CSC

2024-2025 Domain Security Report

INTRODUCTION

CSC has been at the forefront of reporting on the domain security posture of the Forbes Global 2000 companies annually for the past five years. We analyze the adoption of domain security measures used to mitigate cyber risks found in the Global 2000 companies' domain ecosystem that lay outside a company's firewall, as well as incidences of potential online brand abuse, and infringement by third parties.

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 to improve all organizations' domain security postures.

As CSC celebrates the fifth anniversary of its annual "Domain Security Report," we reflect on our ongoing commitment to analyzing the domain security posture of the Forbes Global 2000 companies. This year, coinciding with CSC's 125th anniversary, we continue to elevate awareness about cyber risks outside a company's perimeter in the digital space, and the need for robust domain security measures.

SUMMARY OF KEY FINDINGS

HEALTHCARE EQUIPMENT AND SERVICES INDUSTRY DROPPED IN RANKING FOR DOMAIN SECURITY DESPITE INCREASE IN PROMINENT CYBER ATTACKS

This year, the most notable shift in domain security by industry was seen in Healthcare Equipment and Services companies, dropping seven spots from 5th in 2023 to 12th in 2024. Conversely, Technology Hardware and Equipment rose eight spots from 13th in 2023 to 5th in 2024.

80% OF THE REGISTERED WEB DOMAINS THAT RESEMBLED GLOBAL 2000 BRANDS (HOMOGLYPHS) ARE OWNED BY THIRD PARTIES AND DO NOT BELONG TO THAT BRAND

Of the 80% of homoglyph (lookalike fake) domains owned by third parties other than the Global 2000 brand owners, we found that 42% have MX records (email exchange records) compared with 40% in 2023. MX records can be used to send phishing emails or to intercept email.

107 OF THE GLOBAL 2000 COMPANIES HAVE A DOMAIN SECURITY SCORE OF ZERO

5% of the Global 2000 companies do not deploy any of the recommended domain security measures and therefore have the highest level of risk. Based on our analysis of the adoption of key domain security measures, a security score of zero indicates no adoption of any measure, leaving those companies at the highest risk of domain security threats.

USE OF REGISTRY LOCK HAS GROWN BY 7 PERCENTAGE POINTS SINCE 2020, BUT OVERALL ADOPTION IS LOW AT 24%

Registry locks enable end-to-end domain name transaction security to mitigate human error and third-party risk. It's a highly cost-effective means of protecting domain names against accidental or unauthorized modifications or deletions.

USE OF DMARC HAS GROWN BY 32 PERCENTAGE POINTS SINCE 2020

In 2023, the Anti-Phishing Working Group (APWG) reported a record of almost five million logged phishing attacks, making 2023 the worst year for phishing. This rise in attacks helped increase 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.

THE EXTERNAL ATTACK SURFACE IS WHERE THE DOMAIN ECOSYSTEM LIVES

As cyber threats become more AI-powered, attacks continue to rise. This makes domain security an important part of a company's highest-level cyber risk assessment, which must include a company's domain ecosystem as a real vulnerability to the attacks shown in Figure 1. Compromised or hijacked legitimate domains or malicious domain registrations are used to enable all of the attacks in Figure 1.

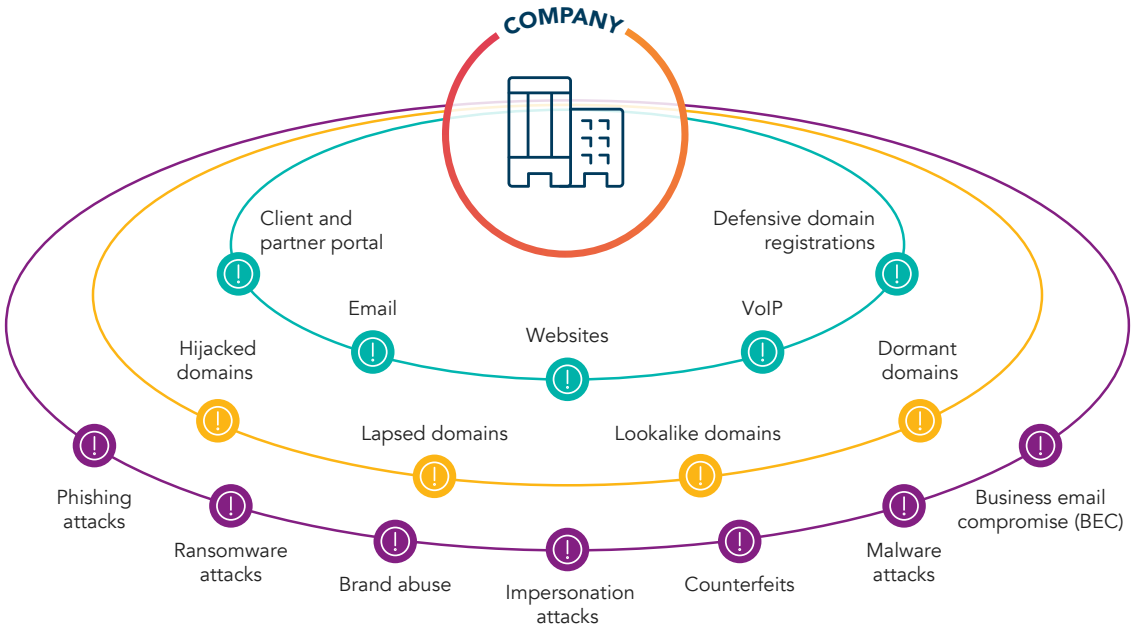
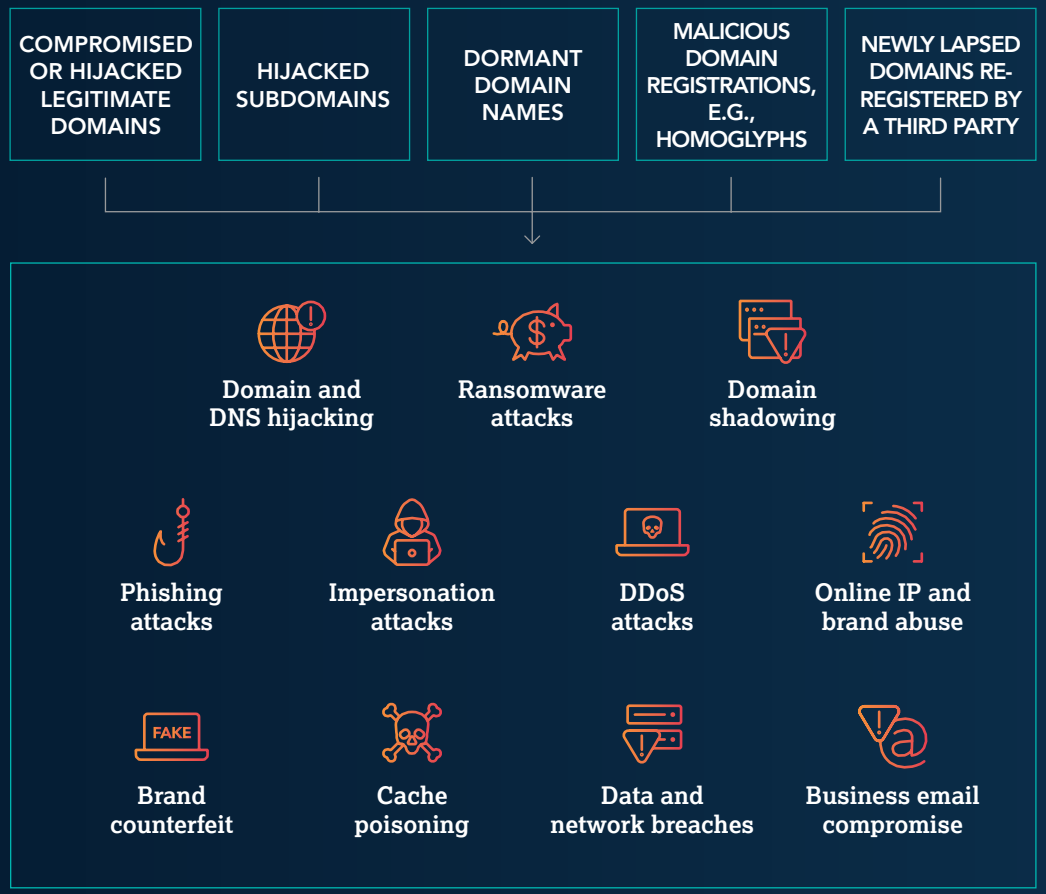


Figure 1: The galaxy of the domain name ecosystem

DOMAIN SECURITY DEFINED

Global businesses rely on the internet for everything—websites, email, authentication, voice over IP (VoIP), client portals, supplier applications, 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 them and addressing their capacity for harm. This means domain names are crucial elements of an organization's cybersecurity posture since the internet and domain names are essential to business infrastructure and continuity.



COMPROMISED OR HIJACKED LEGITIMATE DOMAINS

Cyber criminals will compromise any domains left unsecured. Companies should start with a layered, defense-in-depth approach to protect against hijacking.

HIJACKED SUBDOMAINS

A subdomain hijack is an attack where cybercriminals gain control of a legitimate subdomain that's no longer in use to host malicious content to target companies with phishing or malware attacks. They do this by exploiting forgotten domain name system (DNS) records (dangling DNS) to point to their own content.

DORMANT DOMAIN NAMES

Cybercriminals may register and hold onto branded domains keeping them dormant until they're ready to weaponize them in a phishing or malware attack. Dormant domains often escape initial detection because they don't immediately have any of the indicators of a domain registered to launch an attack—e.g., an active MX record—which would usually raise a red flag.

MALICIOUS DOMAIN REGISTRATIONS

There are endless domain spoofing permutations and homoglyphs that are easily used by phishers and malicious third parties. The intent of these fake domain registrations is to leverage the consumer trust in the targeted brand to launch convincing phishing attacks or other forms of digital brand abuse.

NEWLY LAPSED BRANDED DOMAINS RE-REGISTERED BY A THIRD PARTY

Companies may choose to lapse previously defensively registered domain names due to cost pressures. Cybercriminals wait for this and immediately re-register these domain names for malicious purposes. They're constantly on the lookout for available, branded domains they can weaponize.

FINDINGS AND ANALYSIS: GLOBAL 2000 ADOPTION OF DOMAIN SECURITY MEASURES

In this analysis, CSC looked at the adoption of five key domain security measures—namely DMARC, DNS redundancy, registry locks, certificate authority authorization (CAA) records, and DNS security extensions (DNSSEC)—across the Global 2000 list. We then performed a deep analysis into the adoption levels across industry groups and regions.

TRENDS IN ADOPTION OF DOMAIN SECURITY MEASURES (2020-2024)

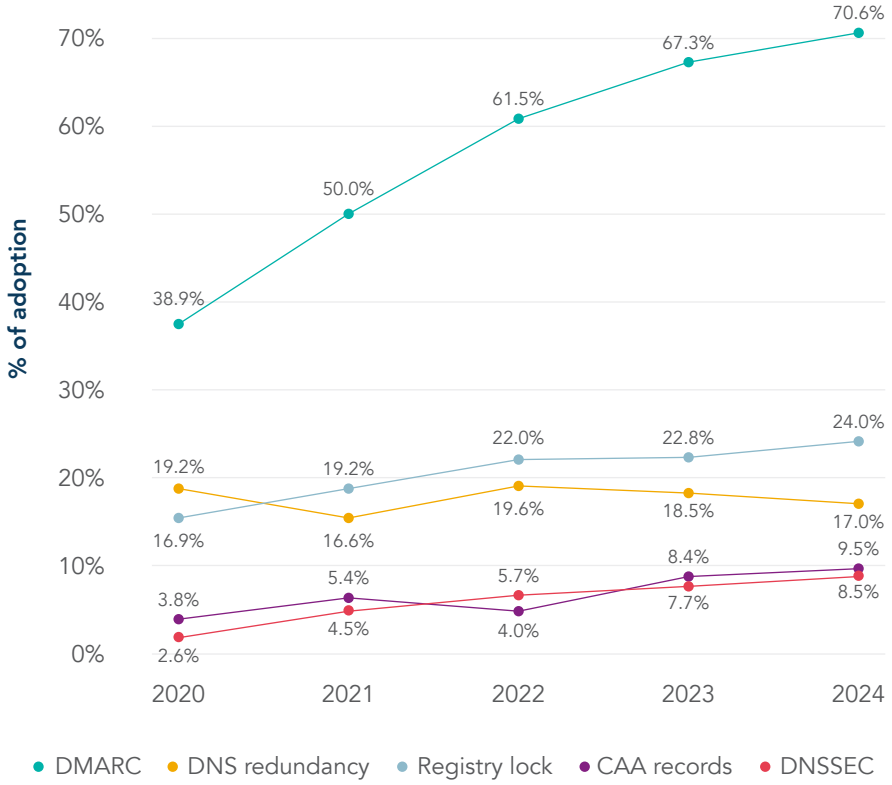


Figure 2: Global 2000 adoption of the five key domain security measures, 2020-2024

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 adoption has risen quickly from 39% in 2020 to 71% in 2024 (Figure 3).

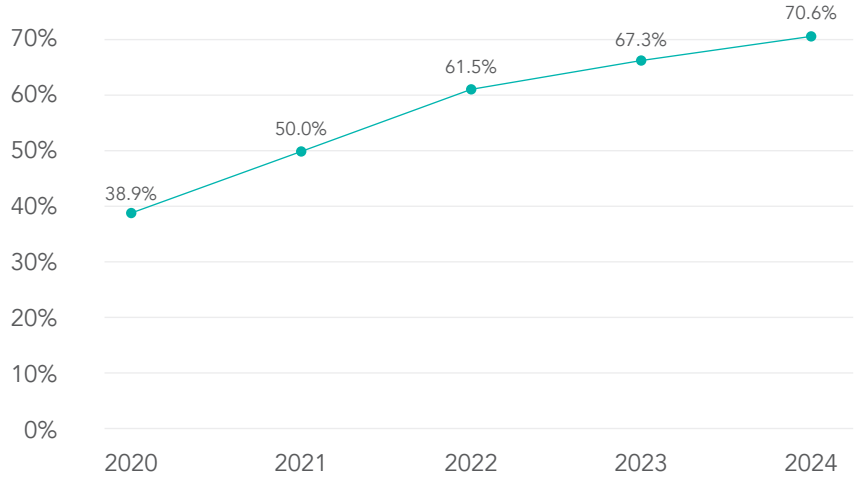


Figure 3: DMARC adoption rates 2020-2024

Another factor driving growth in DMARC adoption could be the increased use 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.

STEADY BUT SLOW GROWTH IN REGISTRY LOCK USE

Adoption rates of registry locks rose from 17% of companies in 2020 to 24% in 2024. We also observed that companies that use enterprise-class registrars also use registry lock more frequently at 45% in 2024. With increasing pressure to tighten cybersecurity, more registries are offering locks on their domain extensions to enable end-to-end domain name transaction security—mitigating human error and third-party risk.

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

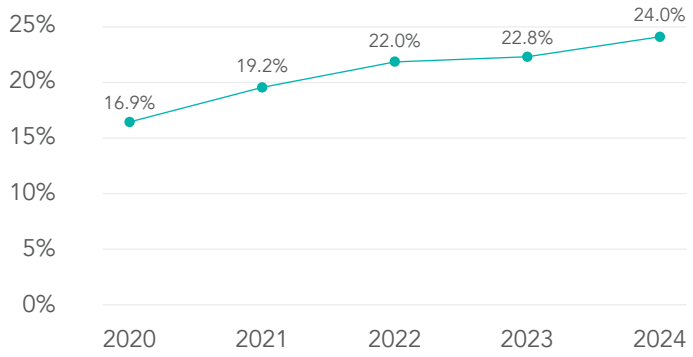


Figure 4: Registry lock adoption rates 2020-2024

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

While still low, the percentage of companies deploying DNSSEC has tripled over the past five years from 3% in 2020 to 9% in 2024. DNSSEC works by providing authentication and data integrity to DNS queries and responses, which in turn prevents cybercriminals from redirecting internet traffic to malicious websites, such as phishing websites.

Surprisingly, DNS redundancy went down by 1% again this year, bringing the percentage of companies that prioritize DNS redundancy lower this year than in 2020. 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.

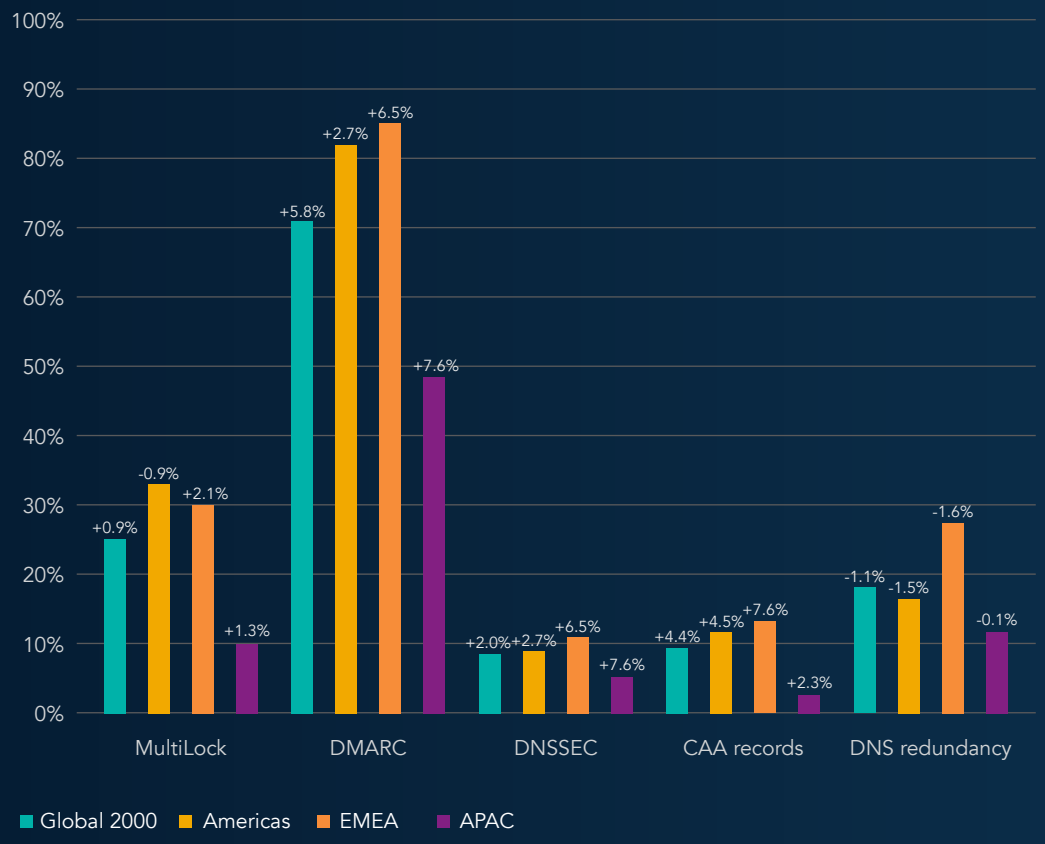
Lastly, the use of CAA records increased this year to 10% in 2024, up from 4% in 2020. CAA records allow companies to designate a specific certificate authority (CA) to be the sole issuer of digital certificates for their company's domains. This prevents cybercriminals from using a non-authorized certificate authority to gain a new digital certificate, as their request will fail, and the company will receive an alert.

We also observed that companies that use enterprise-class registrars also use registry lock more frequently at 45% in 2024.

DOMAIN SECURITY MEASURES

BY REGION

EMEA has shown the largest growth in domain security adoption between 2023 and 2024.



+/- % change from previous year

Figure 5: Domain security adoption by region

BY INDUSTRY

Healthcare drops seven spots in ranking in 2024.

Industry classification	2024 rank	2023 rank	
Technology Hardware and Equipment	5	13	↑
Health Care Equipment and Services	12	5	↓

Across 26 Forbes Global 2000 industries, **Healthcare Equipment and Services** fell seven spots and out of the top five industry ranking it previously held. The drop in ranking from 5th in 2023 to 12th in 2024 stands in stark contrast to the prominent rise in cyber attacks on hospitals and healthcare systems this year, especially considering the healthcare sector is now the most frequent target for ransomware attacks.[1] Already in 2024, the healthcare sector has reported 280 cyber incidents. This is "24% of all United States cyber events in 2024, putting healthcare ahead of every other industry."[2]

Technology Hardware and Equipment rose eight spots to rank 5th. It is certainly advantageous for technology companies to be ranked in the top five, and their growth may have to do with the security measures these companies have been putting into place since major supply chain attacks began in 2020 with Solar Winds.

HIGHEST PERFORMING INDUSTRIES

- Business services and supplies
- IT software and services
- Media
- Retailing
- Technology hardware and equipment

LOWEST PERFORMING INDUSTRIES

- Construction
- Food, drink, and tobacco
- Food markets
- Materials
- Oil and gas operations

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.

Many companies have a misconception that all registrars are the same. There's misplaced trust put into consumer-grade registrars that may not prioritize or even offer domain security measures, which 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.

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.

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.

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

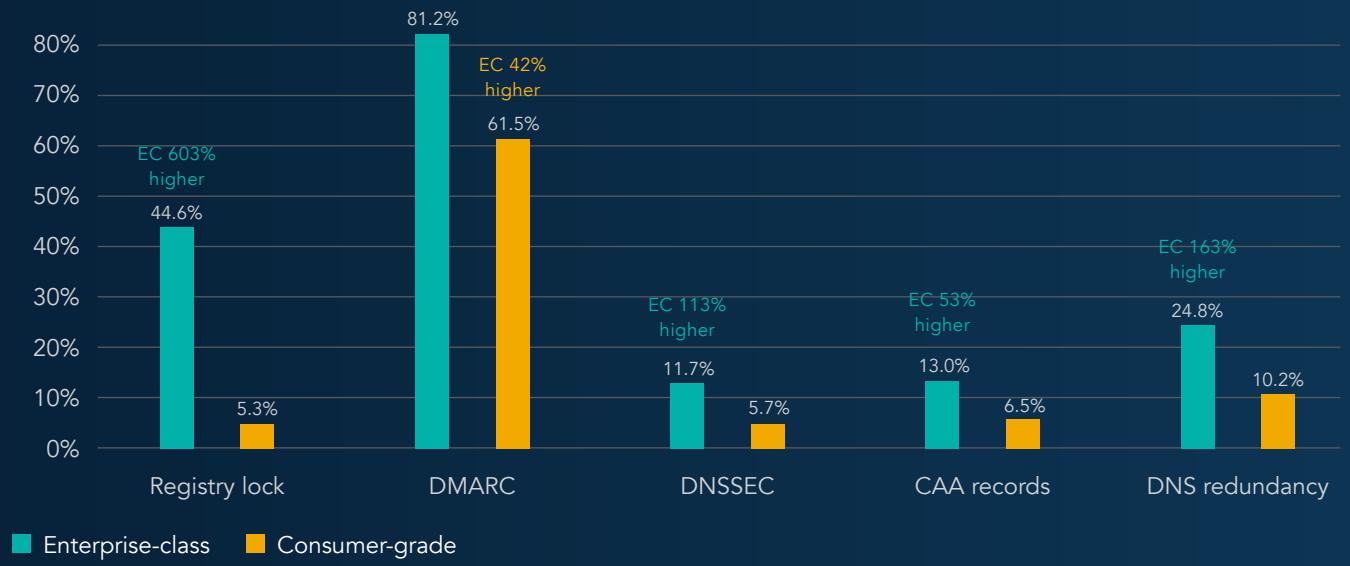


Figure 6: Maturity level of security measures—enterprise-class (EC) vs consumer-grade (CG) registrars

DOMAIN SECURITY POSTURE

Looking at the importance of an expanded list 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 (MultiLock)
- CAA records
- DNS redundancy
- DNSSEC
- Sender policy framework (SPF)
- DomainKeys identified mail (DKIM)
- DMARC

DOMAIN SECURITY RISK LEVELS

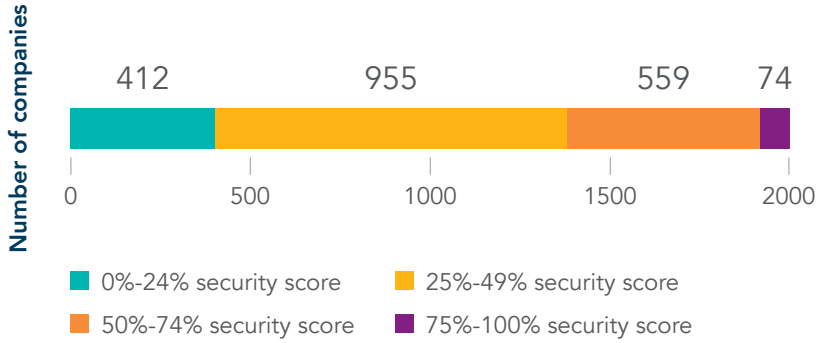


Figure 7: Domain security scores and associated domain security risk levels of Global 2000 companies

68% of all Global 2000 companies have less than half of the recommended security measures implemented.

HIGHEST PERFORMING COMPANIES

There is only one company that has a 100% score and had a 100% score last year. There are 12 companies that have a score of 7 out of 8.

LOWEST PERFORMING COMPANIES

107 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 Global 2000 brand names with more than six characters that were not owned by the brands themselves. The intent of these third-party domain registrations is to leverage the trust placed on the targeted brand to launch phishing attacks, other forms of digital brand abuse, or IP infringement. These lead to revenue loss, traffic diversion, and a diminished brand reputation for the affected brand.

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

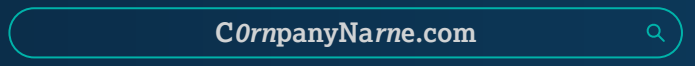
WE INTENTIONALLY FOCUS ON COMMON HOMOGLYPHS AS THEY ARE ONE OF THE MOST EGREGIOUS ATTACK METHODS USED BY THREAT ACTORS

DOMAIN SPOOFING TACTICS

Figure 8: Common domain spoofing tactics

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 C0rnpanyNarne.com to look like CompanyName.com.



Most popular character substitutions

c → e	0 → 0	m → n	l → I	m → rn
g → q	E → 3	S → 5	B → 8	l → 1

Figure 9: Common homoglyphs (fuzzy matches) in .COM domains

80% OF HOMOGLYPH DOMAINS ARE OWNED BY THIRD PARTIES

Out of the third-party owned domains:

42% have MX records in 2024. This compares with 40% in 2023. MX records can be used to send phishing emails or to intercept email.

HOW ARE THIRD-PARTY DOMAINS BEING USED?

48% point to advertising, pay-per-click ads, or are being used for domain parking.

33% have inactive websites.

2% point toward malicious content that could damage a brand's reputation and customer confidence.

17% resolve to a live website not associated with the brand owner.

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

- GoDaddy®
- Namecheap™
- Network Solutions

SUSPICIOUS AND MALICIOUS DOMAINS: WHO'S BEING TARGETED?

INDUSTRY	FAKE DOMAIN THREAT % OF TOTAL
Banking	19.9%
Diversified financials	7.2%
IT software and services	7.2%
Construction	6.4%
Insurance	6.3%
Oil and gas operations	6.2%
Utilities	6.1%
Capital goods	5.5%
Consumer durables	5.3%
Business services and supplies	5.0%
Transportation	4.9%
Materials	4.7%
Retailing	4.6%
Technology hardware and equipment	4.2%
Drugs and biotechnology	3.5%
Food, drink, and tobacco	3.4%
Health care equipment and services	3.4%
Telecommunications services	3.0%
Semiconductors	2.9%
Chemicals	2.6%
Aerospace and defense	2.0%
Hotels, restaurants, and leisure	1.7%
Household and personal products	1.7%
Food markets	1.5%
Trading companies	1.2%
Media	1.1%

DOMAIN SECURITY INSIGHTS: LESSONS LEARNED FROM DOMAIN SURGES DURING THE OLYMPICS IN 2024

As with other major global events, the Olympic Games in Paris, July 2024, faced digital threats from scammers seeking to exploit its global reach through counterfeit items, fake tickets, fraudulent streaming sites, and phishing attacks. Monitoring domain ecosystems globally—including lookalike, dropped, re-registered, or newly registered domain names—should be a priority in any corporate security posture and brand's online strategy to mitigate these digital threats. Companies should be especially vigilant for **dormant domains**—those not yet weaponized but showing signs of a developing attack infrastructure.

HIGHLIGHTS

Through our research, we identified 8,857 unique third-party domain names containing the term "Olympics" or related keyword terms like "Paris 2024" (see Figure 10). Our analysis examined domain activity, including new registrations, dropped registrations, and re-registrations, during the period from August 1, 2023, to August 13, 2024. As shown in the figure 10, we observed a particular surge in new registration activity coinciding with the start of the Olympics on July 26 and the end on August 13. Of the domains that are still registered, 49% were dormant, and did not have an active website. However, of those domains, 25% had an MX record and 8% had an SSL certificate tied to it.

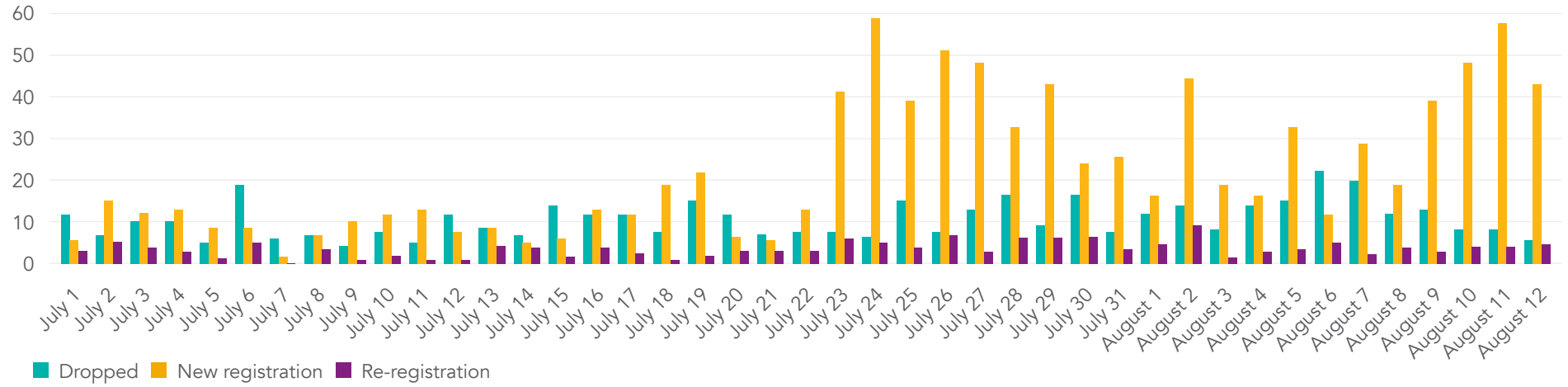


Figure 10: Domain registration trends between July 1, 2024, and August 1, 2024 (60 days)

KEY TAKEAWAY

Ongoing real-time monitoring of these domains is crucial, as the weaponization of dormant domains can occur at any time. By tracking domain names with malicious intent, organizations can better identify potential risk factors before they become active.

CONCLUSION

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

If companies are not already doing so, they should be conducting searches across the complete global domain name ecosystem, including generic top-level domains and country code top-level domains. Advanced monitoring services like CSC's 3D Domain Security and Enforcement solution can detect a wider range of domain variations beyond basic exact matches, wildcards, and typos. Additionally, companies need to partner with a provider that can execute takedowns on various threats, including phishing sites, malware downloaders, typosquatting domains, deceptive search engine optimization sites, social media portals, mobile app stores, and marketplaces selling counterfeit products.

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

Download our Domain Security Checklist.

CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands (Interbrand®) with focus areas in domain security and management, along with digital brand and fraud protection. As global companies make significant investments in their security posture, our DomainSec℠ platform can help them understand cybersecurity oversights that exist and help them secure their online digital assets and brands. 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. CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—with a multidimensional view of various threats outside the firewall targeting specific domains. Fraud protection services that combat phishing in the early stages of attack round out our solutions. 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.

Get in touch

cscdbs.com

[1]npr.org/sections/shots-health-news/2024/09/17/nx-s1-5111590/cyberattacks-ransomware-health-care-federal-response

[2]tebra.com/theintake/practice-operations/medical-news/the-major-cyberattacks-that-have-affected-healthcare-systems-in-2024

DBS01102025