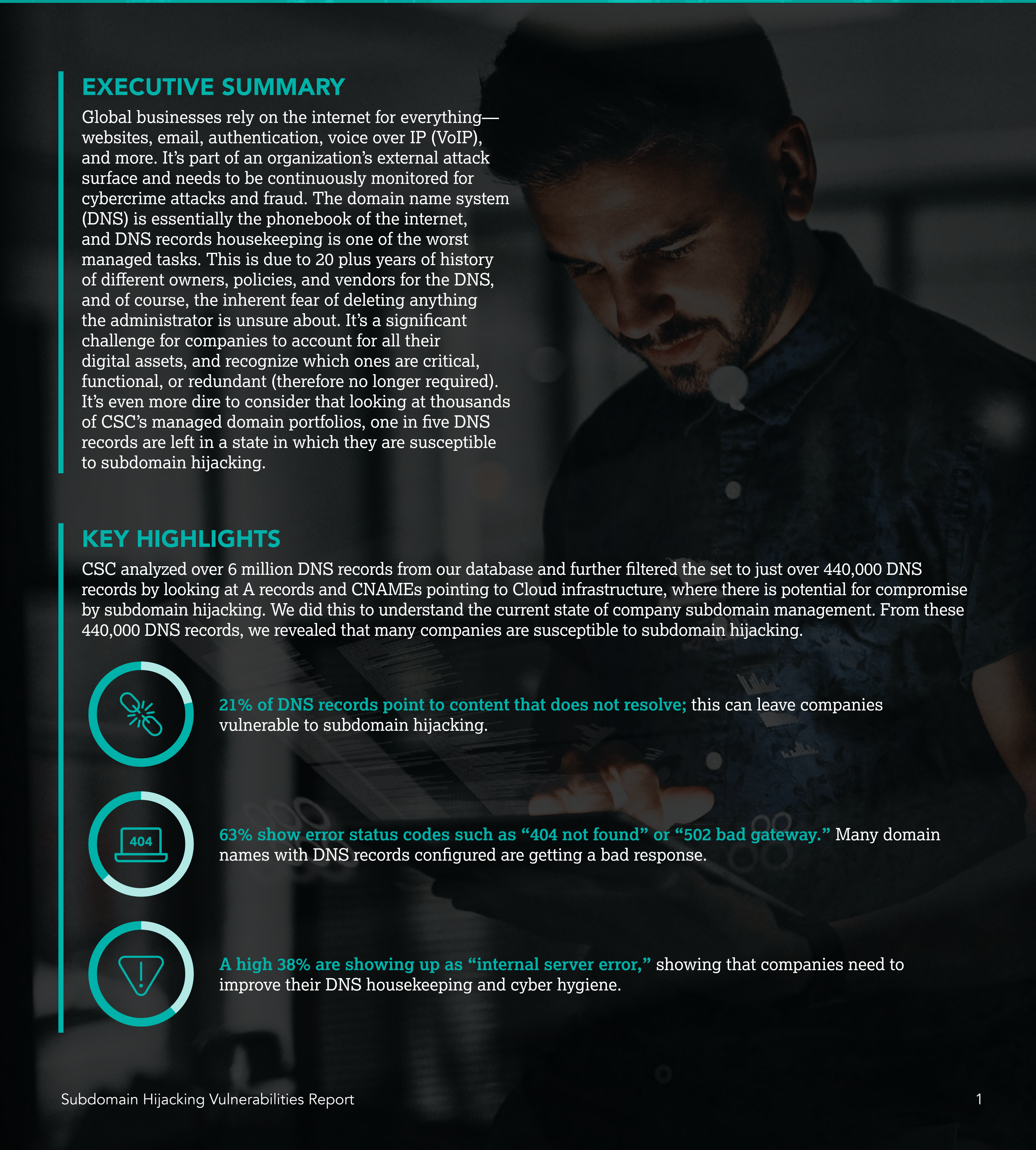
CSC

SUBDOMAIN HIJACKING

VULNERABILITIES REPORT



EXECUTIVE SUMMARY

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 attacks and fraud. The domain name system (DNS) is essentially the phonebook of the internet, and DNS records housekeeping is one of the worst managed tasks. This is due to 20 plus years of history of different owners, policies, and vendors for the DNS, and of course, the inherent fear of deleting anything the administrator is unsure about. It's a significant challenge for companies to account for all their digital assets, and recognize which ones are critical, functional, or redundant (therefore no longer required). It's even more dire to consider that looking at thousands of CSC's managed domain portfolios, one in five DNS records are left in a state in which they are susceptible to subdomain hijacking.

KEY HIGHLIGHTS

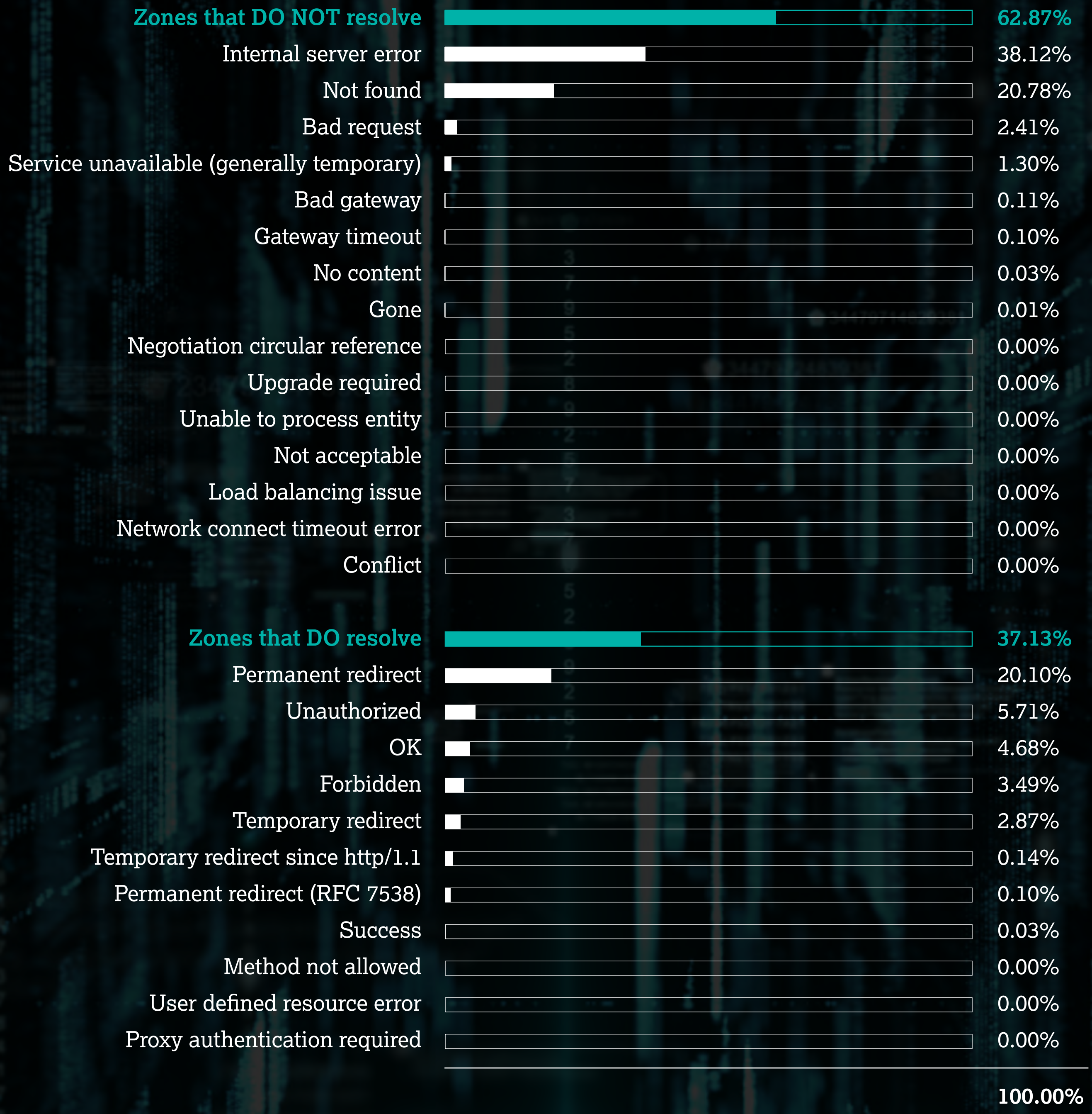
CSC analyzed over 6 million DNS records from our database and further filtered the set to just over 440,000 DNS records by looking at A records and CNAMEs pointing to Cloud infrastructure, where there is potential for compromise by subdomain hijacking. We did this to understand the current state of company subdomain management. From these 440,000 DNS records, we revealed that many companies are susceptible to subdomain hijacking.

21% of DNS records point to content that does not resolve; this can leave companies vulnerable to subdomain hijacking.

63% show error status codes such as "404 not found" or "502 bad gateway." Many domain names with DNS records configured are getting a bad response.

A high 38% are showing up as "internal server error," showing that companies need to improve their DNS housekeeping and cyber hygiene.

ANALYZED DNS RECORDS



Zones that DO NOT resolve	**62.87%**
Internal server error	38.12%
Not found	20.78%
Bad request	2.41%
Service unavailable (generally temporary)	1.30%
Bad gateway	0.11%
Gateway timeout	0.10%
No content	0.03%
Gone	0.01%
Negotiation circular reference	0.00%
Upgrade required	0.00%
Unable to process entity	0.00%
Not acceptable	0.00%
Load balancing issue	0.00%
Network connect timeout error	0.00%
Conflict	0.00%
Zones that DO resolve	**37.13%**
Permanent redirect	20.10%
Unauthorized	5.71%
OK	4.68%
Forbidden	3.49%
Temporary redirect	2.87%
Temporary redirect since http/1.1	0.14%
Permanent redirect (RFC 7538)	0.10%
Success	0.03%
Method not allowed	0.00%
User defined resource error	0.00%
Proxy authentication required	0.00%
	100.00%

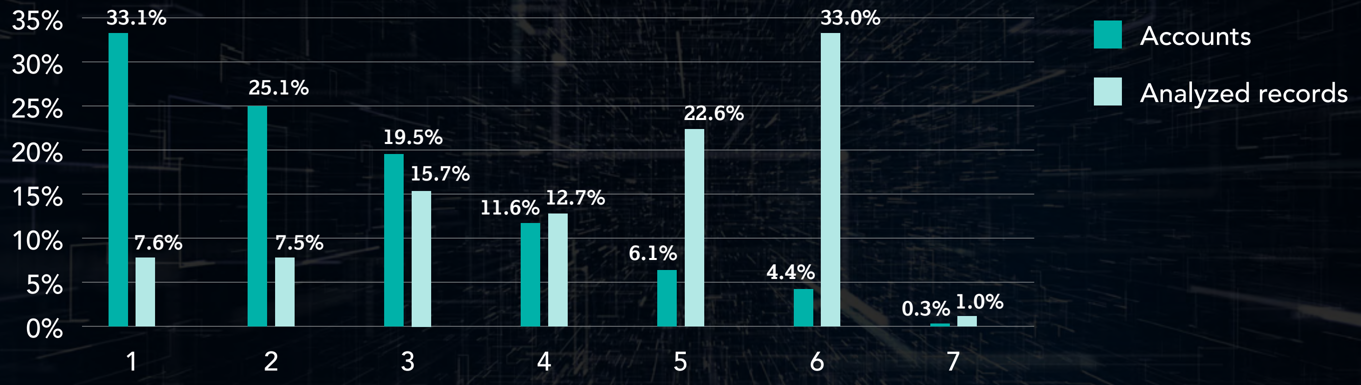
RISK FACTORS: PREVALENCE IN THE USE OF CLOUD PROVIDERS

Among all analyzed records, **more than 82%** are hosted on cloud providers.

This percentage reflects the trend where, over the past few years, businesses have been outsourcing to cloud providers instead of using traditional internal data centers. Using cloud providers gives companies access to new technologies, enables them to be more agile and dynamic, and is more cost effective. However, it opens up more risk to businesses who now need to manage more DNS records than ever before.

RISK FACTORS: DECENTRALIZATION OF PROVIDERS AMONG COMPANIES WITH LARGER PORTFOLIOS

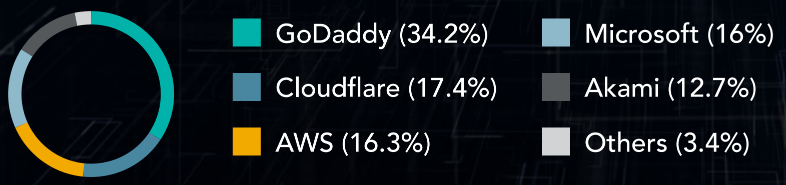
NUMBER OF PROVIDERS USED



58% of companies analyzed appear to be doing a better job at consolidating their subdomains under just one or two cloud providers, however, they tend to own smaller portfolios that are more easily managed.

Conversely, 11% of the companies analyzed in this research used five or more cloud providers. These companies account for more than half of all DNS records analyzed and some have large portfolios with thousands of records per company. This shows that companies with large portfolios may not have centralized management of their cloud providers, making it a challenge for them to have a good oversight of all their DNS records.

DISTRIBUTION OF CLOUD PROVIDERS USED



Over 96% of all DNS records analyzed are distributed across five of the largest cloud providers—GoDaddy®, Cloudflare®, AWS, Microsoft®, and Akamai.

MITIGATE CYBER THREATS WITH SUBDOMAIN MONITORING

Large organizations with diverse brand portfolios and international operations are often unaware of the scale of their digital footprint. Digital records accumulate over time, and this makes maintaining cyber hygiene a real challenge.

Without proper oversight of digital records and administration, organizations accumulate “noise” that makes simple cyber hygiene and housekeeping more complex, resulting in easy exploits for cybercriminals. This buildup of inactive zones that don’t point to content are known as “dangling DNS” and are at risk of subdomain hijacking. This opens a gateway for other cyberattacks such as phishing, malware, and ransomware, that could result in reputation damage, loss in consumer confidence, and more damaging data and security breaches. Administrators unaware of the history of each domain are hesitant to delete these legacy records—fearing they may be tied to critical infrastructure that will inadvertently bring down operations.

It’s a challenge for companies to account for all their digital assets, and recognize which ones are critical, functional, or redundant (therefore no longer required). DNS records housekeeping is one of the worst managed tasks in business due to 20 plus years of history with different owners, policies, vendors, and of course—the inherent fear of deleting anything they’re unsure about.

Additionally, subdomain hijacking is one of many domain security threats that exists today, including domain and DNS hijacking, domain shadowing, and cache poisoning. These threats often serve as enabling attacks to launch more egregious phishing and ransomware attacks, along with business email compromise (BEC), email spoofing, or even data breaches.

We recommend all companies adopt a subdomain monitoring solution that not only alerts you when changes to your DNS records are detected, but also provides you context so you can make informed decisions and take appropriate action to prevent a subdomain hijack.

Learn more about CSC’s Subdomain Monitoring solution here.

CSC

CSC is the trusted security and threat intelligence 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.

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.