

2023

DOMAIN
SECURITY
REPORT

CSC has been at the forefront of reporting on the domain security posture of the Forbes Global 2000 companies annually for the last four years. This year, we're seeing some companies putting a greater emphasis on security, but there are still a large portion of enterprises with considerable domain security risk. It's our intent to elevate the awareness of these threats and share domain security best practices.

We analyzed the adoption of domain security measures used to mitigate cyber risks found in the Global 2000 companies' domain ecosystem that lies outside a company's firewall, as well as incidences of potential online brand abuse and infringement by third parties.

SUMMARY OF KEY FINDINGS



43% OF .AI DOMAINS ARE REGISTERED TO THIRD PARTIES

Companies have either disregarded purchasing their branded .AI domain names, or they're now finding out that many savvy online fraudsters have purchased these domains instead. This is evidenced by a 350% year-over-year increase in domain dispute cases involving .AI extensions in 2023.



21% OF DNS RECORDS FROM SUBDOMAINS POINT TO CONTENT THAT DOES NOT RESOLVE, LEAVING COMPANIES VULNERABLE TO SUBDOMAIN HIJACKING

CSC analyzed over 6 million domain name system (DNS) records from our database and further filtered the set to just over 440,000 DNS records by looking at A records and CNAMEs pointing to Cloud infrastructure, where there is potential for compromise by subdomain hijacking.



79% OF THE REGISTERED DOMAINS THAT RESEMBLE THE GLOBAL 2000 BRANDS (HOMOGLYPHS) ARE OWNED BY THIRD PARTIES

Of the 79% of homoglyph (fake) domains owned by third parties other than the Global 2000 brand owner, 40% have MX records that could be used in a future phishing attack.



46% OF COMPANIES THAT USE ENTERPRISE-CLASS REGISTRARS ALSO USE REGISTRY LOCK

A registry lock enables end-to-end domain name transaction security to mitigate human error and third-party risk. It's a highly cost-effective means to protect domain names against accidental or unauthorized modifications or deletions. Only 7% of companies that use consumer-grade registrars have registry lock deployed. ([See enterprise-class vs consumer-grade registrar.](#))



112 COMPANIES HAVE A DOMAIN SECURITY SCORE OF 0%

6% of the Global 2000 companies do not deploy any of the recommended domain security measures and have the most risk. Based on our analysis of the adoption of key domain security measures, a company's risk level at 0% indicates no adoption of any measure, leaving them at the highest risk of domain security threats.

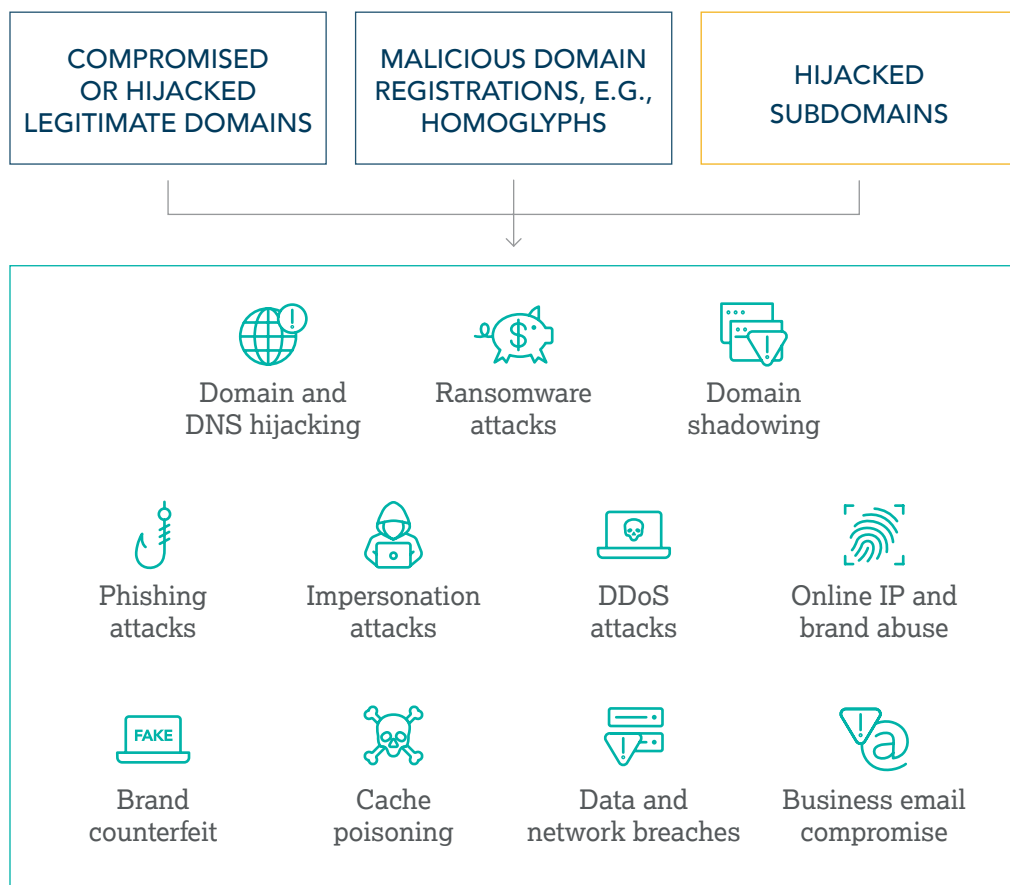


6% GROWTH IN DMARC AND THE HIGHEST GROWTH IN THE PAST FOUR YEARS

The adoption of domain-based message authentication, reporting, and conformance (DMARC)—an email validation system designed to protect a company's email domain from being used for spoofing and phishing scams—has grown 28% since 2020.

2023 EMPHASIZES A COMPELLING BUSINESS CASE FOR DOMAIN SECURITY

As cybersecurity becomes more AI-powered, attacks continue to rise, making domain security an important part of a company's highest-level cyber risk assessment. The following three domain security threats are used to enable all of the attacks listed below.



DOMAIN SECURITY DEFINED

Global businesses rely on the internet for everything— websites, email, authentication, voice over IP (VoIP), and more. It's part of an organization's external attack surface and needs to be continuously monitored for cybercrime and fraud. As cyber risks continue to increase, organizations and cyber insurers face greater challenges in quantifying risks and addressing their capacity for harm. Seemingly every day, we learn about new developments involving supply chain attacks, ransomware, and phishing attacks, along with additional layers of complexity in terms of what coverage they require and how to stop them.

Using proprietary technology, CSC administers domain security with a layered approach. First and foremost, it involves securing the domain portfolio to ensure a brand's online presence is safe—which may consist of multiple brands through acquisitions—and an online DNS footprint. Secondly, we monitor, analyze, and enforce on threat vectors targeting online brands.

WHAT IS A SUBDOMAIN HIJACK?

A subdomain hijack is an attack where cybercriminals gain control of a legitimate subdomain that's no longer in use and load their malicious content to target companies with phishing or malware campaigns. They can do this by cleverly exploiting forgotten DNS records to point to their own content.

EMERGING THREAT: SUBDOMAIN HIJACKING

21% of DNS active subdomain records do not resolve, leaving companies vulnerable to subdomain hijacking.

CSC analyzed over six million DNS records from our database—by looking at A records and CNAMEs pointing to major cloud infrastructure—and identified over 440,000 active subdomain records. This can result in a subdomain hijacking by bad actors. We did this investigation to understand the current state of company subdomain management and how it impacts overall corporate security posture.

HOW TO PROACTIVELY DETECT A SUBDOMAIN HIJACK

1. Conduct a full audit of existing DNS zone files and interrogate every record.
2. Identify the domain names and their corresponding subdomain names that should be active.
3. Monitor continuously through periodic scans of the DNS active records to capture any status change and generate immediate alerts to the SOC 24x7x365 team.
4. Take immediate enforcement action against any illegally launched sites and use an internet blocking ability to prevent the harmful online content.

HOW CAN YOUR LEGITIMATE SUBDOMAINS GET HIJACKED WITHOUT ACTUALLY BEING HACKED?

Large organizations with diverse brand portfolios and international operations are often unaware of the scale of their globally dispersed, digital footprint. Digital records accumulate over time, and this makes maintaining cyber hygiene a real challenge. Businesses have been outsourcing to cloud providers for access to new technologies, yet this increase in DNS records—more than ever before, in addition to increasingly complex environments—opens them up to increased risk. Without proper oversight of digital records and daily monitoring, organizations accumulate “noise” that makes simple cyber hygiene more complex, resulting in easy exploits for cybercriminals.

Cybercriminals scan infrastructures such as the cloud and publicly available services. This includes searching DNS zone records that point to web services that are no longer used by a brand. By hosting content on cloud providers who don't run verification checks, criminals can request a previously used zone destination and start to receive web users landing on these subdomains loaded with their own illegitimate content, all without infiltrating an organization's infrastructure or third-party service account. It was reported by ZDNet that [Microsoft® was hijacked](#) by bad actors to showcase poker casinos on their subdomains.

This buildup of inactive zones that don't point to content is known as “dangling DNS”—putting companies at risk of subdomain hijacking.

This opens a gateway for other cyberattacks targeting brands such as phishing and malware attacks that can result in revenue loss, data exfiltration, loss in consumer confidence, and reputation damage due to security breaches. Research conducted by Vienna-based IT security consulting firm Certitude Consulting recently published in Security Week warning that [thousands of entities are vulnerable](#) to these attacks.

It's imperative that managing DNS records needs to be part of today's cyber hygiene. For more than 20 years, companies have been at risk for mismanagement because they employ different owners, policies, and vendors to manage DNS, which is further complicated if they undergo mergers and acquisitions. In addition, there's also the inherent fear of deleting anything owners are unsure about.

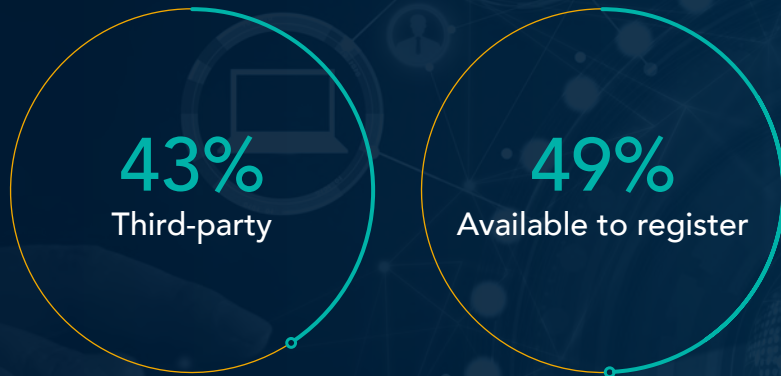
Subdomain hijacking is one of many domain security threats that exist today, including domain and DNS hijacking, domain shadowing, and cache poisoning. These threats often serve as enabling cyberattacks to launch more egregious phishing and ransomware attacks, business email compromise (BEC), or data exfiltration.



[Read our Subdomain Hijacking Vulnerabilities Report or contact CSC to learn more!](#)

43% OF .AI DOMAINS ARE REGISTERED TO THIRD PARTIES

Companies have either disregarded purchasing their branded .AI domain names, or they're now finding out that many savvy online fraudsters have purchased these domains instead.



The technological landscape has seen a remarkable shift with the proliferation of artificial intelligence (AI) technologies. This shift is evident in the notable rise in the registration of .AI domain names, reflecting the widespread adoption and enthusiasm surrounding AI. CSC has been at the forefront of this trend, proactively advising our clients of the importance of having a registration and enforcement strategy for .AI domains¹.

In addition, 2023 has marked a significant increase in domain dispute cases involving .AI extensions. As of September 2023, there has been a substantial increase compared to previous years. This 350% year-over-year increase for 2023, and the fact that the total number of cases has already exceeded the combined total of the previous four years, underscores the growing need for vigilance and regulation².

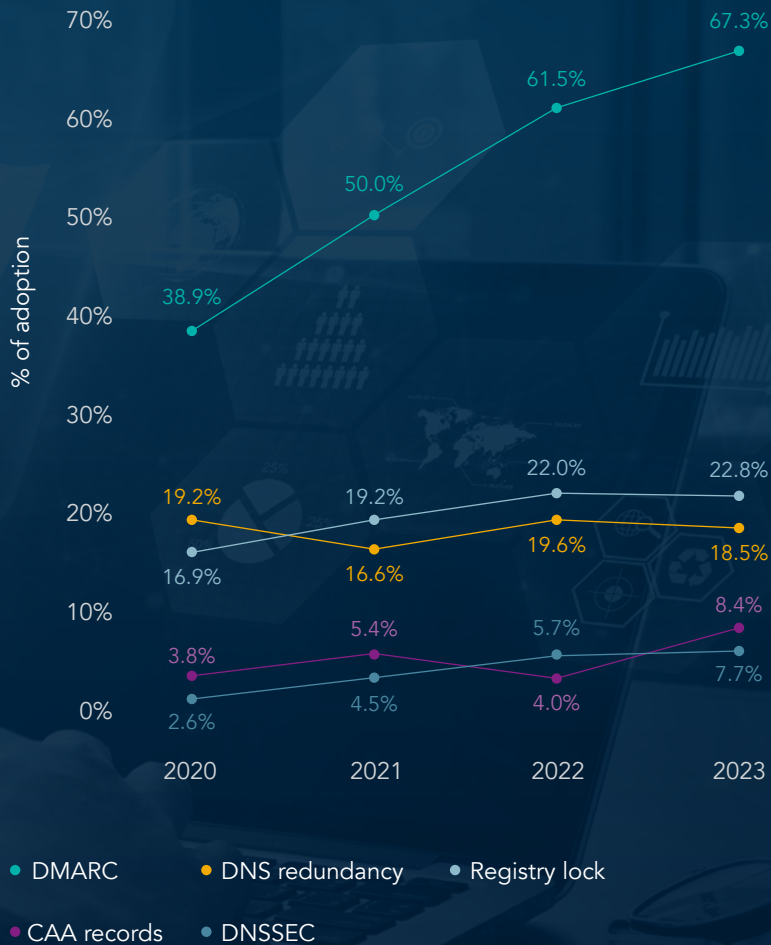
The overall third-party registration or infringement is at 43% for the Global 2000 companies. Of those companies with branded domains registered for .AI, 84% are owned by third parties. 49% are available. Certain industries, such as banking, diversified financials, and IT software and services see the highest percentage of taken .AI domains.

Governments are intensifying regulation on AI tools, but companies continue to develop and adopt AI systems and processes. This trend suggests that the demand for .AI domains will likely rise further. Additionally, the recent decision by Google[®] to treat .AI domains as generic top-level domains rather than a country code signifies a recognition of AI's global relevance³.

The growth in .AI domain registrations is indicative of the broader technology landscape. As AI continues to permeate various aspects of daily life, the associated responsibilities and challenges must be met with diligence and foresight.

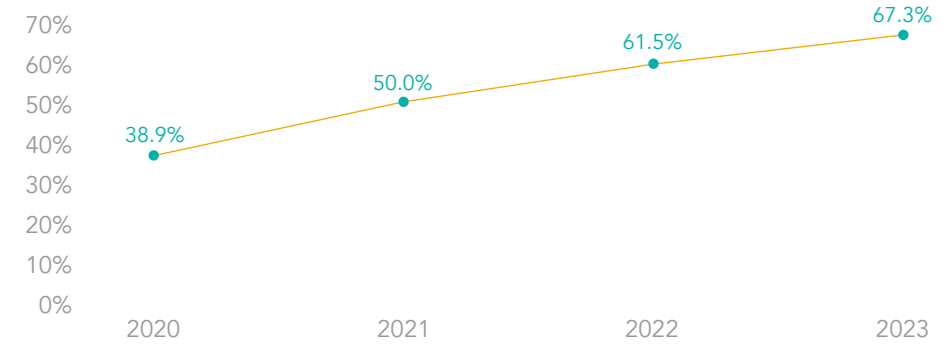
This year, domain dispute cases involving .AI extensions have increased by 350%.

TRENDS IN ADOPTION OF DOMAIN SECURITY MEASURES (2020-2023)



DMARC HAS THE FASTEST GROWTH

It's no surprise given all the news about phishing attacks—including their increase in volume and complexity—that DMARC use has risen quite quickly from 39% in 2020 to 67% in 2023.



The most recent figures from APWG show that 2022 was a record year for phishing with over 4.7 million attacks logged, and BEC attacks in Q4 2022 averaged at \$132,559. Since the beginning of 2019, the number of phishing attacks has grown by more than 150% per year, with over a million phishing attacks quarterly in recent years, targeting about 600 distinct brands each month.

TOTAL MONTH NUMBERS OF UNIQUE PHISHING ATTACKS (APWG)



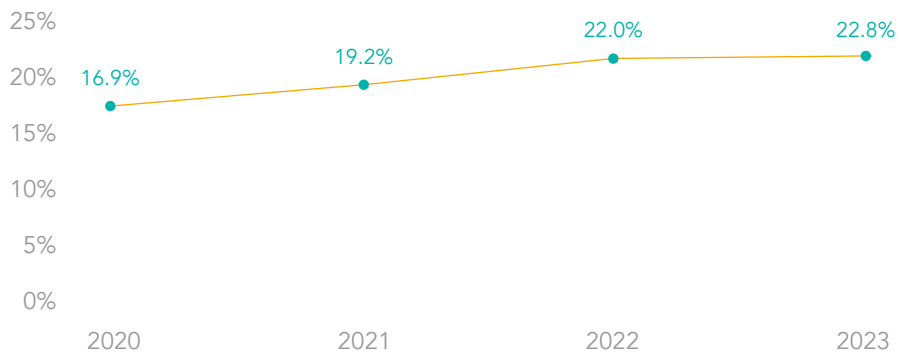
Also, driving growth in DMARC is the increased adoption of brand indicators for message identification (BIMI) on email clients that allow brand logos to be displayed against authenticated emails. DMARC is a security pre-requisite to set up BIMI, and both work in tandem to verify the authenticity of a company's identity on an email domain.

SLIGHT GROWTH IN REGISTRY LOCK BUT STILL HIGH RISK FOR GLOBAL 2000

Companies having registry lock turned on went from 17% adoption in 2020 to 23% in 2023. We also observed a higher incidence where 46% of companies that use enterprise-class registrars also use registry lock. With increasing calls to tighten cybersecurity and remove DNS abuse risks by government agencies, and as a response to regulation and industry pressure, more registries are offering locks on their domain extensions. A registry lock enables end-to-end domain name transaction security to mitigate human error and third-party risk. It's a highly cost-effective means to protect domain names against accidental or unauthorized modifications or deletions. However, some domains may remain unlocked, as not every registry around the world offers lock services.

As a company's portfolio of domains is constantly changing, CSC uses a predictive-modeling algorithm that assesses over 20 attributes of a domain name to identify whether that name is conducting business-critical work for your company operations and online brand, and recommends vital domains that should be locked.

REGISTRY LOCK

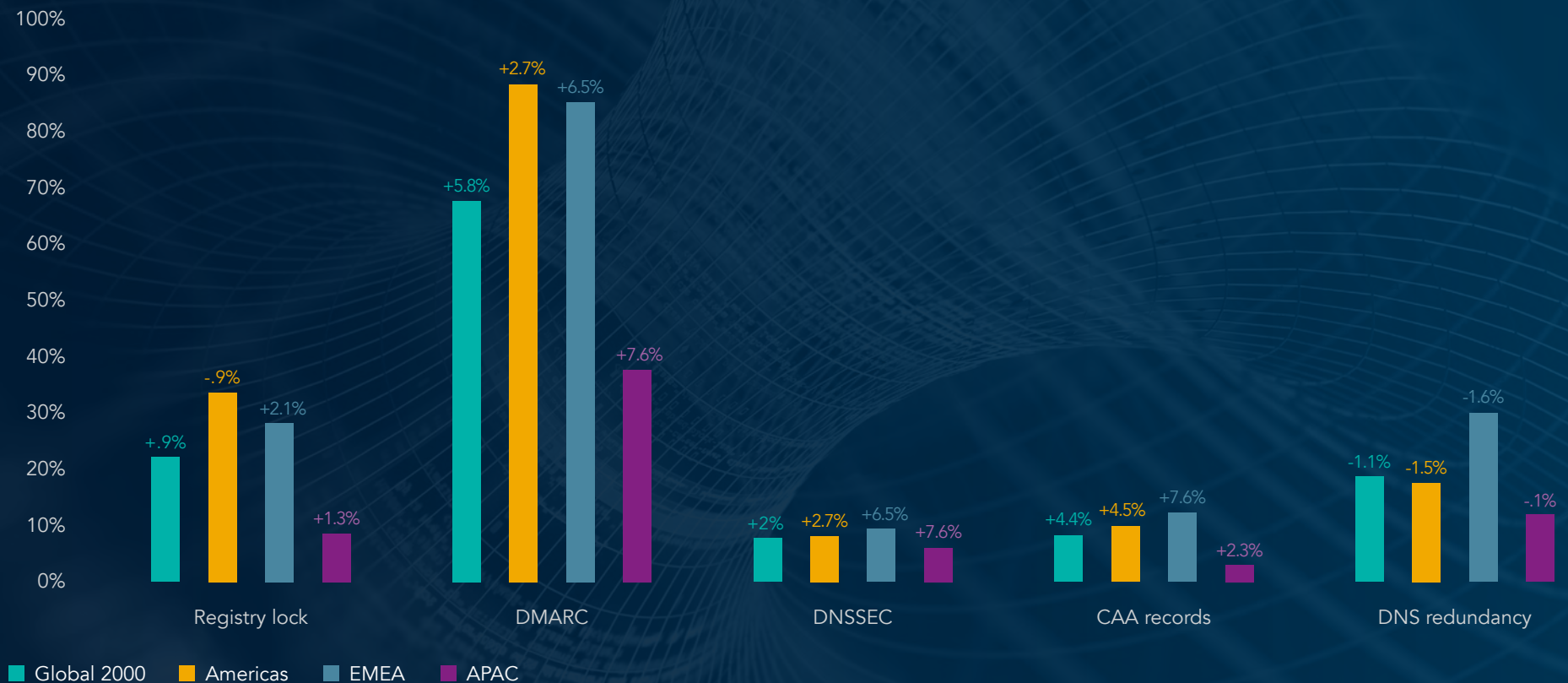


SECURITY MEASURES SUCH AS DNS REDUNDANCY, DNSSEC, AND CAA RECORDS HAVE BEEN INCONSISTENT

While still low, companies deploying domain name system security extensions (DNSSEC) have more than doubled over the past three years from 3% in 2020 to 8% in 2023. Surprisingly, DNS redundancy went down by 1% over last year to 19% even though more government agencies are calling for resilience in DNS. DNS redundancy is a critical component in any organization's core infrastructure, and we're seeing adoption for this security measure decreasing, which could be attributed to companies needing to plan for increasing cost and resource allocation.

Lastly, the use of certification authority authorization (CAA) records increased quite a bit this year moving from 3.8% in 2020 to 8.4% in 2023. CAA records allow companies to designate a specific certificate authority (CA) to be the sole issuer of certificates for their company's domains. This prevents cybercriminals from using a non-appointed certificate authority to get a new certificate, as their request will fail, and the company will receive an alert. However, many companies still don't fully use this security control, as it's often difficult for them to navigate the requirements, especially when they use multiple providers for their domains, DNS, and secure sockets layer (SSLs).

2023 DOMAIN SECURITY MEASURES BY REGION



+/- % change from previous year

2023 DOMAIN SECURITY MEASURES BY REGISTRAR TYPE

For this report, we analyzed the trend of domain security adoption with respect to the type of domain registrar used by the companies that make up the Global 2000.



Consumer-grade registrars:

A consumer-grade registrar is geared for domain services, websites, and email for personal use, entrepreneurs, and small businesses that are just getting started.



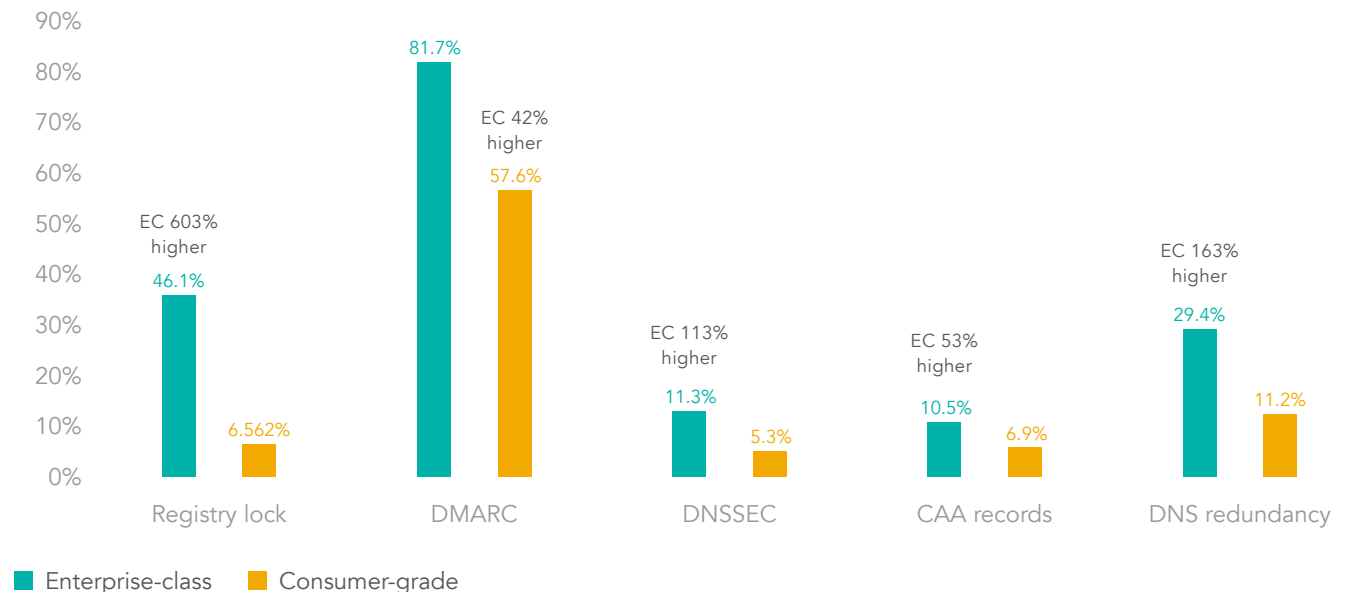
Enterprise-class registrars:

An enterprise-class registrar specializes in working with corporations and brand owners that require advanced business practices, capabilities, expertise, and support staff in relation to domain and DNS management as well as security, brand and fraud protection, data governance, and cybersecurity.

Many companies have a misconception that all registrars are the same. There's misplaced trust put into consumer-grade registrars that may not have been designed for domain security that can impact a company's overall security posture. This is especially apparent for the adoption of registry locks, as most consumer-grade registrars don't support them.

COMPANIES THAT RELY ON ENTERPRISE-CLASS CAPABILITIES HAVE A HIGHER ADOPTION OF DOMAIN SECURITY MEASURES

Maturity level of security measures, enterprise-class (EC) vs consumer-grade (CG) registrars



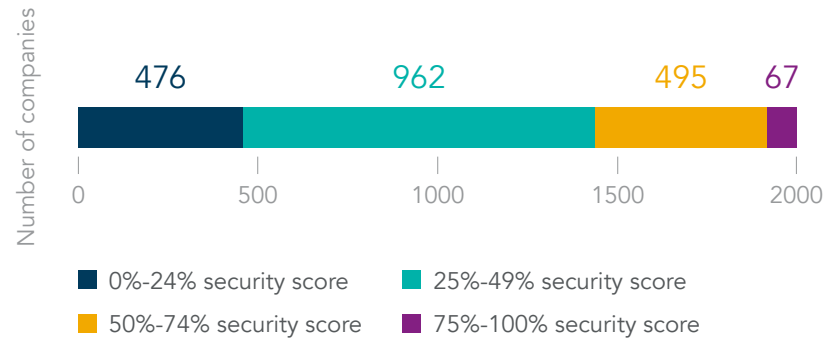
OVERALL DOMAIN SECURITY POSTURE

Looking at the importance of eight key security measures that we grouped according to a company's domain security risk level, CSC derived an average score for each company. This average makes up the company's security score with a higher score denoting a stronger security posture—meaning companies are at less risk of domain security threats.

KEY DOMAIN SECURITY MEASURES:

- Enterprise-class registrar
- Registry lock
- CAA records
- DNS redundancy
- DNSSEC
- Sender policy framework (SPF)
- DomainKeys identified mail (DKIM)
- DMARC

DOMAIN SECURITY RISK LEVELS OF THE GLOBAL 2000



72% of all companies have less than half of the security measures implemented



HIGHEST PERFORMING INDUSTRIES

- IT software and services
- Media
- Business services and supplies
- Hotels, restaurants, and leisure
- Health care equipment and services



HIGHEST PERFORMING COMPANIES

- Only two companies had the highest security score with the most adoption of 100% of domain security measures.



LOWEST PERFORMING INDUSTRIES

- Utilities
- Trading companies
- Food markets
- Construction
- Materials



LOWEST PERFORMING COMPANIES

- 112 companies have a domain security score of zero.
- These companies are primarily from the Asia-Pacific region, making up 87% of the zero-score companies.

SUSPICIOUS OR MALICIOUS DOMAIN ACTIVITY TARGETING THE GLOBAL 2000

We identified and analyzed domains containing brand names with more than six characters from the Global 2000 companies that were not owned by the brands themselves. The intent of these fake domain registrations is to leverage the trust placed on the targeted brand to launch phishing attacks or other forms of digital brand abuse or IP infringement that leads to revenue loss, traffic diversion, and a diminished brand reputation.

There are endless domain spoofing tactics and permutations that can be used by phishers and malicious third parties.

WE INTENTIONALLY FOCUS ON COMMON HOMOGLYPHS AS THEY ARE ONE OF THE MOST EGREGIOUS ATTACK METHODS USED BY THREAT ACTORS

Domain spoofing tactics

- Fuzzy matches
- Homoglyphs-IDNs
- Cousin domains
- Keyword match
- Homophones (Soundex)

Common homoglyphs (fuzzy matches) in .COM domains

Based on frequent observation of use in phishing domains, our analysis included common Latin-character substitutions, for example, using C0rnpanyName.com to look like CompanyName.com

Most popular character substitutions

i → l m → n i → 1 s → 5 o → 0
e → 3 l → 1 l → i w → vv

OVER 79% OF HOMOGLYPH DOMAINS ARE OWNED BY THIRD PARTIES

Out of the third-party owned domains:

87% have their WHOIS or ownership details masked in 2023, compared to 82% in 2022. This increase could be intentional or by virtue of redaction due to privacy policies such as the General Data Protection Regulation (GDPR). However, attempts to mask or hide ownership and identity, especially on third-party domains, lean towards registration with nefarious intentions.

40% have MX records in 2023. This compares to 48% in 2022. MX records can be used to send phishing emails or to intercept email.

HOW ARE THIRD-PARTY DOMAINS BEING USED?

36% point to advertising, pay-per-click ads, or are being used for domain parking.

49% had inactive websites.

1% point toward malicious content that could damage a brand's reputation and customer confidence.

14% resolve to a live website not associated with the brand holder.

With the recent launch of Threads by Instagram in July 2023, brands are already feeling the effects of third-party domain registrations, some being used to claim affiliation, logo abuse, brand impersonation, and more.



Read more: [New CSC Research Indicates Launch of Threads by Instagram is Already a Growing Target for Fraud and Brand Abuse](#)

SUSPICIOUS AND MALICIOUS DOMAINS: WHO'S BEING TARGETED?



DOMAIN REGISTRARS MOST ASSOCIATED WITH FAKE DOMAIN REGISTRATIONS OWNED BY THIRD PARTIES:

 GoDaddy®

 Namecheap™


 Network Solutions

CONCLUSION

The risk of a company not addressing their domain security can be catastrophic. Unprotected domains pose a significant threat to cybersecurity posture, data protection, consumer safety, intellectual property, supply chains, revenue, and reputation.

Our research shows that 43% of .AI domains associated with the Global 2000 companies are registered with third parties. As evidenced by a 350% year-over-year increase in domain dispute cases involving .AI extensions in 2023, companies that did not secure their .AI domains are now finding out that many savvy online fraudsters have purchased these domains instead.

To complement strategic domain registrations, companies need to apply domain security using a layered security model within the Zero Trust framework to create a robust corporate security posture with the least risk to the business. A partnership with an enterprise-class registrar is necessary not only to gain visibility into exposed surfaces (which includes domain names and DNS), and to analyze threat vectors targeting a company's online presence, but also to offer mitigating solutions and enforcement action.

 View CSC's list of defensive and proactive security measures to safeguard your domains and brands using a multi-layered, defense-in-depth approach to domain security.

[Download our Domain Security Checklist.](#)

ABOUT CSC'S DOMAINSEC PLATFORM

CSC's 3D Domain Security and Enforcement solution was created by harnessing the power of CSC's DomainSecSM platform. DomainSec is a software as a service (SaaS) cybersecurity platform that CSC invented, and is the industry's first holistic approach for securing and defending brands' domain ecosystems. It uses proprietary machine learning deep search technology and combines machine learning, artificial intelligence, and clustering technology to identify lead indicators of compromise.

DomainSec brings CSC's domain management and domain security into one platform, along with brand protection and fraud protection solutions—meaning we can offer exponentially better protection and help organizations refine their Zero Trust security model, going beyond just safeguarding perimeters.



CSC is the trusted security and threat intelligence provider of choice offering domain security solutions for the Forbes Global 2000 and the 100 Best Global Brands® including secure domain portfolio management, domain name system (DNS), digital certificate management, as well as digital brand and fraud protection. As global companies make significant investments in their security posture and continue efforts to protect their external attack surface, CSC can help them understand their domain security risks and how it aligns to their zero trust model. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss, and significant financial penalties because of policies like the General Data Protection Regulation (GDPR). CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—taking a holistic approach to digital asset protection, along with fraud protection services to combat phishing. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia-Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve. Visit cscdbs.com.

¹CSC's Blog, "AI You Ready? A Domain to Add to Your Portfolio—Before Someone Else Does." cscdbs.com/blog/ai-you-ready-a-domain-to-add-to-your-portfolio-before-someone-else-does/

²DNDISPUTES.COM, "AI: Domain Name Dispute Cases with AI Extension" dndisputes.com/case/domain/extension/ai/

³Search Engine Land, "Google now treats .ai domains as generic top-level domains" searchengineland.com/google-now-treats-ai-domains-as-generic-top-level-domains-427770

Copyright ©2023 Corporation Service Company. All Rights Reserved.

CSC is a service company and does not provide legal or financial advice. The materials here are presented for information purposes only. Consult with your legal or financial advisor to determine how this information applies to you.