CyberProof®
A UST Company

CYBER THREAT INTELLIGENCE (CTI)
RESEARCH REPORT

A Deep Dive into Attacker-Controlled Infrastructures

OCTOBER 2022

CyberProof®
A UST Company

Table of Contents

Introduction

This report provides key insights from the CyberProof Cyber Threat Intelligence (CTI) team – which were obtained by evaluating numerous malicious network infrastructures and IOCs during the first half of 2022.

The CyberProof CTI team continuously tracks developments in the cyber threat landscape, including major malware and ransomware operations, evasive phishing techniques, and critical vulnerabilities and exploits. This coverage also focuses on the collection, active exposure, and validation of Indicators of Compromise (IOCs) and Indicators of Attack (IOAs) associated with malicious activities. These indicators are utilized to develop optimal detection, response and prevention capabilities for CyberProof's clients.

> The Russia-Ukraine conflict had a significant impact on the threat landscape during this period – which is reflected clearly in CyberProof's CTI data and statistics.

The media coverage that surrounded the conflict worldwide lead many countries and organizations to choose sides, which meant that many banned services associated with Russia. The complex situation led both pro-Ukrainian and pro-Russian hacktivists to take steps, for ideological reasons, which resulted in extensive cyber-attacks in both countries as well as in other areas around the globe.

We were able to uncover some noteworthy discoveries by focusing on the Russia-Ukraine conflict and correlating it with data and statistics, while maintaining a broader point of view. These discoveries provide a greater understanding of recent trends in the cyber threat landscape and how to protect your organization against them, including:

- Attackers' preferences regarding network infrastructures
- Attackers' perceptions of how security teams think
- How global events such as the Russia-Ukraine conflict can impact the cyber threat landscape

Attacker Behavior & Notable Trends

Here are some key insights gleaned by the CyberProof CTI team about the behavior patterns of malicious actors:

- **Hacker preferences:** Malicious actors always prefer to use services, infrastructures, providers,or geolocations that:
  - Enable them to act freely and anonymously
  - Involve minimal legal intervention
  - Don't involve significant expense
- **Geolocation bans:** Although many cyber-attacks were executed by pro-Russian attackers during the Russia-Ukraine conflict in the first half of 2022, Russia holds the seventh place in terms of geolocation associated with malicious activity. This suggests that Russian and other threat actors bypassed the geolocation bans by operating via VPNs or proxies from other geolocations, such as:
  - **China** is in the first place, regarding its association with malicious IP addresses. It is possible that China did not use the necessary enforcements to block Russian and other attackers from leveraging Chinese infrastructure in attacks against global targets. This assumption is supported by the fact that Russia-related malware like SolarMarker operated from Chinese state-owned Autonomous System Numbers (ASNs) during the first half of 2022.
  - **The United States** is in the second place, regarding its association with malicious IP addresses. The US was targeted extensively in pro-Russian attacks during the first half of 2022. Operating from the US might have enabled Russian attackers to operate more freely, particularly against American targets, without triggering security alerts for traffic from suspicious geolocations.
- **Malicious .ru domains:** Russia was targeted by pro-Ukraine attackers during the first half of 2022. This is supported by the high volume of malicious domains that contained the .ru country code top-level domain (ccTLD). This might imply (1) the targeting of Russian-speaking users, (2) the compromise of .ru domains for malicious activities, or (3) the minimal legal intervention against malicious .ru domains; many domain registrars banned registration of .ru domains during the conflict, and those who supported registration did not apply enough enforcements.
- **Chinese-owned ASNs:** Two of the top three ASNs that were most reported as being associated with malicious IP addresses, are owned by the Chinese-state government.

- **URL extensions:** Phishing and credential-harvesting related URL extensions such as PHP and HTML were more prevalent than macro-enabled Office documents in malicious URLs. This shift by attackers is likely related to Microsoft's announcement that they will start blocking Office macros from the internet by default.
- **Compromising WordPress sites:** Attackers consistently compromised legitimate WordPress websites during the first half of 2022, i.e., by planting malicious payloads without being detected. WordPress is an extensively targeted CMS that poses fertile ground for abuse.
- **Abusing DuckDNS:** The legitimate, dynamic DNS service DuckDNS was abused extensively by attackers. It was used to distribute malicious payloads while remaining under the radar. Other legitimate storage services such as Google Firebase Storage were also extensively misused for malicious activities.

The following sections provide a deeper analysis that help explain some of the malicious IOCs used in the first half of 2022.

Malicious IP Addresses

Attackers may use malicious IP addresses in the following ways:

- **Servers and IP addresses** are not only fundamental to how the Internet operates; they are also fundamental to all cyber-attacks. Attackers usually purchase net-ranges and/or IP addresses from legitimate hosting providers and abuse them during an attack, mostly as Command & Control (C&C) servers or nodes in malicious network infrastructure – as well as for malware distribution via malicious phishing domains.
- **Legitimate servers** also are consistently compromised by malicious actors. A type of malware known as a botnet abuses these types of compromised servers – for port and vulnerability scanning, the execution of exploit codes, and spam and phishing email distribution – to enlarge the botnet's scope and impact.
- L**egitimate VPN and proxy service providers** are often leveraged by malicious actors as part of their attacks to evade detection and conceal the actual origin of the attacks.

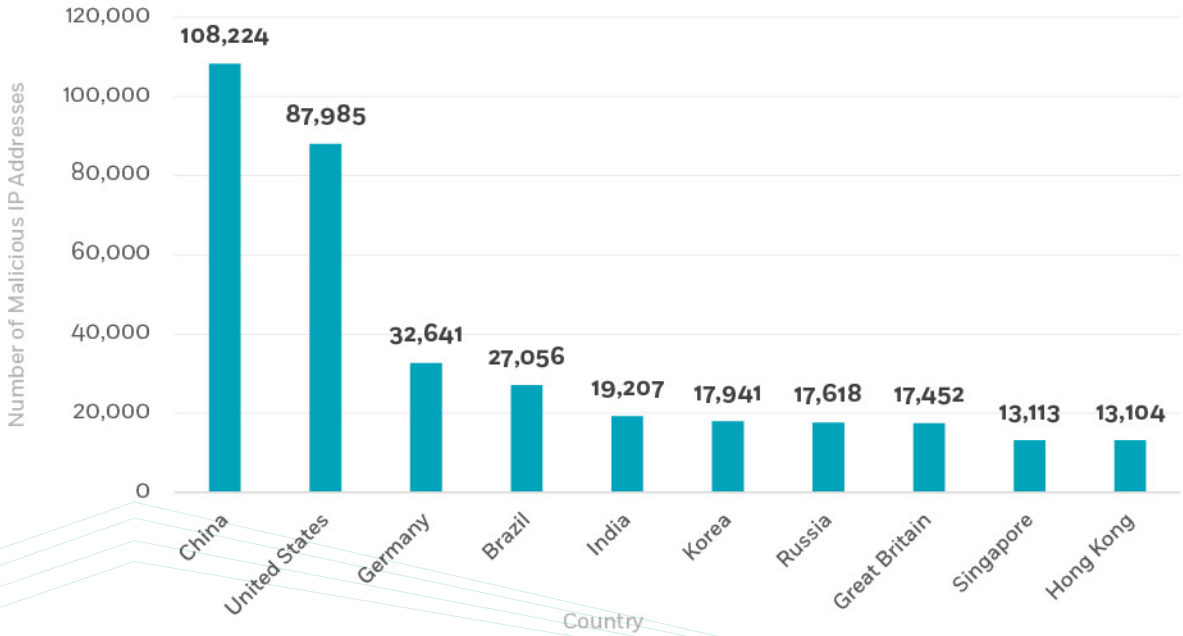
Top 10 Reported Geolocations

One possible method of identifying suspected malicious activity is based on identifying its geolocation of origin. This method relies on several assumptions regarding the perceptions of attackers:

- Attackers often perform malicious activities from countries that do not have proper cybersecurity enforcements and active legal intervention, thus providing fertile ground for executing malicious tasks without their being detected or prevented.
- Attackers prefer operating through systems and countries that have a high volume of both legitimate and malicious web traffic – i.e., where they can conceal malicious operations behind other traffic. Examples of such countries are China and the United States.
- Attackers usually prefer operating in the same countries as the organizations they are targeting. Attackers are aware that security teams are looking for suspicious access logs from countries that are not connected to the organization. For example, when targeting an organization located in the United States, attackers prefer using a North American IP address that will look legitimate in the access logs.
- Attackers might operate from other geolocations to spoof other APTs and create diplomatic crises and complex political situations at the government level.

The following is a breakdown of countries that had the highest number of malicious IP addresses reported in the first half of 2022:

Top 10 Geolocations of Malicious IP Addresses



China is in first place, providing hosting services for 19.73% of the reported IP addresses, followed by the US (16.04%), Germany (5.95%), Brazil (4.93%), and India (3.5%).

Analysis of Russia's Ranking

It is surprising that Russia is only in seventh place, since Russia is known as the source of many cyber-attacks from cyber criminals and state-sponsored APTs, especially during the Russia-Ukraine cyber warfare.

A possible explanation relates to the legal intervention of countries and organizations during Russia-Ukraine conflict. Many countries and organizations condemned Russian war crimes and started banning and blocking access to services for Russian users. It makes sense that Russian attackers bypassed these bans by operating from other geolocations.

Top 10 Reported ASNs

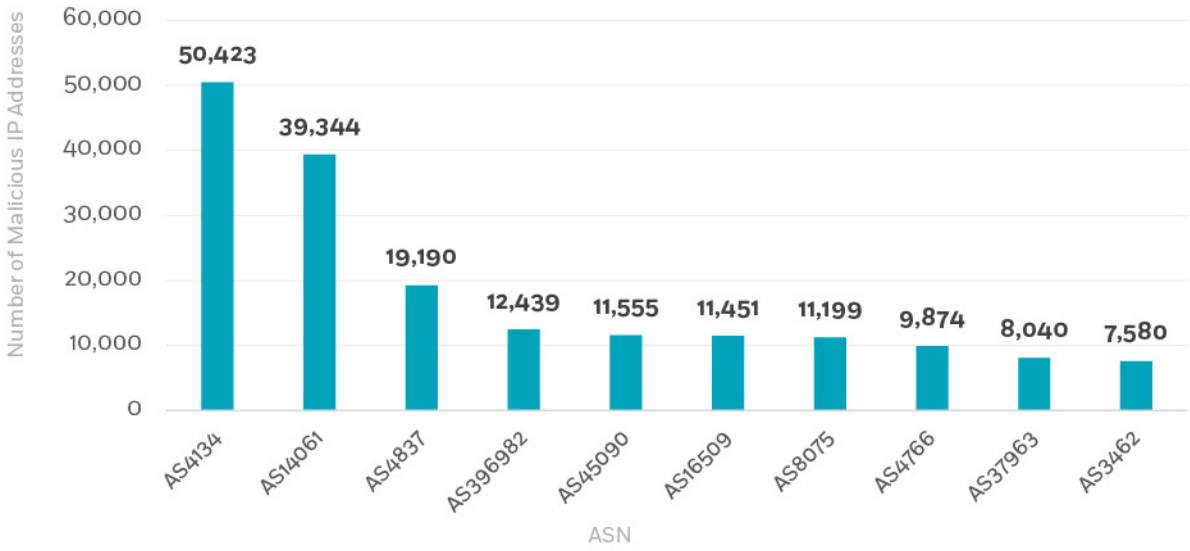
Below is a breakdown of the ASNs associated with the highest number of malicious IP addresses during the first half of 2022.

In layman's terms, an Autonomous System (AS) is a set of Internet routable IP prefixes belonging to a network or a collection of networks that are managed, controlled and supervised by a single entity or organization.

The breakdown below is an indication of which network providers are most favored by malicious actors:

	Organization	AS Name	ASN	Main Location
1	ChinaNet (China Telecom)	CHINANET-BACKBONE	AS4134	China
2	DigitalOcean, LLC	DIGITALOCEAN-ASN	AS14061	United States
3	CHINA UNICOM	CHINA169-Backbone	AS4837	China
4	Google LLC	GOOGLE-CLOUD-PLATFORM	AS396982	United States
5	Shenzhen Tencent Computer Systems Company Limited	TENCENT-NET-AP	AS45090	China
6	Amazon.com, Inc.	AMAZON-02	AS16509	United States
7	Microsoft Corporation	MICROSOFT-CORP-MSN-AS-BLOCK	AS8075	United States
8	KT Corporation (formerly Korea Telecom)	KIXS-AS-KR	AS4766	South Korea
9	Hangzhou Alibaba Advertising Co. Ltd.	ALIBABA-CN-NET	AS37963	China
10	Chunghwa Telecom Co., Ltd.	HINET	AS3462	Taiwan

Top 10 ASNS Associated with Malicious IP Addresses



Key Takeaways

Here are some key points that the CTI team was able to establish based on this research:

- **Two out of the top three malicious ASNs (AS4134 and AS4837) are owned by the Chinese state government.**
- AS4134 is in first place, hosting 9.22% of the reported IP addresses, followed by AS14061 (7.2%), AS4837 (3.51%), AS396982 (2.27%), and AS45090 (2.11%).
- The most frequently observed ASN, AS4134, is owned by ChinaNet (China Telecom) - a Chinese state-owned telecommunication company that hosts around 110 million IP addresses. Multiple IP addresses under AS4134 were reported to be involved in malicious activities during the first half of 2022, including:
  - Port and vulnerability scanning
  - Various phishing and squatting campaigns
  - Malware distribution
  - Cyber-espionage operations of Chinese APTs (LuoYu hacking group)
- During the first half of 2022, the AS4134 and AS4837 (both Chinese ASNs) were associated with several types of known Chinese malware such as WinDealer and CosmicStrand, but also with a remote access trojan (RAT) named SolarMarker - which is known to be operated by Russian threat actors. **The fact that Russian operators leveraged Chinese ASNs for malware operations strengthens the hypothesis that Russian attackers may have shifted into operating from other geolocations like China, due the global ban against the Russian war crimes in Ukraine.**

- Many security agencies like CISA released security advisories throughout the Russia-Ukraine conflict, warning western organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. The Russian attacks that were observed include distributed denial-of-service (DDoS) and data-wiping attacks against organizations and individuals worldwide.
- The high number of North American ASNs in the above table could be due to attackers preferring to operate in the same countries as the organizations they are targeting, as well as to cover their tracks and increase the likelihood of success. This assumption is supported by the insight that Russian data wipers that attacked both Ukraine and the US were operated and controlled using C&C servers located in the US.
- Attackers seem to prefer to use reputable hosting providers and ASNs within the United States (DigitalOcean, Google, and Amazon), apparently to prevent security teams from identifying malicious activities and to block/monitor such large and active network infrastructures.

Malicious Domains

Domains are web entities hosted on servers (IP addresses) and are often used to host websites and web pages. Almost any Internet user accesses domains and websites as part of their daily routine - when surfing online over the HTTP/S protocols.

The fact that domains are so prevalent provides an opportunity for abuse by malicious actors:

- **Attackers consistently compromise legitimate, unsecured domains** and bundle them within their malicious network infrastructures - mainly to host phishing web pages, deliver malicious payloads, or evade security detection by leveraging the legitimate reputation of the domains.
- **Attackers also purchase malicious domains directly from domain registrars** and certain hosting providers. They look for opportunities to make cheap, easy, and anonymous purchases, for domains with low records of active intervention or takedown possibilities.

[1] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

Top 10 TLDs in Malicious Domains

Top-Level Domain (TLD) refers to a part of the domain name infrastructure, and it plays a crucial role in how Domain Name System (DNS) protocol works. In simple words, TLDs are related to the second phase in the DNS hierarchy. They are used to detect the relevant DNS records of a given domain in web requests sent over the Internet.

TLDs can be divided into two main categories:

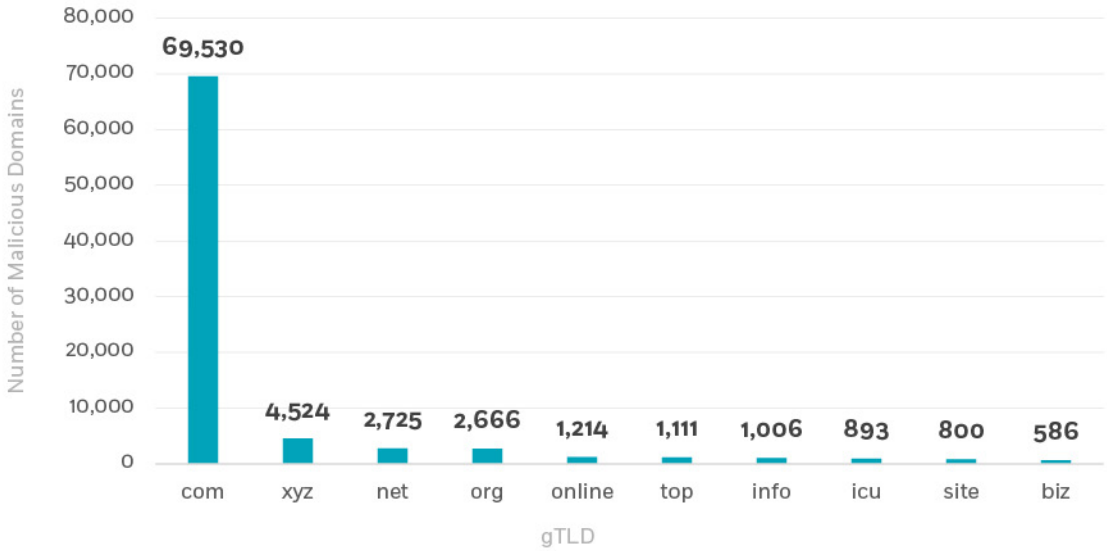
- **Generic TLD (gTLD) –** represents the purpose of a domain, such as .com, .org, .net, etc.
- **Country-code TLD (ccTLD) –** represents a specific country associated with the domain and/or the website content, including ru (Russia), cn (China), su (Soviet Union), etc.

The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization responsible for managing the Domain Name System (DNS) and enforcing related policies - assigning both gTLDs and ccTLDs.

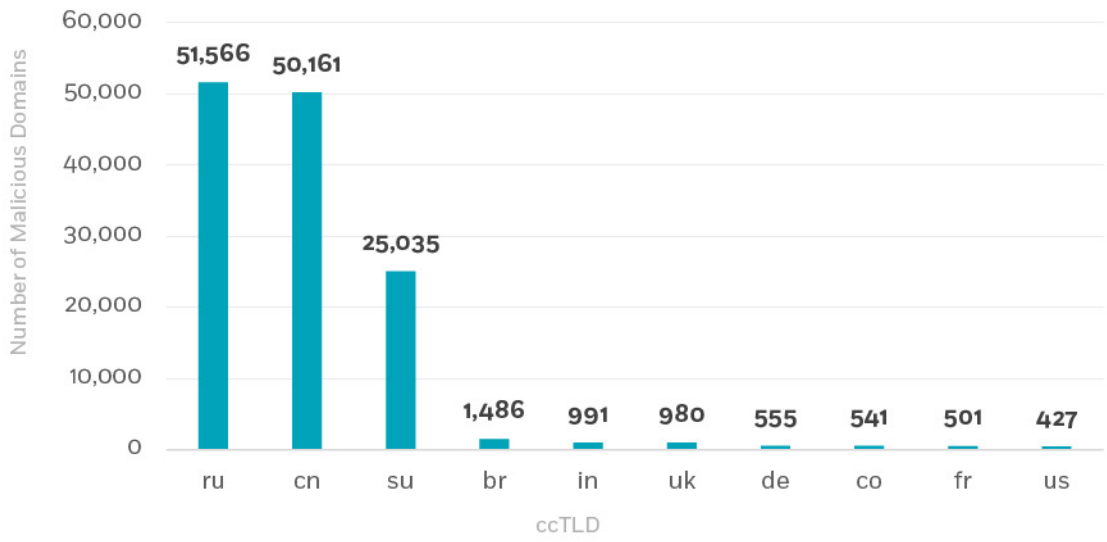
The actual price of a domain name is affected by the chosen TLD, i.e., a domain that uses a prevalent TLD such as .org will usually cost more than TLDs that are used less often, such as .online.

The following table illustrates the TLDs observed in the highest number of malicious domains:

gTLDs with Highest Rate of Malicious Domains



ccTLDs with Highest Rate of Malicious Domains



Key Takeaways

Here are some of the key points that the CTI team was able to establish based on this research:

Generic Top-Level Domains (gTLDs)

- The .com (commercial) gTLD was observed in the highest number of malicious domains (29.22%), followed by .xyz (1.9%), .net (1.15%), .org(1.1), and .online (0.5%) gTLDs.
- The .com gTLD is highly favored by threat actors since it is widely used in both corporate and private domains and cannot directly indicate a malicious activity. The .com gTLD is responsible for nearly half of all registered domains online. **While less common TLDs can be blocked or at least monitored by security teams, it is impossible to do the same on the .com gTLD due to huge rates of False Positive alerts.**
- A possible reason that the .xyz gTLD was more prevalent in malicious domains than common TLDs such as .org or .net could be its relatively low price. As previously mentioned, domains that use common TLDs usually cost more than rare ones. It is usually not the first pick of domains registrants, and is less common.

Country-code Top-Level Domains (ccTLDs)

- The .ru (Russia) ccTLD was observed in the highest number of malicious domains (29.22%), followed by .cn (21.09%), .su (10.52%), .br (0.63), and .in (0.47%) ccTLDs.
- ccTLDs are often used by search engines to determine the geolocation of a domain or website. This means that 29.22% of reported domains in the first half of 2022 were registered as if they are intended for Russian citizens or a Russian audience (ru ccTLD).
- Although the Russian ccTLD (.ru) holds the first place in relation to malicious domains, Russia holds seventh place in terms of geolocation associated with malicious IP addresses. This miscorrelation in the statistics may be explained as follows:
    - Registration of ccTLDs is subject to restrictions that prove a relation to the associated country. The nature of the restrictions differs from country to country. Perhaps the registration of .ru domains is not subject to particularly harsh registration restrictions.
    - Usually, cyber warfare between countries leads to a high volume of targeted cyber-attacks. During the first half of 2022, Russian citizens were highly targeted by pro-Ukrainian attackers in response to Russian war crimes. This could explain why many malicious domains were intended for Russian speakers. It is also possible that legitimate Russian domains were compromised and abused in attacks, and were later detected by security vendors as malicious IOCs.

Top 10 Domain Registrars

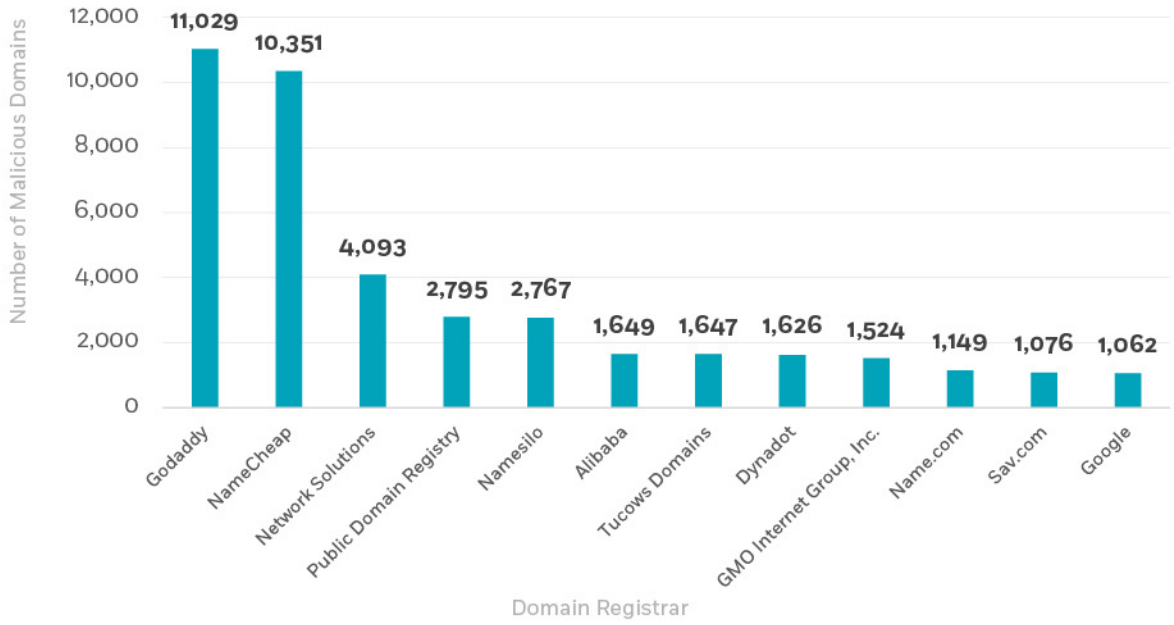
Attackers usually prefer to register malicious domains via registration entities that will enable them to operate anonymously. They can directly register malicious domains via domain registrars and hosting providers.

Another key concept in the domain registration process is WHOIS - a standard for publishing the contact and nameserver information for all registered domains. Each registrar maintains their own WHOIS service, based on ICANN's guidelines. Over the years, many registrars start providing personal data redaction on WHOIS information, in an attempt to protect registrant contact information against phishing and spam abuse. Attackers also enjoy this standard, as it enables them to register malicious domains anonymously.

The following is a breakdown of the most abused domain registrars, i.e., registrars that were associated with the highest number of malicious domains in the first half of 2022. The reported domains include:

- Legitimate domains reported as being compromised
- Domains that were directly registered by attackers for malicious tasks

Top 12 Domain Registrars Associated with Malicious Domains



Key Takeaways

Here are some key points that the CTI team was able to establish based on this research:

- GoDaddy is associated with the highest number of malicious domains (5.8%), followed by the NameCheap (5.4%), Network Solutions (2.15%), Public Domain Registry (1.47%), and NameSilo (1.45%) domain registrars.
- In the first half of 2022, there was a spike in the number of infected websites hosted on GoDaddy's managed WordPress service. **This malicious operation was attributed to a backdoor malware that apparently operated from Russia.**
- NameCheap in another popular web hosting provider that is consistently abused by malicious actors. **During the first half of 2022, this registrar was highly misused by Russian attackers against Ukrainian entities in large-scale malware operation.** Eventually, NameCheap announced that due to Russia's war crimes, it would stop providing services to all users registered in the country.

[2] https://www.wordfence.com/blog/2022/03/increase-in-malware-sightings-on-godaddy-managed-hosting/

[3] https://cert.gov.ua/article/37704

[4] https://www.namecheap.com/support/knowledgebase/article.aspx/10519/5/faq-transfer-of-russian-customers-services-from-namecheap/

Malicious URLs

Simply put, a URL is a unique address the represents a directory or file structure of a domain. As part of the DNS hierarchy and HTTP/S traffic, a domain name represents a digital space on a particular server that can be used to host websites, where URLs refer to specific resources on the domain and server, such as directories, web pages, or files of any type. URLs may also include parameters that are used to instruct the web server to retrieve specific data.

Like domains, URLs are widely utilized by threat actors to execute for various malicious tasks, including planting phishing login panels and delivering malicious payloads.

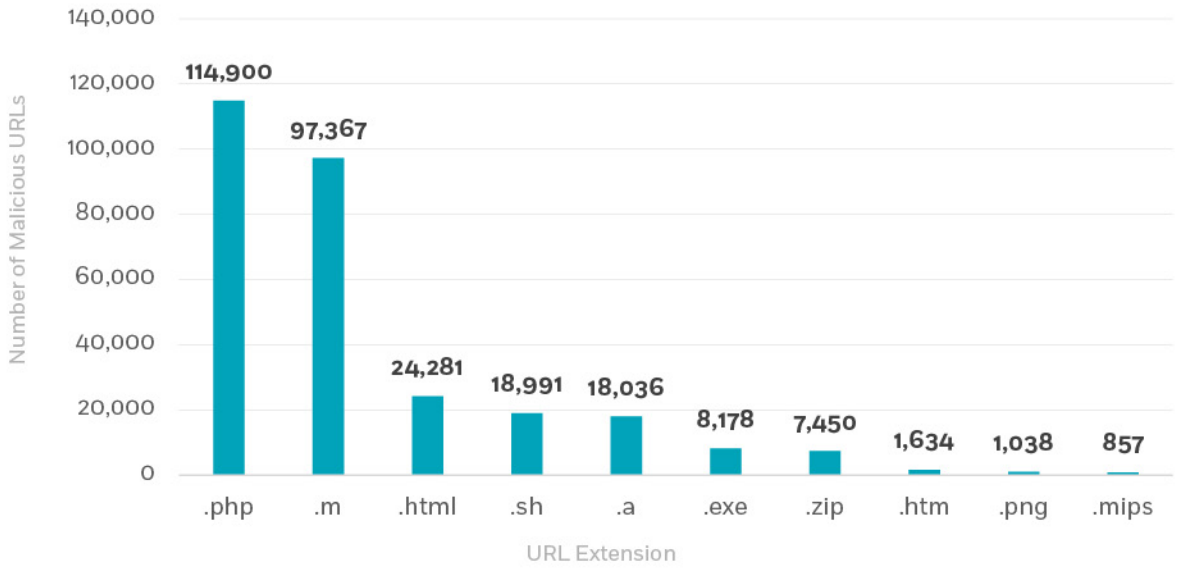
Top 10 URL Extensions

Because URLs are used to instruct web servers to present or initiate the download of certain content or files for website visitors, they are perceived by attackers as providing a great opportunity for executing malicious activities, including:

- Planting phishing web pages on compromised or malicious websites
- Distributing malware payloads
- Injecting malicious code
- Hosting malicious components and resources to create a complex network infrastructure that evades security detection

The following is a drill down of the most observed URL extensions in malicious URLs in the first half of 2022. Because URL extensions do not always represent the actual file/content type - as attackers may try to hide extensions to evade detection - the extensions listed here are the ones that are visible - both to website visitors and in security network logs.

Top 10 URL Extensions Observed in Malicious URLs



Key Takeaways

Here are some key points that the CTI team was able to establish based on this research:

- PHP, a popular programming language, is often used to develop web applications processed by a PHP engine on a web server. Since PHP files are a common part of the website structure, attackers often abuse them. PHP files are used to host malicious resources such phishing web pages (in particular, as credential-harvesting login panels); to inject and load malicious code (like JavaScript); and more. **The PHP extension was observed in 21.67% of the reported domains.**
- Another interesting insight regarding three of the most observed URL extensions is related to one of the most **active peer-to-peer (P2P) botnets – Mozi. During the first half of 2022, Mozi was observed operating aggressively to enlarge its bot army, and leveraging URLs with .m, .a, and .sh extensions to retrieve malicious ELF executables. This is a spoofing technique that is very common since it enables attackers to efficiently trick users and evade detection.**
- ZIP archives continued to be one of the most dominant ways to deliver malicious payloads in both phishing and malware campaigns. Encrypted ZIP and other archive types are efficient at evading detection, since malicious code or payloads that are stored within such encrypted files aren't scanned or discovered by security solutions.
- The PNG extension might look legitimate at first glance, but it has been widely used for C&C infrastructures of different malware types such as SOCGHOLISH and ZLOADER.

- DLL was relatively low in number. This is surprising, since DLLs are very common components of cyber-attacks. The statistics might indicate an understanding by attackers that security teams focus their efforts on detecting this highly abused file extension, and leverage advanced techniques to retrieve and execute DLLs in later phases of an attack.
- Microsoft Office related extensions such as .doc, .docx, .xls, and .xlsx were also relatively low in number, although they used to be one of the most common initial access vectors in both malware and phishing operations due to the embedded VBA Macros functionality that was extensively abused to execute malicious code. The decrease in use of this file type could be related to Microsoft's announcement during the first half of 2022 that, by default, Office will start blocking macros from the Internet. As a result, it is possible that attackers shifted to using other extensions for their malicious tasks, such as ISO and ZIP.
- Viewing the data more globally, it seems that attackers are focusing their efforts on gaining initial access to corporate networks by using fake credential-harvesting login panels, which usually are hosted on PHP or HTML-related extensions. Other attack vectors - like malicious, macro-enabled Office documents, are becoming less common.

Most Abused DNS and Cloud Storage Services

From a security perspective, a malicious domain is usually enough to indicate the potential maliciousness of URLs hosted on the domain. However, a malicious URL does not always indicate the potential maliciousness of an associated domain, since it refers only to a specific resource. For example, a malicious URL on the drive.google.com domain does not indicate that whole domain is used for malicious activities.

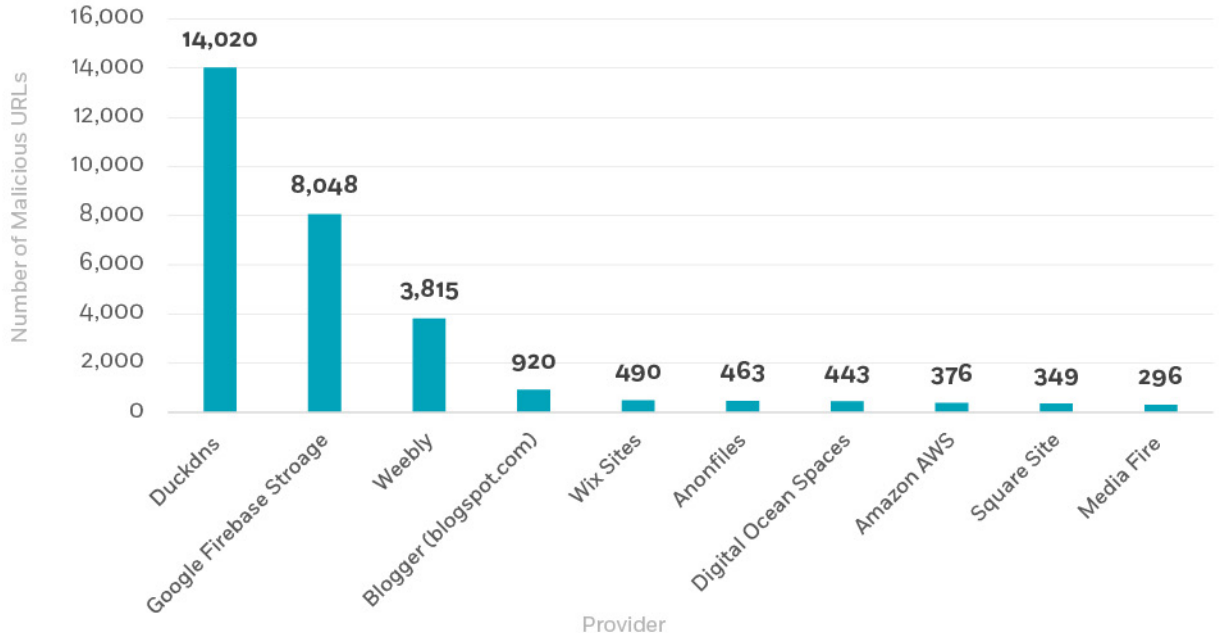
This is a key reason why URLs on legitimate domains are so favored by malicious actors. Attackers consistently abuse legitimate cloud-storage and DNS providers to host malicious payloads and infrastructure. Many providers offer users the ability to host content on their actual domains or infrastructure as subdomains or URLs. This condition makes detection and prevention efforts harder for security teams, who can't monitor or block traffic associated with these highly common, legitimate services due to possible disruption of corporate business operation and high False-Positive rates.

[5] https://www.cybereason.com/blog/threat-analysis-report-socgholish-and-zloader-from-fake-updates-and-installers-to-owning-your-systems

[6] https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

The following are the top 12 cloud storage/DNS services that were associated with the highest number of malicious URLs:

Top 10 Storage Services by Malicious URLs



Key Takeaways

- **DuckDNS** was the most abused provider. DuckDNS offers a free, dynamic DNS service that allows users to point a subdomain under the legitimate duckdns.org domain to a chosen IP address. Attackers consistently abuse this functionality to point subdomains to malicious resources. These malicious resources are challenging to detect, since not all DuckDNS-related traffic will be defined as malicious by security solutions.
- Google Firebase Storage is a Google-backed service that allows the storage of files and images in a Google cloud storage bucket. During the first half of 2022, this Google service was extensively leveraged in both phishing and malware operations to bypass email and other security solutions.
- **URLs that use the WordPress Content Management Systems (CMS) were highly observed among the malicious URLs.** WordPress is one of the most common CMS options - providing users with an easy solution to build and design websites. From a security perspective, WordPress websites may be hosted on various infrastructures and platforms, and are often maintained by actual website owners who are not always aware of the security risks. As a result, WordPress websites may become vulnerable over time and are subjected to various types of attack due to outdated software and plugins. **The vast majority of WordPress websites among the malicious URLs that were researched appeared to be legitimate WordPress websites that had been compromised.**

Conclusion

This research supports the understanding that threat actors always prefer to execute malicious tasks via services, infrastructures, providers, or geolocations that enable them to act freely and anonymously, with minimal legal intervention (or no legal intervention) – and that require a relatively low financial investment. Moreover, it is possible that the Russia-Ukraine conflict prompted many threat actors and hacktivists to take steps that were ideologically motivated. Pro-Russian attackers might have bypassed the ban against Russia by operating from other geolocations and ASNs, such as China and the US.

Organizations can use the data provided here to improve their prevention and detection capabilities, based on the scope and model of their business operations. Such protective steps could include:

- Blocking/monitoring top reported geolocations based on business location and operation models
- Bundling the top reported ASNs and domain registrars as parameters in detection/prevention rules
- Blocking/monitoring suspicious TLDs and URL extensions based on organizational business operation – particularly for commonly-used extensions such as ZIP archives can be blocked/quarantined in email gateways and released based on user demand
- Taking necessary protections against botnets, which are a highly prevalent threat

Working with a Managed Detection & Response provider offers in-house CTI services can help large-scale organizations stay on top of these changing threat trends – and prevent the kind of attack that may have a detrimental impact on the business.

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations. For more information, visit www.cyberproof.com.

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum