decrease in the use of free web hosting for cybercrime, so overall, there is a proportional increase in brand use.

2025 RANK	2024 RANK	EXACT BRAND FOUND IN REGISTERED DOMAIN NAMES	NUMBER OF MATCHES
1	1	United States Postal Service	**85,843**
2	8	Coinbase	**14,447**
3	5	Amazon	**13,016**
4	2	Apple	**11,264**
5	7	Facebook	**9,195**

2025 RANK	2024 RANK	EXACT BRAND MATCHES IN FREE WEB PROVIDER HOST NAMES	NUMBER OF MATCHES
1	4	Webmail	**6,222**
2	1	Facebook	**2,914**
3	10	Shaw Communications	**1,863**
4	5	Netflix	**1,705**
5	–	Meta	**1,376**

Targeted Keywords

Cybercriminals often register domain names or select names used as host names with free web providers that use well-known, yet generic, keywords attempting to fool the unsuspecting user that they are being directed to a relevant website. In some cases, we see examples of multiple keywords being used in the same domain or host name.

The following table shows the most often occurring generic keywords used in domain or host names:

2025 RANK	BRANDS FOUND IN SUBDOMAIN PROVIDER HOSTNAMES	NUMBER OF MATCHES
1	service	**87,757**
2	track	**67,113**
3	login	**72,842**
4	security	**39,301**
5	account	**39,552**
6	delivery	**25,371**
7	secure	**27,123**
8	wallet	**24,127**
9	verify	**17,681**
10	portal	**11,017**

Here are some examples of the over one thousand occurrences where the domain or host name uses both 'login' and 'account' keywords:

your-account-login.com

support-login-account.info

login-verifyaccount.com

accounts-mail-auth-login.ru

account-servicelogin.com

servicelogin-account.com

Tricking Users

We have detected a more prevalent phenomenon in the way domain names or host names used with free web hosting are constructed. This growth has coincided with the period covered by this report. By making use of the well-known TLD names: .COM, .NET, .ORG, and .GOV and using them in domain names or free web hosting host names replacing the dot with a hyphen, cybercriminals are

banking on users either not paying close attention to those names or using screens small enough that the user cannot see the whole name (including the true TLD).

We observe hyphens being used before, after, and in some cases both, the domain or host name. Here we see the most often occurring patterns using TLDs and hyphens:

2025 RANK	COMMON TLDS USED INSIDE DOMAIN OR HOST NAMES	NUMBER OF MATCHES
1	com–	**479,361**
2	gov–	**89,031**
3	org–	**33,900**
4	–gov	**27,315**
5	–com	**13,714**
6	–net	**6,360**
7	–com–	**4,443**
8	net–	**4,270**

Here are some examples of domain names that appear to be intended to deceive users:

www-facebook-com.vn

support-lcloud-com.shop

www-lcloud-com.help

dana-kaget-indonesia-com.vercel.app

Delayed delegation of suspicious domain and web site names can mitigate deceptive cybercrime attacks

Common Visual Deceptions

There are many other ways that cybercriminals can take advantage of users who do not pay very close attention to domain names, host names of free web services, and other parts of URLs.

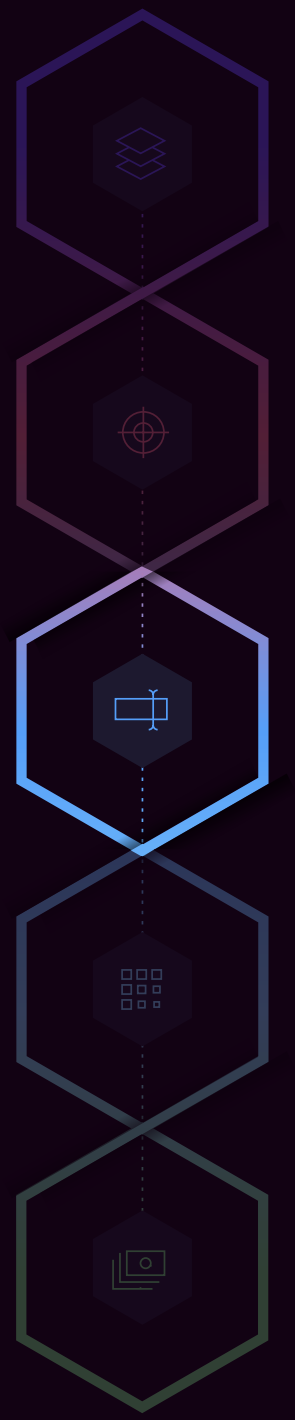
We covered the topic of visual deceptions in URLs in more detail in a recent Substack post.

Approaches for Mitigation

To protect the less technically savvy members of society from deceptive attacks, domain registrars could look for suspected criminal use or misuse of brands during registration, and free web site operators could do so at time of account creation.

Operationally, implementing controls against such registrations is rather simple and effective. While not perfect, such controls increase the friction for cybercriminals. EURID, 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. The .EU policy is effective. gTLD and ccTLD registries as well as web hosting providers should adopt such a policy as a recommended practice. The case for delaying delegation is even stronger when a registry or registrar observes tens, hundreds, or even thousands of exact matches of brands.

Certain opportunities and avenues of recourse are available to Internet users and brands. Consumer advocacy groups (such as AARP) and brand owners could engage operators to express concerns or present grievances in a constructive manner. For example, delegates of an advocacy group or a consortium of brands or merchants could meet with the registry, registrar, or hosting operators identified in any of the top rankings in this study to discuss how the misuse of their operations can be reduced. If constructive efforts have no effect, they could pursue legal recourse. While this is a last resort, it has proven effective in the past.



01
Attack Resources

02
Attack Targets

03
Naming Resources

04
Hosting Resources

05
Cashing Out

Naming Resources

Internet applications locate the Internet's content by using the Domain Name System (DNS). This system permits the registration of names for individuals and organizations and the naming of locations where content is hosted or served, *e.g.,* a web site, a file repository, or a social media platform.

Cybercriminals misuse the DNS by registering domain names for illicit purposes, assigning these names to hosted content and including them in hyperlinks that direct users to the fake or harmful pages set up for the attack.

We measured criminal misuse of name resources for a yearly period and compared these to our prior study period. The findings in both measurement sets are disturbing.

Cybercriminals used more than 19.5 million unique domains during our 2025 study period, an 126% increase year over year

Cybercrime Activity Across the Domain Name Space

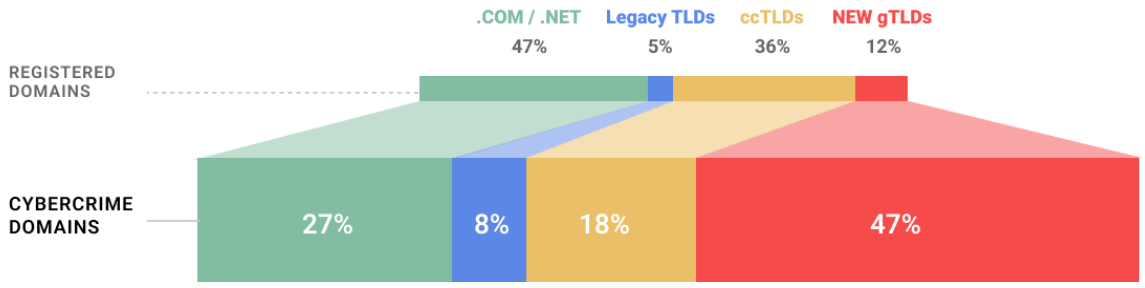
According to Domain Tools, at the end of August 2025, there were over 357 million registered domains in the global domain name space. We identified domains reported for cybercrime activity in 972 of the approximately 1,500 existing TLDs during the current study period.

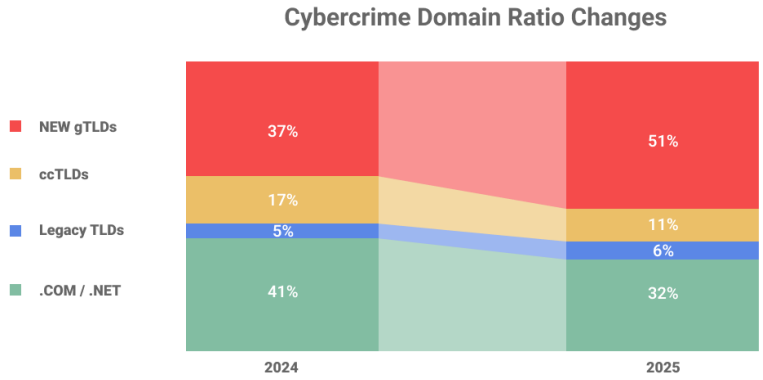
For our studies, we divided the overall domain name space into four segments:

- the .COM and .NET registries, operated by Verisign, represent 47% of the domains in the world,
- the country-code domains (ccTLDs) represent 36% of the domains,
- the legacy generic TLDs, those other than .COM and .NET and introduced before 2013 (*e.g.,* .ORG, .BIZ, .INFO) represent 5% of the domains, and
- the new gTLDs introduced from 2014 to the present (*e.g.,* .TOP, .XIN, .BOND) represent the remaining 12% 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.

Registered Domains and Cybercrime Domains by TLD Type





The market shares of our four market segments are relatively unchanged year-over-year; however, the distribution of reported cybercrime domains has changed.

The .COM/.NET TLDs showed a 9% decrease year-over-year in percentage share of cybercrime domains reported.

Since Freenom ceased operations, we have seen a steady, positive improvement in the ccTLD market segment. Our study data for this period showed another strong (6%) decrease year-over-year in percentage share of ccTLD cybercrime domains reported.

Meanwhile, cybercrime domains reported in the new gTLDs segment, dominated by TLDs that offer registrations to anyone without restrictions, continue to increase dramatically in both raw numbers and in percentage of cybercrime domains and is now more than four times market share.

All TLDs

For the September 2024 to August 2025 study period, we observed an overall 126% increase in unique domain names reported for use in cybercrimes.

Seven of the top 10 TLDs – .TOP, .BOND, .CC, .VIP, .INFO, .XYZ, and .SHOP – had more than 10% of their domains under management reported for use in cybercrime activities. By comparison, the 4.9 million cybercrime domains reported represented only 3% of .COM's domains, which also allows registrations to anyone without restrictions.

The .TOP and .BOND gTLDs have replaced .INFO and .NET in the top 5 ranking based on cybercrime domains reported since 2023.

2025 RANK	2024 RANK	TLD	TOTAL CYBERCRIME DOMAINS REPORTED 2025	TOTAL CYBERCRIME DOMAINS REPORTED 2024	CHANGE YEAR OVER YEAR
1	1	.COM	**4,869,496**	3,237,755	+ 1,631,741
2	2	.TOP	**2,837,719**	830,039	+ 2,007,680
3	4	.CN	**1,057,123**	399,748	+ 657,375
4	14	.BOND	**990,591**	96,612	+ 893,979
5	7	.CC	**872,890**	236,869	+ 636,021
6	9	.VIP	**676,721**	169,554	+ 507,167
7	10	.INFO	**662,922**	153,957	+ 508,965
8	3	.XYZ	**548,006**	475,153	+ 72,853
9	5	.SHOP	**541,281**	281,276	+ 260,005
10	6	.NET	**408,761**	271,676	+ 137,085

Domains registered by cybercriminals – malicious domains – increased 149% year over year

ICANN served the .TOP gTLD with a breach notice in July 2024 for failing to satisfy contractual obligations to mitigate DNS abuse but has since posted notice that the TLD has cured the breach. Our data shows that .TOP continues to be exploited, and thousands of domains registered here, along with .XIN, were used in Unpaid Toll Scams. The .TOP was also #2 in our Phishing Landscape 2025 rankings by phishing domains reported.

90% of the cybercrime domains reported in the .BOND gTLD were used for spam. Over 738,000 were registered in February 2025, and an astonishing 627,000 on February 1, 2025. We see evidence of automated name generation throughout this set, for example,

- 29,000 domains contained **online–advertising–**
- 24,000 domain contained **app–software–development–training–**
- 21,000 domains contained **cyber–security–**

We found nearly 200 such sets, each with more than 1,000 domain names that contained one or more anchors (keywords). These often included a 5-digit incrementing number. For many of these sets, we suspected, but were unable to confirm, that these were bulk registered because we could not obtain creation date and time from the .BOND registry RDDS.

We experienced RDDS access issues with .TOP and other RDDS services throughout the year. Limiting access to RDDS impedes investigators, who cannot contact the domain's registrar. Researchers can't accurately measure registrations of registrars whose rate-limiting or other policies prevent them from investigating all cybercrime domains associated with their operation.

Yearly Cybercrime Domain Score

The Yearly Cybercrime Domain Score is a metric to measure the prevalence of cybercrime activity in TLDs. The Cybercrime Domain Score allows criminal activity to be compared between registries of different sizes by considering the total number of registrations in each TLD. The calculation for the metric is:

Yearly TLD Cybercrime Domain Score

=

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

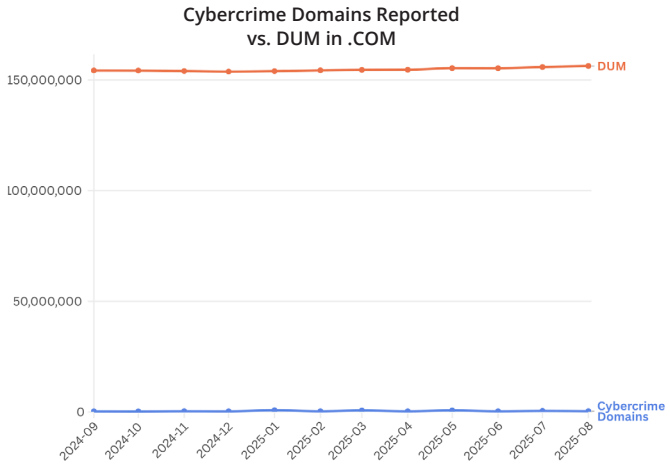
While .COM was the highest ranked TLD by reported cybercrime domains, 46 TLDs had yearly cybercrime domain scores that were more than five times that of .COM (which had a yearly cybercrime domain score of 311.3). This is twice the number of TLDs that we reported with such high scores in our2024 study. The top 5 of these were:

2025 RANK	2024 RANK	TLD	DOMAINS IN TLD	CYBERCRIME DOMAINS 2025	YEARLY CYBERCRIME DOMAIN SCORE
1	2	.BOND	146K	990,591	**67,814.3**
2	–	.XIN	49K	179,346	**36,389.6**
3	–	.PINK	34K	57,199	**16,739.5**
4	–	.PICTURES	33K	48,007	**14,429.9**
5	–	.PIZZA	34K	48,805	**14,163.6**

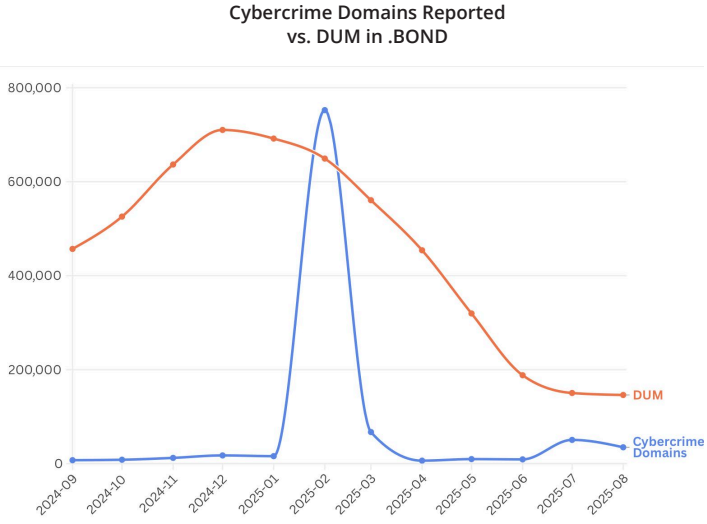
For these yearly scores, we used the TLD domains under management (DUM) for the last month of our study period (August 2025). We next looked at month-by-month data of cybercrime domains reported vs. DUM of the TLDs to learn more.

We used the .COM TLD as a baseline. The .COM TLD had a small standard deviation in domains over management (DUM), and some fluctuation in cybercrime domains

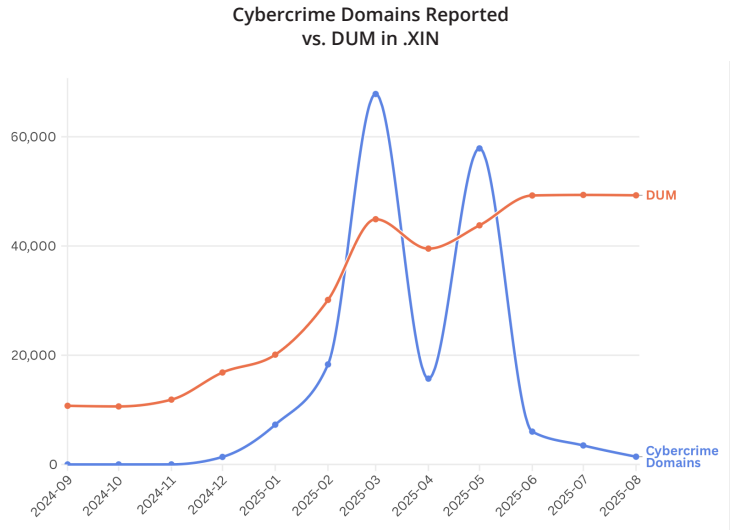
reported but the chart illustrates that while numerically large, the percentage of cybercrime domains in .COM is small.



The .BOND TLD had a large standard deviation in domains under management and one large spike in cybercrime domains reported followed by a steady decline in DUM for the remainder of our study period. Nearly all these domains appear to have been deleted (i.e., they return non-existent domain in the DNS). The spike suggests that there were more domains reported at one point in time than DUM. This is an artifact of how threat intelligence services report cybercrime activity versus the add/drop behavior of the registry.



The .XIN TLD also had a large standard deviation in domains under management and two large spikes in cybercrime domains (which we attribute to Unpaid Toll Scam domains. Their DUM however, continues to grow. Nearly all the domains reported during both spikes were deleted (i.e., they return non-existent domain in the DNS).



While removing the threats these domains posed quickly is commendable, proactive measures to detect and block or delay delegation of tens of thousands of suspicious domains could have reduced the extensive harm and loss from phishing and spam campaigns.

A list of the top 20 TLDs ranked by total cybercrime domains and by yearly cybercrime domain score can be found at the Cybercrime Information Center.

ccTLDs

The ccTLD space had a 36% market share, with roughly 128 million domains registered.
The 3.5 million domains reported for cybercrime activity represent 18% of the overall reported domains.

2025 RANK	2024 RANK	ccTLD	TOTAL CYBERCRIME DOMAINS REPORTED 2025	TOTAL CYBERCRIME DOMAINS REPORTED 2024	CHANGE YEAR OVER YEAR
1	1	.CN	**1,057,123**	399,748	+657,375
2	2	.CC	**872,890**	236,869	+636,021
3	3	.RU	**295,552**	208,705	+86,847
4	4	.CO	**251,933**	76,970	+174,963
5	144	.MY	**145,326**	731	+144,595

The top 5 ccTLDs accounted for 77% of the cybercrime domains in ccTLD name space. While .CC and .CN have appeared each year since 2023, the remaining three spots have changed since Freenom ceased operations in 2023. In 2024, Freenom's commercialized .TK, .CF, and .GQ were

replaced by .CC, .RU, and .CO. These ccTLDs remained in the top 5 ranking in 2025. The .US ccTLD is no longer in the top 5.

In our 2025 data, most of the cybercrime domains reported in these five TLDs were spam domains.

ccTLD	CYBERCRIME DOMAINS	SPAM DOMAINS	PERCENTAGE SPAM
.CN	1,057,123	952,652	**90%**
.CO	251,933	239,515	**95%**
.RU	295,552	248,149	**84%**
.CC	872,890	810,066	**93%**
.MY	145,326	128,364	**88%**

Many appeared to be algorithmically generated or composed using some form of automation. Some of the patterns found in hundreds of domains in these ccTLDs were composed of only digits (**63957.cc**), only letters (**mhiasfbamyonline.cc**), or combinations of letters and digits (**6688cp0810.cc**).

New gTLDs

For the study period ending August 30, 2024, the new gTLDs that offer registrations to anyone without restrictions again accrued the most misuse from cybercriminals.

The new gTLDs held 12% of the market share but accounted for nearly half of cybercrime domains reported

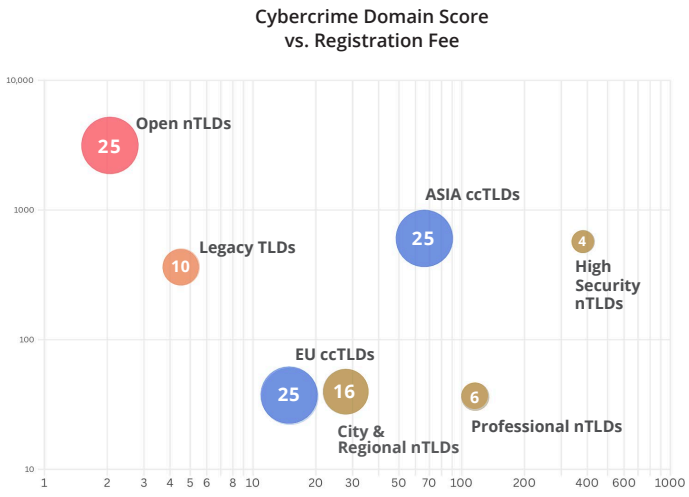
Domain Registration Policies and Pricing Matter

Cybercriminals look for frictionless surfaces, i.e., environments where they can conduct criminal enterprises with little opposition, likelihood of detection, or identification. We tested this proposition in our 2025 Phishing Landscape study. We studied registration policies of European Union ccTLDs and Asia-Pacific region ccTLDs for which we had cybercrime domain data. We also composed a gTLD set of legacy, new, and community gTLDs and found that "requirements of some form or another are effective in deterring malicious registrations."

We also tested the proposition that cybercriminals look to spend as little of their own money as possible when they acquire domains for cybercrimes generally. We used pricing data published by TLD-list.com and fees published by ccTLD registries that process registrations directly. Using the requirements from our prior study, we created a scatter plot of registration requirements vs. cybercrime composite domain score:

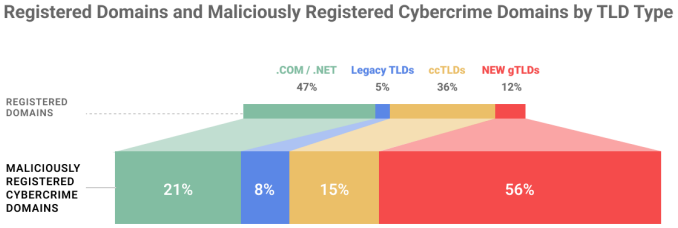
A scatter plot of the seven TLD sets shows that:

- TLDs with no registration restrictions (available to anyone) had the highest composite cybercrime domain score.
- The EU ccTLDs, city and regional community gTLDs, and professional community gTLDs had the lowest composite cybercrime domain scores. These all have requirements of some form or another, *e.g.,* a nexus obligation or identity verification).
- The composite score of the High Security gTLDs for which we had cybercrime data was overly influenced by .ONG which accounted for 96% of the cybercrime domains in this gTLD subset, nearly all flagged as spam domains. The composite cybercrime domain score of the High Security gTLDs without .ONG was 2.9, which would be the lowest among the sets and subsets. As we observed in our phishing study, registration policies matter but they must be enforced.



Malicious Domain Registrations Across the Domain Name Space

We measured the number of unique domains reported for cybercrime activity across a total of 972 TLDs. For our studies, we employ a methodology to determine whether a domain is registered purposely to carry out a malicious or criminal act, and call these maliciously registered domains.



We use a set of criteria to discriminate malicious domains from compromised domains. This includes the time elapsed from domain creation date or first appearance of the domain (in passive DNS data) 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 2,000 brands that we track, labels containing brand similarities, and labels containing suspicious numbers of digits or hyphens in the label. We also look for registration behaviors that are characteristic of bulk registration.

56% of malicious registrations in the new TLD space was nearly five times its market share

Ranking of TLDs by Malicious Domain Registrations

The following table shows the top 5 TLDs with the most maliciously registered domains reported for serving as resources for cybercrime activity.

While .COM has the largest number of domains and has the largest number of domains determined to be malicious registrations, its percentage malicious registrations is 55%.

2025 RANK	2024 RANK	TLD	DOMAINS DETERMINED TO BE MALICIOUS REGISTRATIONS
1	1	.COM	**2,696,762**
2	2	.TOP	**2,174,521**
3	12	.BOND	**977,915**
4	5	.CC	**770,185**
5	6	.VIP	**594,744**

The following table shows the top 5 TLDs with the highest percentage of maliciously registered domains reported for serving as resources for cybercrime activity (only one of which was ranked in the top 20 in the previous study).

2025 RANK	2024 RANK	TLD	MALICIOUS DOMAINS PERCENTAGE
1	–	.PICTURES	100%
2	–	.PIZZA	99%
3	4	.BOND	99%
4	–	.PINK	99%
5	–	.LOAN	98%

Lists of the top 20 TLDs ranked by number and percent of malicious domain name registrations can be found at the Cybercrime Information Center.

High malicious domain percentages suggest that business, pricing, or operational practices have made a TLD attractive for criminal domain registrations. High percentages of malicious registrations have adverse effects on a TLD's reputation. IT administrators will block an entire TLD from local name resolution to protect the organization from illicit activity.

Cybercrime Activity Across All TLD Registrars

We ranked all gTLD and ccTLD Domain Registrars by Cybercrime Domains Reported for the September 2024 to August 2025 study period and reported all domains for which we were able to identify a registrar. The table includes registrars with a minimum of 800,000 reported cybercrime domains in our 2025 data.

2025 RANK	2024 RANK	TLD REGISTRAR	TOTAL REGISTRAR DOMAINS	TOTAL CYBERCRIME DOMAINS REPORTED 2025	TOTAL CYBERCRIME DOMAINS REPORTED 2024
1	5	Dynadot	5,900K	**1,760,785**	371,722
2	3	Gname	5,305K	**1,597,507**	559,075
3	2	GoDaddy	19,361K	**1,083,740**	580,778
4	1	NameCheap	64,422K	**1,066,775**	857,704
5	4	NameSilo	4,934K	**850,714**	522,322

A list of the top 20 registrars ranked by total cybercrime domains can be found at the Cybercrime Information Center.

Malicious Domain Name Registrations and gTLD Registrars

Counts of cybercrime domains help us identify where the most domain names reported for cybercrime were registered. By recognizing 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.

Pre-registration screening for suspicious domains and delayed delegation of domains with suspicious name composition makes it harder for criminals to obtain and use domain names

These are the top 5 TLD registrars with at least 600,000 maliciously registered domains reported for serving as resources for cybercrime activity:

2025 RANK	2024 RANK	gTLD & ccTLD REGISTRARS	CYBERCRIME DOMAINS	DOMAINS DETERMINED TO BE MALICIOUS REGISTRATIONS	PERCENTAGE MALICIOUS DOMAINS
1	4	Dynadot	1,762K	**1,483,153**	84%
2	2	Gname	1,598K	**1,223,567**	77%
3	1	GoDaddy	1,067K	**785,511**	74%
4	5	NameCheap	1,084K	**732,015**	68%
5	3	NameSilo	851K	**611,997**	72%

The following table shows those registrars with at least 75,000 cybercrime domains during the September 2024 to August 2025 study period with at least 80% of those domains registered purposely to abet cybercrime.

2025 RANK	2024 RANK	gTLD & ccTLD REGISTRARS	PERCENTAGE MALICIOUS DOMAINS
1	1	Key-Systems	99%
2	–	Eranet International	91%
3	14	Dominet (HK)	90%
4	7	Dynadot	84%
5	–	Hefei Juming	84%

When we consider registrars with at least 25 cybercrime domains, we determined that 151 registrars had at least 60% of their cybercrime domain names registered maliciously.

Unlike blocking entire TLDs, it is very difficult to determine the registrar of a domain, the reputation of the registrar, and make a "block" determination in real time. Threat intelligence services consider registrar reputation (using metrics like ours) when they assess the risk a domain name poses.

To identify suspicious registration behavior and prevent criminals from registering suspicious domain names,

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

measures are necessary to disrupt the cybercrime supply chain. Registrars should adopt proactive measures (*e.g.,* brand filtering or delayed delegation). A positive reputation will attract customers who will renew registrations and provide recurring revenue.

Lists of the top 20 registrars ranked by number and percentage of malicious domains can be found at the Cybercrime Information Center.

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 – e.g., Crime as a Service, described previously in the Attack Resources section – particularly benefit from the ability to use bulk registration services offered by domain name registrars. Cybercriminals are provided with easy access to these bulk registration practices, which they have exploited year after year. The domain name system was never intended to supply criminals with thousands of domain names in this manner.

For this study, we searched for characteristics of bulk registration behavior among domains already identified as associated with the cybercrimes. Because registrant contact data is now widely unavailable, we look for occurrences where large numbers of cybercrime domain names were registered via the same registrar, each within minutes of the previous. 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

Malicious bulk domain registrations increased 177% year over year

registered by a single registrant, but it seems unlikely that several unrelated (or non-conspiring) registrants would register domain names at the same time, in volume.

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

We found evidence that points to bulk domain registration of cybercrime domain names in 438 registrars. We associated 7,360,726 domain names with bulk domain registration behavior. These occurred in over 100,000 sets. The largest set was 17,590 cybercrime domain names registered at GMO d/b/a Onamae in an eight-hour period on 19 February 2024; domains in that set were then reported for cybercrimes committed between September 2024 and August 2025. There was one other set of over 10,000 cybercrime domain names registered within less than four hours at Alibaba Cloud Computing on 10-11 September 2024.

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

REGISTRATION TIME SPAN (UTC)	BULK DOMAINS	REGISTRAR	SAMPLE CYBERCRIME DOMAINST		
2/19/2024 03:48–11:10	17,590	GMO d/b/a Onamae.com	bonar-quinn.com treu-schweiger.com bradshaw-pitt.com household-grint.com	musa-kimbery.com efler-esmond.com elijah-arthur.com	samuel-greiner.com dostal-bonmann.com pearce-paysen.com
9/10/2024 23:58 – **9/11/2024** 03:24	14,301	Alibaba Cloud Computing	xzrcy.cn hndaf.cn szlianfa.com.cn hstx.net.cn	diyecom.cn iogoo.com.cn nxprotec.com.cn	conbiz.cn jxhtmy.com.cn xjxhq.cn
7/17/2024 00:05–03:04	9,934	Alibaba Cloud Computing	agkwpq.cn dmnxtf.cn jhmglk.cn sayoml.cn	cwesaj.cn oxfgir.cn tjgnyb.cn drutqn.cn	sxwwxu.cn fqjzok.cnt vplnpl.cn xnfctv.cn
1/18/2024 01:27–06:11	8,099	DomainCostClub	o54l2o3lt.sbs bsdg3ds1t.sbs djvhigthy.sbs hmn2phyqe.sbs	u1ebxlci7.sbs jeg2e3j90.sbs dd164lnxs.sbs	a9nfnjwhd.sbs va5o28xue.sbs pkj3uend8.sbs
3/29/2025 21:45 – **3/30/2025** 02:14	7,507	Xiamen Nawang	zjdzcjt.cn zjgycw.cn zjfpdkj.cn zjhpdgw.cn	zjdzckj.cn zjgzcjt.cn zjfqckj.cn zjfqdgw.cn	zjdzdjt.cn zjgzdgw.cn zjfqcw.cn zjfqdkj.cn
12/2/2024 11:59–13:29	6,570	Dominet (HK)	donxi.net idawn.net quaizb.net sxen.net	lyssyc.net szwan.net vpsw.net xzwm.net	114eb.net lshan.net ljzp.net yjdy.net

These examples show that domain names containing pseudo randomly or otherwise autogenerated strings are common in bulk registrations. However, just as domain names can be composed by automation, they can also be identified prior to processing a domain registration through automation. And they could be readily identified or confirmed by human inspection as suspicious.

Common Patterns in Bulk Registrations

Among the bulk-registered domains, we identified instances of deceptively composed names; for example, 6,672 domains started with the string **"usps"**, most of which were registered in TLDs such as .INFO, .COM, .TOP, .ICU, .XYZ, and .CFD. The vast majority were registered through Dominet (HK) and NameSilo. Two-thirds were registered between September 2024 and August 2025. In our Phishing Landscape 2025 report, we identified USPS as the most impersonated brand.

Bulk registrations Used for Unpaid Toll Scams

We found 4,123 bulk-registered cybercrime domains that started with the string **"com-tollbill"**, over 3,000 of which were registered in .XIN and .WORLD through Dominet (HK) Limited during March to June 2025. There were 1,550 bulk-registered domains that started with the string **"gov-tollbill"**, in eighteen different gTLDs, with most in .LIVE, .WORLD, .BID, .LIFE, and .XIN, registered through Dominet (HK) during March to June 2025. And we identified 2,691 bulk-registered domains that started with the string **"paytoll"**, over 2,000 of which were registered in .VIP. Almost all were registered through Hefei Juming, Dominet (HK), Gname, NameSilo, and Dynadot during February to April 2025. All of these strings have been associated with the Unpaid Toll scam, and are discussed in our Phishing Landscape 2025 report.

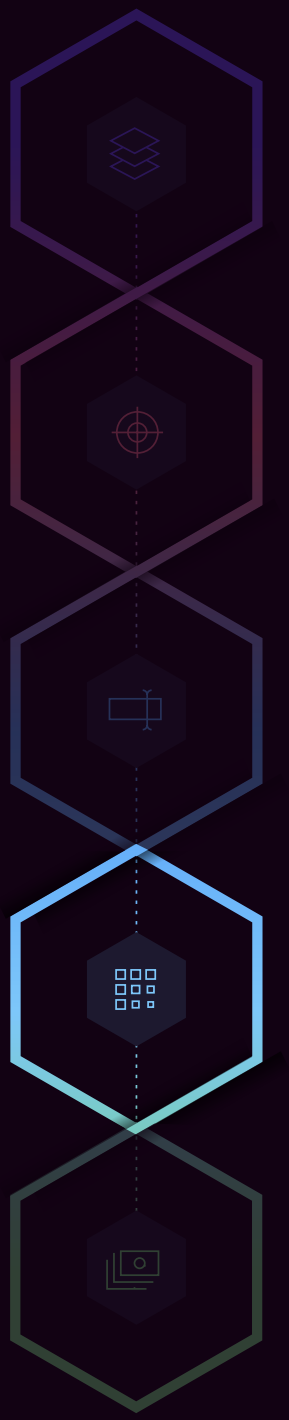
We identified five gTLD registrars responsible for more than three-quarters of the domains reported as resources for cybercrime activity associated with a bulk registration:

2025 RANK	REGISTRAR	IANA ID	DOMAINS ASSOCIATED WITH BULK REGISTRATION BEHAVIOR	PERCENTAGE CYBERCRIME DOMAINS REPORTED
1	DomainCostClub.com	1463	39,363	**100%**
2	Key-Systems	1345	482,962	**89%**
3	Kenpai International	4543	667	**84%**
4	eName	1331	65,376	**81%**
5	Global Domain Name Trading	3792	1,993	**76%**

The five gTLD registrars with the highest number of domains associated with bulk registration behavior were:

2025 RANK	2024 RANK	gTLD REGISTRAR	IANA ID	TOTAL CYBERCRIME DOMAINS REPORTED	DOMAINS ASSOCIATED WITH BULK DOMAIN REGISTRATION
1	6	Dynadot	472	1,760,785	**1,127,568**
2	3	Gname.com	1923	1,597,507	**1,003,998**
3	2	NameCheap	1068	1,083,740	**751,271**
4	4	NameSilo	1479	850,714	**504,494**
5	1	GoDaddy	146	1,066,775	**500,378**

Registrars and registries should monitor and scrutinize high-volume transactions for suspicious registration behavior



01
Attack Resources

02
Attack Targets

03
Naming Resources

04
Hosting Resources

05
Cashing Out

Hosting Resources

Attack resources provide the content that criminals want users to visit or download. Name resources provide user-friendly names of locations. Hosting resources provide the addresses of those locations.

Hosting resources provide attackers with places to host their fake web sites or malware payloads, or to operate spam mail services. To acquire hosting, cybercriminals subscribe to cloud accounts or content (*e.g.,* web site, or WordPress) services; alternatively, they may host their content on accounts, servers, or devices that they have compromised.

Cybercrime Activity Across Hosting Networks (ASNs)

Hosting resources are typically identified by their IPv4 addresses. 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 events 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 to identify the hosting network where the cybercrime activity was hosted. IPv6 addresses were not reported in our cybercrime feeds; thus, the following sections consider cybercrime activity that was hosted on IPv4 addresses only.

> The number of IP addresses reported for hosting cybercrime activity decreased 20% year over year

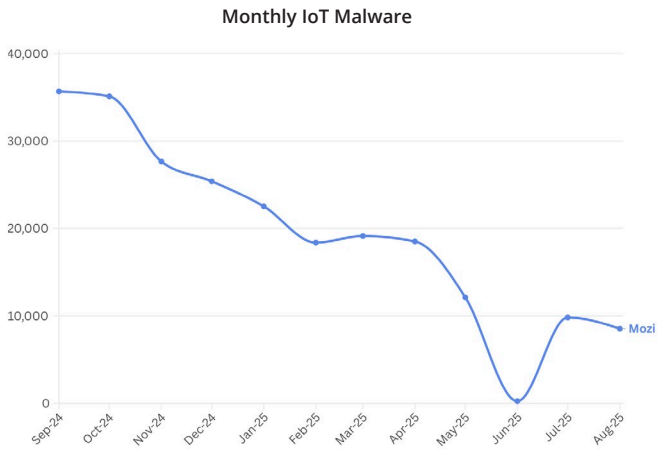
We found cybercrime activity in 29,490 hosting networks (ASNs), a year-over-year increase of 5%. **The number of distinct IP addresses reported for hosting cybercrime activity decreased by 20% year over year**, from 5,068,799 to 4,106,342.

Here we show those hosting providers with more than 100,000 unique IP addresses reported for hosting cybercrime activity. The complete Top 20 list of hosting providers can be found at the Cybercrime Information Center.

2025 RANK	2024 RANK	HOSTING PROVIDER	COUNTRY	UNIQUE CYBERCRIME IP ADDRESSES REPORTED 2025	UNIQUE CYBERCRIME IP ADDRESSES REPORTED 2024	CHANGE
1	1	Bharat Sanchar Nigam (AS9829)	India	**749,820**	567,977	**+ 181,843**
2	2	ChinaNet Backbone (AS4134)	China	**330,209**	473,445	**- 143,236**
3	3	China169 Backbone (AS4837)	China	**278,508**	288,137	**- 9,629**
4	4	DigitalOcean (AS14061)	United States	**137,892**	116,444	**+ 21,448**
5	10	Chunghwa Telecom (AS3462)	Taiwan	**135,501**	73,777	**+ 61,724**

IP addresses reported for hosting malware represent an important percentage of the unique addresses reported overall. Here, we look at where malware was hosted most prevalently.

Our 2025 study data show a decline in IP addresses reported for hosting Mozi, an IoT botnet malware:



Three of the top 5 ASNs accounted for 77% of the IP addresses reported for hosting Mozi, and IoT botnet malware.

HOSTING PROVIDER	IP ADDRESSES REPORTED FOR HOSTING MOZI
Bharat Sanchar Nigam (AS9829)	**61,495**
China169 Backbone (AS4837)	**58,128**
ChinaNet Backbone (AS4134)	**9,752**

ChinaNet Backbone (AS4134) and China169 Backbone (AS4837) were also among the top 5 ASNs with the most IP addresses for PHP Forum Spam (a traffic injector).

HOSTING PROVIDER	IP ADDRESSES REPORTED FOR HOSTING PHP FORUM SPAMMER (TRAFFIC INJECTOR)
ChinaNet Backbone (AS4134)	**59,297**
3xK Tech (AS200373)	**44,871**
Amazon (AS14618)	**37,505**
Google (AS396982)	**32,603**
China169 Backbone (AS4837)	**24,887**

Digital Ocean (AS14061), ChinaNet Backbone (AS4134), and China169 Backbone (AS4837) were also the top 3 ASNs with the most IP addresses of SSH attack ware.

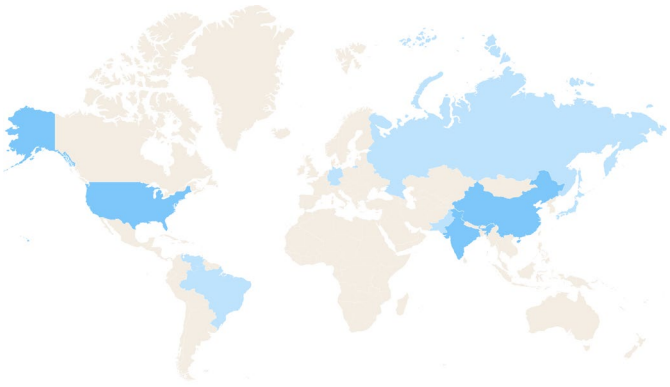
HOSTING PROVIDER	IP ADDRESSES REPORTED FOR HOSTING SSH ATTACK WARE
Digital Ocean (AS14061)	**29,870**
ChinaNet Backbone (AS4134)	**23,218**
China169 Backbone (AS4837)	**9,360**
Google (AS396982)	**8,414**
Amazon (AS16509)	**7,904**

In 2025, the United States (1,099,672), India (900,603), and China (796,212) again ranked the top three for the number of unique IP addresses used for cybercrime. Hong Kong, Taiwan, Germany, the Russian Federation, Brazil, Vietnam, and Great Britain rounded out the top 10 ASNs.

Here we list the most frequently reported malware by name and type and show how these three countries ranked for each.

MALWARE	UNITED STATES		INDIA		CHINA	
	COUNT	RANK	COUNT	RANK	COUNT	RANK
Mozi (IoT)	2,820	4	64,815	2	70,405	1
WordPress (malicious document)	3,062	1	N/R		119	6
Quakbot (infostealer)	1,050	1	N/R		68	8
CobaltStrike (loader)	1,767	1	N/R		1,577	2
Gafgyt (backdoor)	1,099	1	N/R		162	4
PHP Forum (traffic injector)	234,796	1	70,795	3	110,233	2
SSH (attack ware)	78,455	1	11,522	4	53,561	2

The United States, China, and India accounted for nearly ¾ of the IP addresses reported against the Top Ten. Among the Top Ten, the countries that experienced the largest increases were Hong Kong (137%) and Germany (49%).



COUNTRY	CYBERCRIME IP ADDRESSES 2025	2024	MALWARE
United States	**1,099,672**	984,968	+ 114,704
India	**900,603**	729,642	+ 170,961
China	**796,212**	958,744	– 162,532
Hong Kong	**363,417**	153,023	+ 210,394
Taiwan	**151,132**	87,260	+ 63,872
Germany	**149,765**	100,205	+ 49,560
Russia	**141,329**	159,024	– 17,695
Brazil	**118,928**	*181,987*	– 63,059
Vietnam	**117,499**	*81,674*	+ 35,825
Great Britain	**92,978**	95,865	– 2,887

Worldwide, the United States, China, and India again had the most IP addresses reported for serving as resources for cybercrime activity.

- IP addresses reported for cybercrime activity in the United States increased from 984,968 to 1,099,672 year over year and remained the highest among all countries in our study data.
- Hong Kong saw the largest numeric increase (**+210,394**). India, too, saw a significant increase (**+170,961**).

China saw the largest numeric decrease (**-162,532**).

These findings raise questions for the United States, China, and India. Hosting providers in these countries have the technical expertise and ample resources to monitor or mitigate hosting resource abuse voluntarily but have neither the incentives nor the obligations (policy or regulatory) to compel them to do so.

Hosting providers should adopt industry-wide commitments for removing content that is used to perpetrate cybercrimes

Abuse of Free Web Hosting for Cybercrime

Free web hosting providers (also referred to as subdomain providers) offer web page construction, web hosting, and DNS services on a registered domain name that the provider owns, *e.g.,* **webapp.com, pages.dev, ru.com, and weebly.com**. Customers operate their web sites on the web hosting provider's infrastructure, with a name delegated from a domain name that the provider has registered. In most cases, users only need to provide an email address or username and a password to create an account. They are then assigned a hostname of the form: **subdomain.domainname.tld**

Many of these providers offer free accounts. Some attack kits, especially ones used by phishers, provide attackers with the means (or instructions) to sign up for and use subdomains in an automated fashion. (This is discussed in more detail in the Attack Resources section.) This allows the cybercriminals generally and phishers to launch large numbers of attacks, and to abuse these services repeatedly and at scale. The recent Interisle Phishing Landscape 2025 report provides a case study of such large-scale abuse of a free web hosting provider.

2.7% of all cybercrime attacks in our study data were hosted at free web hosting providers, which is down from 7.4% in the previous study period. Most of the difference can be attributed to a drop in the total number Google Blogger hostnames (**blogspot.***) which dropped

from 331,051 in the previous study period to just 31,891 in this study period. In the previous reporting period, Google's free web hosting was responsible for 56% of all cybercrimes from free web hosting sites; this dropped to 15% in the current reporting period.

31% of cybercrime attacks hosted at free web hosting providers were perpetrated from maliciously acquired free web hosting provider hostnames, down from 39% in the previous reporting period. We determine that a hostname was obtained maliciously if the hostname is reported to a cybercrime feed within 14 days of it first appearing in DNS queries.

The free web hosting providers with the largest numbers of hostnames reported were:

2025 RANK	2024 RANK	FREE WEB HOSTING PROVIDER	CYBERCRIME HOSTNAMES REPORTED	PROVIDER'S UNIQUE DOMAINS	TOP PROVIDER'S DOMAINS
1	4	Weebly	**109,817**	2	weebly.com weeblysite.com
2	2	CentralNIC	**106,982**	15	ru.com sa.com za.com eu.com es.com de.com
3	1	Google	**102,044**	77	page.link web.app blogspot.com firebaseapp.com appspot.com blogspot.tw blogspot.md blogspot.ro blogspot.be blogspot.ru
4	11	Vercel	**51,757**	1	vercel.app
5	3	Cloudflare	**47,243**	4	pages.dev workers.dev r2.dev trycloudflare.com

Cyberattacks hosted at free web hosting provider services are hard to mitigate. Since the free web hosting providers are responsible for their naming, addressing, and content hosting, only they are positioned to disable malicious accounts or take down malicious web pages. Any action upstream, such as blocking the second-level domain, would have an impact across the provider's whole customer base. At the same time, many free web hosting providers permit anonymous registration and cannot respond to complaints that request customer contact information. Providers that offer services at free or low cost may have limited resources to spend on security controls.

Hosting providers should implement recommended (best) content management practices to reduce vulnerable attack surfaces

One phenomenon, which appeared to occur most often with Google's blogspot service, is where the same hostname was then accessible via multiple different free web hosting provider domain names.

The cybercriminal, by creating a single account with the service provider, now has as many as 67 distinct hostnames that they can use. The service provider, Google's Blogger in this case, allowed the same name to be accessed via **blogspot.com, blogspot.sn, blogspot.mx, blogspot.pt, blogspot.tw, etc.**

Examples of hostnames detected for cybercriminal activity across multiple service provider domain names include:

- **coinbaselogindesk**
- **facebooksecurity**
- **paypalloginin-usa**
- **uspsservicetrack**

What was intended as a convenience to users is being abused by cybercriminals.

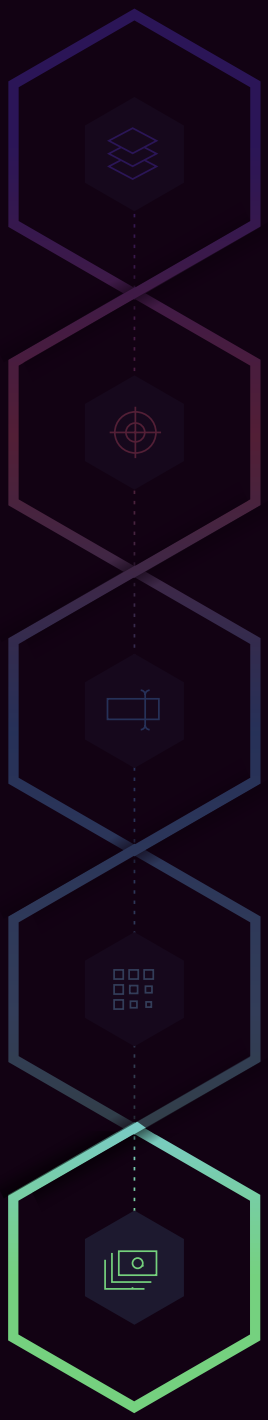
Cybercriminals have learned how to create accounts in bulk at some of these services. Cybercrime hostnames

Over 680,000 free web hosting hostnames served as resources for cybercrime attacks, a 42% decrease over our 2024 study period

in multiple Blogger domains detected during this period include eight instances of the hostname **hachown** with different numbers appended – each of these is multiplied by the number of blogspot domains to amplify the total number of places from or through which cybercrime can occur.

The significant drop in hostnames using Google's Blogger service has shown that measures can be used to drive down abuse, but criminals will be looking elsewhere. Free web host providers are encouraged to adopt similar anti-abuse measures.

Free web hosting providers must adopt effective, proactive measures to keep criminals from creating accounts and abusing their services



01
Attack Resources

02
Attack Targets

03
Naming Resources

04
Hosting Resources

05
Cashing Out

Cashing Out

Most cybercriminals expect to profit from their criminal activities. Ultimately, they want cash in their bank accounts, they want the cash to be "clean", and they want the transactions to appear legitimate to law enforcement.

Getting paid by victims is usually the first of a series of transactions that launder illicit gains into usable (legitimate) currency or goods. Ideally, criminals want to be paid by victims in a way that makes the payments difficult to track, for example in cryptocurrency or gift cards. At the same time, criminals usually want to convert these payments into financial assets or property they can use in the real world.

Laundering is a potential Achilles' heel for cybercriminals because law enforcement vigorously "follows the money" to track down the perpetrators as well as their suppliers. While some cybercriminals operate out of nation-states that protect them from direct prosecution, others try hard to avoid detection or intervention by law enforcement through all steps involved in the execution of cybercrime. This is particularly true for payouts: if illegitimate payments are frozen "on the way", a cybercriminal might not have to worry about being arrested but they would still lose the associated gains.

A dark economy exists to facilitate criminal payments processing, preventing or hindering law enforcement's observing transaction flows and the inter-relationships between the criminal supply chain players. The dark web, which provides a marketplace for these suppliers and integrators, interacts with the real-world economy to convert victim payments into legitimate currencies. Specialized criminals design and use elaborate schemes and supply chains to convert financial assets and hide the associated transactions.

Many laundering methods exist, including gift card payments, mules, or cryptocurrency conversion. Cryptocurrencies have become the coin of the dark economy. In addition to being a means for capturing criminal revenue, cryptocurrencies have become the primary way criminals pay other criminals for tools or services. For example, ransomware operators or protection racketeers often demand victim payments in some form of cryptocurrency. Other cybercriminals directly steal cryptocurrency from victim wallets or operate crypto mining operations using stolen computing resources. Blockchain-based cryptocurrency was initially attractive because it was believed to provide transaction anonymity. But law enforcement has developed effective techniques for exposing these transactions and associating them with recipients. Cryptocurrency must be laundered in much the same manner as drug cartels launder cash, and crypto-laundering services now exist to allow criminals to obfuscate their transactions through cryptocurrency exchanges or through mixers that interfere with transaction tracing by law enforcement. Nevertheless, a key issue remains that various countries do not pursue cybercriminals, be this due to a lack of resources, because they do not care about predominantly Western victims, or because they consider cybercrime part of their hybrid conflict strategies.

> Cybercriminals launder cryptocurrency in much the same way that drug cartels launder cash

Our Recommendations

Recommendations for Disrupting the Cybercrime Supply Chain

In this report, we provided measurements that showed how criminals assembled resources to conduct their business and that they did so through legitimate markets and supplies as well as through dark economies. Our analyses showed that the intersections between cybercriminal enterprises and the legitimate economy were numerous, and their resource acquisition behavior and strategies were highly observable.

Cybercriminals rely on naming, hosting, and nexus with financial industries in the legitimate economy to perpetrate crimes. After years of studies including ours, these industries must be aware of how their products, services, and platforms are used in the perpetration of cybercrime, but cybercrime continues to grow each year.

Opportunities exist to make criminal access to resources across the supply chain more difficult or costly to acquire, but several of the more obvious opportunities to disrupt cybercrime have not been acknowledged or be addressed in a uniform and formal manner.

Cybercrime mitigation strategies should include action aimed at disrupting the cybercrime supply chain

We continue to advocate for balanced policies that will make it harder for criminals to obtain and use domain names, while keeping it easy for law-abiding, legitimate registrants and content providers to get the resources they need. We recommend the implementation of a series of measures to curb the criminal abuse of resources and more effectively remediate cybercrime problems when they are found.

1. Verify Customer Registration Information

Our phishing landscape studies and this series of studies all established strong correlations between stricter verification requirements and lower rates of abuse. The INFERMAL study sponsored by ICANN found similar correlations. Cybercriminals frequently provide false or suspicious customer information. Industry should use (international) address or identity verification methods that are widely used across e-merchant and other online industries to screen customer data, which costs mere pennies per transaction.

We recommend that the domain and hosting industries adopt the European Union NIS 2 Directive standards. NIS 2 requires that registries and registrars take steps to ensure accurate and complete registration information. European ccTLD registries use automated screening tools today to meet these requirements. This approach has proven to be effective practical, scaleable, and efficient.

2. Implement Bulk Domain Name Registration Requirements

Bulk registration is one of the most egregious domain name acquisition techniques used by criminals. Criminals continue to routinely register hundreds or thousands of domains over the course of a few hours. Measures must be taken to stem this registration abuse.

We recommend that registrants should be required to apply and undergo enhanced identity and verification checks before accessing high volume registration services. Verification could conceivably be implemented in a variety

of ways, for example on a registrar-by-registrar basis or through a credential recognized industry-wide.

Registrars and registries should monitor and investigate high-volume transactions for suspicious registration behavior. The Abuse Prevention and Early Warning System (APEWS) created by EURid has proven successful in the field. Adoption of this or similar systems will strip cybercriminals of a deception technique that remains successful despite awareness campaigns and phishing simulations.

Many registrars and registry operators suspend their portfolios of domains of newly discovered criminal activity and their associated accounts, and we applaud these efforts. But cybercriminals routinely register domains in multiple TLDs for resiliency against such independent efforts. Identifying them all, quickly, across multiple registries and registrars, is challenging. We recommend that the domain name industry consider a form of Information Sharing Analysis Center (ISAC), where an operator that has identified a malicious behavior or actor can share intelligence across the domain industry.

3. Limit High Volume Account Creation

The use of free web hosting accounts by criminals for phishing attacks (*e.g.,* **<subdomain>.blogspot.com**) has decreased by 40% from 2024. We attribute much of this decline to the adoption of one or more proactive measures to identify and block automated (bot) account creation (*e.g.,* reCAPTCHA, AI, behavioral analysis, and multifactor authentication). We commend those operators that have adopted such measures. Operators that have not done so should be encouraged by the apparent successes.

4. Deploy Automated Systems to Screen for Suspicious Resource Behavior

Cybercriminals often exhibit identifiable patterns of suspicious registration behavior. Our study data for this period revealed that criminals are continuing to register domain names closely matching famous and well-known brands, names deceptively similar to brands, and algorithmically generated names, among other suspicious behavior. Such behaviors, often in tandem with bulk registrations, can be observed during registration. Screening based on tell-tale criminal registration behavior reduces the need to scrutinize content associated with every registration.

Automated monitoring technology for registries and registrars is indicated in an earlier recommendation, but **we advocate uniform and formal adoption broadly across the name resources industries**. Actively monitoring systems for criminal abuse and relevant violations of terms of service and suspending suspicious accounts must become the industry norm.

Similarly, hosting operators (including public code repository and file sharing platforms) should make use of cybercrime reporting services or data sources to determine what domains have been registered by their customers. By doing so, hosting operators can check for other suspicious domains their customers may have registered. We selected the data contributors to Interisle's Cybercrime Information Center based on their broad adoption, reliability, and accuracy and use these reports to assist registry and registrar operators regularly.

5. Offer Trusted Reporter Programs

Trusted reporters (also known as trusted flaggers) are organizations or individuals that are skilled at finding and documenting abuse and have proven that they have low false-positive rates. All name and hosting resources providers should offer a way for trusted reporters to submit abuse reports.

A variety of companies operate trusted reporter programs to address a range of abuses, including some of the large hosting and cloud providers, and online safety authorities, the European Union's Digital Services Act, and NIS 2 Directive created trusted flagger programs. Under these laws, Internet providers can be fined if they do not promptly process reports from trusted flaggers. Customer contact data should also be made readily accessible to law enforcement, public safety, and trusted private sector cyberattack responders.

6. Require Corrective Action

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

Policies or regulatory action are needed to incent consistently poor performers to reduce misuse of their operations by criminals. Operators who fail to do so should face penalties, including increased fees, suspended or reduced ability to process gTLD domain registrations, and possible de-accreditation.

A Call for Enhanced Outcome-Oriented, Cross-Sector Collaboration

Cybercrime is a multi-sector, multi-industry concern. While individual sector and industry efforts are needed, coordination, cooperation, and consistent action from stakeholders across the Cybercrime Supply will be most effective in combatting this systemic problem.

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

- Pro-active, effective enforcement of acceptable use policies that prohibit fraudulent, illegal, or deceptive practices, including spam, phishing, malware distribution and other cybercrimes.
- Adoption of industry-wide commitments for taking down web pages and other resources (such as attack kits) used to perpetrate cybercrime.
- Recommended content management practices that can reduce vulnerable attack surfaces.
- Uniform and timely cooperation with law enforcement, cybercrime and brand protection services, and private-sector cyber investigators to shut down criminal access to resources within hours, rather than days or weeks, of identification.
- Development of solutions to facilitate effective and timely data sharing within and across industries for the purpose of identifying and reducing criminal use of resources.

Further, sustainable change will only occur if a broad range of stakeholders (including governments, where necessary) step-up and implement real-world solutions to reduce criminal access to resources:

- Consumer groups should participate in anti-cybercrime advocacy: participate in relevant industry fora, advocate for the adoption of anti-abuse measures, communicate the real-world impact of cybercrime on consumers, and represent consumers in cybercrime litigation.
- Code repository platforms, subdomain providers, hosting companies, and financial and cryptocurrency institutions should be actively involved in cross-industry anti-abuse discussions, solution development, and implementation.
- Banking, payments, and cryptocurrency industries should work closely with resource providers and public/private sector investigators to combat fraudulent use of payment platforms in the registration of resources and conversion of illicitly obtained assets.

Effective disruption of the cybercrime supply chain requires international, intergovernmental, and industry collaboration to implement practical solutions to reduce abuse. This is especially true among industries and countries that are shown to be consistently prone to resource abuse.

About the Authors & 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.

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

Dr. Colin Strutt has published and spoken extensively on networking technology, name collisions, enterprise management, eBusiness, and scenario planning, and has represented the interests of Digital Equipment, Compaq, and the Financial Services Technology Consortium in national and international industry standards bodies. He holds six patents on enterprise management technology and has 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 and of resources used for cybercrime. Dr. Strutt holds a B.A. (with First Class Honours) and Ph.D. in Computer Science from Essex University (UK).

Chuck Wade has devoted most of his career to adapting innovations in networking technologies and distributed services to real-world business problems in areas ranging from academic networks to stock exchange networks to payments systems. Over the past decade, he has focused on the needs for security and business resilience in a variety of consulting engagements for clients that have included a 2-centuries old stock exchange, multi-national institutions, start-up ventures, and industry consortia.

Pete Strutt is Principal Creative Director at Common Co., based outside of Boston, with 20+ years of experience building brands. He has a passion for data visualization and finding the simplest way to display complex information in print and on screen.

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 the IRIS investigations platform.
- April Lorenzen and Zetalytics, for access to passive DNS data.
- John Levine, for operational support.
- Laurin Weissinger and Matt Thomas, for the constructive comments on an earlier draft.
- All the security personnel and law enforcement who fight cybercrime.

About Interisle Consulting Group

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