Top 24 Domain, IP, and DNS Intelligence Trends and Cybersecurity Statistics for 2022–2023

Posted on March 20, 2023

Aggregated domain and DNS data is a rich source of intelligence, providing security researchers, companies, and solutions with contextual information for multiple business and cyber processes, including threat detection and response, attack surface management (ASM), third-party risk management, brand protection, and identity and access management (IAM).

Over the years, WhoisXML API has conducted several cyber investigations and collated some facts and statistics from our most recent work below.

Cybersecurity Statistics Related to Threats, Malicious Campaigns, and Malware Families

We continuously scrutinize and expand lists of indicators of compromise (IoCs) involved in different malicious activities. Below are some high-level trends we noticed across threats and malicious actors.

- 60% of the IP addresses identified as IoCs and used by non-U.S.-based threat actors were geolocated in the U.S.
- Besides the U.S., the Netherlands, Japan, and Thailand were among the top geolocation countries of the IP addresses identified as IoCs and used by non-U.S.-based threat actors.
- 69% of the domains and URLs identified as IoCs and used by non-U.S.-based threat actors indicated the U.S. as their registrant country.

- Besides the U.S., Russia, China, and the Netherlands were among the top registrant countries of the domains and URLs identified as IoCs and used by non-U.S.-based threat actors.

Note: The stats above were derived from the analysis of the threats and threat actors behind the Syrian Electronic Army, Hive ransomware campaigns, BlackEnergy-enabled DDoS attacks, and the Ducktail operation. These analyses were concluded between October 2022 and February 2023.

Cybersecurity Statistics Related to Impersonation or Cybersquatting

Newly registered domains (NRDs) are commonly used for brand impersonation and phishing attacks targeting Fortune 500 companies. We looked into several cybersquatting and domain impersonation trends across industries.

- 99.04% of the NRDs containing the brand names of major financial organizations didn't have matching WHOIS records with the brands' legitimate domains.
- 97.81% of the NRDs containing the brand names of major chat apps didn't have matching WHOIS records with the brands' legitimate domains.
- 99.41% of the NRDs containing the names of the top electronic health record (EHR) software providers didn't have matching WHOIS records with the companies' legitimate domains.
- 12% of the newly added domains and subdomains possibly used to impersonate Fortune 500 companies were malicious. The remaining 88% may not have been weaponized but still shared suspicious patterns observed among the properties found malicious.
- 79% of the malicious domains impersonating Fortune 500 companies used urgency-based text strings (e.g., ***auth***, ***login***, ***pay***, ***register***, and ***update***), while 21% mimicked company departments like marketing, support, finance, and security.
- Four of the top 10 ISPs managing the IP hosts of the cybersquatting domains targeting CEOs and Fortune 500 companies were among the worst ISPs in terms of spam and botnet infection.

Note: The stats above were derived from our analyses of Gigabud RAT, destructive supply chain attacks, healthcare-related cyber attacks, malware distribution through Google search ads, and business impersonation. These analyses were concluded between July 2022 and February 2023.

Cybersecurity Statistics by Theme and Event

Our researchers also tracked the effects of certain global events and news on the DNS, particularly in terms of domain registration. Here are some of the news, themes, and events we kept an eye on.

- 13% of the tax season-related domains added in Q2 2022 were malicious.
- Holiday-related domain registrations picked up 2–3 weeks before each event's date.
- The number of NRDs containing ***Russia*** or ***Ukraine*** increased by 150% in the week following the start of the 2022 Ukraine-Russia war.
- The registration of domains containing ***Russia*** or ***Ukraine*** dropped by the thousands a month after the war started, but it still exceeded prewar levels.
- 56% of the holiday-themed domains were registered in the U.S. although they were celebrated across several countries.
- Besides the U.S., Iceland, Canada, and China were among the top registrant countries of the holiday-related domains.
- 80.5% of the IP addresses the holiday-themed domains resolved to were also geolocated in the U.S.

Note: The stats above were derived from the Domain Registration Trends Report—Q2 2022 and August 2022: DNS Highlights. These analyses were concluded between August and September 2022.

Cybersecurity Statistics of Commonly Abused TLDs

In early 2023, we profiled thousands of domains sporting the most-disreputable TLDs listed by Spamhaus in our DNS Abuse Trends white paper, and these are our key findings.

- About 64% of the domains under the most-abused TLDs had redacted WHOIS records, making threat attribution challenging if they figure in malicious campaigns.
- 67% of the IP resolutions of the NRDs under the most-abused TLDs were geolocated in the U.S.
- Besides the U.S., China, Singapore, and Germany were the most popular IP geolocations of the resolving NRDs under the most-abused TLDs.
- The U.S. was the registrant country of 28% of the NRDs under the most-abused TLDs.
- Besides the U.S., China, Iceland, and the U.K. were the most popular registrant countries of the NRDs under the most-abused TLDs.

Cybersecurity Statistics Relevant to Suspicious Bulk Domain Registration

With several threat actors leveraging the bulk domain registration features offered by registrars, we studied some of the suspicious patterns behind bulk-registered domains.

- Based on an analysis of typosquatting data feed files, more than 24% of similar-looking domains registered on a given day could be attributed to the same registrar.
- The entire domain name portfolio of threat actors can be 140 times the size of what they register in bulk on a given day.

—

We will continue leveraging our cyber threat intelligence sources to investigate threats, map out

malicious infrastructures, and track domain registration trends.

If you want to learn more about how WhoisXML API can help with your cyber processes and solutions, don't hesitate to contact us.