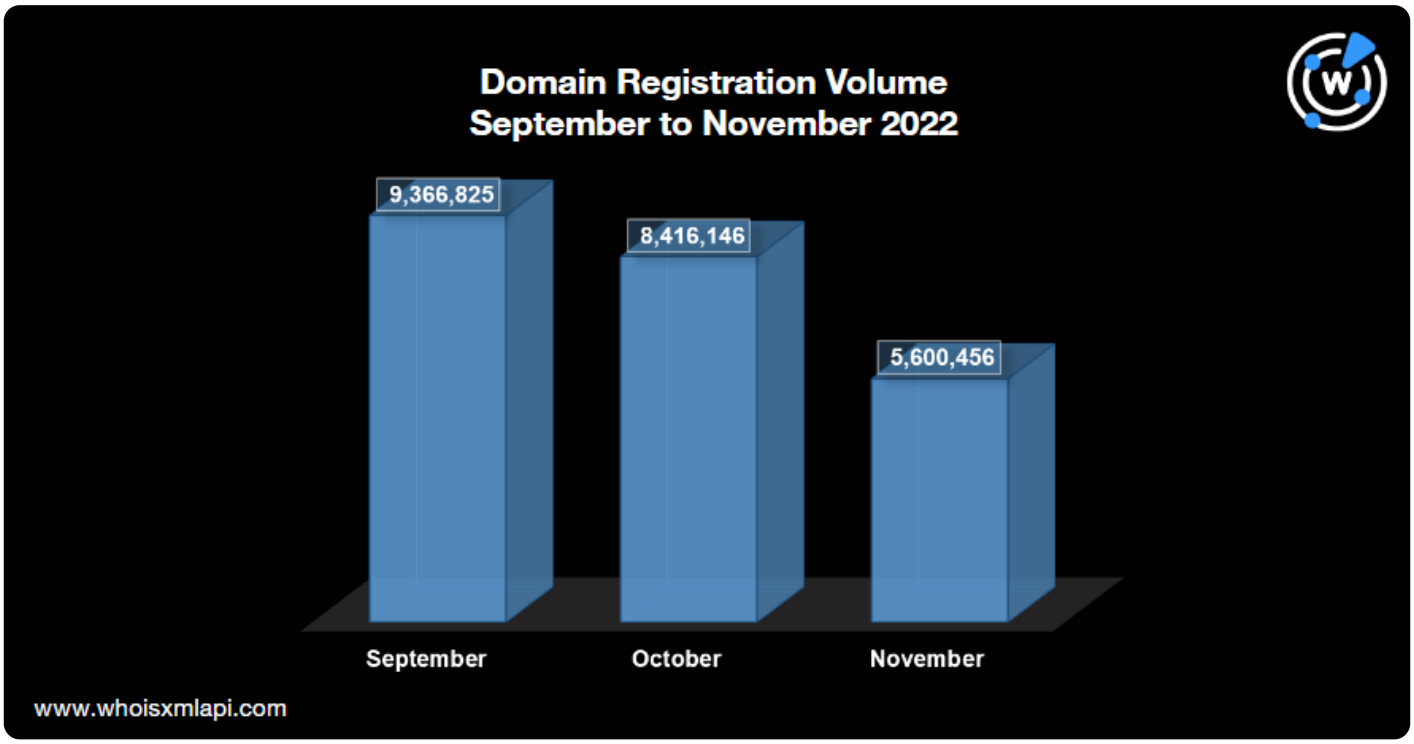
November 2022: New Domain Activity Highlights

Posted on December 12, 2022

WhoisXML API analyzed more than 5.6 million newly registered domains (NRDs) added on 1–30 November 2022 to detect trends, such as top-level domain (TLD) and text string usage. We also looked at the WHOIS data redaction status and registrar and registrant country distribution of the NRDs. Check our findings below, along with threat reports our researchers put together using domain, DNS, and IP intelligence.

Domain Registration Volume in the Past Three Months

We continued to detect a decline in the overall domain registration volume in November. From 8.4 million in October, the number decreased by about 33% the following month. The chart below shows the monthly registration volume in the past three months.

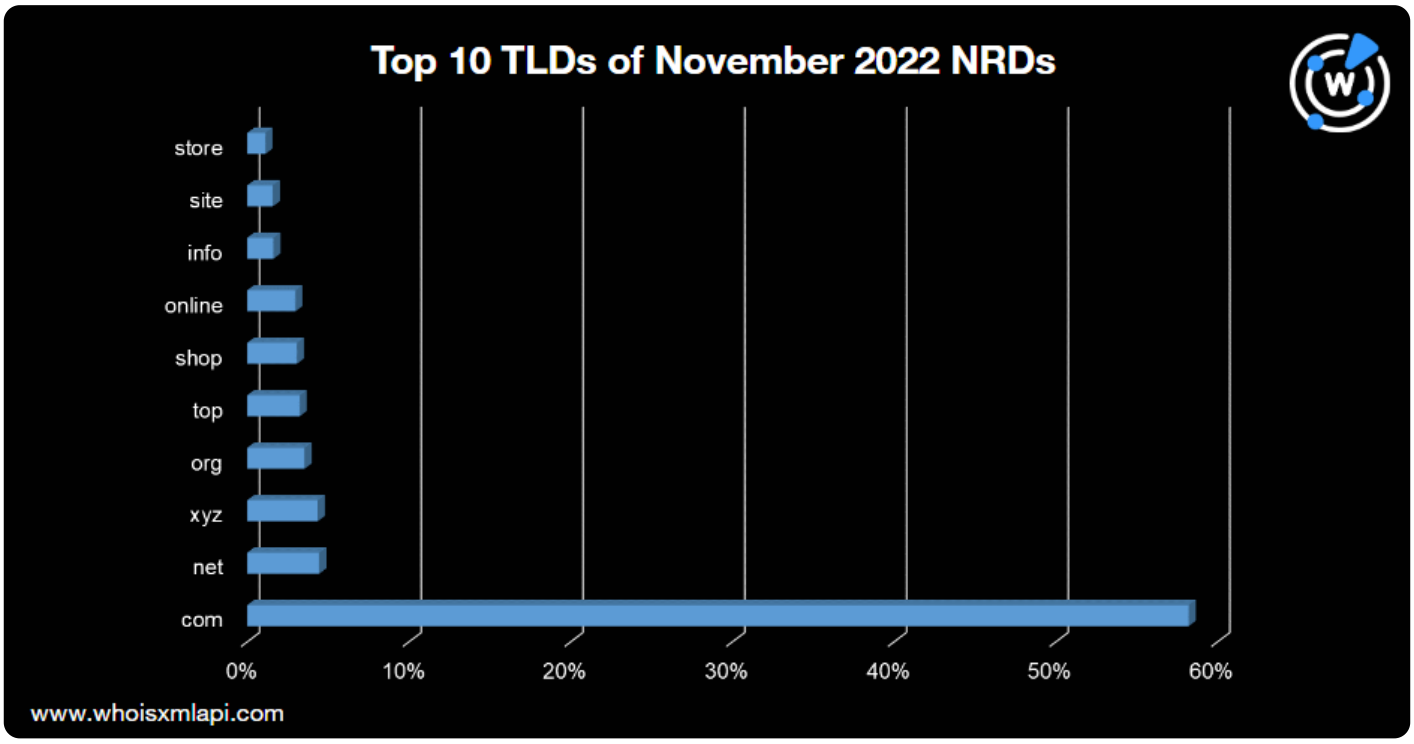


Zooming in on the November NRDs

Using a sample comprising 1.1 million NRDs, we sought to determine the top TLDs and most commonly used text strings among the November NRDs.

TLD Distribution

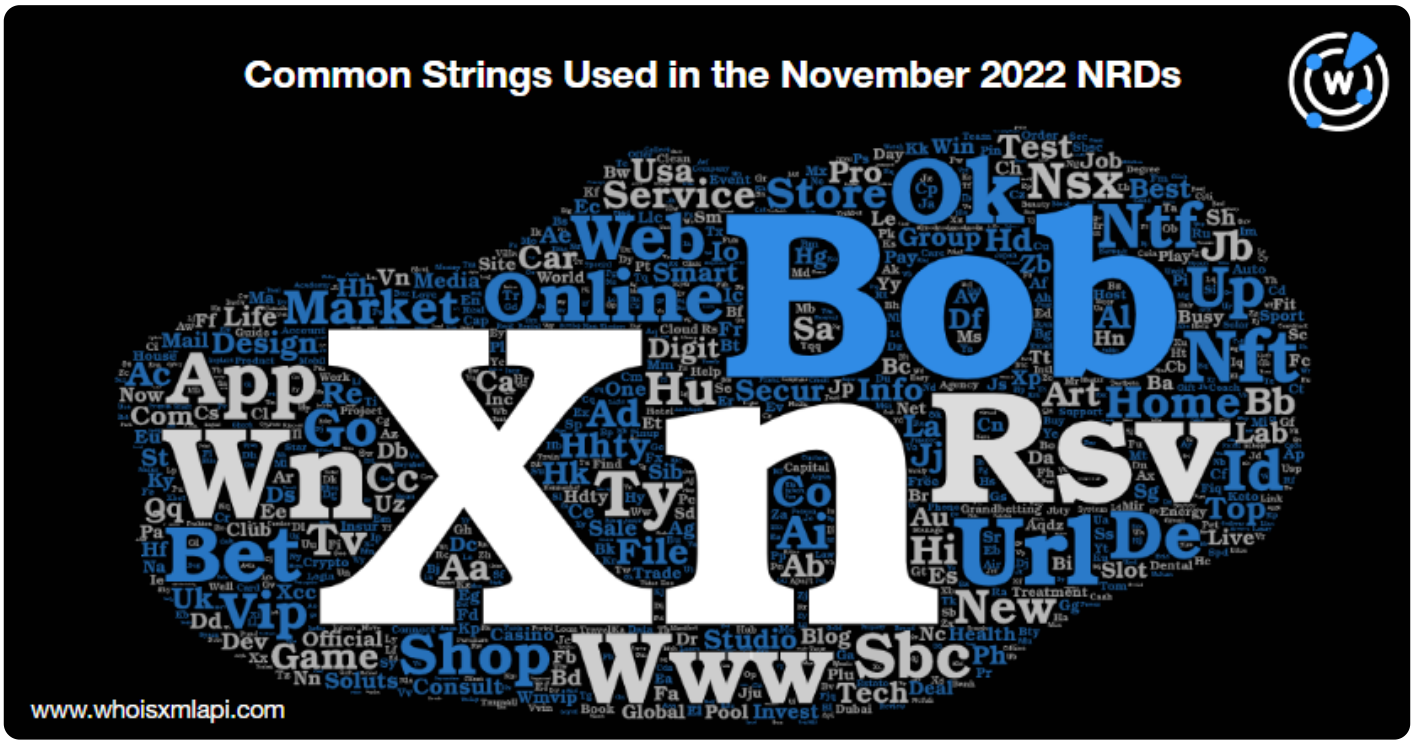
As in the previous months, the top TLD remained .com, accounting for 58% of the total domain registration volume. Generic TLDs (gTLDs) .net and .org also remained in the top 10, each accounting for 4% of the domains. New generic TLDs (gTLDs), such as .xyz, .top, .shop, .online, and .site, continued to be prominent, as shown in the chart below.



Appearance of Common Strings among the SLDs

For three months in a row, internationalized domain names (IDNs) continued to trend, as evidenced by the recurrence of “xn” among the November NRDs.

Generic tech terms also remained popular, as shown in the word cloud below, where strings like “web,” “online,” “www,” and “app” are evident. Gambling- and finance-related terms were also noticeable. A few examples include “bet,” “nft,” and “market.”

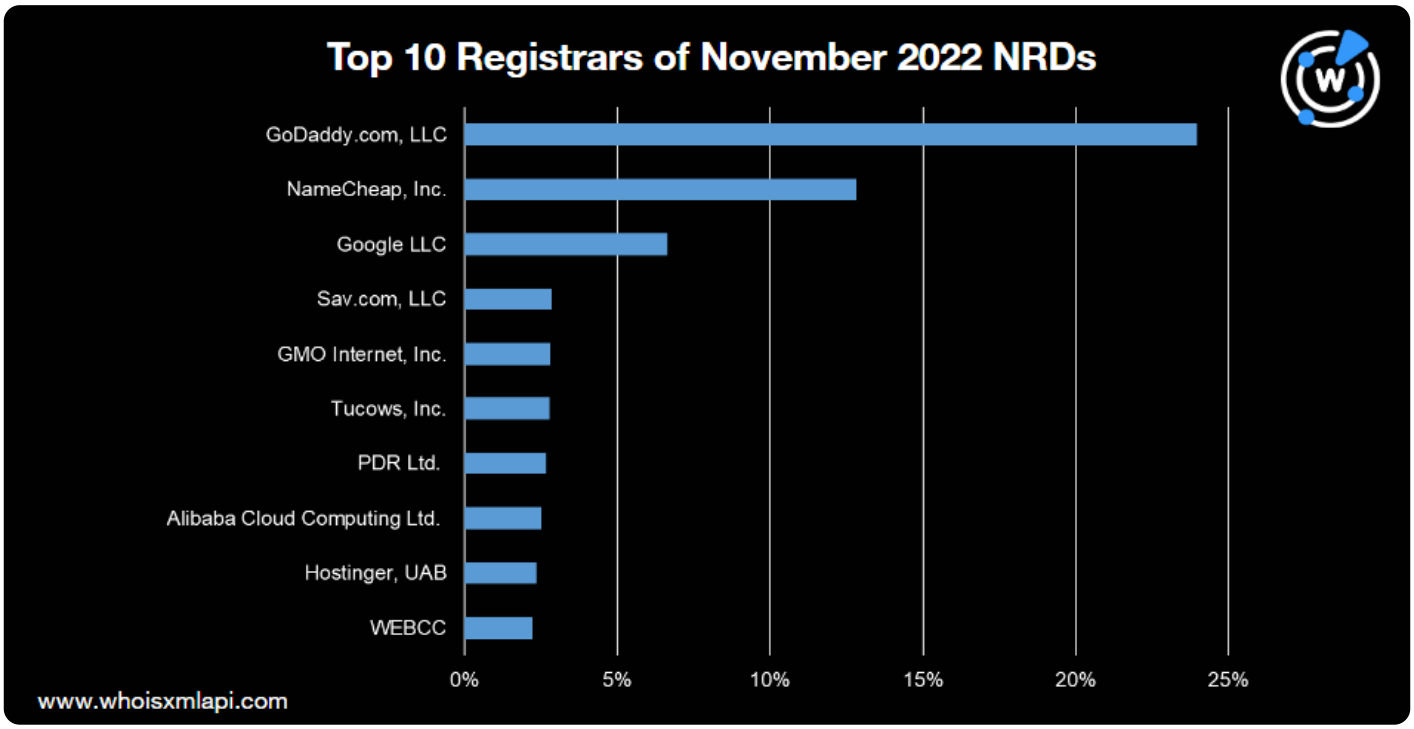


We will continue to monitor the DNS for registration trends that could be relevant to organizations making critical business decisions.

Next, we analyzed the WHOIS records of the NRDs using a sample comprising 20,018 domains.

Registrar Distribution

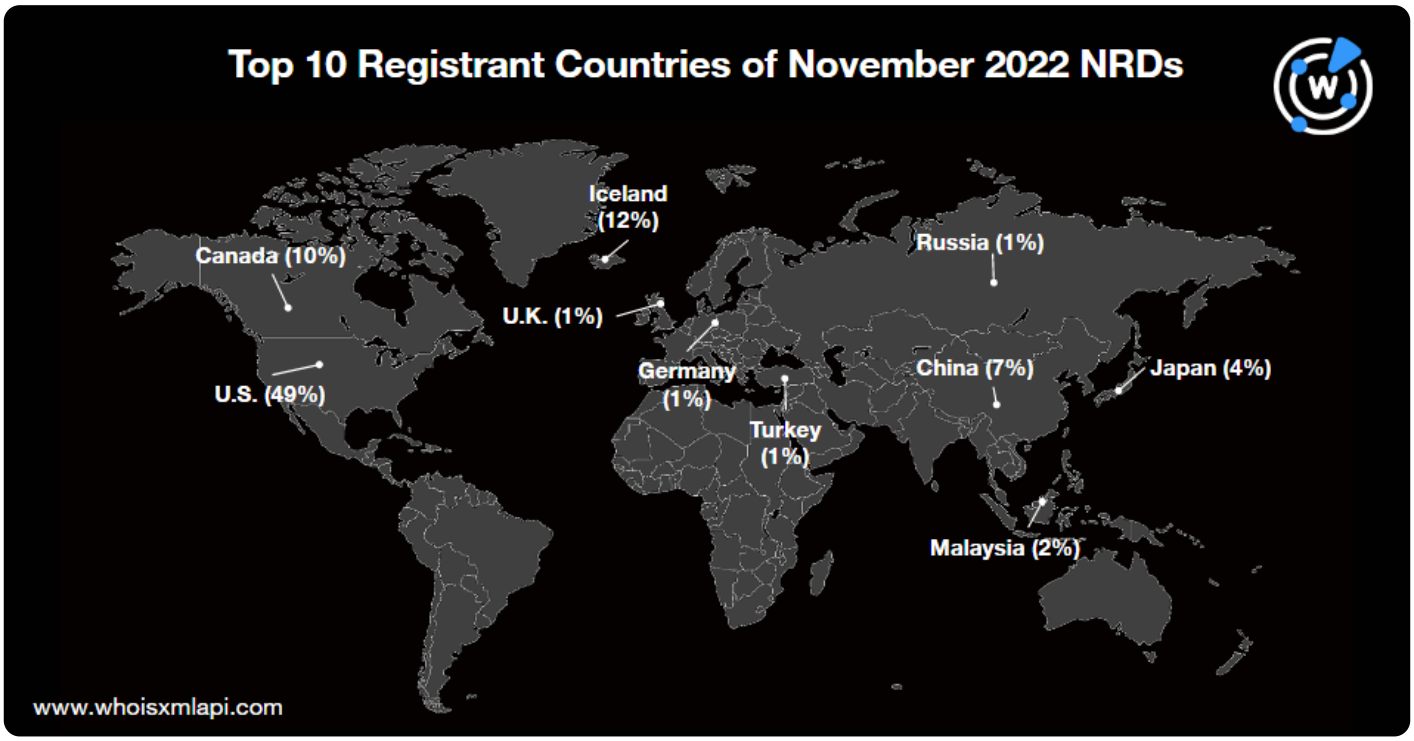
The first thing we did was to determine which institutions managed the November NRDs. GoDaddy was the top registrar, accounting for 24% of the NRDs. Namecheap followed with 13% and Google with 7%. The rest of the registrars on the top 10 each accounted for less than 4% each of the domain registrations.



Top Registrant Countries

Nearly half of the NRDs' WHOIS records cited the U.S. as the registrant country. It was followed by Iceland with 12% of the domains. Most of these domains were also managed by Namecheap and employed WHOIS data protection service provider Withheld for Privacy.

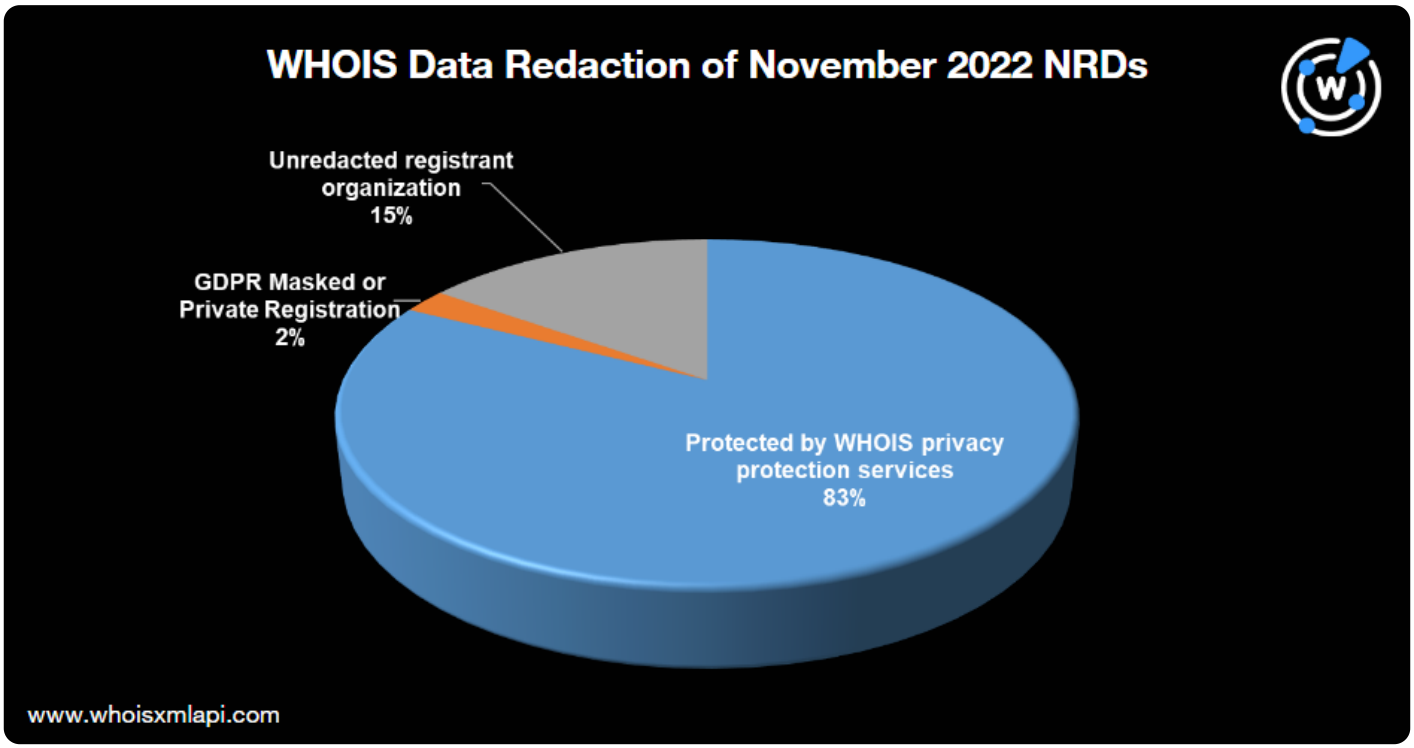
The other registrant countries in the top 10 were Canada, China, Japan, Malaysia, Russia, the U.K., Germany, and Turkey. We mapped them out below.



WHOIS Data Redaction

Privacy protection service providers protected a majority (83%) of the domains' WHOIS information. We conducted further analysis using the details in the registrant organization field.

More than one-third of the privacy-protected domains employed the services of Domains By Proxy, LLC, while 16% were served by Withheld for Privacy EHF. About 10% were protected by Contact Privacy, Inc., while the rest were distributed across hundreds of other WHOIS data protection providers.



A small percentage of the WHOIS records were marked “GDPR Masked” or “Private Registration,” which could mean they were covered by the General Data Protection Regulation (GDPR) or other privacy regulations. About 15% of the domains had unredacted registrant organization fields.

This Month’s Cybersecurity through the DNS Lens

WhoisXML API is always on the lookout for opportunities to enrich cyber threat intelligence with IP, DNS, and other Internet-related data to hasten threat detection and prevention. This November, our researchers looked into different types of threats, including Magniber, investment-related cybersquatting, and threat actor RomCom. Below are some of the threat reports we published.

- **Investment-Related Cybersquatting: Another Way to Lose Money?:** With the increasing volatility of the stock market, our researchers decided to investigate cybersquatting attacks targeting Nasdaq and Forex. We found 9,000+ investment-themed domains added between

1 August and 31 October 2022.

- **Nothing Funny or Romantic about These RomCom IoCs and Artifacts**: Our researchers followed the trail of threat actor RomCom who has been known to use sites posing as belonging to popular software like Keepass, Veeame, and SolarWinds. We found thousands of artifacts connected to known threat indicators of compromise (IoCs) and cybersquatting NRDs that could potentially serve as threat vehicles.

- **Beware That Software Update, It Could Be Magniber in Disguise:** Our in-depth investigation of an ongoing massive Magniber ransomware campaign revealed hundreds of domains containing text strings used in weaponized domains.

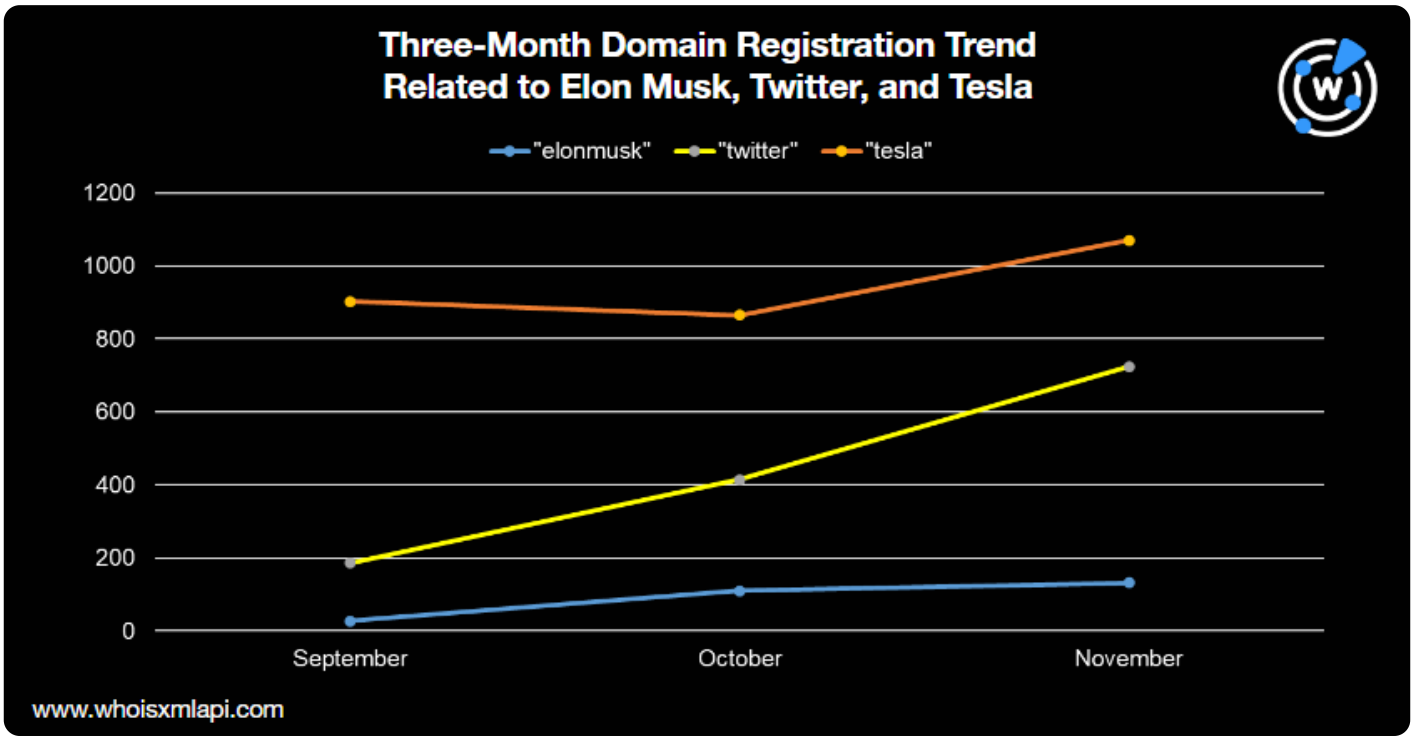
- **The Business of Cybercrime: Does Malicious Campaign Planning Take as Long as Legitimate Marketing Campaign Planning?:** In this investigation, we focused on some of the most sought-after tech releases of 2022. We found more than a thousand digital properties that contained strings cybercriminals would likely use in malicious campaigns.

You can find more reports created in the past months here.

In the News

From his Twitter takeover to selling US$3.95 billion worth of Tesla shares, news related to Elon Musk seemed to dominate the Internet in November. The DNS reflected this, too.

The registration of domains containing “elonmusk,” “twitter,” and “tesla” significantly increased from September to November. This upward trend is reflected in the chart below.



Please do not hesitate to contact us for more information about the domain registration events and analyses mentioned above or any inquiries about enterprise commercial solutions.

Download our NRD data sample to test the data in your environment.