



Interisle

Cybercrime Supply Chain 2024

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

CONTENTS

Introduction	6
Attack Kits	11
Attack Resources	16
Naming Resources	19
Hosting Resources	30
Cashing Out	34
Recommendations	36

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 to advance a safer digital environment for all. Founded in 2004, M3AAWG provides a trusted and collaborative worldwide forum to help 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 top priorities in the fight against online abuse include: Organization; Readiness; Data and Identity Protection; Communications; and Supply Chain.

<https://www.m3aawg.org/>



EXECUTIVE SUMMARY

Cybercrime has flourished and continues to grow because it is a highly profitable business.

Cybercriminals pocket trillions of dollars every year, amassing earnings that easily surpass the GDP of countries as large as the Netherlands, Indonesia, and Turkey. The costs inflicted on society by the cybercrime business, however, are orders of magnitude greater than the earnings pocketed by criminals – causing an estimated global toll of US\$9.5 trillion in damages in 2024.

Like any other business, cybercriminals must gather the resources and services needed to conduct their 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 the criminal enterprises and should be part of the overall strategy to mitigate the systemic scourge of cybercrime.

Interisle's Cybercrime Supply Chain framework provides a means to analyze this criminal resourcing. By assessing it

like any other business, revealing opportunities to starve criminals of the resources needed for their lucrative and costly attacks. This second 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.

We collected malware, phishing, and spam reports from eleven publicly and commercially available threat intelligence or reputation services. 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 subdomain providers that represent the greatest amount of cybercrime activity based on raw counts and comparative metrics.

Our analysis reveals that:

The total number of malware, phishing, and spam attacks grew by nearly 54%, to nearly 16.3 million attacks. Of the three types of attacks, spam grew at the most alarming rate, doubling from 4 million to 8 million unique attacks.

Cybercriminals sharply increased their consumption of domain name resources for cyberattacks. Over 8.6 million unique domains were used in cyberattacks compared to 4.8 million last year – an 81% increase.

The registration of high volumes of domain names over short periods of time (bulk registration) was heavily exploited by cybercriminals. Over 2.6 million domains used in cyberattacks were registered in bulk, a 106% increase compared to last year. In one instance, over 17,000 cybercrime domains were registered in under 8 hours at the same registrar.

Cybercriminals steeply increased their use of subdomain providers as a key resource for attacks over the past year. Nearly 1.2 million subdomain hostnames were found to be used in attacks, an increase of over 114% compared to last year.

Attracted to cheap prices and easy registration, cybercriminals continue to flock to new generic top-level domains (new gTLDs) as preferred suppliers of naming resources. New gTLDs accounted for 37% of cybercrime domains reported while holding only 11% of the total domain name market.

The number IPv4 addresses reported for hosting cybercrime nearly doubled in both China and India, while decreasing slightly in the United States. While the United States remains the top source of cybercrime reported IPv4 addresses, China's 94% growth placed it nearly on par with the United States.

Clear opportunities exist to squeeze criminal access to resources across the supply chain by making it more difficult or costly to acquire them. Yet progress has been slow in reducing even the most obvious areas of abuse.

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 bulk register domain names and limit the number of accounts and subdomains a customer can register at subdomain providers.

Expand the deployment of automated systems across industries in the supply chain to screen for 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.

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

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 business.

Revenues from cybercrime – that is, the financial gains realized by cybercriminals from their activities – [amount to trillions of US\\$ annually](#), according to academic research. When compared to the GDP of nation states, global cybercrime would easily rank [within the top 20 economies](#), surpassing countries such as the Netherlands, Indonesia, and Turkey.

Cybercrime today is a professionalized multinational industry with a vast array of suppliers, service providers, and specialized marketplaces where criminal enterprises and entrepreneurs alike buy and sell the resources they need to ply their trade. These supplies and services are sourced from both the legitimate and dark economies, with transactions that range from easily observed to more hidden and complicated to track.

The business management strategies, industry structures, and profit drivers within the cybercrime industry [resemble those found in the legitimate economy](#) and would be familiar to any real-world executive. Pay rates and benefit packages sometimes rival that of real-world corporate jobs too. [Recent research by Kaspersky](#), for example, found dark web job postings for IT roles paying as much as US\$20,000 per month, with benefits including paid time off and sick leave.

The costs inflicted on society by the cybercrime business, however, are orders of magnitude greater than the earnings pocketed by criminals. Cybersecurity Ventures predicts cybercrime will inflict [US\\$9.5 trillion in damages](#) globally in 2024, this includes various types of financial impact, such as direct financial losses to consumers and business, data theft and destruction, disruption of economic activity, and related recovery expenses. The World Economic Forum (WEF) in fact has [ranked](#)

[cyberthreats](#) as one of the most severe risks to global and economic stability in the near future.

Over \$1.5 Trillion USD

Revenues Earned by Cybercriminals Annually

Source: [Prof. Michael McGuire](#)

\$9.5 Trillion USD

Estimated total annual cost of Cybercrime on the Global Economy

Source: [Cybersecurity Magazine](#)

880,000+

Number of Cybercrime Incidents Reported in the US in 2023

Source: [FBI](#)

\$1,542,333 USD

Average Ransomware Payment Cost in 2023

Source: [Sophos](#)

\$219 Billion USD

Global Spending

Source: [IDC](#)

Cybercrime is a complex, systemic problem. Cybercriminals can easily perpetrate attacks across borders, obscure operations, establish and disband attacks quickly, and achieve a global reach impacting all sectors of society. To change such a problem, one must understand the drivers, systems and structures that perpetuate it and target solutions towards disrupting or improving them.

Specialists and experts, of course, need useful analytical frameworks to identify key nexus points and opportunities for change. Lawmakers, product managers of legitimate resources commandeered for criminal purposes, and other non-technical stakeholders need to reasonably understand the problem to take informed, appropriate action.

Cybercrime has flourished and continues to grow because it is a highly profitable business. Cybercriminals operate in an environment where permissive policies or business practices ensure that they can easily and cheaply access resources with little or no risk of punishment to act as deterrents. Analyzing cybercrime as a business can reveal insights into the factors that fuel the criminal trade economy and make it lucrative, as well as areas where the business model can be disrupted. Ultimately this criminal trade economy relies on the legitimate economy to obtain input resources and realize the outputs of financial gain. Actions that make it more difficult and costly for criminals to acquire these resources, conduct crimes, and convert criminal proceeds to cash, would help reduce the profitability and attractiveness of the business. Making these resources more difficult and costly for criminals to acquire should be part of the overall strategy to mitigate the systemic scourge of cybercrime.

Key opportunities to disrupt the business model exist in places where cybercriminals acquire the tools, resources, and services needed to conduct attacks. Interisle calls the assemblage of these resources the “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.

Analyzing cybercrime as a business reveals opportunities to starve criminals of the resources needed for attacks.

Scope & Focus of this Study

This is Interisle’s second annual Cybercrime Supply Chain report. Consistent with our 2023 study, we focus our analysis on three of the most common types of profit-oriented cybercrimes and cybercrime attack vectors – malware, phishing, and spam. In addition to being individually significant, these three cybercrimes are also highly related and used together in attack campaigns. They are also three cybercrimes for which Interisle has access to reliable datasets that can be analyzed to track criminal use of key cybercrime supply chain resources.

For each of the five supply chain links -- Attack Kits, Attack Targets, Naming Resources, Hosting Resources, and Cashing Out – this report provides a narrative overview of how cybercriminals acquire and use the associated resources. In addition, we conducted detailed data measurements and analyzed the sources, suppliers, and strategies commonly used by cybercriminals to acquire Attack Targets, Naming Resources, and Hosting Resources, and report our results in each of those supply chain links. Interisle does not have relevant data to provide

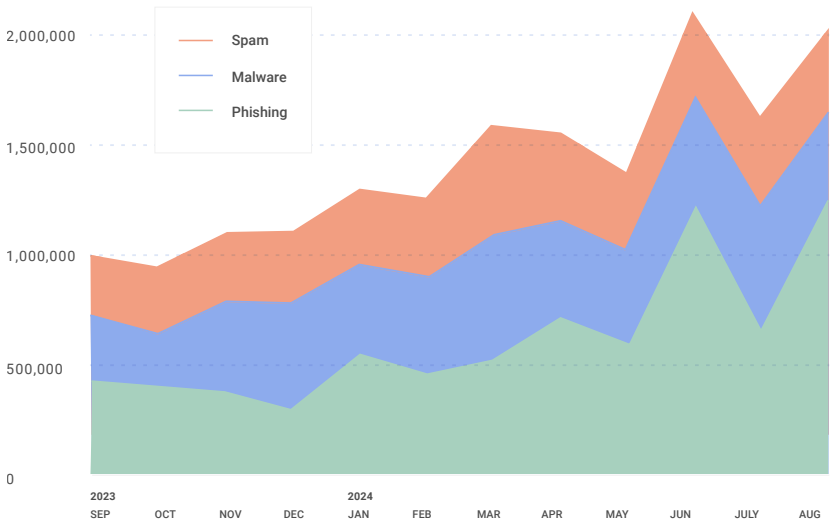
a comprehensive quantitative analysis of Attack Kits and Cashing Out links of the supply chain, however, the narrative overviews describe their function and challenges in mitigating criminal access to associated resources.

To conduct our quantitative analysis for the Attack Target, Naming Resources, and Hosting Resources links, we collected spam, malware, and phishing reports from eleven publicly and commercially available threat intelligence or reputation services (see our list of [data contributors](#) at the Cybercrime Information Center).

From these sources, we identified nearly 16.3 million unique cybercrime events, a 54% growth over last year’s study. 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 subdomain providers that represent the greatest amount of cybercrime activity based on raw counts and comparative metrics.

Spam activity doubled from 4 million to 8 million events

MONTHLY CYBERCRIME EVENTS Sep 2023 to AUG 2024



Cybercrime overall grew by 54% from 10 million to 16 million events year over year

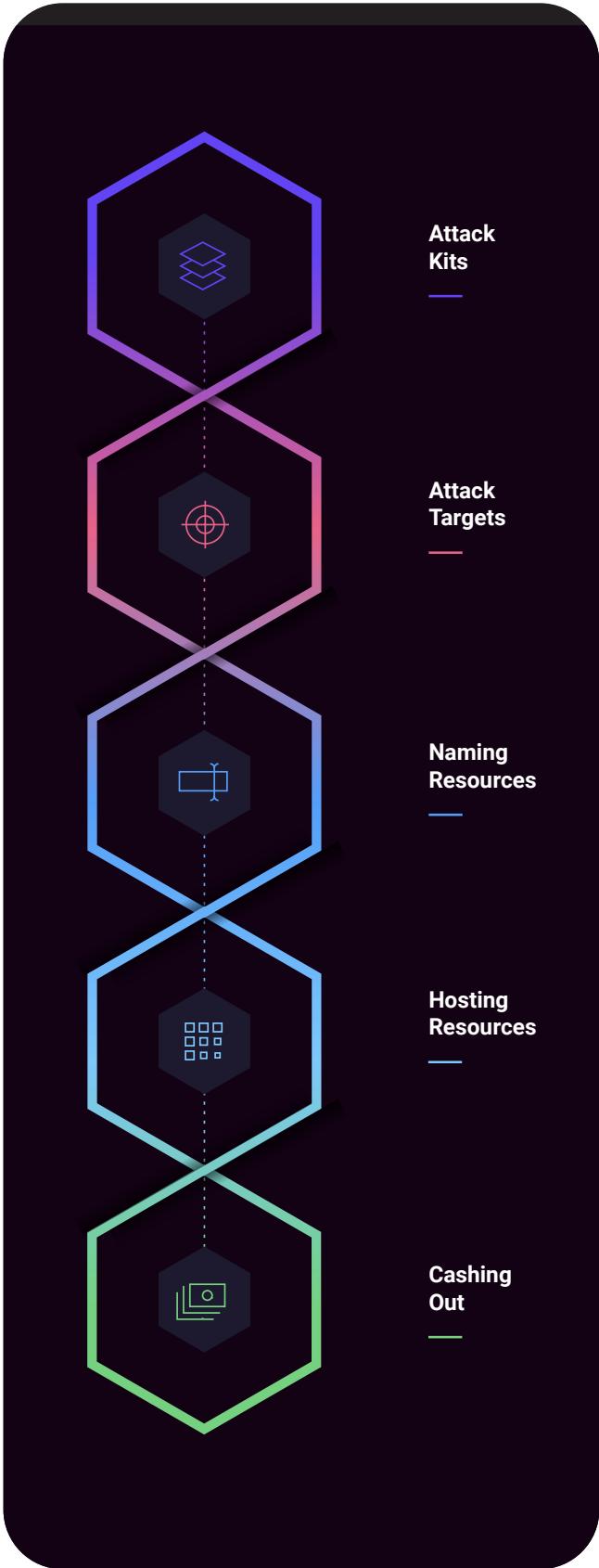
This study uses Interisle's [methodology](#) for distinguishing attacks where domain names were purposely (maliciously) registered by criminals from attacks that were hosted on compromised domains or web sites. This distinction is important because it indicates where additional prevention and mitigation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

The 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 smartphone by itself has only minimal value. To make smartphones usable, 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:



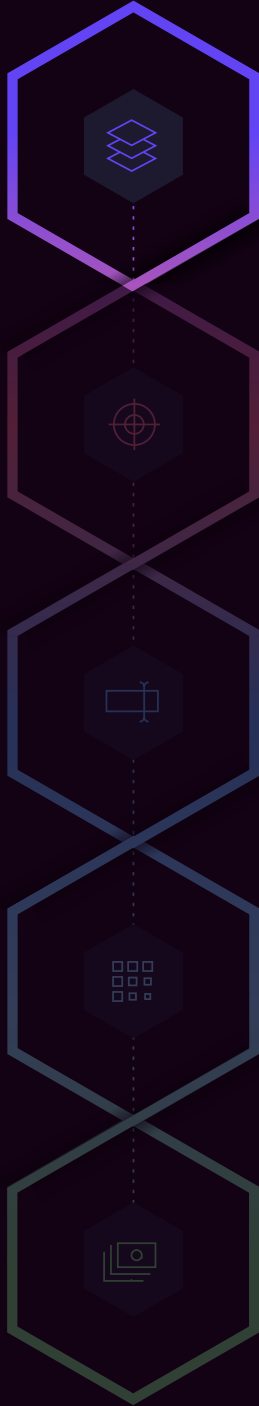
Attack Kits These are veritable “cyberattack in a box” starter kits frequently used by criminals. They are often composed of a set of files and scripts that allow a criminal to impersonate a well-known organization or brand. Attack kits are usually customized to suit a particular kind of attack, e.g., a fake web site for phishing or a web page that hosts malware.

Attack Targets Internet end users are primary targets for cybercrimes. Acquiring targets involves obtaining contact information 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, and thus merchants, manufacturers, governments – virtually any organization with an online presence – are both targets and 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 and convert these into tangible assets.



01
Attack Kits

02
Attack Targets

03
Naming Resources

04
Hosting Resources

05
Cashing Out

Attack Kits

Attack kits provide a web page, message content, or a file that a criminal wants a user to visit, read, open, or download. Attack kits can be obtained on public repositories, on the dark web, and even social media sites. Kits are typically sets of files and scripts that provide a criminal with tools to conduct an attack quickly and easily and are usually specific to certain types of crime:

Exploit kits can be used in different contexts and provide the buyer with malicious software that takes advantage of software vulnerabilities.

Phishing attack kits commonly include ready-made webforms and logos impersonating known organizations.

Exploit kits commonly contain a delivery method (e.g., a loader) that, once installed, can “call home” for additional payloads such as an information stealing executable (e.g., banking trojan or remote administrative tool, RAT) or an executable that can send email (e.g., spambot).

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

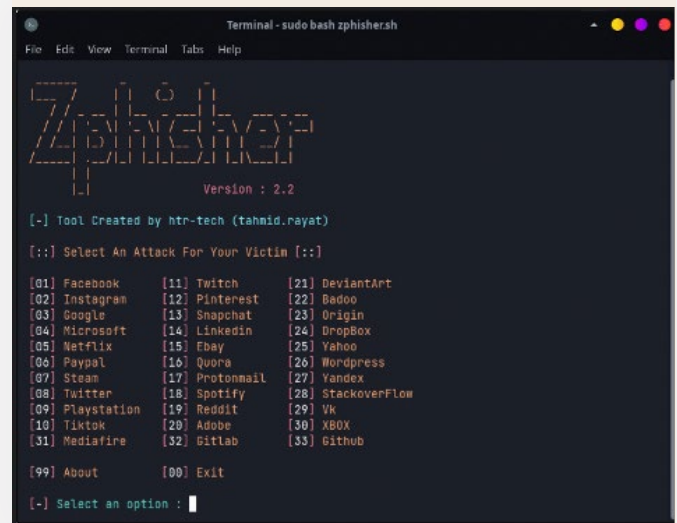
Exploit Kits

[Exploit kits](#) may contain malware that takes advantage of a software vulnerability 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 kind of malware (a “loader”) that is designed to deliver additional malware. Once installed, the loader can “call home” for additional payloads such as an information stealing executable (e.g., banking trojan or remote administrative tool, RAT), an executable that can send email (e.g., spambot). After deployment, the exploit malware is typically hosted on a web page. The URL of the exploit malware is distributed through spam or phishing messages or social media pages. Visitors are drawn to or “drive by” the web page, then by clicking the URL they will download an initial infection, a “loader”, which is used to download additional information-stealing malware, ransomware, or **spambots**. 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

Phishing kits include web forms where Internet users are lured to sites impersonating a known organization or brand. Phishing kits are typically archived files (e.g., a zip file) that contain all the components needed to carry out a phishing attack. These can be obtained from public repositories like Github or SourceForge. An example of such a kit is an open-source tool called [zphisher](#). Once installed, a phisher chooses to impersonate (currently, 33) well-known brands. For certain brands, zphisher offers a choice of web page templates and generates phishing URLs. The phisher can now send email or text messages that contain the URL or post the URLs to social media.



Case Study: Phishing Message and Fake Web Page Composition

Phishers are cybercriminals that perpetrate online frauds through deception or impersonation. The perpetration is a multi-staged attack. First, the phisher crafts a message that serves as “bait” to convince a recipient to visit a merchant web page, healthcare portal, bank, or social media account login, etc. The recipient who takes the bait is “hooked” when they visit the web page and the phishing attack is completed when they submit personal, financial, or other sensitive information at the visited web page.

Phishing activity increased nearly 40% from 1.9 million to 2.6 million events

Many phishing attacks instill fear, uncertainty, or doubt to exploit human emotions and stress levels. For example, phishers achieve this by mimicking a large credit card expense or checking account overdraft notice, that may cause a recipient to react without examining the message or web page carefully. Others exploit desires or needs, for example the promise of discounts or free merchandise. Strategy notwithstanding, phishers typically incorporate the following elements into their attacks.

Impersonation – Messages and web pages that appear authentic are most convincing and likely to succeed. Phishers can “[clone](#)” most web sites directly from a browser or by using a [web scraping](#) tool. The web page elements obtained through cloning or scraping are the basic elements for the fake web page.

Obfuscation – Successful phishers are aware that security measures are employed to thwart phishing in messaging applications, browsers, and dedicated security devices (e.g., email gateways, firewalls, intrusion detection, or web proxies). To evade detection, phishers often employ some form of obfuscation; for example, they may encode text messages in a [Base64](#) character set; for example, the text “this is a test” when encoded in Base64 becomes “dGhpcyBpcyBhIHRic3QK” which may bypass security measures.

Information Harvesting – Phishers use submission forms that are familiar to web users at their fake web pages to collect personal, financial, or other sensitive information. Simple forms of this kind are easy to obtain; for example, Microsoft Co-Pilot returned this form when asked, “php script that collects name address and phone number and sends as email”:

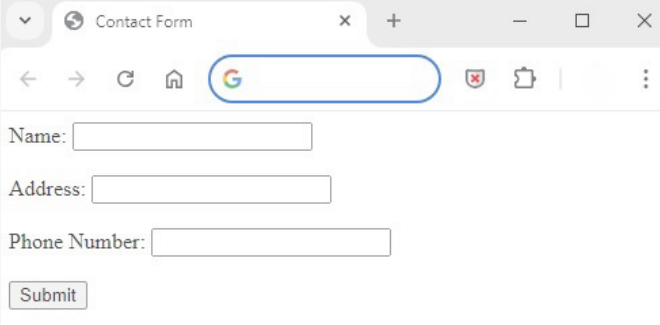
```
<!DOCTYPE html >
<html >
<head>
  <title>Contact Form</title>
</head>
<body>
  <form action="send_email.php" method="POST">
    <label for="name">Name: </label>
    <input type="text" id="name" name="name" required<br><br>

    <label for="address">Address: </label>
    <input type="text" id="address" name="address" required<br><br>

    <label for="phone">Phone Number: </label>
    <input type="text" id="phone" name="phone" required<br><br>

    <input type="submit" value="Submit">
  </form>
</body>
</html >
```

The web form appears in a browser as:



The screenshot shows a web browser window titled "Contact Form". The address bar contains a search engine icon. The form consists of three text input fields labeled "Name:", "Address:", and "Phone Number:", each followed by a "Submit" button.

Co-Pilot also returned a script that will send the collected name, address and phone number to the phisher’s email address.

```
<?php
if ($_SERVER["REQUEST_METHOD"] == "POST") {
  $name = $_POST['name'];
  $address = $_POST['address'];
  $phone = $_POST['phone'];
  $to = "your-email@example.com"; // Replace with your email address
  $subject = "New Contact Form Submission";
  $message = "Name: $name\nAddress: $address\nPhone: $phone";
  $headers = "From: webmaster@example.com"; // Replace with your sender email address

  if (mail($to, $subject, $message, $headers)) {
    echo "Email sent successfully!";
  } else {
    echo "Failed to send email.";
  }
}
?>
```

Webforms are commonplace in legitimate business and private realms, and often serve as examples in teaching people how to code. This example underlines how easy it is to abuse chatbots (and other services) to find webforms that can be modified for criminal purposes and gain.

The phisher uses the web page elements obtained through cloning or scraping to determine exactly what the submission form should collect. With little or modest scripting skills, they can modify the web form and script to imitate the original form.

Creating the phishing message is straightforward. The phisher can imitate a typical correspondence, *e.g.*, a required login, from a bank or merchant or from an organization's system administrator. By creating an email that contains HTML content, they may also use Base64 encoding for any content that they wish to hide from security measures.

Measurements of Attack Kits

The threat intelligence feeds that Interisle uses to analyze cybercrime activity do not measure attack kits per se. To accurately estimate the number of phishing or exploit kits found among URLs reported during our yearly period would require more data. For example, several of our feeds only report URLs as hosting Malicious Documents or Malicious Scripts; by obtaining copies of the files in the reported URLs, we could analyze these to determine how many URLs hosted phishing kits. We could take a similar approach for other malware types.

From our study period data, however, we collected metadata from several of our feeds to classify and count URLs containing several types of malware that infects endpoint devices:

MALWARE TYPE	DESCRIPTION (from Interisle's Malware taxonomy)	COUNT
Malicious Executables	Includes Windows, Linux, and Android executables	138,910
Malicious Scripts	Includes PHP, JavaScript, and other common web development languages	80,936
Malicious Documents	Includes compressed files such as zip and rar, MS Office documents, etc.	29,005
Loaders	Malware that installs other malware, also called "droppers"	8,969
Backdoors (RATs)	Malware that provides remote access or administration of an infected endpoint	8,278
Information Stealers	Malware that steals account, credit card, or sensitive data	7,729

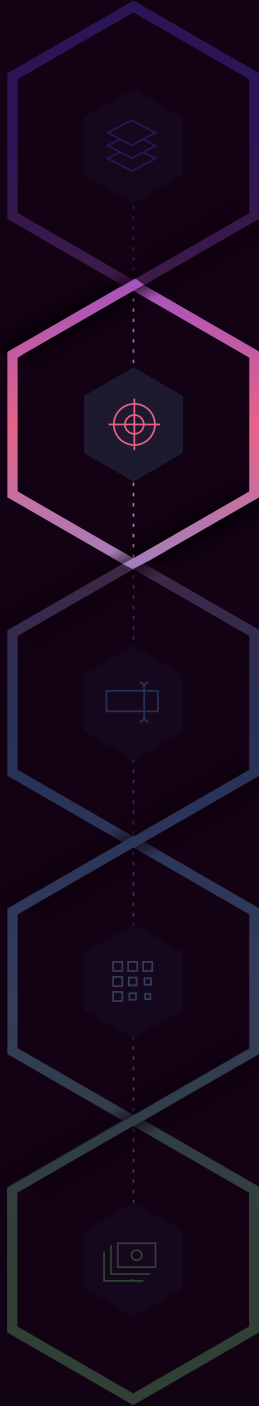
In the absence of additional metadata or such files, we can only speculate that, among the URLs identified during the study period, there might be thousands of sources for phishing kits and exploit kits.

Disrupting access to attack kits poses several challenges:

- While repositories or file sharing services, such as GitHub, have [acceptable use policies](#) (AUPs), the simplicity of accessing attack kits suggests that AUPs are either not rigorously enforced, and/or that providers struggle to identify malicious code on their platforms.
- Neither AUPs nor uniformly enforceable controls are present industry-wide to prevent misuse.
- Authors allege that their kits are published for educational purposes only and 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.

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.

Rigorous enforcement of file sharing service AUPs can reduce misuse by cybercriminals



01
Attack Kits

02
Attack Targets

03
Naming Resources

04
Hosting Resources

05
Cashing Out

Attack Targets

Attack kits provide the means to perpetrate online crime. Attackers next 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 transactionable 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 sophisticated attacks criminals often impersonate brands or conduct research to identify high value targets that can be targeted with individualized messages. In such cases, the impersonated brand or organization is both a lure and a victim, as merchants lose revenue when their products or services are used to lure users to counterfeit goods sites and may see their reputation being affected.

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 this convincing correspondence, cybercriminals often register legitimate-looking domain names for cybercrimes to facilitate the perpetration of

Many cybercriminals exploit the exact name of a well-known organization or product brand in cyberattacks

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.

Targeted 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 in 219,444 domain names and in 45,047 subdomain provider host names. Cybercriminals also use visually similar strings (e.g., faceb00k, pa1pal) so these figures are a low estimate of brand misuse in domain name or subdomain hostname composition.

We observed a 29% increase in brand names appearing in domain names year over year, and a disturbing 99% increase in brand names appearing in subdomain provider host names.

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.

2024 RANK	2023 RANK	BRANDS FOUND IN REGISTERED DOMAIN NAMES	NUMBER OF MATCHES
1	3	United States Postal Service	44,516
2	1	Apple	10,854
3	5	Google	8,764
4	2	Amazon	6,557
5	-	Bet365	4,642

2024 RANK	2023 RANK	BRANDS FOUND IN SUBDOMAIN PROVIDER HOSTNAMES	NUMBER OF MATCHES
1	7	Facebook	4,093
2	18	Instagram	3,448
3	-	Telstra	3,004
4	10	Webmail	2,746
5	-	Netflix	1,747

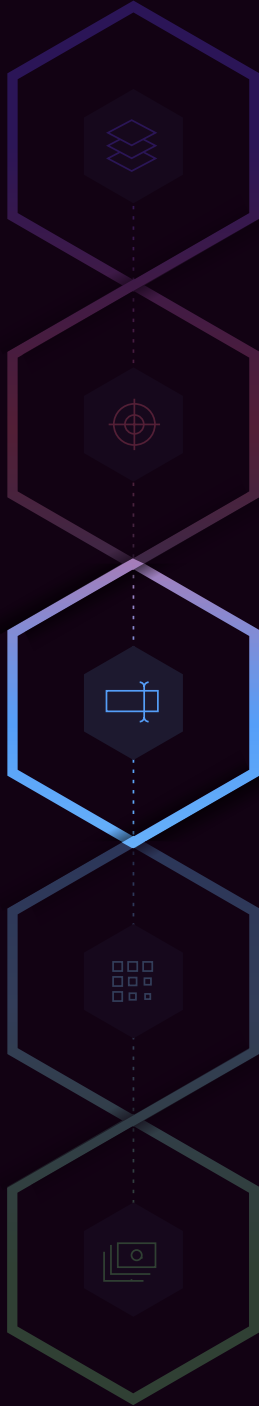
Operationally, implementing controls against such registrations is rather simple and effective – and while not perfect, such controls increase the friction for cybercriminals. EURID, the .EU registry currently [screens registered domains](#) based on lexical features and similarity to known brands. If 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

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

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. In our [2023 Phishing Landscape Study](#), we noted that Freenom had been forced through litigation to shut down operations and lawsuits had been filed against domain registrars for cybersquatting, false designation of origin and trademark. This is a last resort but has proven effective.

Cooperation by operators with consumer advocacy groups could lead to a reduction of cybercriminal activity



01
Attack Kits

02
Attack Targets

03
Naming Resources

04
Hosting Resources

05
Cashing Out

Naming Resources

Domain names and hyperlinks (uniform resource locators, URLs) are familiar to most users and often do not raise suspicion, so they are an important means for criminals to identify the location of fake web pages and malware hosting sites.

Internet users navigate the Internet’s vast 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 and by assigning names to hosted content. These names are commonly included 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.

Domains registered by cybercriminals – malicious domains – increased 112% year over year

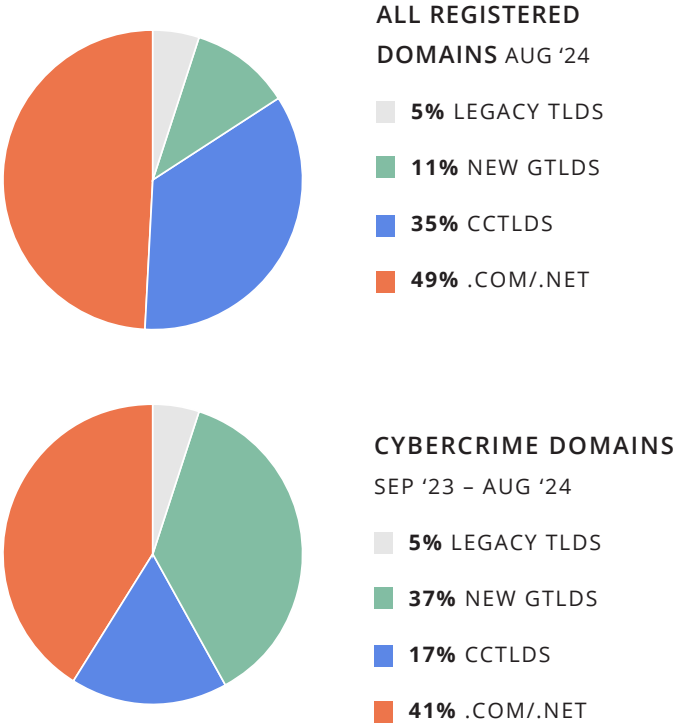
Cybercrime Activity Across the Domain Name Space

According to [Domain Tools](#), at the end of August 2024, there were over 341 million registered domains in the global domain name space. We identified domains reported for cybercrime activity in 904 of the approximately 1,500 existing TLDs during the current study period.

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

- the .COM and .NET registries, operated by Verisign, representing 49% of the domains in the world,
- the country-code domains (ccTLDs) representing 35% of the domains,
- the legacy generic TLDs – those other than .COM and .NET and introduced before 2013, e.g., .ORG, .BIZ, .INFO – representing 5% of the domains, and
- the new gTLDs introduced from 2014 to the present (e.g., .TOP, .CAM, .VIP, .XYZ, .SHOP) representing the remaining 11% of the domains.

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



All TLDs

For the September 2023 to August 2024 study period, we observed an overall 81% increase in domains.

Here are the top 10 TLDs:

2024 RANK	2023 RANK	TLD	DOMAINS IN TLD	TOTAL CYBERCRIME DOMAINS REPORTED 2023	TOTAL CYBERCRIME DOMAINS REPORTED 2023	% CHANGE
1	1	com	154,724,782	3,237,755	1,742,619	+ 86%
2	3	top	2,811,545	830,039	206,512	+ 302%
3	11	xyz	3,628,102	475,153	89,959	+ 428%
4	2	cn	9,073,931	399,748	290,070	+ 38%
5	10	shop	3,161,163	281,276	93,725	+ 200%
6	5	net	12,634,280	271,676	139,275	+ 95%
7	25	cc	1,363,369	236,869	31,075	+ 662%
8	16	ru	5,644,026	208,705	53,277	+ 292%
9	27	vip	1,026,746	169,554	25,564	+ 563%
10	4	info	3,532,577	153,957	179,762	- 14%

Overall, we observed an overall 81% increase in domains reported for use in cybercrimes. Six of the top ten TLDs had increases of 200% or more. Four of the top 10 TLDs – .TOP, .XYZ, .CC, and .VIP – had more than 10% of their domains under management reported for use in cybercrime activities. Worst among these was .TOP, where 30% of that TLD’s domains under management were reported for cybercrime use. By comparison, the 3.2 million cybercrime domains reported in .COM represented only 2% of that TLD’s domains under management.

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:

$$\text{Yearly TLD Phishing Domain Score} = \frac{\text{(number of unique phishing domains reported in a TLD across the year / number of domains delegated from a TLD)} * 10,000}{}$$

While .COM was the highest ranked TLD by reported cybercrime domains, 23 TLDs had yearly cybercrime domain scores that were more than five times that of .COM (which had a yearly cybercrime domain score of 209.3). **The top 5 of these were:**

2024 RANK	2023 RANK	TLD	DOMAINS IN TLD	CYBERCRIME DOMAINS 2024	YEARLY CYBERCRIME DOMAIN SCORE
1	2	rest	55,237	46,302	8382.4
2	-	ooo	39,050	22,107	5661.2
3	62	tk	78,944	43,798	5548.0
4	-	cam	42,639	15,726	3688.2
5	15	top	2,811,545	830,039	2952.3

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 35% market share, with roughly 120.7 million domains registered per our data set.

The 1.5 million domains reported for cybercrime activity represent 17% of the overall reported domains. This is a healthy decline from the 27% reported in [our 2023 study](#), where the much-abused Freenom commercialized ccTLDs negatively influenced this market segment.

2024 RANK	2023 RANK	ccTLD	DOMAINS IN TLD	TOTAL CYBERCRIME DOMAINS REPORTED 2024	TOTAL CYBERCRIME DOMAINS REPORTED 2023	% CHANGE YEAR OVER YEAR
1	1	cn	9,073,931	399,748	290,070	+ 38%
2	11	cc	1,363,369	236,869	31,073	+ 662%
3	6	ru	5,644,026	208,705	53,190	+ 292%
4	9	co	3,402,618	76,970	43,486	+ 77%
5	3	us	2,091,528	47,593	65,900	- 28%

The top 5 ccTLDs accounted for 68% of the cybercrime domains in ccTLD name space, representing a 50% increase over our 2023 study period.

New gTLDs

For the study period ending August 30, 2024, the new gTLDs again accrued the most misuse from cybercriminals.

The Top 5 new gTLDs, ranked by cybercrime domains reported, all offer open registrations.

2024 RANK	2023 RANK	New gTLD	DOMAINS IN TLD	TOTAL CYBERCRIME DOMAINS REPORTED 2024	TOTAL CYBERCRIME DOMAINS REPORTED 2023	% CHANGE YEAR OVER YEAR
1	1	top	2,811,545	830,039	206,512	302%
2	6	xyz	3,628,102	475,153	89,959	428%
3	5	shop	3,161,163	281,276	93,725	200%
4	11	vip	1,026,746	169,554	25,564	563%
5	16	club	610,966	135,863	20,353	568%

The new gTLDs held 11% of the market share but accounted for 37% of cybercrime domains reported

Cybercriminals wish to avoid detection or spend as little of their own money as possible. Some new gTLD registry operators compete by offering cheap or free registrations with no verification requirements. In the wake of the shutdowns of Freenom's commercialized ccTLDs, these registries have attracted more cybercriminals.

Dirty Deeds and Domains Done Dirt Cheap

Interisle's recent [Phishing Landscape 2024](#) study explored the effects of imposing identity verification requirements on domain registration. For example, individuals may be asked for proof of residency, citizenship, or a real connection to the country before registering a domain name in a ccTLD. Businesses may be asked to demonstrate a commercial presence (e.g., headquarters) in the country. Our analysis of the registration requirements of ccTLDs in the European Union and Asia-Pacific region revealed that imposing verification requirements on domain registrations correlates with lower phishing and malicious registrations. We also found that TLDs generally that offered registrations with no restrictions ("open registrations") yielded higher phishing scores. The phishing study also explored pricing and found that the combination of open registration policy and cheap registration fees make the gTLD space generally, and the new gTLDs, more attractive.

For this cybercrime supply chain study, we identified the 25 TLDs with the highest cybercrime domain scores. We again used comparative pricing data published by [TLD-list.com](#). We used their Cheapest Price History chart for each TLD to confirm that the fees have been offered frequently during

50 new gTLDs accounted for 98% of cybercrime domains in new gTLDs

our yearly study. Among the new gTLDs with the highest cybercrime domain scores:

- Nine offered registration fees for less than US\$1.00
- Twenty-two offered registration fees for less than US\$2.00
- By comparison, the cheapest price identified for .COM was US\$5.91

The finding here again supports the widely held view that cybercriminals are attracted to TLDs that offer registrations that are either cheap, easy to acquire, or preferably both. When registering such names, cybercriminals spend less money and time obtaining more resources, while the availability of open registration effectively provides them with greater anonymity. Unsurprisingly therefore, the study data also show that cheap ccTLD registration fees (e.g., for .TK and .CC) were attractive as well.

The appeal of TLDs with open registrations and cheap domains is unlikely to change unless proactive, preventative measures are adopted. This not only applies to TLDs delegated in the first new gTLD program, but

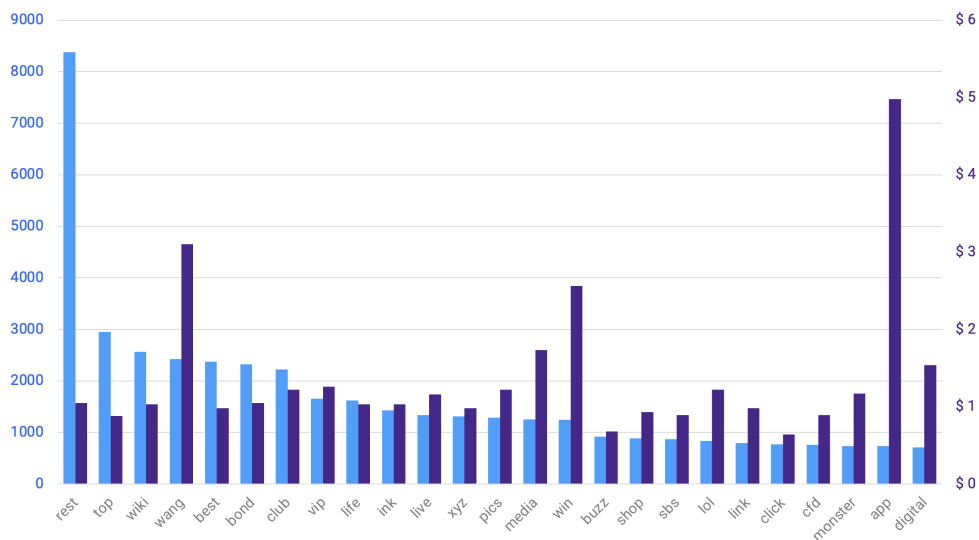
future delegations as well.

ICANN has announced that “[the New gTLD Program: Next Round](#) is expected to open in April 2026. This timing is based on [Policy Implementation](#) work, which is estimated to conclude in May 2025 with the completion of the Applicant Guidebook (AGB).”

ICANN should consider the history of cybercrime activity in new TLDs that offer open registrations and cheap domains carefully as it processes applications. The objective of fostering competition has arguably led to unanticipated and unwanted consequences. Adding more TLDs without a much stricter registration policy will likely further expand an already plentiful greenfield for cybercriminals.

For example, nearly all the cities that were granted gTLDs have low or no cybercrime activity reported. We looked at cybercrime activity that occurred in 36 city gTLDs. These city gTLDs typically have registration restrictions and higher registration fees compared to the open and cheap registration gTLDs, making the former much less attractive for criminal abuse. Among the city gTLDs, only .TOKYO had a notable number of cybercrime domains reported (3,101 in 2024, down from 12,135 in 2023), and this particular new gTLD has had persistent (phishing) activity since we first measuring [criminal abuse of domain names](#) in 2019. No other city TLD had more than 150 cybercrime domains reported during 2024. The policy, business, operational, and public safety (abuse detection and mitigation) practices of these cities would serve all consumers and registrants well.

New gTLDs: Cybercrime Domain Scores and Cheapest Registration Fee



Adding more TLDs without a much stricter registration policy will likely further expand an already plentiful greenfield for cybercriminals

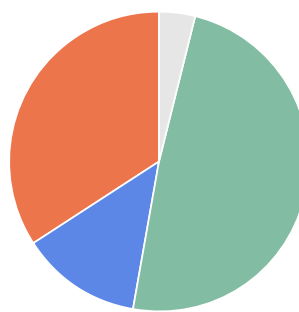
Malicious Domain Registrations Across the Domain Name Space

We measured the number of unique domains reported for cybercrime activity across a total of 904 TLDs. For our studies, we classify a domain reported for cybercrime activity as being either a domain registered purposely to carry out a malicious or criminal act ([maliciously registered domain](#)) or a domain registered for legitimate purposes but co-opted (“compromised”) by criminals through a cyberattack.

The percentage of malicious registrations in the new TLD space was more than four times its market share

We use a set of criteria to discriminate malicious domains from compromised domains including the time elapsed from domain creation date or first appearance of the domain to its being reported for cybercrime activity. We also look for characteristics of suspicious label composition; for example, we look for atypically long labels, labels containing exact matches of over 2,000 brands that we track, labels containing brand similarities, and labels containing suspicious numbers of digits or hyphens in the label. We also use the metadata provided by the [threat intelligence data that we collect](#) which can identify a brand target associated with a cybercrime report. We also look

for registration behaviors that are characteristic of bulk registration.



MALICIOUSLY REGISTERED CYBERCRIME DOMAINS

SEP '23 – AUG '24

- 4% LEGACY TLDs
- 49% NEW GTLDS
- 13% CCTLDS
- 34% .COM/.NET

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 (one of which was not ranked in the top 20 in the previous year’s study).

2024 RANK	2023 RANK	TLD	CYBERCRIME DOMAINS	DOMAINS DETERMINED TO BE MALICIOUS REGISTRATIONS	MALICIOUS DOMAINS PERCENTAGE
1	1	com	3,237,755	1,704,957	52.7%
2	2	top	830,039	734,931	88.5%
3	11	xyz	475,153	393,022	82.7%
4	5	shop	281,276	223,019	79.3%
5	-	cc	236,869	191,974	81.0%

While .COM has the largest number of domains determined to be malicious registrations, it has the lowest percentage among the top TLDs.

The following table shows the top 5 TLDs with the highest percentage of maliciously registered domains reported for serving as resources for cybercrime activity (none of which was ranked in the top 20 in the previous study).

2024 RANK	2023 RANK	TLD	CYBERCRIME DOMAINS	DOMAINS DETERMINED TO BE MALICIOUS REGISTRATIONS	MALICIOUS DOMAINS PERCENTAGE
1	-	bond	96,612	93,947	97.2%
2	-	club	135,863	130,354	95.9%
3	-	lol	47,714	45,056	94.4%
4	-	rest	46,302	43,298	93.5%
5	4	vip	169,554	151,916	89.6%

High malicious domain percentages suggest that business, pricing, or operational practices have made a TLD attractive for criminal domain registrations. Percentages in the 80% or higher range contribute to a negative reputation for that TLD.

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

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

Cybercrime Activity Across All TLD Registrars

We ranked all gTLD and ccTLD Domain Registrars by Cybercrime Domains Reported for the September 2023 to August 2024 study period and reported all domains for which we were able to identify a registrar. The table includes registrars with a minimum of 300,000 reported domains in our 2024 data.

#1-ranked GoDaddy experienced a 300% increase in cybercrime domains reported. Over 700,000 of these domains were registered in .COM, an increase of more than 400,000 over our 2023 study period. The .XYZ TLD was similarly exploited using GoDaddy as a registrar, with an increase from ~5,300 reported domains to nearly 96,000.

In #2-ranked NameCheap, cybercrime domains reported in .ONLINE decreased from ~20,000 to 1,300, and in .SITE, from ~12,000 to just over 1,000.

In #3-ranked Gname, .COM registrations increased over 500% over the 2023 study period. Domains reported in .CC, .CLUB, and .XYZ accounted for most of the remaining increase.

The increase in reported cybercrime domains at #4 NameSilo were spread across .COM, .NET, .ORG, and .XYZ. Domains reported in .COM also increased significantly year over year in #5 Dynadot (428%). The increase in reported cybercrime domains at #6 GMO resulted from a migration to .LOL, SBS, and .XYZ.

2024 RANK	2023 RANK	TLD REGISTRAR	TOTAL REGISTRAR DOMAINS	TOTAL CYBERCRIME DOMAINS REPORTED 2024	TOTAL CYBERCRIME DOMAINS REPORTED 2023
1	3	GoDaddy	65,666,123	857,704	285,945
2	1	NameCheap	17,371,563	580,778	686,221
3	9	Gname	5,037,707	559,075	90,713
4	4	NameSilo	4,591,413	522,322	291,103
5	10	Dynadot	4,080,535	371,722	77,391
6	5	GMO d/b/a Onamae	5,708,225	349,719	268,644

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 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. The top 5 TLD registrars with at least 25,000 maliciously registered domains reported for serving as resources for cybercrime activity were:

2024 RANK	2023 RANK	gTLD & ccTLD REGISTRARS	CYBERCRIME DOMAINS	DOMAINS DETERMINED TO BE MALICIOUS REGISTRATIONS	PERCENTAGE MALICIOUS DOMAINS
1	4	GoDaddy	857,704	604,880	70.5%
2	9	Gname	559,075	358,716	64.2%
3	2	NameSilo	522,322	316,633	60.6%
4	14	Dynadot	371,722	287,133	77.2%
5	1	NameCheap	580,778	269,984	46.5%

The following table shows those registrars with at least 50,000 cybercrime domains during the September 2023 to August 2024 study period with at least 80% of those domains registered purposely to abet cybercrime.

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

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

2024 RANK	2023 RANK	gTLD & ccTLD REGISTRARS	CYBERCRIME DOMAINS	DOMAINS DETERMINED TO BE MALICIOUS REGISTRATIONS	PERCENTAGE MALICIOUS DOMAINS
1	-	Key-Systems	88,168	86,555	98.2%
2	-	Wild West Domains	54,488	46,663	85.6%
3	-	Spaceship	109,742	93,859	85.5%
4	-	URL Solutions	199,003	167,116	84.0%
5	14	Web Commerce	86,384	61,587	82.5%

These top registrars represent just the tip of an iceberg: from our data, considering registrars with at least 25 cybercrime domains, we determined that 89 registrars had at least 60% of their domain names registered maliciously. 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 – botnets and Ransomware or Phishing as a Service (RAAS, PhAAS) – particularly benefit from the ability to use bulk registration services offered by domain name registrars.

For this study, we searched for characteristics of bulk registration behavior among domains already identified as associated with 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 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 examine domain names that have already been identified as resources for cybercrimes, so any suggested or supposed reason for a legitimate person or legal entity to register tens, hundreds, or thousands of domains in a matter of minutes falls outside the scope of this report. Yet cybercriminals are provided with easy access to these resources through bulk registration practices, which they have exploited year after year. The domain name system was never intended to supply criminals with thousands of domains in this manner.

We found evidence that points to bulk domain registration of domain names in 360 registrars. We associated 2,656,228 domain names with bulk domain registration

We associated 2,656,228 domain names with bulk domain registration behavior

behavior. These occurred in 56,591 sets. The largest set was 17,687 cybercrime domain names registered at GMO d/b/a Onamae in an eight-hour period on 19 February 2024. There were two sets of over 10,000 cybercrime domain names each registered within less than three hours at Alibaba Cloud Computing in September and November 2023.

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

REGISTRATION TIME SPAN (UTC)	BULK DOMAINS	REGISTRAR	SAMPLE CYBERCRIME DOMAINS
2/19/2024 03:48 - 11:35	17,687	GMO d/b/a Onamae.com	hqkzmsi.lol nlaxbwt.d.lol xohxkvb.i.lol nzyaxjf.lol wpimhcl.lol gqrwxeb.lol hznsttlm.lol ozztavmv.lol wifthlsu.lol ownnubyw.lol gneoazzwz.lol ioszozla.lol
9/20/2023 10:50 - 13:26	13,796	Alibaba Cloud Computing	chesuyi.cn adhzu.cn flema.cn adlra.cn adndv.cn afhvn.cn afhti.cn cckqpi.cn agiti.cn cqcdjd.cn yisuixin.cn agqii.cn edfmdt.cn ycsjjqr.cn
11/12/2023 14:10 - 16:53	12,732	Alibaba Cloud Computing	otgqlhs.cn ougtwjb.cn pdrodwc.cn piyjuee.cn otthzcf.cn uulzmzt.cn uqazqnr.cn vaymsuh.cn uuocmwy.cn uuhxtaw.cn veflkmd.cn vemluqr.cn
8/22/2024 07:36 - 11:48	9,885	GMO d/b/a Onamae.com	college-mwiz.xyz rbmgls-small.xyz fxiucd-direction.xyz drai-discussion.xyz kqrf-attention.xyz weah-news.xyz rielac.com iogmti-force.xyz order-yhkmfo.xyz zxfiy-school.xyz qvlso-six.xyz usuij-rest.xyz
9/18/2023 04:02 - 07:35	8,827	July Name	limls.net lexiom.net llpl.net lmey.net mahko.net matanca.net megye.net mengfei.net mfarltd.net mfhv.net mfyp.net midten.net
9/19/2023 00:03 - 03:00	8,418	Alibaba Cloud Computing	gzrao.cn gxhzu.cn gxmuc.cn gxpww.cn gxqin.cn fjxxv.cn gxnou.cn fjppa.cn gxfca.cn gxphm.cn fjklo.cn fjpge.cn

Over 2.6 million domains exhibited characteristics of malicious bulk domain registration behavior, a 106% year over year increase

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

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

REGISTRATION TIME SPAN (UTC)	REGISTRAR	SAMPLE CYBERCRIME DOMAINS	
4/29/2024 14:21 – 5/14/2024 12:15	NameSilo	uspsmypackage-1.xyz uspsmypackage-2.xyz uspsmypackage-3.xyz ...	uspsmypackage-38.xyz uspsmypackage-39.xyz uspsmypackage-40.xyz
5/9/2024 20:49 – 20:49	Sav.com	appleofficial-icloud.info appleofficial-cloud.info appleofficial-lcloud.info appleofficial-icloud.info appleofficial-cloud.info appleofficial-cloud.info appleofficial-lcloud.info	appleofficial-icloud.info appleofficial-lcloud.info appleofficial-cloud.info appleofficial-icloud.info appleofficial-lcloud.info appleinc-live.com
11/12/2023 14:10 – 16:53	Gname.com	googleopdqa.xyz googleopded.xyz googleopdws.xyz googleopdcv.xyz googleopdtg.xyz, googleopdgh.xyz googleopdas.xyz googleopdui.xyz	googleopdty.xyz googleopdqw.xyz googleopdbn.xyz googleopdop.xyz googleopddf.xyz googleopdlz.xyz googleplmjy.xyz googleplmcs.xyz

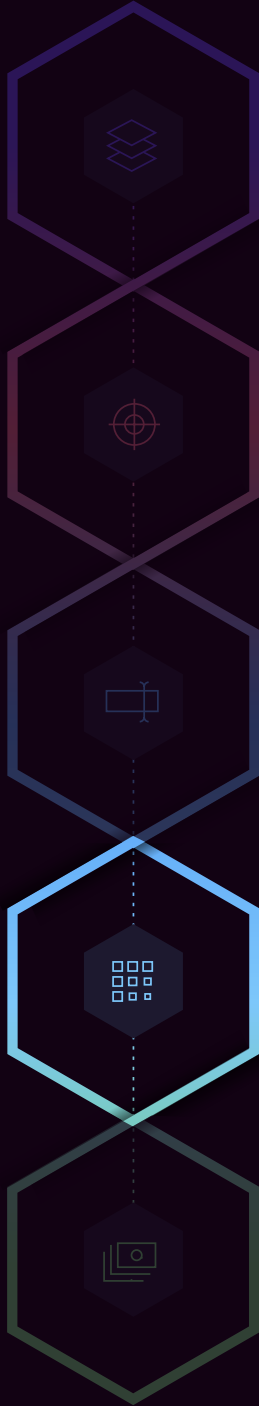
We identified four registrars where more than three-quarters of the domains reported as resources for cybercrime activity were associated with a bulk registration:

2024 RANK	2023 RANK	REGISTRAR	IANA ID	DOMAINS ASSOCIATED WITH BULK DOMAIN REGISTRATION	PERCENTAGE CYBERCRIME DOMAINS REPORTED
1	-	Name SRS	638	129	136%
2	-	Beijing Zhuoyue Shengming	1914	638	99%
3	-	Chengdu Fly-Digital	1605	256	84%
4	46	Hongkong Kouming	3972	13,857	77%

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

2024 RANK	2023 RANK	gTLD REGISTRAR	IANA ID	DOMAINS ASSOCIATED WITH BULK DOMAIN REGISTRATION	CYBERCRIME DOMAINS REPORTED
1	4	GoDaddy	146	387,028	857,704
2	1	NameCheap	1068	310,879	580,778
3	6	Gname	1923	250,619	559,075
4	3	NameSilo	1479	243,717	522,322
5	2	GMO d/b/a Onamae	49	199,610	349,719

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



01
Attack Kits

02
Attack Targets

03
Naming Resources

04
Hosting Resources

05
Cashing Out

Hosting Resources

Attack kits 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.

Attackers need a place to host their fake web sites or malware payloads, or to operate spam mail services. These hosting resources are typically identified by their IPv4 addresses. To acquire hosting, cybercriminals have compromised cloud accounts, servers, or devices. They gain administrative control over web or other system services.

Cybercrime Activity Across Hosting Networks (ASNs)

We studied where cybercrime activity was hosted and where unsolicited messaging associated with cybercrime originated, to identify hosting providers that criminals find attractive or exploit. We collected the IP addresses (DNS A records) to which cybercrime 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.

We found cybercrime activity in 28,114 hosting networks (ASNs). **While the number of hosting networks decreased (by 9%), the number of IPv4 addresses reported for hosting cybercrime activity increased more than 30% year over year, from 3,864,207 to 5,068,799.**

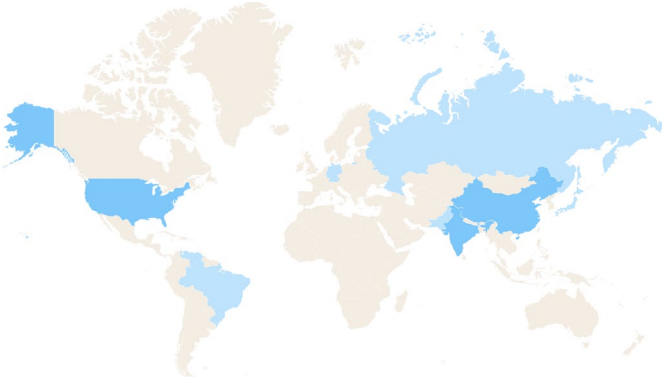
The number of IPv4 addresses reported for hosting cybercrime activity increased 30% year over year

Here we show those hosting providers with more than 90,000 unique IPv4 addresses. The complete Top 20 list of hosting providers can be found at the [Cybercrime Information Center](#).

2024 RANK	2023 RANK	HOSTING PROVIDER	COUNTRY	IPv4 ADDRESSES IN ASN	UNIQUE CYBERCRIME IPv4 ADDRESSES REPORTED 2024	UNIQUE CYBERCRIME IPv4 ADDRESSES REPORTED 2023	% CHANGE
1	3	Bharat Sanchar Nigam (AS9829)	India	11,869,696	567,977	179,952	+ 216%
2	1	ChinaNet Backbone (AS4134)	China	121,083,904	473,445	362,403	+ 31%
3	2	China169 Backbone (AS4837)	China	58,530,816	288,137	233,924	+ 23%
4	4	Digital Ocean (AS14061)	United States	2,960,128	116,444	128,365	- 9%
5	7	Amazon AES (AS14618)	United States	17,135,616	90,981	64,955	+ 40%

In 2024, India’s Bharat Sanchar Nigam (AS9829) was the hosting network with the most IPv4 addresses reported for hosting cybercrime activities, a 216% increase over our 2023 finding. China’s ChinaNet Backbone (AS4134) and China169 Backbone (AS4837) and the United States’s Digital Ocean (AS14061) and Amazon AES (AS14618) completed the top 5.

In our 2023 study, the United States as a country had the most IPv4 addresses reported for serving as resources for cybercrime activity. China, India, Australia, and Hong Kong rounded out the top 5. The Russian Federation, Great Britain, and three European countries (France, Germany, and Brazil) completed the top 10.



In 2024, the **United States (984,968)**, **China (958,744)**, and **India (729,642)** again ranked the top 3, followed by Brazil, the Russian Federation, Hong Kong, Venezuela, Japan, Germany, and Pakistan. The United States, China, and India accounted for nearly ¾ of the IPv4 addresses reported against the Top Ten. Among the Top Ten, the countries that experienced the largest increases were Venezuela (298%) and Japan (161%).

Worldwide, the United States, China, and India again had the most IPv4 addresses reported for serving as resources for cybercrime activity.

- IPv4 addresses reported for cybercrime activity in the United States decreased from 1,030,019 to 984,968 year over year but remained the highest among all countries in our study data.
- China saw the largest numeric increase, from 492,932 to 958,744.
- India’s reported IPv4 addresses doubled, from 365,143 to 729,642.

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

COUNTRY	IPv4 ADDRESSES 2024	IPv4 ADDRESSES 2023	% CHANGE YEAR OVER YEAR
United States	984,968	1,030,019	- 4%
China	958,744	492,932	+ 94%
India	729,642	365,143	+100%
Brazil	181,987	182,975	- 1%
Russia	159,024	157,922	+ 1%
Hong Kong	153,023	120,072	+ 27%
Venezuela	123,975	31,160	+ 298%
Japan	122,627	47,003	+ 161%
Germany	100,205	122,659	- 18%
Pakistan	99,664	51,908	+ 92%

Abuse of Subdomain Providers for Cybercrime

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 subdomain 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

Over 1.18 million subdomain hostnames served as resources for cybercrime attacks, a 114% increase over our 2023 study period

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. cybercriminals generally and phishers in particular to launch large numbers of attacks, and to abuse these services repeatedly and at scale. Interisle's recent Phishing Landscape 2024 study provides a case study of such large-scale abuse of a subdomain provider.

7.2% of all cybercrime attacks in our study data were hosted at subdomain providers. More than half of these took advantage of services operated by Google, Inc., using services such as Blogspot. 30% of cybercrime attacks hosted at subdomain providers were perpetrated from maliciously acquired subdomain provider hostnames.

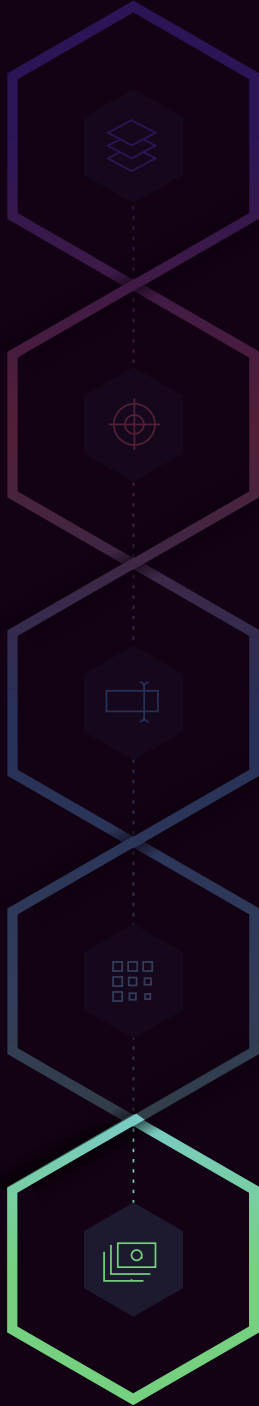
The subdomain providers with the largest numbers of hostnames reported (with a minimum of 75,000 reports) were:

2024 RANK	2023 RANK	SUBDOMAIN PROVIDER	TOTAL CYBERCRIME HOST NAMES REPORTED	COUNT OF PROVIDER'S UNIQUE DOMAINS REPORTED
1	1	Google	649,485	76
2	3	CentralNIC	100,491	16
3	5	Cloudflare	90,024	3
4	4	Weebly	84,449	2

Cyberattacks hosted at subdomain provider services are hard to mitigate. Since the subdomain providers are responsible for their naming, addressing, and content hosting, only they can 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 subdomain providers offer free or cheap services, and many permit anonymous registration; thus, they have limited resources to spend on security controls, and often cannot respond to complaints that request customer contact information.

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

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



01
Attack Kits

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 a first of a series of transactions that convert or “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 a 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

Cybercrime is a profitable, growing business that wields devastating impacts on individuals, institutions, and economies at large year after year while continuing to enrich the criminals that perpetrate it. Like any other business, criminals assemble resources to conduct their business and do so from across both the legitimate and dark economies. As shown in this report, the intersections between cybercriminal enterprises and the legitimate economy are numerous and their resource acquisition behavior and strategies are highly observable.

Cybercriminals rely on numerous industries in the legitimate economy to perpetrate crimes. Many of these industries are aware yet permissive of how their products, services, and platforms are used in the perpetration of cybercrime. While opportunities exist to make criminal access to resources across the supply chain more difficult or costly to acquire, several of the more obvious opportunities to disrupt cybercrime have not been acknowledged or address in a uniform and formal manner.

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

We advocate for balanced policies that will make it harder for criminals to obtain and use domain names, while keeping it easy for law-abiding, legitimate registrants and content publishers 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. Implement Bulk Domain Name Registration Requirements

Bulk registration is one of the most egregious domain name acquisition techniques used by criminals. Our analysis found that nearly half of all domain names reported for malware, phishing, or spam were registered in bulk by criminals who routinely registering hundreds and thousands of domains over the course of a few hours.

Registrants requiring bulk registration 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. The U.S. registrar GoDaddy, for example has implemented an [account verification system for domain auctions](#) that could be applied with great effect to mitigate bulk registration misuse.

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

2. Limit High Volume Account Creation

The use of subdomain providers by criminals for phishing attacks (e.g., <subdomain>.blogspot.com) has grown remarkably. This year, we found over 1.18 million instances of subdomain use in the three cybercrimes we measured – a 114% increase over last year’s analysis. Many of these services allow the creation of large numbers of accounts at one time, which is highly exploited by criminals.

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

Similarly, other industries that provide resources in the cybercrime supply chain (such as public repositories and financial institutions) should ensure their systems protect against abusive account registration activity.

3. Deploy Automated Systems to Screen for Suspicious Resource Behavior

Cybercriminals often exhibit identifiable patterns of suspicious registration behavior. All name resource providers should screen registration transactions for names matching known brands, for names that are deceptively similar to known brands, and for algorithmically generated names. If a string contains a known brand, and the registrant is not the brand owner, the registration request should be delayed until it can be investigated further.

Automated monitoring technology (such as the EURid APEWS) should be uniformly and formally implemented across the name resources industries. All name resource operators should make use of one or more cybercrime reporting services or data sources to determine what domains have been registered by their customers and to check for other suspicious domains their customers may have registered. Registrars and registry operators should suspend the entire portfolio of domains of newly

discovered criminal activity and their associated accounts. Similarly, hosting operators should adopt equivalent measures to suspend suspicious accounts in a timely way. Public code repositories and other platforms where attack kits and resources are distributed should also more actively monitor their systems for criminal abuse and relevant violations of terms of service and suspend suspicious accounts.

4. Offer Trusted Reporter Programs

“Trusted reporters” or “trusted flaggers” are companies or organizations that are skilled at finding and documenting abuse and have proven that they have low false-positive rates. 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.

Trusted reporter programs that facilitate the swift suspension of cybercrime resources identified by recognized and trusted cybercrime monitors should be created and/or strengthened across companies and organizations that offer resources used in the Cybercrime Supply Chain. Customer contact data should also be made readily accessible to law enforcement, public safety, and trusted private sector cyberattack responders.

5. Require Corrective Action

Every quarter we measure and analyze cybercrime activity taking place across domain name registries, domain registrars, subdomain providers, and hosting operators. Year after year, our research finds a high level of consistency in the operators that are most commonly 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.

6. Enhance 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 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 and assistance to implement practical solutions to resource abuse, especially where industries in certain geographies 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 led 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.

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

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

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