CYBER SECURITY REPORT

June 2019

Ken Linscott *product director, Domains and Security*

Quinn Taggart *senior domain product manager*

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, allowing you to quickly scan the news that's important to you and your brand.

Domain security

CSC manages over 65% of the TOP global brands

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

In this issue, we focus on the media industry. With changes in technology and customers consuming more on-demand content, traditional forms of media have been replaced by digital and mobile formats. Social media, online streaming, and internet advertising are examples born over the past 25 years in this era of change. Many media brands now have an online presence, and collect more customer data than before. With companies collecting login and payment information—as well as the possibility of cyber attacks disrupting or even hijacking media distribution channels—it's become imperative that brands take measures to secure themselves and their customers from the risk of attacks and breaches.

Here, we've analyzed some of the largest media conglomerates around the world, their entities, and brands across a spectrum of channels, including advertising, publishing, television, and radio, as well as a few online-only brands, to discover how this industry has adopted domain security.

Domain security and observation trends

Based on 120 media brands

CSC's last report focused on finance and insurance sectors. With a focus on media this time, it's interesting to observe how each sector weighs in on the various elements of domain security. 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 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—are the hardest for companies to implement.

Registrar provider

78% CORPORATE REGISTRAR

22% 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

78% of the media industry uses corporate registrars

When assessing domain security at the base level, a few key elements are under the scrutiny—locks, email, domain name system (DNS), and secure sockets layers (SSLs). Of course, management of the overall domain portfolio by a reputable corporate registrar versus a retail registrar will make some of these elements much easier to implement, which appears to be why much of the media industry prefers corporate registrars to manage their domain portfolios.

Registry lock

43% REGISTRY LOCK ON

37% REGISTRY LOCK OFF

20% *REGISTRY LOCK UNAVAILABLE

RISK

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

OBSERVATIONS

43% have registry locks in place

These locks are gaining popularity because they prevent unauthorized changes to DNS that could take a site offline or redirect users to malicious content.

DNS provider

25% INTERNAL DNS

55% CORPORATE OR ENTERPRISE DNS

20% OTHERS (HOSTING OR RETAIL DNS)

RISK

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

SSL always on

78% SSL ALWAYS ON, DEPLOYED

22% SSL ALWAYS ON, NOT DEPLOYED

RISK

Safe encryption with SSL 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 DDoS attack, or defacing a website.

DNSSEC

3% DNSSEC ON

97% DNSSEC OFF

RISK

Lack of deployment of domain name system security extension (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.

OBSERVATIONS

55% use enterprise-level DNS providers; 3% use DNSSEC

The preference for corporate registrars also seems to cascade into a preference for enterprise-level DNS providers with almost half of media brands using them. Almost 25% are using their own DNS architecture and 20% use a retail provider. DNS is certainly one of those areas where companies shouldn't skimp on quality and reliability—DNS is the engine behind an online presence. DNSSEC is another method to help protect the overall communication between users and web properties, however, adoption rates for DNSSEC have been very low at only 3%.

SSL type (EV, OV, or DV)

2% EV

74% OV

24% DV

RISK

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

OBSERVATIONS

74% use OV certificates, yet 24% are using DV certificates

Similar to DNS, it's not wise to skimp on digital certificates. If DNS is the door to a home, SSL 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 SSLs are validated. Domain validation, requiring the lowest level of verification, is used by 24% of the media brands, meaning that if a hacker gained access to internal email, they could easily validate SSLs on company owned domains for malicious purposes. This played out in a recent hack via the retail registrar GoDaddy®.

Email authentication

27% DMARC

79% SPF

6% DKIM

RISK

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

OBSERVATIONS

27% use DMARC

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. For companies communicating with millions of users, the low adoption rates are surprising.

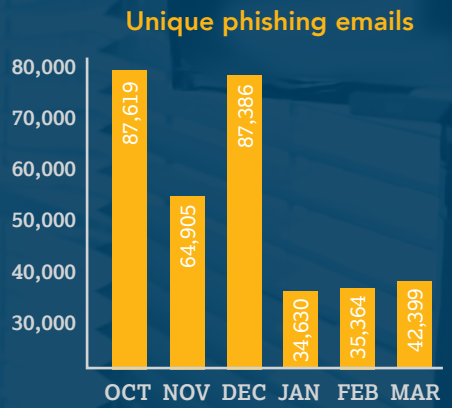
Phishing and email fraud

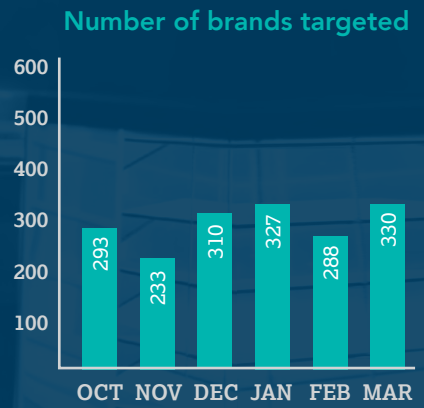
Major increase in phishing websites over the year

In Q1 2019, about 58% of phishing websites had SSL certificates, a significant increase when compared to 46% in the previous quarter, and less than 5% at the end of 2016. There are two possible reasons for this increase. First, attackers can create domain validated certificates, which are freely available. Second, more websites are using SSLs in general, and with most phishing being hosted on legitimate, hacked sites, the number of phishing websites with SSLs increases by extension. 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 Q1 2019 was 180,768, a 31% increase from the previous quarter.





Most targeted industry sectors

For the first time, the software as a service (SaaS) and webmail category is the most phished sector, while online payment services and financial institutions remain among the top three most targeted industries for phishing in Q1 2019.

SOURCE: APWG Phishing Activity Trends Report, Q1 2019

Most used top-level domains (TLDs) in phishing websites

Legacy 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

.com #1 • 2,098 domains	.pw #2 • 374 domains	.net #3 • 175 domains	.org #4 • 154 domains
.uk #5 • 121 domains	.cf #6 • 84 domains	.info #7 • 83 domains	.br #8 • 82 domains
.ml #9 • 78 domains	.ga #10 • 68 domains	.in #11 • 58 domains	.us #12 • 45 domains
.ru #13 • 44 domains	.tk #14 • 40 domains	.gq #15 • 37 domains	.it #16 • 37 domains
.xyz #17 • 37 domains	.online #18 • 33 domains	.pl #19 • 28 domains	.ca #20 • 26 domains

SOURCE: APWG Phishing Activity Trends Report, Q4 2018

Every organization is at risk

Examples in the news

AMERICA

Major U.S. Newspapers Crippled by Ryuk Ransomware Attack

Ransomware disabled the infrastructure of major newspapers, affecting the publication and distribution of print edition newspapers nationwide.

csoonline.com/article/3330645/major-us-newspapers-crippled-by-ryuk-ransomware-attack.html

AMERICA

Newsquest Websites Compromised by Security Breach

Hundreds of titles from a media group's website were infected with malware that hijacked mobile and web browsers when users tried to access local news, redirecting them to an unaffiliated website for a chance to win prizes.

uknip.co.uk/2019/02/newsquest-websites-compromised-by-security-breach/

FRANCE

Video Sharing Platform Targeted by Credential Stuffing Attacks

Cyber criminals targeted a video-sharing platform with credential stuffing or brute-force attacks—guessing or re-using passwords from data breaches—to hijack users' accounts.

securityboulevard.com/2019/01/video-sharing-platform-targeted-by-credential-stuffing-attacks/

THE PHILIPPINES

Big, Rich Tech Teams Attack PH Alternative Media Websites

Politically motivated hacktivists have been attacking Filipino media websites with DDoS attack sizes 40,000 times their normal traffic, launching up to 40 attacks a week.

news.abs-cbn.com/news/02/07/19/big-rich-tech-teams-attack-ph-alternative-media-websites

AMERICA

New Mirai Malware Variant Targets Signs TVs and Presentation Systems

Researchers have discovered a new strain of the Mirai botnet that targets enterprise IoT devices, to potentially launch massive DDoS attacks similar to 2016's Mirai attack on a DNS provider, which interrupted major websites and internet services across North America and Europe.

zdnet.com/article/new-mirai-malware-variant-targets-signage-tvs-and-presentation-systems/

Recommendations

1. AUTO-RENEW DOMAINS

With retail registrars, if the credit card on file expires or is cancelled, automatic renewal become moot and domains go offline, or worse, get deleted. Working with a corporate registrar will ensure domains are automatically renewed unless a company explicitly indicates no renewal for certain domains—providing peace of mind that domains will not be dropped.

cscdigitalbrand.services/blog/an-abandoned-domain-name-could-hurt-you/

2. LOCK VITAL DOMAINS

Another reason to work with a corporate registrar is the support structure. It's a balance of technology combined with experts who know the industry. To lock vital domains, companies need to know which ones are vital—and they might not be obvious. CSC Security Center℠ gives us the technology to identify vital domains, looking at more than just traffic, analyzing multiple vectors to layer security.

cscglobal.com/service/csc/press-csc-alerts-companies-to-increased-dns-hijacking/

3. ADOPT DOMAIN SECURITY MEASURES

Without a good foundation, the fortress crumbles. Once a corporate domain registrar is on board, carefully inventory the domain portfolio and the protections in place. The security landscape is continuously evolving making a dedicated, trusted partner essential for evolving strategy. Security is not a once and done event, it's cyclical due to cyber criminals also developing new attack techniques.

cscdigitalbrand.services/blog/dns-the-neglected-building-block-part-5/

4. ENGAGE OTHER STAKEHOLDERS

Domain security and portfolio management is not a one-person job; it touches stakeholders in marketing, legal, brand management, and IT. Everyone's input is valuable when it comes to the management of the domain portfolio. We recommend companies start a domains council because security is everyone's job.

5. FAMILIARIZE THE BOARD WITH DNS RISKS

With global attacks, and mega breaches, in addition to regulatory compliance, cyber security is now a top priority for the board. Among the risks identified in the Business Continuity Institute Horizon Scan Report, DNS plays a contributing factor to four of the top 10 risks.

cscdigitalbrand.services/blog/dns-the-neglected-building-block-part-6/

CSC helps businesses thrive online. We help effectively manage, promote, and secure our clients' valuable brand assets against the threats of the online world. Leading companies around the world choose us to be their trusted partner, including more than 65% of the Interbrand® 100 Best Global Brands. Leveraging state-of-the-art technology, Digital Brand Services delivers outstanding outcomes through our unique account management structure. With our expert, dedicated team, you'll have a daily point of contact to ensure your brand has the strength it needs to succeed in the 21st century. We help consolidate and secure, monitor and enforce, then optimize and promote your brands to maximize your digital presence, secure your digital intellectual property, and reduce costs.

cscdigitalbrand.services