WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

WHITE PAPER

Mapping the Business Impersonation Landscape through the DNS – 2022 Edition

Contents

1 Executive Summary

Business impersonation can take many forms. Among the most rampant is domain and subdomain spoofing, also known as "cybersquatting." In this type of cyber attack, threat actors register web properties that look similar or relevant to the target company. They may use the organization's name (e.g., logincitigroup-help[.]com) or take advantage of its executives (fraser-jane[.]pages[.]dev) and departments or the organization as a whole (e.g., citigroup-finance[.]com).

Domain spoofing is often the first step in the nefarious business impersonation scheme. Threat actors can use the cybersquatting domain as a starting point for dangerous campaigns, such as phishing, business email compromise (BEC) scams, counterfeiting, and other cyber attacks that can damage the target company's reputation, business processes, and finances.

Detecting business impersonation through the Domain Name System (DNS) can help mitigate the threat early, ideally before actors mobilize the look-alike web properties. In line with this, Whois API researchers launched a large-scale mapping of the past year's business impersonation landscape. The researchers examined the domain footprint of 29 Fortune 500 companies and 20 top CEOs, which yielded a total of 49,158 domains and subdomains. Our analysis led to these key takeaways and findings:

- Less than 2% of the web properties can be publicly credited to the legitimate companies, leaving the vast majority unattributable.
- More than half of the resolving properties are geolocated and registered in the U.S.
- The leading registrar is Public Domain Registry (PDR) Ltd., followed by some of the most popular registrars, including GoDaddy, Mark Monitor, and Namecheap.
- Four of the top 10 ISPs managing the cyber resources' IP addresses are among the worst ISPs in terms of spam and botnet infection.
- Some malicious properties still host questionable content, including login forms and look-alike pages.
- Almost 13% of the cyber resources found were flagged as malicious.

These findings are detailed in the succeeding sections.

2 Methodology and Tools

Whois API researchers have done two similar research projects in the past, each focusing on CEO impersonation and the digital footprint of Fortune 500 companies. They had interesting results that show how the DNS can help pinpoint possible business impersonation cases. This 2022 edition of our business impersonation research builds on 2021 edition's general findings, narrowing down the data sample to identify three forms of business impersonation. These are detailed in the table below.

Business Impersonation Type	Description	Search Terms Used	Number of Properties Uncovered
CEO impersonation	Signified by domains and subdomains bearing the names of Glassdoor top CEOs, including: • Kevin Murphy (Ferguson Enterprises) • Rene Jones (M&T Bank) • Tim Ryan (PwC) • Marc Benioff (Salesforce) • Ben Peterson (Blue Raven Solar) • Matthew Stevens (The Bay Club) • Abby Johnson (Fidelity Investments) • Tim Pierce (Morrison Healthcare) • Jane Fraser (Citi) • Charles C. Butt (HEB) • Tim Byrne (Lincoln Property Company) • Gary C. Kelly (Southwest Airlines) • Michael F. Mahoney (Boston Scientific) • Christophe Weber (Takeda Pharmaceuticals) • Dan Burton (Health Catalyst) • Alex Gorsky (Johnson & Johnson) • Sundar Pichai (Google) • Jack Little (MathWorks)	• "kevin + murphy" • "rene + jones" • "timryan" • "marc + benioff" • "ben + peterson" • "matthew + stevens" • "abby + johnson" • "tim + pierce," excluding "time" • "jane + fraser" • "charles + butt" • "tim + byrne," excluding "time" • "gary + kelly" • "michael + mahoney" • "christophe + weber" • "dan + burton," excluding "jordan" • "alex + gorsky" • "sundar + pichai" • "jack + little," excluding "jackfruit" and "jacket"	**285**

Table 1: *Types of business impersonation found on the DNS*

Business Impersonation Type	Description	Search Terms Used	Number of Properties Uncovered
Organizational department or company impersonation	Pertains to web properties imitating the marketing, support, finance, security, and recruitment departments of the target companies or the company in general	Names of the Fortune 500 companies in the study, alongside: • "marketing" • "support" • "finance" • "security" • "recruit"	**11,470**
Urgency-based business impersonation	Relies on the use of company names, alongside keywords that promote a sense of urgency among the victims, which are also commonly used in verified phishing URLs	Names of the Fortune 500 companies in the study together with: • "login" • "signin" • "register" • "pay" • "auth" • "sale" • "update" • "verif" • "recover"	**40,615**

Table 1: *Types of business impersonation found on the DNS*

The number of digital properties found totaled 52,085. After duplicate items and obvious false positives were removed, 49,158 domains and subdomains were left. The analysis was performed with the help of threat intelligence tools that provide domain, DNS, and IP intelligence, including:

- Domains & Subdomains Discovery to retrieve web properties added from 1 June 2021 to 31 May 2022
- Bulk WHOIS Lookup to see the ownership details of the properties and determine whether they can be publicly attributed to the target company or not
- Bulk IP Lookup to find out which cyber resources had active IP resolutions and identify their geolocations
- Domain Malware Check API to determine if any of the web properties have been reported as malicious by malware engines
- Screenshot Service to see the types of content hosted on the cybersquatting resources

3 Data Analysis and Findings

The researchers focused on determining four main characteristics of the cyber resources in the study, namely, attribution, connections and associations, content, and malicious usage. These are detailed below.

Attribution: Do the Web Properties Belong to the Rightful Owners?

Among the first scores to settle is the ownership of the cybersquatting properties uncovered. There wouldn't be a need to be alarmed if they were owned by the companies they imitated. But if someone else controls them, these resources can potentially be used in malicious campaigns targeting the organization, its employees, third parties, clients, and other stakeholders.

While privacy redaction has been quite prevalent, large organizations, such as those in this study, mostly choose to make their WHOIS details publicly available. As such, the researchers determined the attribution of the domains and subdomains by looking at their WHOIS registrant organization.

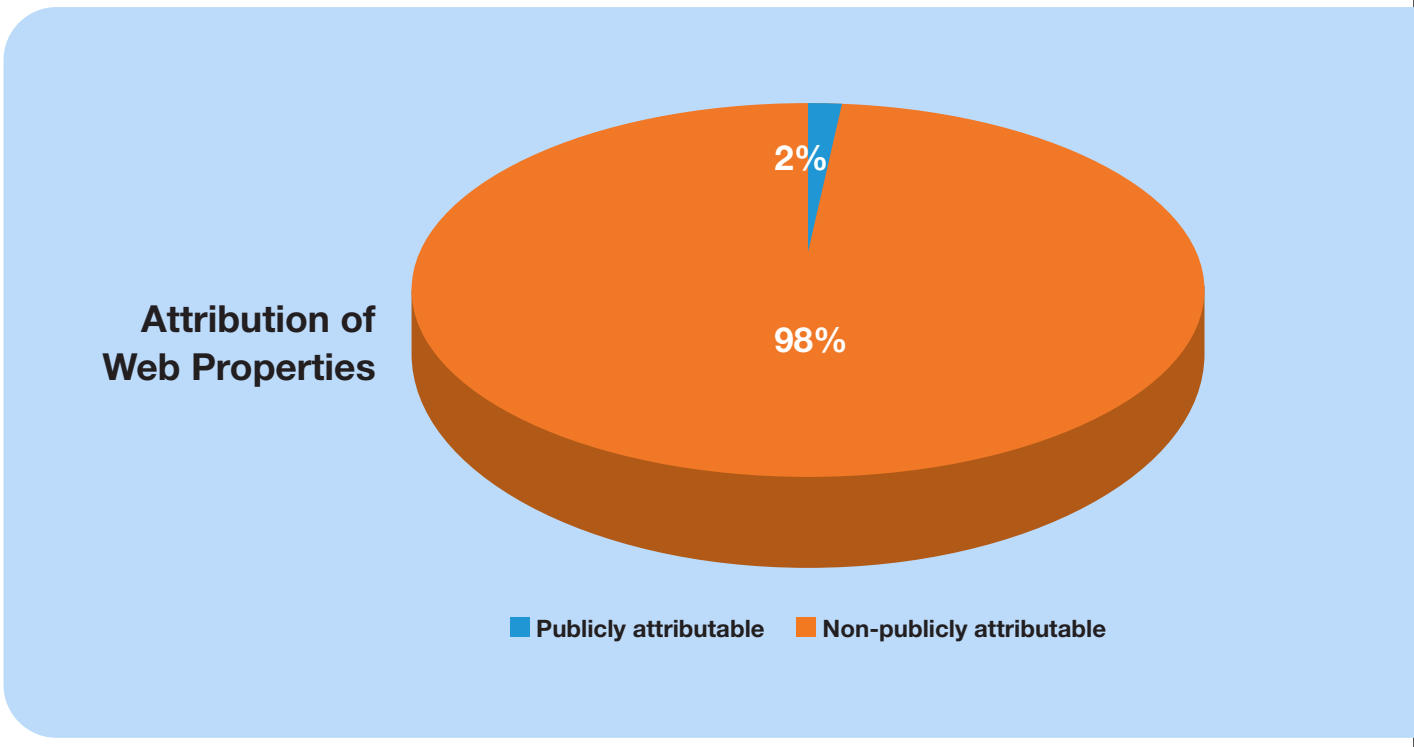


Figure 1: *Attribution of web properties impersonating selected sample of Fortune 500 companies and top CEOs*

Only 1.71% of the cyber resources could be publicly attributed to their rightful owners, meaning their registrant organizations matched the company names in their domain names. We provided a few examples of attributable properties and their registrant organizations below.

domainName	registrant_organization	domainName	registrant_organization
amazon--payments.com	Amazon Technologies, Inc.	meta-marketingsummit.com	Meta Platforms, Inc.
amazon-2-factor-authentication.com	Amazon Technologies, Inc.	metaauthorizedpartners.net	Meta Platforms, Inc.
amazon-multi-factor-authentication.com	Amazon Technologies, Inc.	metaauthorizedsalespartners.net	Meta Platforms, Inc.
amazon-two-factor-authentication.com	Amazon Technologies, Inc.	metaauthorizedpartners.com	Meta Platforms, Inc.
amazon2factorauthentication.com	Amazon Technologies, Inc.	metainstagram.security	Meta Platforms, Inc.
amazon2-factorauthentication.com	Amazon Technologies, Inc.	metalogin.asia	Meta Platforms, Inc.
amazonastrosupport.com	Amazon Technologies, Inc.	metalogin.ai	Meta Platforms, Inc.
amazonastrotechsupport.com	Amazon Technologies, Inc.	metalogin.best	Meta Platforms, Inc.
amazonastrocustomersupport.com	Amazon Technologies, Inc.	metalogin.bar	Meta Platforms, Inc.
amazonaws-cybersecurity.com	Amazon Technologies, Inc.	metalogin.cam	Meta Platforms, Inc.
amazonaws2-factorauthentication.com	Amazon Technologies, Inc.	metalogin.fun	Meta Platforms, Inc.
amazonaws2-factor-authentication.com	Amazon Technologies, Inc.	metalogin.host	Meta Platforms, Inc.
amazonaws-two-factorauthentication.com	Amazon Technologies, Inc.	metalogin.icu	Meta Platforms, Inc.
amazonaws2factorfuthentication.com	Amazon Technologies, Inc.	metalogin.net	Meta Platforms, Inc.
amazonawssecurity.com	Amazon Technologies, Inc.	metalogin.online	Meta Platforms, Inc.
amazonaws-multi-factor-authentication.com	Amazon Technologies, Inc.	metalogin.press	Meta Platforms, Inc.
amazonawsmultifactorauthentication.com	Amazon Technologies, Inc.	metalogin.site	Meta Platforms, Inc.

Figure 2: *Screenshot of the WHOIS records of publicly attributable domain properties*

In contrast, a huge majority of the properties, 98.29% to be exact, could not be publicly attributed to the target organizations. Several had their WHOIS records redacted or privacy-protected.

domainName	registrant_organization	domainName	registrant_organization
3dmetapayments.com	Privacy Protection	acareerinsalesforce.com	Domains By Proxy, LLC
3metapayment.xyz	Privacy Protection	account-confirm-verification-amazon-sign12.com	NAOKO SHIMAZAKI
3dmetaversepay.com	Privacy Service provided by withheld	accesssalesforce.com	Domains By Proxy, LLC
3metaversepay.xyz	Privacy Protection	account-confirm-verification-amazon-sign13.com	NAOKO SHIMAZAKI
3metapayments.xyz	Privacy Protection	account-confirm-verification-amazon-sign17.com	NAOKO SHIMAZAKI
3metaversepayment.com	Privacy Protection	account-confirm-verification-amazon-sign15.com	NAOKO SHIMAZAKI
3metaversepayments.xyz	Privacy Protection	account-confirm-verification-amazon-sign11.com	NAOKO SHIMAZAKI
3metapayment.com	Privacy Protection	account-confirm-verification-amazon-sign14.com	NAOKO SHIMAZAKI
3metapayments.com	Privacy Protection	account-confirm-verification-amazon-sign20.com	NAOKO SHIMAZAKI.
3metaversepayment.xyz	Privacy Protection	account-confirm-verification-amazon-sign16.com	NAOKO SHIMAZAKI
3metaversepay.com	Privacy Protection	account-confirm-verification-amazon-sign19.com	NAOKO SHIMAZAKI
4gnitewifi-applepay.com	TipTopWebsite.com	account-confirm-verification-amazon-sign2.com	
3metaversepayments.com	Privacy Protection	account-salesforce.com	Domains By Proxy, LLC
4salebymeta.com	Domains BY Proxy, LLC	account-update1-amazon.com	Statutory Masking Enabled
4salemetaverse.com	Domains BY Proxy, LLC	account-update3-amazon.com	Statutory Masking Enabled
4salebymetaverse.com	Domains BY Proxy, LLC	account-update2-amazon.com	Statutory Masking Enabled
401kmarketingmeta.com	Domains BY Proxy, LLC	account-wellsfargosecurity.com	Solidware Solutions
4saleonmeta.com	Domains BY Proxy, LLC	accountrecovery-amazon.com	Data Redacted
4saleonmetaverse.com	Domains BY Proxy, LLC	accountsecuritysoftmicrosoft.com	Contact Privacy Inc. Customer 7151571

Figure 3: *Screenshot of the WHOIS records of non-publicly attributable domain properties*

Connections and Associations: What Organizations Are Responsible for the Domains?

Half of the cybersquatting properties had active IP resolutions pointing to 8,663 unique IP addresses. These resolutions were mostly geolocated in the U.S. At the same time, less than 40% were distributed across 78 other locations led by Germany, Canada, the U.K., the Netherlands, Russia, France, Ireland, the Virgin Islands, and Brazil. The chart below shows the geolocation distribution of the IP resolutions.

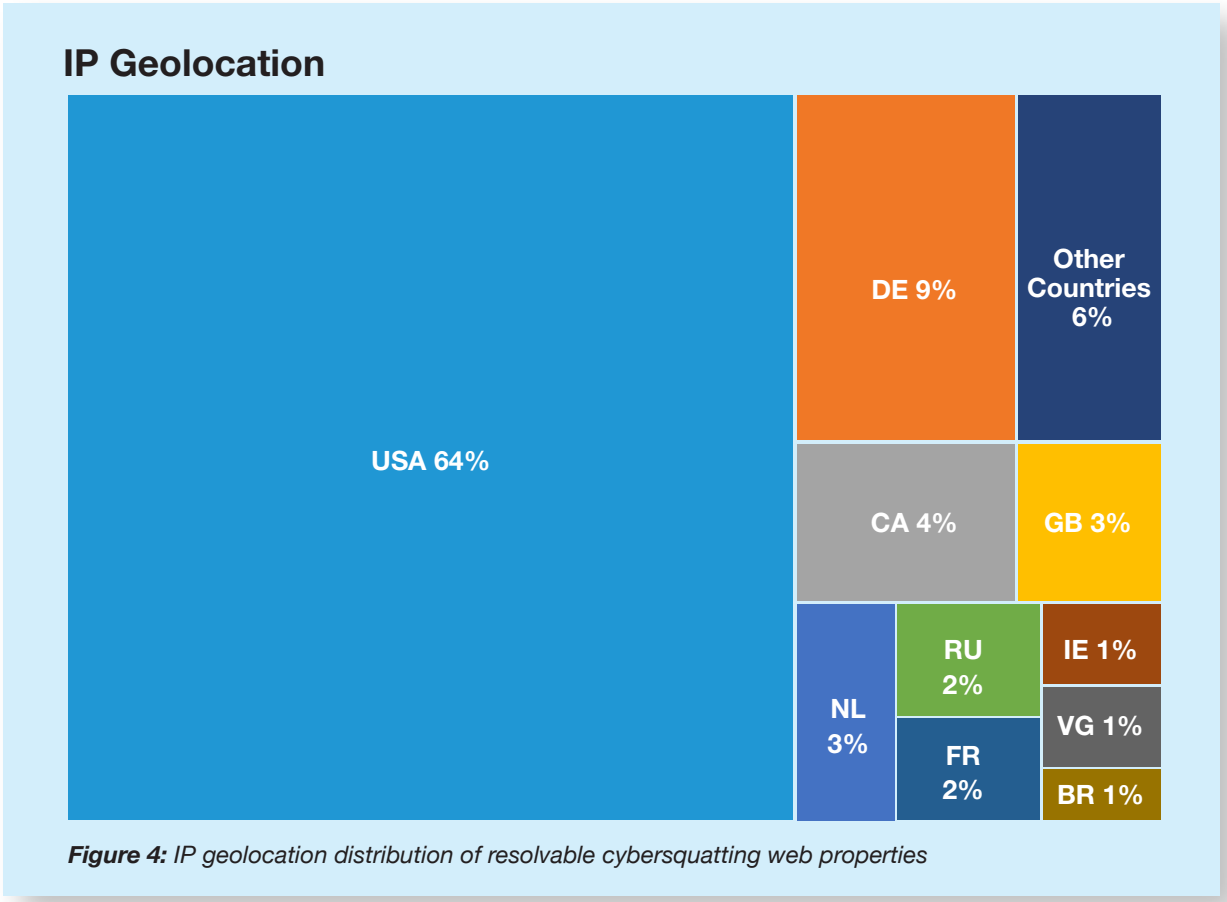


Figure 4: *IP geolocation distribution of resolvable cybersquatting web properties*

The IP geolocation details were roughly the same as the registrant countries of the cybersquatting properties. The U.S. also took the bulk of the registrations, while the rest were divided across 119 other countries and territories. Canada, the Netherlands, the U.K., Germany, and France remained in the top 10 as shown in the chart below.

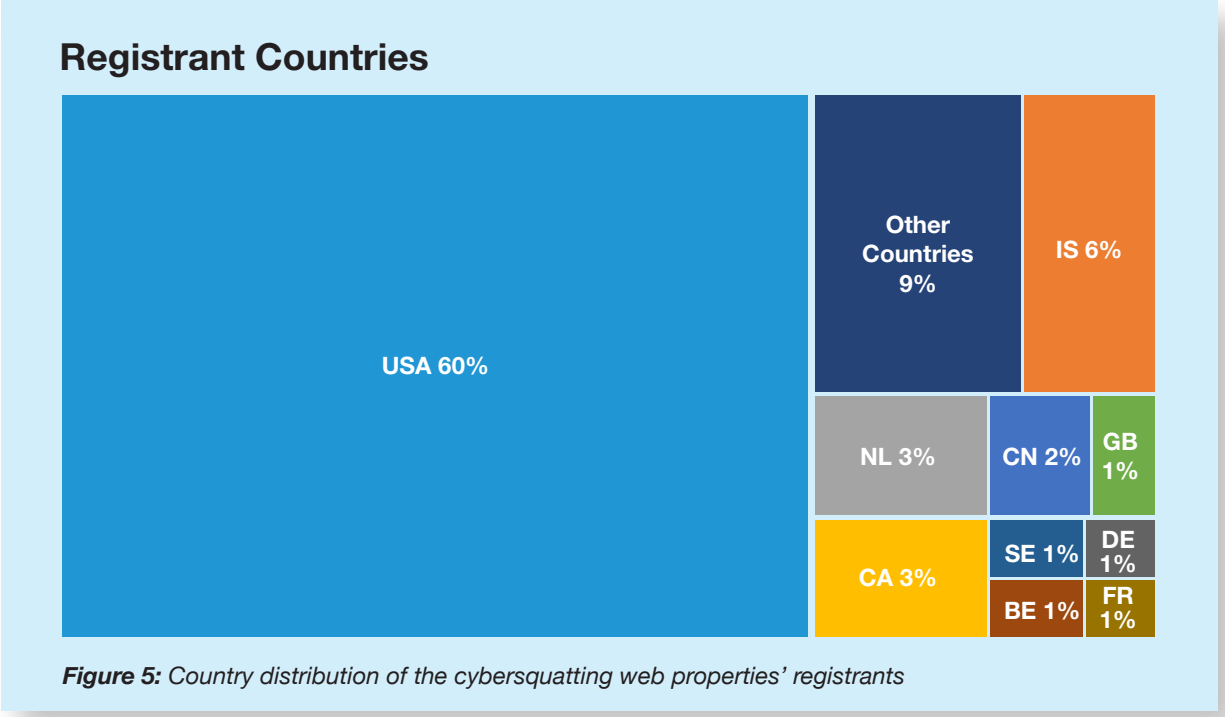


Figure 5: *Country distribution of the cybersquatting web properties' registrants*

The researchers also looked at the organizations administering the properties. The leading registrar of the non-publicly attributable digital properties was PDR Ltd., which managed 38% of the domains. GoDaddy, MarkMonitor, and Namecheap were among the top ten registrars.

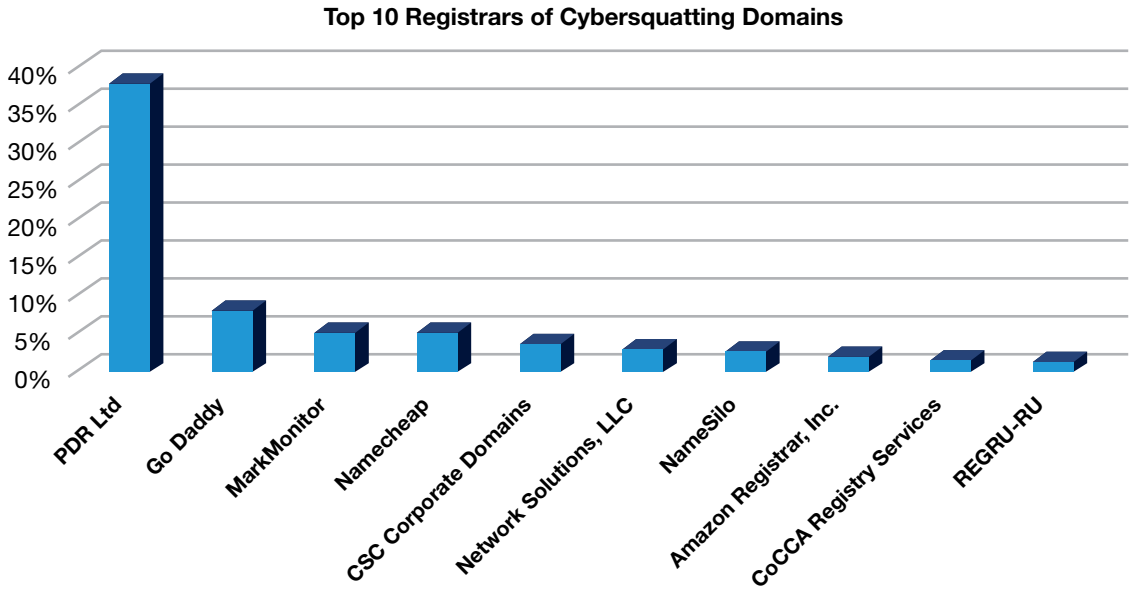


Figure 6: *Top 10 registrars used by the cybersquatting web properties*

The ISP distribution took into account resolving cyber resources only. Of the 889 ISPs, Amazon took the lead with 27% of the total IP resolutions, followed by Cloudflare and Google with 11% each. The rest of the top 10 ISPs are shown in the following chart.

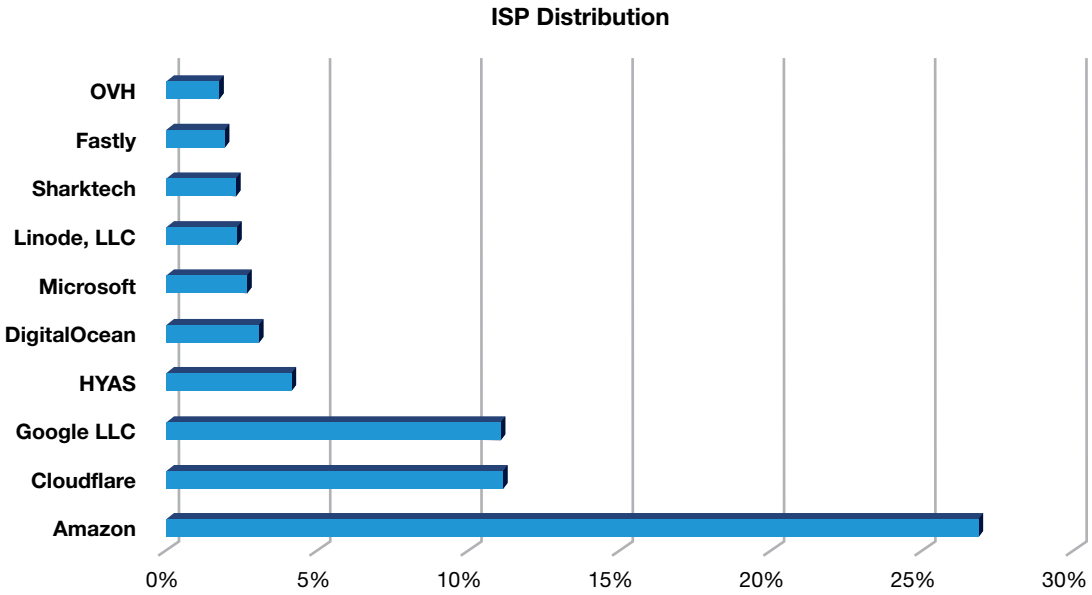


Figure 7: *Top 10 ISPs of the resolving cybersquatting web properties*

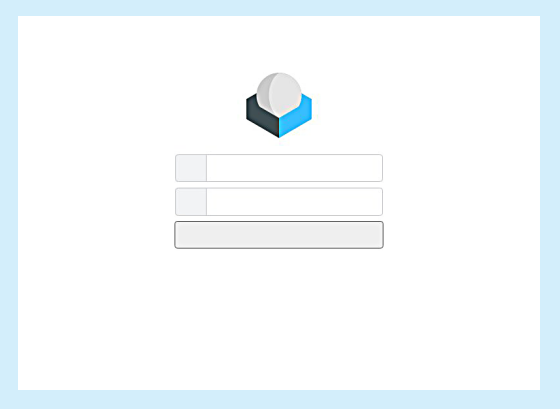
Four of these ISPs were tagged by Spamhaus as having the highest number of spam or botnet infections as of 9 June 2022.

The World's Worst Spam Support ISPs			The 10 Worst Botnet ISPs		
As of 09 June 2022 the ISPs with the highest number of known ongoing spam problems are:			As of 09 June 2022 the world's worst botnet infected ISPs are:		
1	uninet.net.mx	Number of Current Known Spam Issues: **654**	1	amazon.com	Number of bots: **397871**
2	microsoft.com	Number of Current Known Spam Issues: **613**	2	airtel.in	Number of bots: **253476**
3	stc.com.sa	Number of Current Known Spam Issues: **545**	3	djaweb.dz	Number of bots: **153482**
4	antel.net.uy	Number of Current Known Spam Issues: **498**	4	chinanet-ah	Number of bots: **117682**
5	cloudflare.com	Number of Current Known Spam Issues: **472**	5	chinanet-js	Number of bots: **117032**
6	google.com	Number of Current Known Spam Issues: **419**	6	telkom.net.id	Number of bots: **113697**
7	claro.com.do	Number of Current Known Spam Issues: **383**	7	unicom-in	Number of bots: **72081**
8	chinanet-gd	Number of Current Known Spam Issues: **319**	8	tot.co.th	Number of bots: **60969**
9	chinanet-js	Number of Current Known Spam Issues: **298**	9	vnpt.vn	Number of bots: **56021**
10	wind.com.do	Number of Current Known Spam Issues: **245**	10	ptcl.com.pk	Number of bots: **54757**

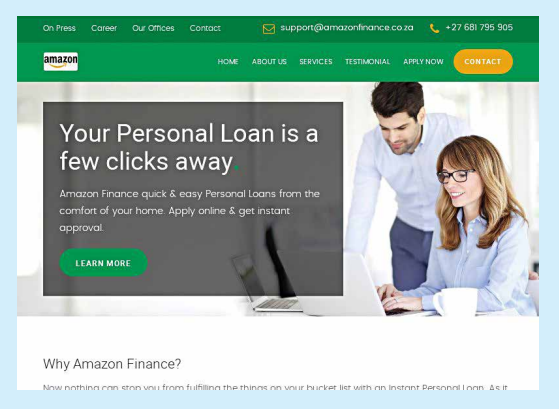
Figure 8: *Top 10 World's Worst Spam Support and Botnet ISPs*

Content: What Do the Properties Look Like?

As expected, several domains were either parked, for sale, or undergoing development. Some also resolved to 403 and 404 pages. And while these were interesting, more pressing types of content were hosted on some cybersquatting properties. Below are some examples.



Screenshot of amazonbillsupport[.]info



Screenshot of amazonfinance[.]co[.]za

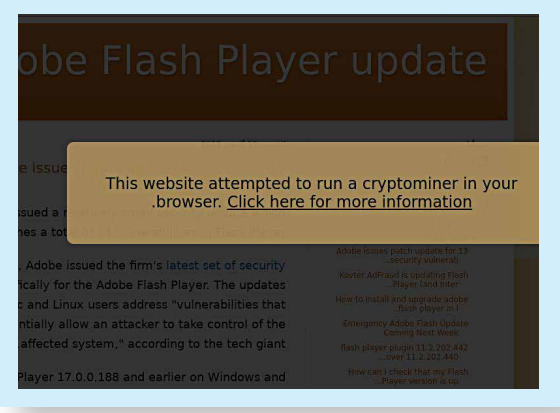
The domain amazonbillsupport[.]info was flagged as malicious but continues to host a login page. Although most browsers and security solutions may already block access to this page, some vulnerable users can still fall victim.

In contrast, the domain amazonfinance[.]co[.]za isn't being flagged as malicious. However, there are still red flags that make it suspicious. For one, it was only created on 18 March 2022, making it entirely new. The page sports Amazon's official logo but if you look closely, the logo seems to be copied off the Web because of its background.

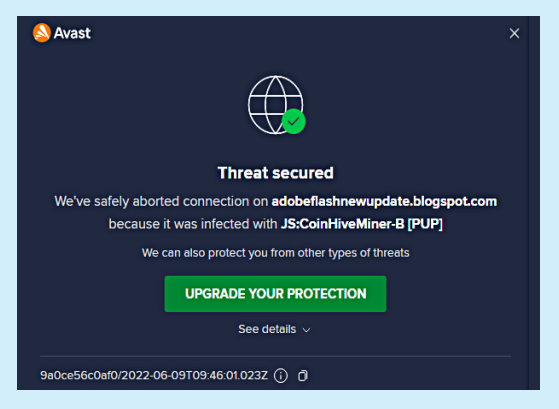
It also appears that Amazon only offers its loan products to businesses and the details can be found on one of the company's official subdomains (sell[.]amazon[.]com/programs/amazon-lending) instead of a different website.

Other examples of questionable content are shown below, with one attempting to infect devices with a crypto miner. Fortunately, the researchers' browser and antivirus software were able to block the threats. Other users may not be as lucky.

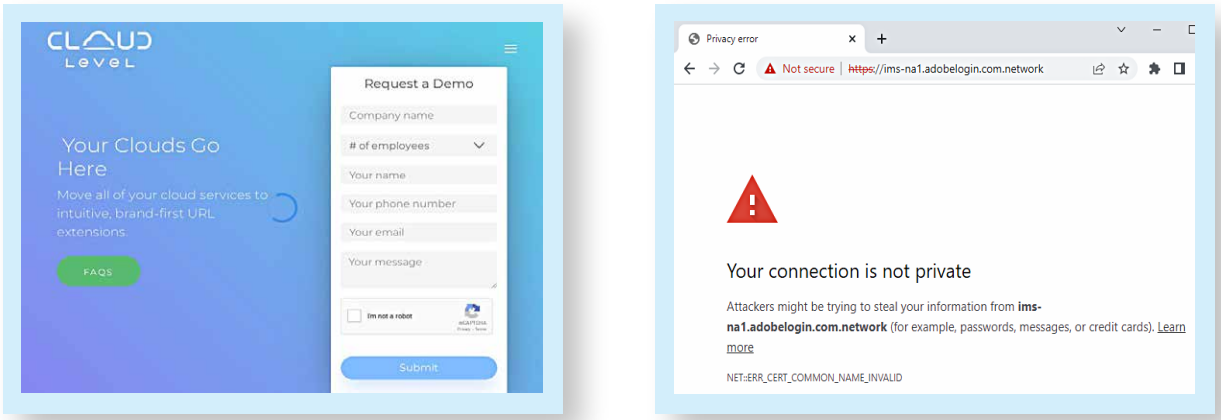
Remote Website Screenshot



Live Security Alert When Visiting the Website



Screenshot of adobeflashnewupdate[.]blogspot[.]com



Screenshot of ims-na1[.]adobelogin[.]com[.]network

Malicious Usage: Have Threat Actors Used the Resources Before?

About 12.32% of the cyber resources have been reported as malicious by various malware engines. Note, too, that there were more malicious subdomains than domains. That could mean that in addition to registering NRDs, threat actors also exploited legitimate root domains and created malicious subdomains or took over vulnerable ones.

Of the urgency-based keywords, "auth" had the highest volume of malicious properties, followed by "login," and "signin." On the other hand, most of the department-targeted malicious resources impersonated the organizations' support services. The chart below shows the breakdown.

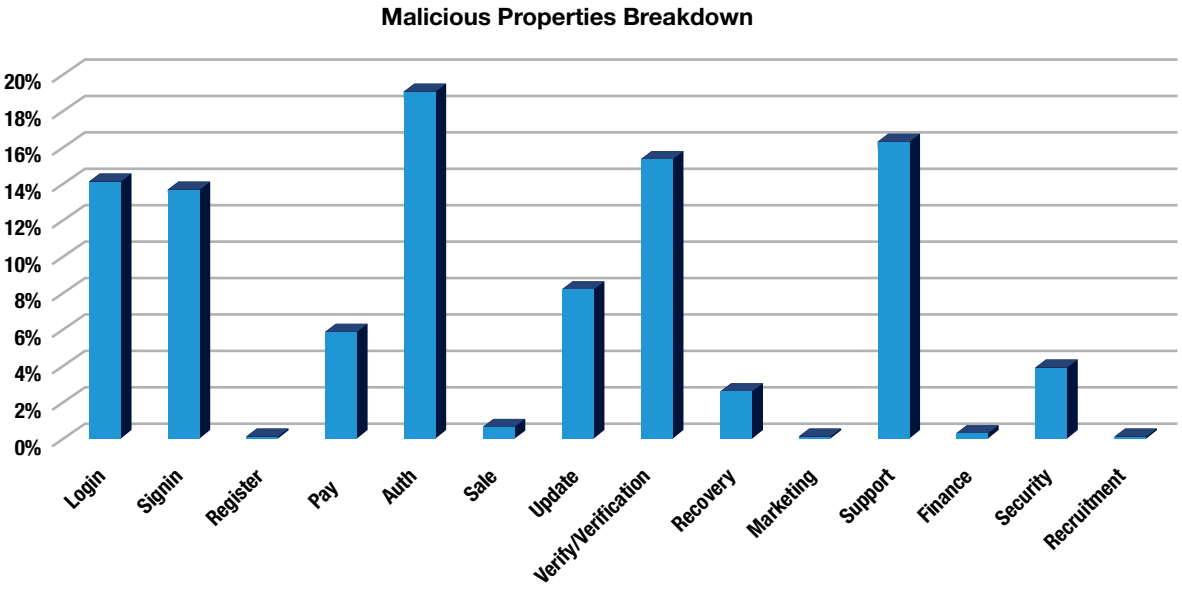


Figure 9: *% of web properties containing certain strings and identified as malicious*

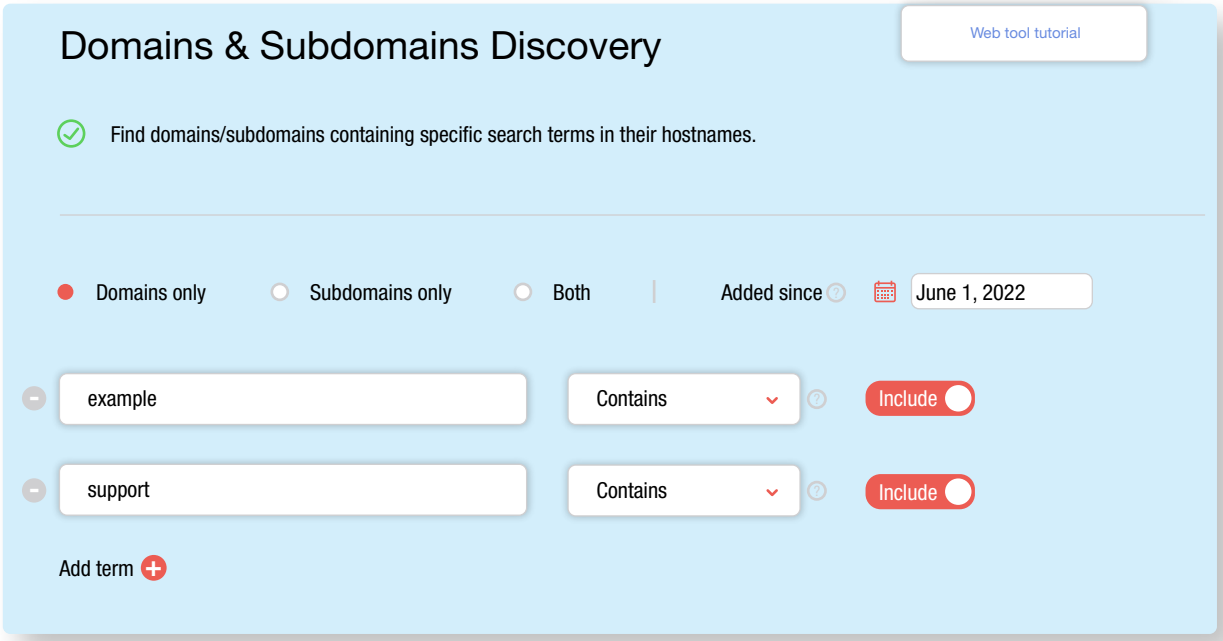
Note that none of the CEO-targeted resources have been flagged as malicious as of this writing.

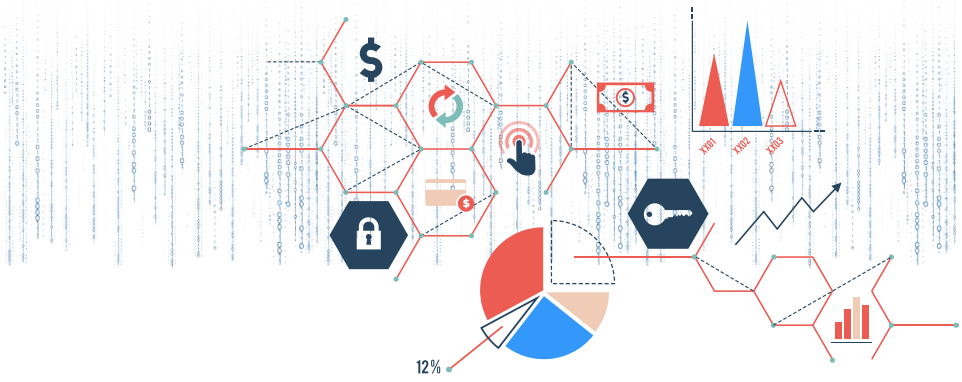
4 DIY Business Impersonation Detection and Analysis

The whole process of detecting cybersquatting domains and subdomains and weeding out potentially dangerous ones can be done within your environment. Here are some actionable tips for effective DIY threat detection and analysis.

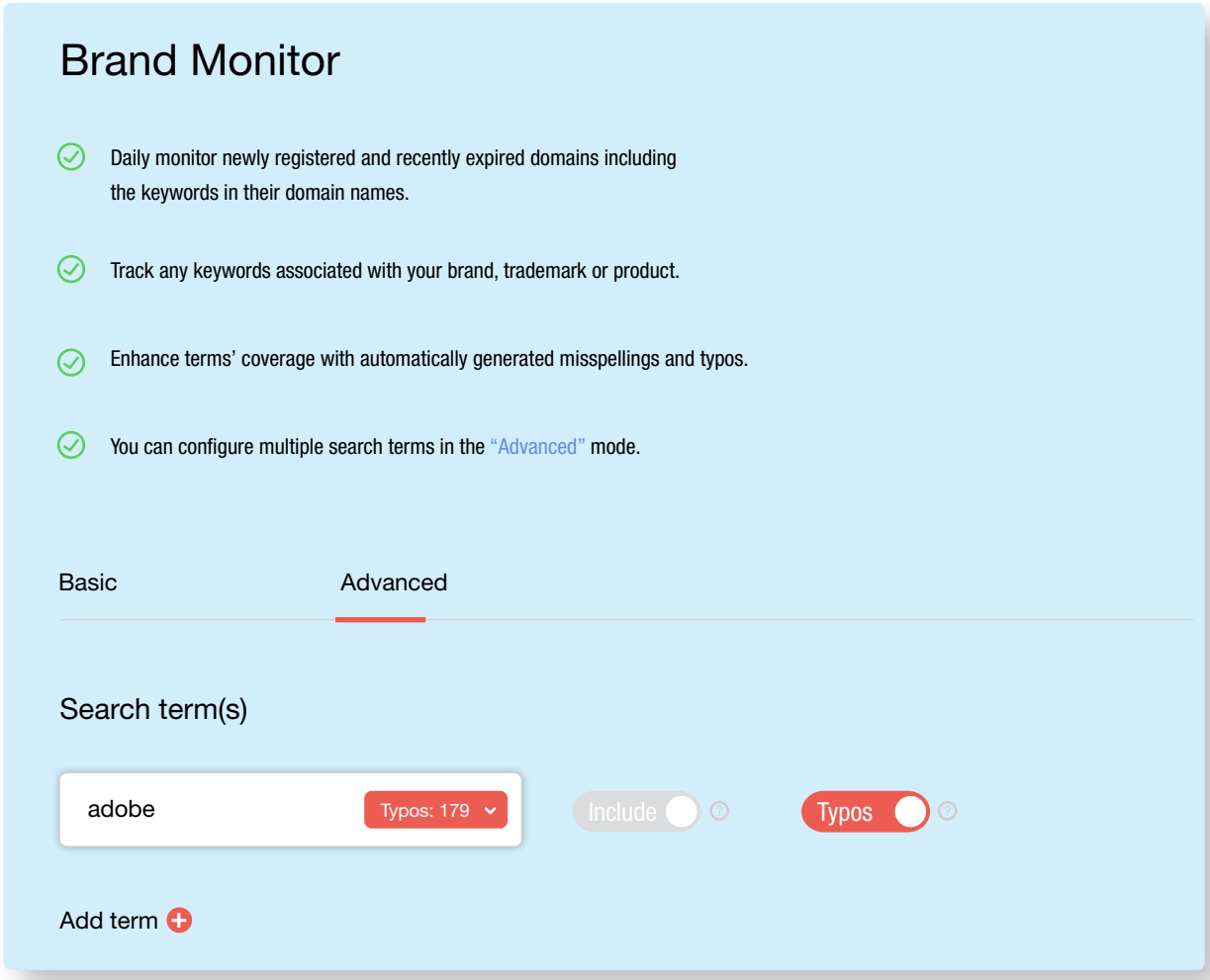
1. Choose a consumption model. DNS, WHOIS, and IP intelligence can be accessed through API calls, downloadable data feeds, or web-based solutions. The key is understanding your organization's data, integration, and data format requirements.

2. Manually retrieve cybersquatting properties targeting your brand, company departments, or chief executives. Input relevant search strings on Domains & Subdomains Discovery Service or look for them in the NRD Database. The screenshot below shows how this can be done using Domains & Subdomains Discovery within the web-based Domain Research Suite (DRS).





3. Automate the discovery process. You may also set up an automatic retrieval operation using Brand Monitor, where you can monitor newly added, recently updated, and expired domains containing company-related keywords. You may also include typos, such as the example below where the tool detected 179 typos for Adobe and included them in its monitoring.



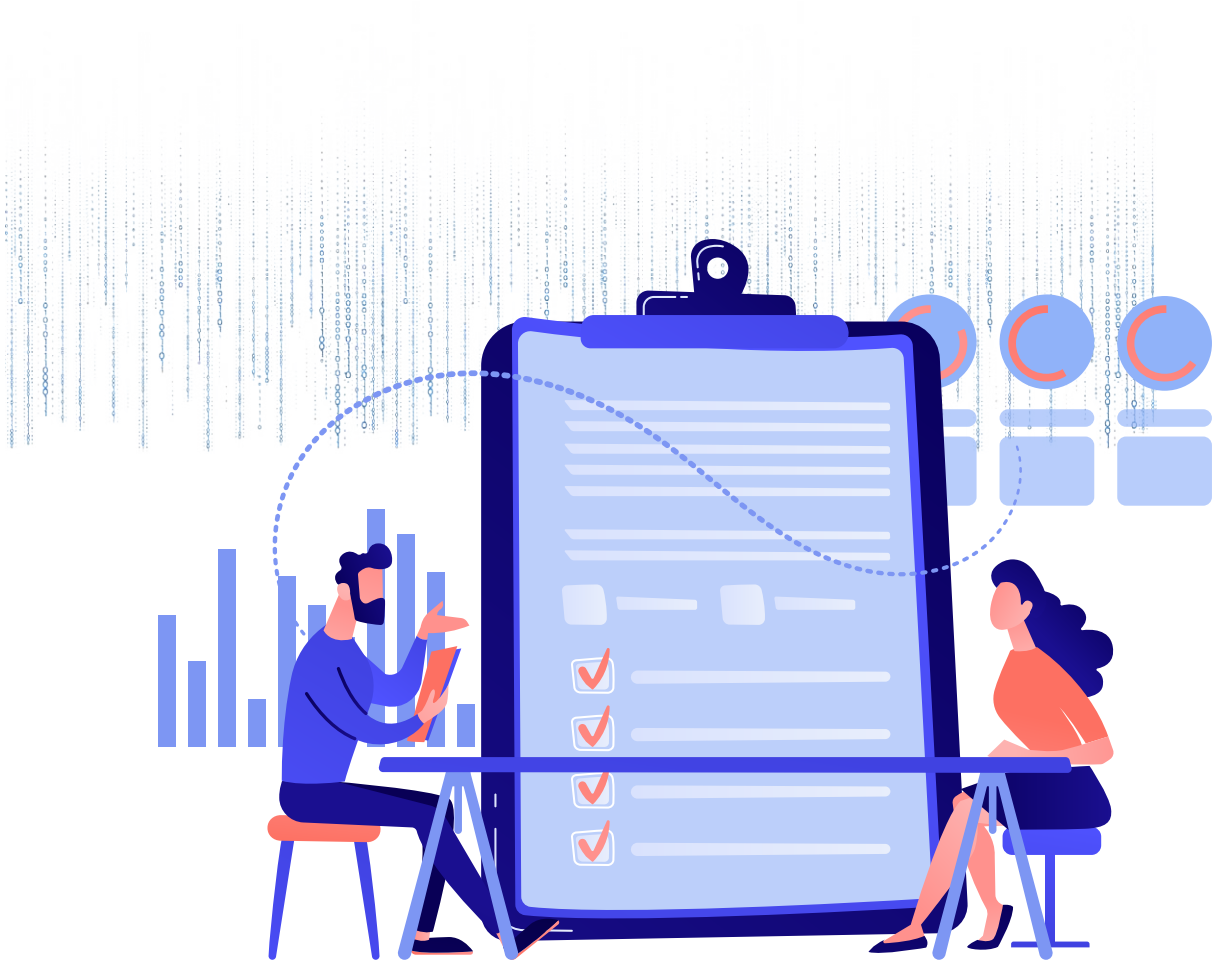
4. Add context to cybersquatting properties. Every domain and subdomain you discover can be enriched with WHOIS information, DNS resolution details, IP geolocation data, content information, and other DNS details. Contextualizing them is crucial for threat prioritization.

5 Conclusion

Business impersonation can facilitate myriad kinds of cybercrime, including financial fraud, phishing, malware attacks, counterfeiting, and BEC scams. It is highly lucrative for cybercriminals. The Federal Trade Commission (FTC) pegged losses to impersonation fraud at US$2 billion between October 2020 and September 2021.

Mitigating this threat is an urgent concern requiring early detection of domain spoofing since domains are among its primary vehicles.

If you wish to perform a similar investigation, feel free to contact us. We are on the lookout for potential research collaborations.



About Us

WhoisXML API is a cyber intelligence provider that gives enterprises access to one of the largest repositories of well-parsed domain, subdomain, IP, and DNS data that enhances cybersecurity platforms' capabilities and helps security teams gain superior network security.

The data that WhoisXML API provides comes in different consumption models, ranging from APIs, data feeds, monitoring tools, and lookup tools, all of which make the Internet more secure and transparent. WhoisXML API has more than 50,000 satisfied customers, spanning law enforcement agencies, cyber forensics analysts, threat hunters, and cybersecurity solutions developers.