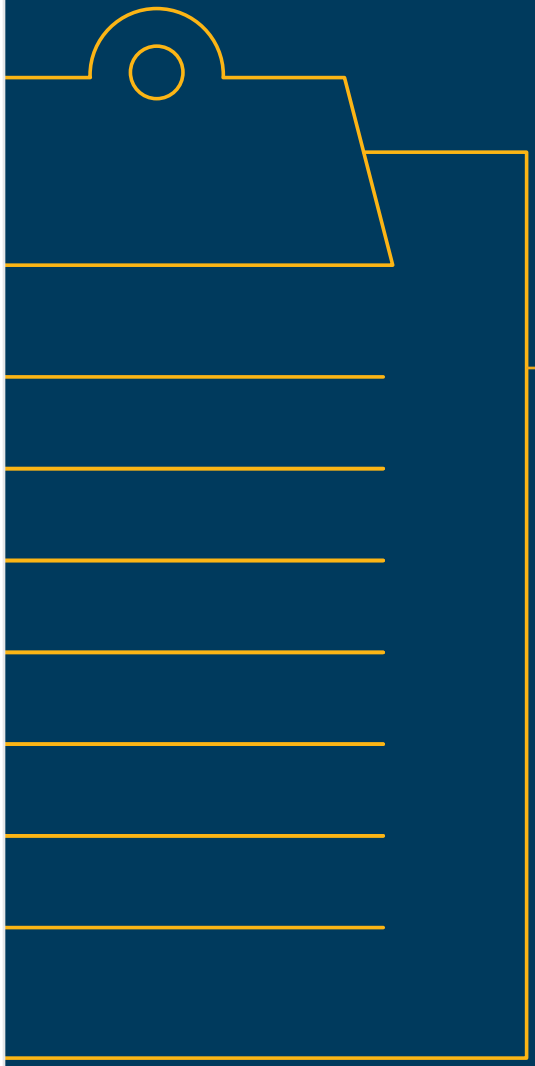
WHERE DOMAIN SECURITY MEETS THE SUPPLY CHAIN CRUNCH

cscdbs.com



Executive summary

New research from CSC indicates that fraudsters took advantage of the 2022 baby formula shortage to target consumers with fake, branded domain names. Key findings show a surge in baby formula related domain registrations that leverage trusted brands to steer consumers away from authentic websites and apps. **84%** of those web domains created since 2021 are fake e.g., owned by third parties other than the brand owner. This is potentially a real concern for consumers in terms of product safety, phishing attacks, financial hardships, and data exfiltration—as well as for the companies that own these brands. In addition to the market for baby formula, we saw the same type of fake domain registrations mimicking chip manufacturers in the semi-conductor industry. **95%** of registered branded domain names created since 2021 are owned by third parties other than the brand owner.

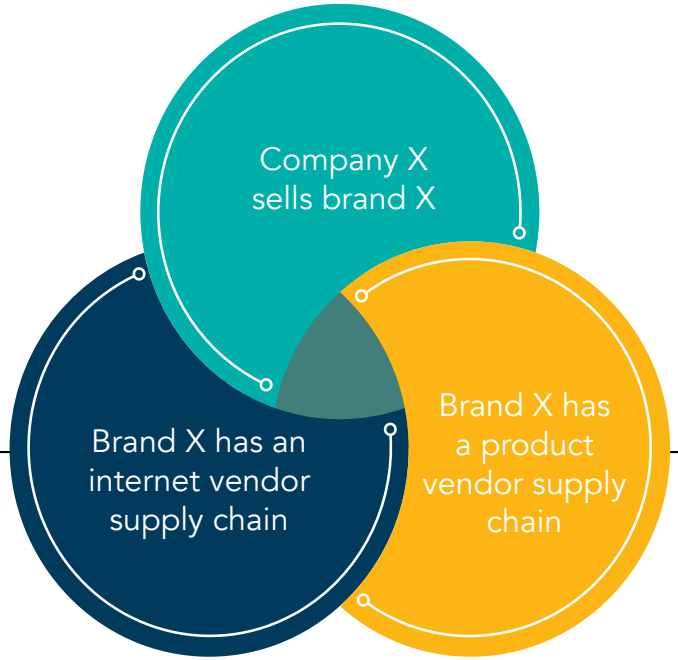
Lastly, a substantial number of companies lack domain security hygiene, putting themselves at greater domain security risk, and showcasing the breadth of the problem across critical infrastructure sectors. If a widescale attack (i.e., domain name system (DNS) hijacking or distributed denial of service (DDOS) attack) on a cloud provider or a domain registrar were to take place—or social engineering or phishing attacks—domain security hygiene can make an organization more resilient in the face of these risks.

Domain security connection to the supply chain

Over the last two years, we've all faced supply shortages on items that we previously never fathomed could be in short supply. Businesses' management teams are asking, "What is it that we should know, but don't?" There is a significant corporate risk factor that continues to go unnoticed—the security of branded web domain registrations.

As we've seen with recent supply chain attacks such as **Colonial Pipeline** and **JBS Foods**, an attack on one company through a singular point of compromise has the potential to disrupt an entire network of connected companies and products, partners, vendors, and customers—and can create exponential returns for the attacker. Due to the connected nature of domain names and the DNS, a single compromise at a domain registrar or cloud provider, or a phishing attack using a fake domain, can extend beyond the internet supply chain and into product and infrastructure supply chains.

Online fraud involves fake domain registrations and attacks on cloud providers, domain registrars, and DNS hosting providers.



Example:

Baby formula shortages are an offline brand concern that is magnified by cybersecurity risks.

CSC's new research shows that risk increases for companies and consumers experiencing supply chain shortages

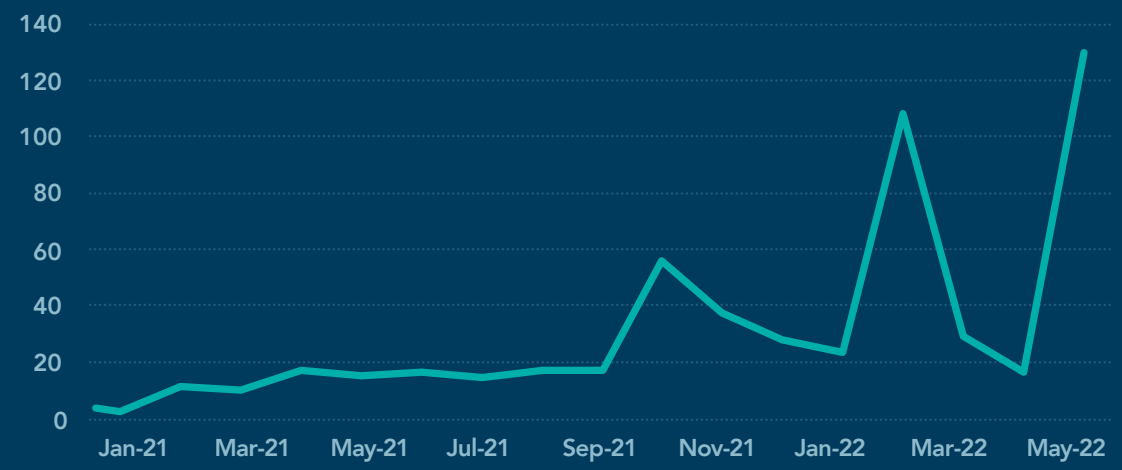
Fake domains are at the epicenter of fraud on the internet, which can create revenue loss, reputation damage, consumer safety issues, and additional cybersecurity concerns for brand owners. CSC has observed that as global and societal events such as supply chain shortages occur, there is a corresponding increase in domain registrations that attempt to capitalize on the event. In January 2022, CSC released **research on the surge in fraudulent COVID-related domain names** based on cybercriminals taking advantage of vaccine-related and health organization brands in this same way.

CSC's research team assessed web domains containing the top baby formula and semiconductor brand names. Consistent with prior research, there was a surge of fake domain registrations between 2021 and May 2022.

Key findings: Baby formula shortage

CSC reviewed domain names containing the top five baby formula brand names and other relevant search terms such as baby- milk, formula, and feed.

Monthly numbers of registrations of third-party domains related to baby formula (brands and keywords)



84%

of the domains are owned by third parties*

**According to our definition of third-party domains, these are not owned by the brand owners and are fake.*

93% used domain privacy services, or also had WHOIS details redacted.

This demonstrates the attempt to mask or hide ownership and identity, suggesting they may have nefarious intentions.

26% are configured with MX (email) records.

Domains with MX records can be used to send phishing emails or to intercept email.

Domain registrars most associated with fake registrations in the analysis:

- GoDaddy.com, LLC
- Sav.com, LLC
- Chengdu West Dimension Digital Technology Co., Ltd

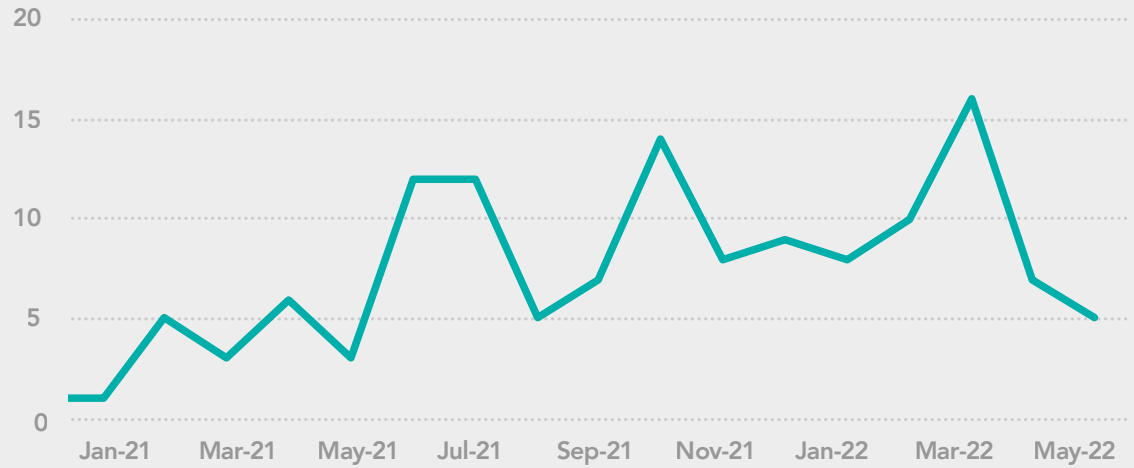
DNS hosting domains most associated with fake registrations in the analysis:

- domaincontrol.com (provider GoDaddy)
- bodis.com (provider Bodis)
- registrar-servers.com (provider NameCheap)

Key findings: Semi-conductor shortages

CSC explored domain names containing the top six semiconductor brand names or other relevant search terms such as semiconductor- and electronic- chip.

Monthly numbers of registrations of third-party domains related to semiconductor chips (brands and keywords)



95%

of the domains are owned by third parties*

**According to our definition of third-party domains, these are not owned by the brand owners and are fake.*

79% used domain privacy services, or also had WHOIS details redacted.

This demonstrates the attempt to mask or hide ownership and identity, suggesting they may have nefarious intentions.

44% are configured with MX (email) records.

Domains with MX records can be used to send phishing emails or to intercept email.

Domain registrars most associated with fake registrations in the analysis:

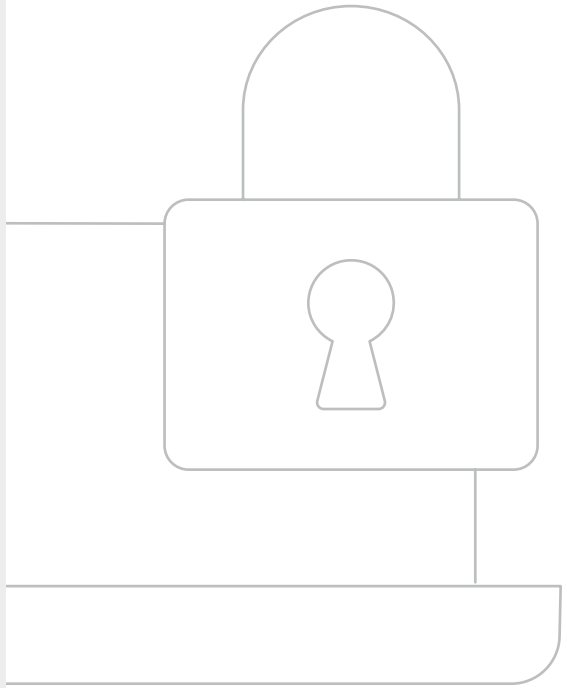
- GoDaddy.com, LLC
- Namecheap Inc.
- Dynadot LLC

DNS hosting domains most associated with fake registrations in the analysis:

- domaincontrol.com (provider GoDaddy)
- registrar-servers.com (provider NameCheap)
- hichina.com (provider Alibaba)

Domain security and cyber hygiene

With domain security, in addition to protecting your company from fake domain registrations, it's imperative to be proactive and use key security controls as part of **domain security hygiene**. CSC recommends a **defense in depth approach**, incorporating the following advanced security measures:



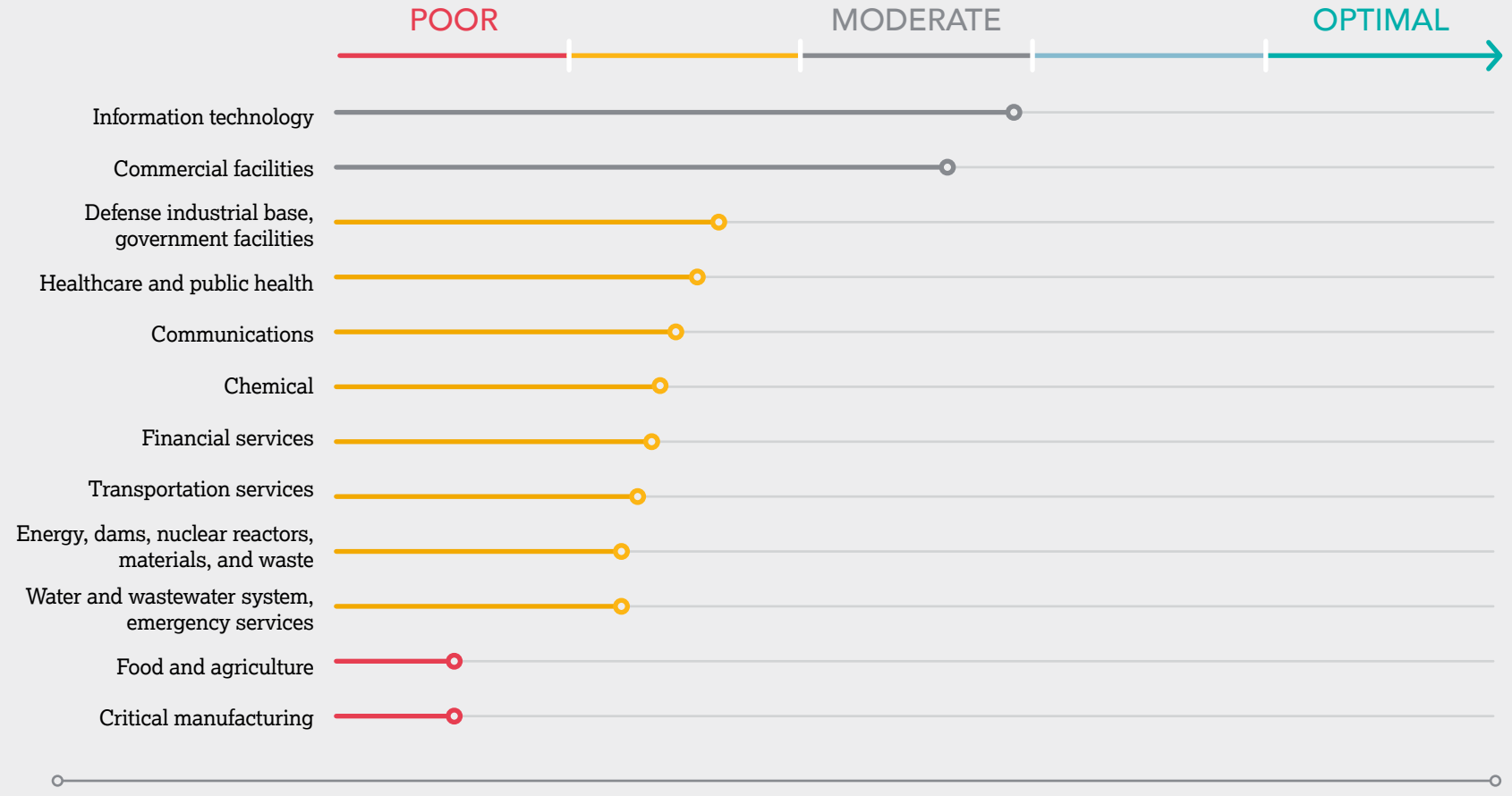
CSC's domain security hygiene measures

Domain security measure	Purpose
DNS hosting redundancy	Mitigates against downtime and DDoS attacks.
Domain Name System Security Extensions (DNSSEC)	Prevents hackers from taking control of an internet browsing session with the goal of redirecting users to deceptive websites.
Sender Policy Framework (SPF)	Email authentication standards mitigate spam, spoofing, and phishing.
Domain-based Message Authentication, Reporting and Conformance (DMARC)	
Domain Keys Identified Mail (DKIM)	
MultiLock	Combines registry- and registrar-level locks and a WHOIS lock to prevent unauthorized changes of DNS records and domain hijacking.
Certification Authority Authorization (CAA) records	Ensures that only authorized certification authorities can issue a certificate.
Use of an enterprise-class registrar	Specializes in working with enterprises 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.

Looking at the bigger critical industries picture

Using our data from the **Domain Security Report**, we looked at the Global Forbes 2000 companies, and mapped the underlying industry sectors to one of the 16 **CISA critical infrastructure sectors**. We then observed the eight domain security hygiene signals as noted on the previous page to rank the adoption of domain security measures by these critical infrastructure sectors.

Risk mitigation effectiveness scale



These latest findings give context to the larger underlying issue facing the industries that semiconductors and baby formula fall into—critical manufacturing, and food and agriculture—and show that domain security posture across the board remains weak with minimal improvement.

CSC's Domain Security Report: Forbes Global 2000 offers a deeper analysis on the domain security posture of the most critical business industries around the globe.

81% are at greater risk of domain name and DNS hijacking because they have NOT adopted basic domain security measures like domain registry lock.

57% rely on consumer-grade domain registrars with limited protection against domain and DNS hijacking, DDoS, man-in-the-middle-attacks (MitM), or DNS cache poisoning.

50% use DMARC records as an email authentication method.

Risks lead to desperate measures and requires action

Buyers of goods in short supply will go to great lengths to find a way to purchase what they need. Brands and the domain industry must be vigilant in ensuring consumers are visiting safe and authorized domains. Weak domain security posture is not a new challenge, but it's becoming a front and center issue that needs greater strategic emphasis. Companies need to scour the internet to locate and address anything that may dilute or harm their brand and takes their end-consumer down a path to fraudulent activity. These risks are avoidable and the consumer experience of navigating online to find what they need only to be met by a cybercriminal must stop. Better domain security measures must be implemented and the business community must embrace and adopt broad domain security standards.

Brands have made significant investments in digital transformation, brand protection, and cybersecurity risk mitigation. Yet, the resulting systemic risks with domains and within the DNS are leading to supply chain vulnerabilities, phishing, fraud (i.e., ransomware and business email compromise), brand abuse, and counterfeiting. Companies that supply critical infrastructure need to demonstrate more of what they can do to improve their security posture. Domain security is a part of this and is a systemic business risk.

Additionally, the cyber insurance industry should evaluate these risks too. Cyber insurance premiums and the underwriting experience is changing for many companies with insurers starting to look at new metrics that can influence the insurance policy. A weak domain security posture reflected in these metrics could have long-term consequences for these companies. Inaction when it comes to domain security is not an option. CSC sees an urgent need for broader domain security standards, as well as policy or regulations relating to daily activity and behavior over the DNS.

To learn more about how to ensure your organization is protecting itself, visit:

DOMAIN SECURITY RECOMMENDATIONS IN OUR SUPPLY CHAIN BLOG POST →

CSC is the trusted provider of choice for the Forbes Global 2000 and the 100 Best Global Brands® in enterprise domain names, 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, CSC can help them understand known 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, 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**.

Vincent D'Angelo, global director, Corporate Development and Strategic Alliances

Quinn Taggart, senior advisor, Global Brand Security

Sue Watts, global leader, Marketing

David Barnett, head of Consultancy, Brand Monitoring

DBS07082022