CYBER SECURITY REPORT

October 2019

Vincent D'Angelo *Global Director, Corporate Development and Strategic Alliances*

Quinn Taggart *Senior Domain Product Manager*

Ken Linscott *Product Director, Domains and Security*

Letitia Thian *Marketing Manager*

Research and editorial prepared by CSC

This CSC Cyber Security Report culls all the most important information about cyber crime and cyber security for you in one comprehensive piece—giving you the most up-to-date information in one place, allowing you to quickly scan the news that's important to you and your brand. In this special issue, we highlight the adoption of domain name security controls by the global defense industry.

Domain security

CSC manages over 65% of the TOP #1 global brands

CSC helps manage the online presence of over 65% of the top global brands (Interbrand®). Using our proprietary tools, we help our corporate clients uncover security gaps and strategic opportunities in their domain portfolio. With this same methodology, we analyze the main domain names of organizations around the world to see how they fare in terms of domain security.

In this issue, we focus on global government defense contractors. Due to the continued attacks on government agencies and contractors resulting in breaches[1], it's imperative we continue to share these matters, as they can impact the security of a nation and the well-being of its citizens. Since domain names, the domain name system (DNS), and certificates power the basic infrastructure of the internet, sensitive apps, tools, systems, and information relying on this infrastructure can fall into the wrong hands if not secured with proper DNS controls[2].

We've analyzed some of the largest global defense contractors from 24 nations to discover how this industry has adopted domain security controls.

Domain security and observation trends

Based on 100 global defense contractors

DNS hijacking background

We started 2019 with a DNS hijacking alert[3] from the U.S. Cybersecurity and Infrastructure Agency. Since then, there have been related warnings from industry experts, such as *Brian Krebs*[4] and global government agencies such as the U.K.'s Cybersecurity Centre, the NSCS[5]. These efforts have raised awareness about the ongoing risks related to DNS and domain name hijacking occurrences, however most industries remain exposed, as CSC's Cyber Security Reports on the financial and media sectors[6] demonstrate. The target of these attacks are also not limited to companies of a particular industry, size, or geographic location. For instance, a California-based hospital recently had its domain name stolen[7] and lost access to its website, email, apps, and related information.

Registrar provider

29% CORPORATE REGISTRAR

71% RETAIL REGISTRAR

RISK

Historically, retail registrars have been frequent targets for cyber attacks. Companies should partner with an enterprise-class registrar that invests heavily in security at the technology level, as well as security training of employees, including instilling company values of vigilance, and knowing how to identify malicious intent, especially for core domains.

OBSERVATIONS

29% of the defense industry uses corporate registrars

Malicious attacks against domain names, email, DNS, and digital certificates have increased. Therefore, management of the overall domain name portfolio by a reputable corporate registrar versus a retail registrar will make the adoption of domain name security standards much easier to implement and monitor. Furthermore, regular assessment of domain name registrar controls, processes, tools, and security will become a critical component of an organization's cyber security posture moving forward.

Registry lock

13% REGISTRY LOCK ON

65% REGISTRY LOCK OFF

22% *REGISTRY LOCK UNAVAILABLE

RISK

Unlocked domains are vulnerable to social engineering tactics, which can lead to unauthorized DNS changes and domain name hijacking. Some domains may remain unlocked, as not every registry around the world offers lock services*.

OBSERVATIONS

13% have registry locks in place

Registry locks prevent domain name hijacking and unauthorized changes to DNS that could take a site offline or redirect users to malicious content. Based on continued DNS hijacking risks against governments and critical industries, there was very low adoption of this control by defense contractors.

Alarmingly, 69% of companies that employ the same domain name for their core website, email, and DNS—*and* that were also eligible for registry locks—were not locked.

Domain security and observation trends

DNS provider

32% INTERNAL DNS

13% CORPORATE OR ENTERPRISE DNS

55% OTHERS (HOSTING OR RETAIL DNS)

RISK

Using non-enterprise-level DNS providers poses potential security threats like distributed denial of service (DDoS) attacks, as well as down time, and revenue loss.

DNSSEC

3% DNSSEC ON

97% DNSSEC OFF

RISK

Lack of deployment of DNSSEC—one of the most cost-effective security protocols—leads to vulnerabilities in the DNS, which could include an attacker hijacking any step of the DNS lookup process. As a result, hackers can take control of an internet browsing session and redirect users to deceptive websites.

HTTPS everywhere

77% HTTPS everywhere, DEPLOYED

23% HTTPS everywhere, NOT DEPLOYED

RISK

Safe encryption with digital certificates for all online transactions mitigates the security risk of cyber criminals hijacking web sessions to commit identity theft or install malware on user devices, or hackers infringing on web communications that could lead to a breach, theft of customer data, a distributed denial of service (DDoS) attack, or defacing a website.

OBSERVATIONS

13% use enterprise-level DNS providers; 3% use DNSSEC

The preference of retail domain name registrar use by defense contractors is magnified by the use of non-enterprise grade DNS hosting, which increases exposure to DDoS and related threat vectors. Our research shows that 13% of defense contractors prefer enterprise-level DNS providers, while almost 32% are using their own DNS architecture, and 55% appear to use a retail grade provider. DNSSEC is another method to help protect the overall communication between users and web properties, however, adoption rates for DNSSEC was very low at only 3%.

Digital certificate type

4% EV

84% OV

12% DV

RISK

Digital certificate types that require more authentication, such as extended validation (EV) and organization validation (OV), are less prone to compromise than domain validation (DV).

OBSERVATIONS

84% use organization validated (OV) certificates, yet 12% are using DV certificates

If DNS is the door to a home, a digital certificate is the lock. It doesn't matter how solid the door is if the lock is weak. A key risk factor lies in the way in which digital certificates are validated. Domain validation (DV), requiring the lowest level of validation, is used by 12% of defense contractors, meaning that if a hacker gained access to internal email, they could easily validate digital certificates on company owned domains for malicious purposes.

Email authentication

25% DMARC

85% SPF

3% DKIM

RISK

Authenticating the email channel with domain-based message authentication, reporting, and conformance (DMARC), sender policy framework (SPF), or domain keys identified mail (DKIM) minimizes the incidence of email spoofing and potential phishing.

OBSERVATIONS

25% use DMARC

Domain-based message authentication reporting and conformance (DMARC) is an email validation system designed to protect a company's email domain from being used for email spoofing, phishing scams, and other cyber crime. Since DMARC adoption has been a mandate by some governments[8], increasing adoption of this control by defense contractors is recommended and can help address some of the threats to email communication.

CAA records

4% CAA RECORDS USED

96% CAA RECORDS NOT USED

RISK

A certificate authority authorization (CAA) record is a resource record held on a zone file that allows the domain owner to indicate which certificate authorities (CAs) are authorized to issue a certificate for a given domain name. By adding CAA records, you're able to control the CAs that your company uses. It ensures that only your chosen provider can issue a certificate for your domain names, and is an essential technical control allowing for policy enforcement and mitigating cyber threats like HTTPS phishing of hijacked sub domains

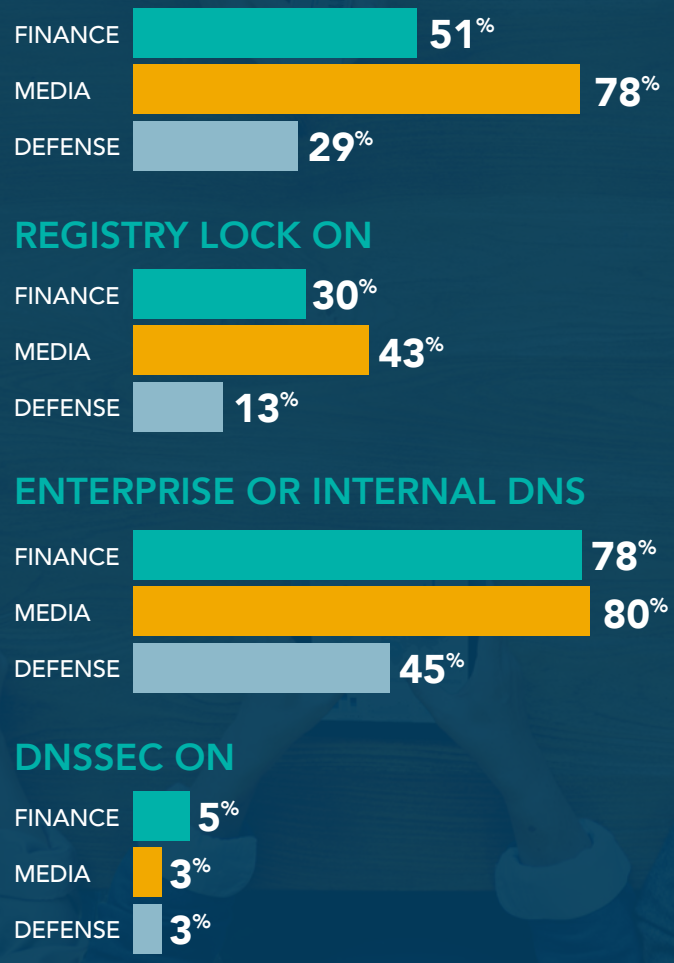
OBSERVATIONS

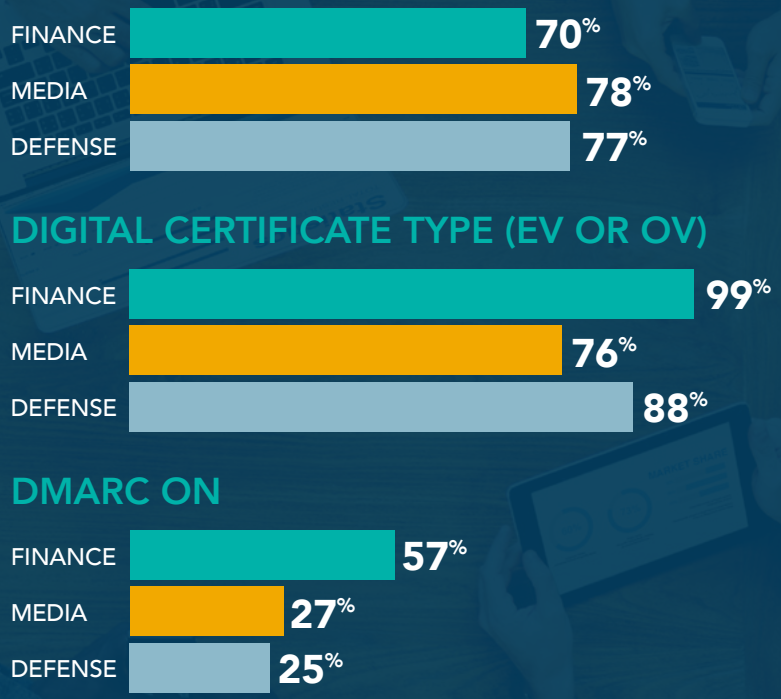
4% use CAA records

When we looked at CAA records for the defense industry, only 4% of the companies have them. Yet out of that, half were allowing the issuance of certificates by non-enterprise, retail-type vendors. This compares to CAA record use of 3% when observing global public companies.

Domain name security controls: defense vs. media vs. finance

CSC's last two reports focused on the finance and media sectors. With a focus on global defense contractors this time, it appears they have been slower to adopt various elements of domain name security, especially registry locks, the use of a corporate domain registrar, enterprise DNS hosting providers, and DMARC. Most of these controls are recommended by industry leaders, as noted earlier by CSC.





Furthermore, not all security measures cost a lot—especially compared to the cost of a single breach—yet we still see that basic security elements have not reached a level of adoption by the defense sector that would be expected from the increase in cyber threats year over year. What's troubling is that the easiest security techniques—that address overall domain security and user confidence—seem to be the hardest for companies to implement.

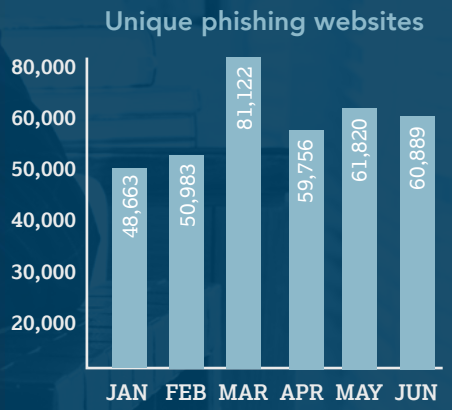
Phishing and email fraud

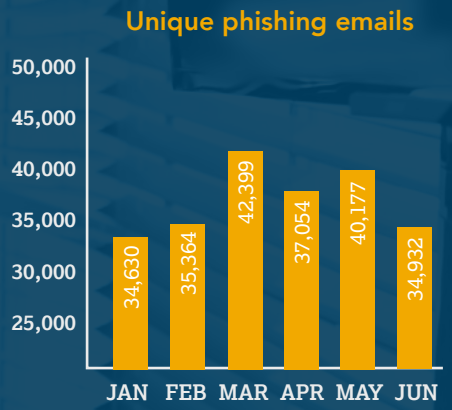
Major increase in phishing websites over the year

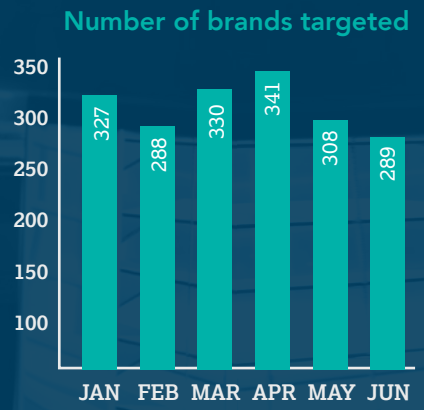
By Q2 2019, more than 55% of phishing websites had digital certificates, negating the effect of giving users an indication if they are on a safe website or not. Phishing sites look more legitimate with the "HTTPS," fooling internet users, and turning an internet security feature against consumers, allowing bad actors to steal personal identity data and account credentials.

Phishing attacks

The number of phishing websites in Q2 2019 was 182,465, a small increase from the previous quarter. However, the combined number of attacks in the first half of 2019 was notably 25% higher than the second half of 2018.







Most targeted industry sectors

Software as a service (SaaS) and webmail, online payment services, as well as banks and financial institutions, remain the top three most targeted industries for phishing in Q2 2019.

SOURCE: *APWG* Phishing Activity Trends Report, 2nd Quarter 2019

Most used top-level domains in phishing websites

Legacy top-level domains (TLDs)—TLDs that were established a long time ago with large numbers of websites tend to host the most phishers, as expected. However, country-code TLDs that have been repurposed, as well as a few new generic TLDs that are often offered at low cost, host notable amounts of phishing compared to all domains in the world.

Type of TLD:
Legacy gTLD | ccTLD | New gTLD

↑ / ↓ Change in rank + / - Change in volume

.com +714 → #1 • 2,812 domains	.net +33 was #3 ↑ #2 • 208 domains	.br +64 was #8 ↑ #3 • 146 domains	.org -9 → #4 • 145 domains
.uk +16 → #5 • 137 domains	.top #6 • 120 domains	.info +36 → #7 • 119 domains	.in +47 was #11 ↑ #8 • 105 domains
.au #9 • 80 domains	.xyz +26 was #17 ↑ #10 • 63 domains	.icu #11 • 59 domains	.cl #12 • 47 domains
.ga -21 was #10 ↓ #13 • 47 domains	.ml -35 was #9 ↓ #14 • 43 domains	.cf -43 was #6 ↓ #15 • 41 domains	.co #16 • 41 domains
.ru -6 was #13 ↓ #17 • 38 domains	.pl +9 was #19 ↑ #18 • 37 domains	.id #19 • 36 domains	.it -1 was #16 ↓ #20 • 36 domains

SOURCE: APWG Phishing Activity Trends Report, 2nd Quarter 2019

Every organization is at risk

Examples in the news

AMERICA

Mitigate DNS Infrastructure Tampering

The U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency tracked a series of tampering incidences, and released an emergency directive to federal agencies to adopt required actions such as auditing DNS records, and securing portal access to mitigate DNS hijacking.

cyber.dhs.gov/ed/19-01/

Alert Regarding Published Reports of Attacks on the Domain Name System

The Internet Corporation for Assigned Names and Numbers (ICANN) sent an alert to organizations to implement best practices and measures such as DNSSEC, and registry locks to protect their systems against malicious activity targeting the DNS.

icann.org/news/announcement-2019-02-15-en

A Deep Dive on the Recent Widespread DNS Hijacking Attacks

KrebsOnSecurity researched the complex and widespread DNS hijacking attacks to understand its origins and extent, showing that multiple governments around the world have been impacted due to breaches at key internet infrastructure providers.

krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

Secret Service Investigates Breach at U.S. Govt IT Contractor

An IT contractor for more than 20 federal agencies suffered a breach due to malware from an email attachment, which compromised email correspondence and credentials that could give access to the databases of the affected agencies.

krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/

UNITED KINGDOM

Ongoing DNS Hijacking and Mitigation Advice

The U.K. National Cyber Security Centre published an advisory that the large global DNS hijacking campaign continues to show activity affecting multiple regions and sectors, and provided mitigation advice around registrar, nameservers, and web application security.

ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice

BULGARIA

An Entire Nation Just Got Hacked

Bulgaria's national tax agency was breached, compromising the personal data and financial records of 5M citizens in a country with a population of 7M.

edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/

ECUADOR

Nearly Everyone in Ecuador is the Victim of a Data Breach

Detailed personal information of about 20M in Ecuador, including its president, was left exposed on a local contractor's server, with data from government registries, and other organizations.

engadget.com/2019/09/17/ecuador-data-breach-20-million-citizens/

AUSTRALIA

ACSC to Deploy Protective DNS Service for Govt, Critical Infrastructure

The Australian Cyber Security Centre is piloting a protective DNS service to be adopted by local government and critical infrastructure.

itnews.com.au/news/acsc-to-deploy-protective-dns-service-for-govt-critical-infrastructure-520138

Recommendations

Defense in Depth (DiD) Approach

EMPLOY ADVANCED SECURITY FEATURES FOR BUSINESS-CRITICAL DOMAINS

MultiLock, DNSSEC, HTTPS, DMARC, and CAA Records

CONTROL USER PERMISSIONS

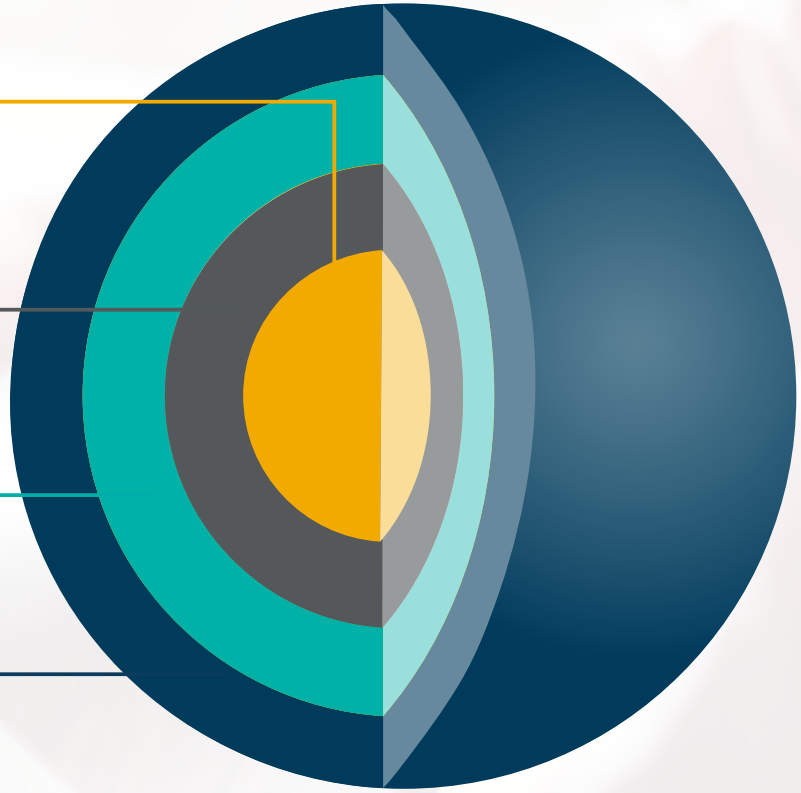
Visibility on elevated permissions and notifications

SECURE PORTAL ACCESS

IP validation, two-factor authentication, and federated ID

ENTERPRISE CLASS PROVIDER

Systems, staff, policies, and processes



CSC supports companies that are making significant investments in their security posture by exposing blind spots that exist within fundamental internet assets such as domain names, DNS, and digital certificates. By leveraging our proprietary security solutions, CSC secures companies from cyber threats to their digital assets, helping them avoid devastating revenue loss, brand reputation damage, or significant financial penalties as a result of policies like GDPR. Along with internet assets, CSC protects online brands that are being exploited via counterfeit websites, fraud, and IP violations, and helps monitor and mitigate this, providing enforcement and advisory services to protect many of the world's largest brands. Learn more at ***cscdigitalbrand.services***.

References

1. krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/
2. cscglobal.com/cscglobal/pdfs/DBS/Digital-Asset-Security-Checklist-EN.pdf
3. us-cert.gov/ncas/alerts/AA19-024A
4. krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-DNS-hijacking-attacks/
5. ncsc.gov.uk/news/ongoing-DNS-hijacking-and-mitigation-advice
6. cscglobal.com/cscglobal/pdfs/DBS/Cyber-Security-Report-June-2019-EN.pdf
7. beckershospitalreview.com/cybersecurity/hackers-steal-california-hospital-s-website-domain-email-addresses.html
8. eweek.com/security/dmarc-email-security-adoption-soars-as-us-government-deadline-hits