网络安全报告

2019年6月

Ken Linscott 域名与安全部，产品总监
Quinn Taggart 高级域名产品经理
Letitia Thian **市场经理**

研究成果和报告文案均由CSC提供

《CSC网络安全报告》旨在精选有关网络犯罪与安全的重要信息，让您一览全局——通过一份文件了解各项最新信息，快速获取对您品牌有利的内容。

域名安全

CSC的客户涵盖 65% 以上的全球顶级品牌

CSC帮助超过65%的全球顶级品牌管理它们的线上品牌业务。我们通过自己的专利工具帮助企业客户发现它们网络服务中的安全疏漏和重要机遇。通过这种方式，我们分析全球企业的主要域名，了解它们在域名安全方面的做法。

在本期内容中，我们将关注媒体行业。随着技术变革，消费者愈加青睐按需提供的内容，传统形式的媒体已逐渐被数字和移动形式的媒体所代替。回顾过去25年的发展，社交媒体、在线直播和网络广告的诞生就是这一变革最好的例证。许多媒体品牌现在都建立了在线服务，收集的消费者数据与日俱增。随着各公司开始收集登录和支付信息，并逐渐意识到网络攻击以及媒体经销渠道受到干扰乃至劫持的风险，这些品牌有必要采取行动来保护自己和消费者的安全，应对网络攻击的风险。

在此，我们对世界几大主要媒体集团、其子公司、各渠道品牌等进行了分析，内容涵盖广告、出版、电视、广播领域。另外还分析了一些纯在线品牌。我们的目的是探明该行业在域名安全方面的建设情况。

域名安全和趋势观察

基于120家媒体品牌

CSC的上一份报告重点关注金融和保险领域。而这次的重点是媒体行业。事实证明，了解不同行业对域名安全的重视程度是一件十分有趣的事情。不是所有的安全措施都需要耗费巨大的成本——尤其是与网络攻击导致的损失相比——但我们仍然发现，虽然网络安全威胁与日俱增，但基本的安全防护措施却未达到相应的级别。主要问题在于，最简单的安全技术对于各公司来说最难以实现，这些技术可解决综合性域名安全问题，增强用户信心。

域名注册商

78% 企业级注册商

22% 零售级注册商

风险

从历史上来看，零售级注册商最容易成为网络攻击的目标。公司应当与企业级注册商合作，因为企业级注册商往往会不惜重金地加大网络安全技术投入，加强网络安全并提供员工培训，包括培养员工的警觉意识以及分辨（尤其是针对核心域的）恶意行为的能力。

趋势观察

78%的媒体业者都使用企业级注册商

在评估基础级别的域名安全等级时会对一些关键元素进行检测——域名锁、邮箱、域名系统（DNS）和安全套接层（SSL）。当然，让声誉卓著的企业级注册商（而非零售级）来负责管理域名组合会使其中一些元素更容易实现，这也是为什么大部分媒体业者都选择企业级注册商的原因。

注册局锁

43% 注册局锁开启

37% 注册局锁关闭

20% *不提供注册局锁

风险

不锁定的域名很难防范社会工程学攻击，从而导致未经授权的DNS修改。某些域名可能仍出于未锁定状态，因为不是每个注册局都提供域名锁定服务*。

趋势观察

43%部署了注册局锁

这种锁定服务愈来愈受欢迎，因为它能预防DNS遭到未授权修改，防止网站意外离线或将用户引向恶意网址 。

DNS提供方

25% 内部DNS

55% 企业级DNS

20% 其它（主机或零售级DNS）

风险

非企业级的DNS提供方面临着潜在的安全威胁，例如分布式拒绝服务（DDoS）攻击，以及网站瘫痪和收入损失。

SSL时刻开启

78% SSL时刻开启，已部署

22% SSL时刻开启，未部署

风险

为所有在线交易采用SSL证书的安全加密，可以降低以下风险：网络犯罪者劫持网站会话并盗取身份信息、在用户设备上安装恶意软件，或入侵网络通信并破解、盗取用户数据，DDoS攻击或网站内容篡改。

DNSSEC

3% DNSSEC开启

97% DNSSEC关闭

风险

如果缺少域名系统安全扩展（DNSSEC）——最具性价比的安全协议之一——那么DNS就很容易遭到攻击，例如DNS查找流程的某个步骤遭到劫持。这时，劫持者就能够控制网络浏览会话，并让用户跳转到诈骗网站。

趋势观察

55%采用企业级DNS提供方；3%采用DNSSEC

和注册商的选择类似，在选择DNS提供方时，各公司同样更青睐于企业级商家，几乎一半的媒体业品牌都采用企业级DNS提供方。约 25% 的公司采用自己的DNS架构，另有20%选择零售级商家。显然，在DNS的选择上，各家公司都不应该在质量和可靠性上妥协——DNS是在线运营的基石。DNSSEC也有助于保护用户与网站间的通讯。不过，DNSSEC的采用率十分低，仅有3%。

SSL类（EV、OV、DV）

2% EV

74% OV

24% DV

风险

SSL类的认证要求较高，例如组织验证（OV）、扩展验证（EV）。相比域名验证（DV），它更难被破解。

趋势观察

74%采用OV验证，24%采用DV验证

和DNS类似，数字证书的重要性不容忽视。如果DNS是门，SSL就是它的锁。无论门多么坚固，没有锁的话都派不上用场。SSL的验证方式中潜藏着一项重大危险。域名验证的验证等级是最低的，有24%的媒体业品牌采用域名验证，这意味着如果黑客能访问内部邮箱，他们就能轻松通过公司域名的SSL验证，并采取恶意行动。零售级注册商GoDaddy®近期就遭到了类似的入侵。

电子邮箱认证

27% DMARC

79% SPF

6% DKIM

风险

使用基于域名的消息验证、报告及对照（DMARC）、发送者政策框架（SPF）或域名密钥识别邮件（DKIM）来验证邮件渠道，就能够降低邮件诈骗和网络钓鱼的风险。

趋势观察

27%采用DMARC

DMARC是一种邮箱验证系统，用于防止公司邮箱域名被用于邮件诈骗、钓鱼信息和其它网络犯罪。对于用户数量以百万计的各公司来说，DMARC的普及率低得令人吃惊。

钓鱼和电子邮件欺诈

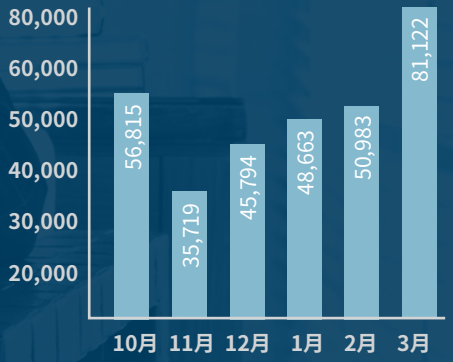
这些年来，钓鱼网站呈现爆发性增长趋势。

在2019年第1季度，58%的钓鱼网站都拥有SSL证书，相比上季度的46%以及2016年末的5%有巨大增长。这种势头背后可能存在两个原因。首先，攻击者可以创建有域名验证的证书，而且可以免费做到。其次，总的来说采用SSL的网站越来越多，而大部分的网络钓鱼犯罪发生在合法但遭到劫持的站点，钓鱼网站数量的增长速度正与日俱增。看似合法的钓鱼网站采用“HTTPS”来欺骗网络用户，用网络安全工具对付用户，以此盗窃个人身份数据和账号凭证。

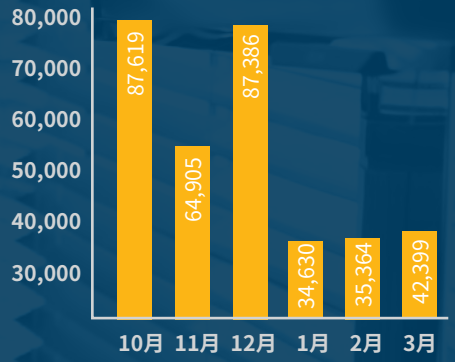
网络钓鱼攻击

2019年第1季度的钓鱼网站数量为180,768个，相比上个季度增加了31%。

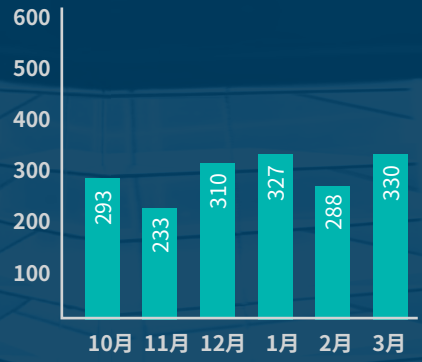
钓鱼网站数（不计重复）



钓鱼邮箱数（不计重复）



受袭击品牌数



受灾严重的行业

在2019年第1季度，软件即服务（SaaS）和网络邮箱首次成为了网络钓鱼犯罪的头号重灾区，而在线支付服务和金融机构继续保持在前三之中。

来源：APWG Phishing Activity Trends Report, Q1 2019

钓鱼网站常用的顶级域名（TLD）

传统TLD——即许多网站在很久之前注册的TLD——不出所料地成为钓鱼犯罪者的首选目标。不过，相比世界上的其它域名，用途被更改过的国家代码TLD和一些注册价格低廉的综合类新TLD更易受到网络钓鱼攻击。

TLD的类型：

传统gTLD　ccTLD　新gTLD

.com #1 · 2098个域名	.pw #2 · 374个域名	.net #3 · 175个域名	.org #4 · 154个域名
.uk #5 · 121个域名	.cf #6 · 84个域名	.info #7 · 83个域名	.br #8 · 82个域名
.ml #9 · 78个域名	.ga #10 · 68个域名	.in #11 · 58个域名	.us #12 · 45个域名
.ru #13 · 44个域名	.tk #14 · 40个域名	.gq #15 · 37个域名	.it #16 · 37个域名
.xyz #17 · 37个域名	.online #18 · 33个域名	.pl #19 · 28个域名	.ca #20 · 26个域名

来源：APWG Phishing Activity Trends Report, Q4 2018

所有组织都面临危险

新闻例证

美国

美国大型报纸企业遭到Ryuk勒索软件攻击

勒索软件瘫痪了多家大型报纸企业的设施，影响到了纸质版报纸的全国出版与发行。

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

美国

Newsquest网站安全遭到破坏

媒体集团网站上的数百个标题被植入了能劫持移动设备和浏览器的恶意软件，用户在点击当地新闻时会被重定向到无关的抽奖网站。

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

法国

视频分享平台遭到撞库攻击

针对视频分享平台开展的撞库/暴力破解袭击——即穷举或利用其它来源泄露的密码——来劫持用户账号。

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

菲律宾

资金充足的大规模技术团队攻击菲律宾非主流媒体网站

受到政治因素驱动的黑客对菲律宾媒体网站下手，利用40,000倍于正常水平的流量发起DDoS攻击，每周发起40次攻击。

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

美国

Mirai恶意软件的新变种袭击标识、电视和演示系统

研究人员发现Mirai僵尸网络的一个新变种，它主要针对企业物联网设备，能够向2016年的Mirai一样，对DNS提供方发起大规模DDoS攻击，导致北美和欧洲地区众多大型网站和网络服务瘫痪。

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

建议

1.自动续期域名

就零售级注册商而言，如果记录中的信用卡过期或被注销，自动续期就无法延续，域名会下线，乃至被删除。和企业级的注册商合作能够保证域名的自动续期，除非公司明确表明不再需要续期特定的域名——这样就能确保域名不会被废弃。

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

2.锁定关键域名

和企业级注册商合作的另一个原因在于它们的服务支持架构。它们拥有资深的专家团队，能提供丰富的技术支持。要锁定关键域名，公司必需知晓哪些是关键域名，而关键域名常常不易分辨出来。CSC Security Center℠的技术能够帮助我们分辨关键域名，综合考虑除流量之外的数据，分析多种安全相关的因素。

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

采取域名安全措施

不积土石，何以成山。一旦与企业域名注册商合作，您的域名组合就能获得有效的管理与防护。安全形势变幻莫测，这就需要一个专注而值得信赖的合作伙伴来为您制定针对性的策略。安全不是一劳永逸的事情，网络犯罪分子也在不断开发新的攻击技术，因此安全防范会呈现周期性的变化。

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

4.与其他相关方携手合作

域名安全和域名组合管理凭一己之力无法完成，需要市场、法务、品牌管理和IT等相关方的配合。在管理域名组合时，每个人的贡献都十分宝贵。我们建议各公司组建一个域名委员会，因为安全是我们每个人的责任。

5.为董事会讲解DNS风险

全球性攻击、大型侵入以及合规要求让网络安全成为了董事会需要关注的头等要务。在《业务持续性协会未来扫描报告》（Business Continuity Institute Horizon Scan Report）中，DNS在10项主要风险中占据了4个位置。

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

CSC 能促进企业的线上经营发展。我们能有效地管理、宣传和保护客户的宝贵品牌资产，应对线上威胁。世界各地的领先企业纷纷选择我们作为可信赖的合作伙伴，他们中包括65%以上的Interbrand®百大全球品牌。借助我们独特的账号管理结构和先进技术，数字品牌服务商就能达成出色的成果。有了我们敬业的专家团队，您就能时刻确保自己的品牌拥有在21世纪取得成功所必须的优势。我们会巩固、保护、监控您的线上运营，执行、优化并推广您的业务，提升您的数字影响力，保护您的数字知识产权，并帮助您降低成本。

cscdigitalbrand.services/cn