网络安全报告

2019年10月

Vincent D' Angelo *企业发展和战略联盟全球总监*

Quinn Taggart *高级域名产品经理*

Ken Linscott *域名与安全部，产品总监*

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。在本期特刊中，我们将重点介绍全球国防行业采用的域名安全控制措施。

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(Interbrand®)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域名组合中的安全疏漏和战略机遇。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。

本期将重点关注全球政府国防工程承包商。由于针对政府机构和承包商的持续攻击导致的信息泄露[1]，会影响国家安全及其公民的幸福生活，因此我们必须继续分享这些事件。由于域名、域名系统（DNS）和证书支撑着互联网基础设施的正常运行，因此，如果依赖该基础设施的敏感应用程序、工具、系统和信息但却没有适当的DNS控制措施[2]进行防护，就可能被别有用心的人所利用。

我们分析了24个国家的一些全球最大的国防工程承包商，以了解该行业如何采取域名安全控制措施。

域名安全和趋势观察

基于100家全球国防工程承包商

DNS劫持背景

2019年初，美国网络安全和基础设施安全局发出DNS劫持警告[3]。自那时起，行业专家（如Brian Krebs[4]）和全球政府机构（比如英国的网络安全中心，NSCS[5]）均发出相关警告。他们的努力提高了人们对DNS和域名劫持等持续性风险的警觉，

然而，CSC关于金融和媒体行业[6]的网络安全报告表明，大多数行业仍然对此漠不关心。这些攻击所针对的目标不限于特定行业、规模或地理位置的公司。例如，加利福尼亚州一家医院的域名最近被盗[7]，导致网站、电子邮件、Apps和相关信息均无法访问。

域名注册商

29% 企业级注册商

71% 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

29%的国防工业使用企业级注册商

针对域名、电子邮件、DNS和数字证书的恶意攻击数量呈上升趋势。因此，由久负盛名的企业级注册商与零售级注册商管理整个域名组合可以确保更加易于实施域名安全标准并进行监控。此外，对域名注册商控制、流程、工具和安全进行定期评估将成为获取组织网络安全态势的关键举措。

注册局锁

13% 注册局锁开启

65% 注册局锁关闭

22% *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

13% 部署注册局锁

注册局锁定防止发生域名劫持和未授权DNS变更，而域名劫持和未授权DNS变更可能使网站离线或将用户重定向到恶意内容。虽然针对政府和重要行业的DNS劫持风险持续存在，国防工程承包商却很少采用这种控制措施。

69%的公司为其核心网站、电子邮件和DNS使用相同的域名，而在注册局锁定可应用的情况下却没有申请锁定，这种情况不容乐观。

DNS提供方

32% 内部DNS

13% 企业级DNS

55% 其它（主机或零售级DNS）

风险

使用非企业级DNS提供商会造成潜在安全威胁，如分布式拒绝服务（DDoS）攻击、停机、以及收入损失。

DNSSEC

3% DNSSEC 开启

97% DNSSEC 关闭

风险

如果缺少最具性价比的安全协议之一——域名系统安全扩展（DNSSEC），那么DNS就很容易遭到攻击，DNS查找流程的任一步骤都可能遭到劫持。此情况下，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。

处处皆加密

77% 处处皆加密，已部署

23% 处处皆加密，未部署

风险

为所有在线交易采用数字证书的安全加密，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。

趋势观察

13% 采用企业级DNS提供方；3%采用DNSSEC

国防工程承包商倾向于使用零售级域名注册商，而使用非企业级DNS托管放大了这一偏好的风险，增加受到分布式拒绝服务攻击（DDoS）和相关威胁向量攻击的几率。我们的研究结果表明，13%的国防工程承包商偏好企业级DNS提供商，而大约32%的承包商使用自有DNS架构，55%的承包商似乎倾向于使用零售级DNS提供商。DNSSEC是另一种可帮助保护用户和网络资产之间全程通信的方法，但DNSSEC的采用率非常低，仅有3%。

数字证书类

4% EV

84% OV

12% DV

风险

数字证书类的认证要求较高，例如组织验证（OV）、扩展验证（EV）。相比域名验证（DV），它更难破解。

趋势观察

84% 采用OV验证，12%采用DV验证

如果DNS是进入家庭的门，数字证书就是门上的锁。如果锁有问题，门再坚固也没用。一个关键风险因素在于数字证书的验证方式。需要进行最低级别验证的域名验证（DV）仅由12%的国防工程承包商使用，这意味着：如果黑客获得内部电子邮件的访问权限，则其可在公司拥有的网域上轻松验证数字证书，以实现恶意目标。

电子邮箱认证

25% DMARC

85% SPF

3% 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

25% 采用 DMARC

DMARC是一种邮箱验证系统，用于防止公司邮箱域名用于邮件诈骗、钓鱼信息和其它网络犯罪。由于一些政府8强制要求采用DMARC，因此建议国防工程承包商更多地采用该控制措施，有助于应对一些针对电子邮件通信的威胁。

CAA 记录

4% CAA 记录已使用

96% CAA 记录未使用

风险

证书颁发机构授权(CAA)记录是保存在区域文件中的资源记录，它允许域名所有者指定由哪个证书颁发机构（CAs）为指定的域名颁发证书。通过添加CAA记录，您能够掌控公司使用的CA动态。它确保只有您选择的提供商才能为您的域名颁发证书，它还是一项关键技术控制措施，支持实施策略并消减网络威胁（比如通过被劫持的子域进行HTTPS网络钓鱼）。

趋势观察

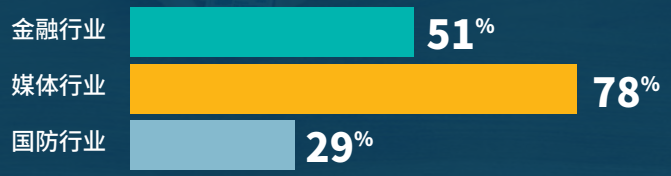
4%的承包商使用CAA记录

我们在查看国防行业的CAA记录时发现，只有4%的公司有相关记录。此外，有一半的公司拥有非企业级零售型提供商颁发的证书。相比之下，全球上市公司中拥有CAA记录的比例是3%。

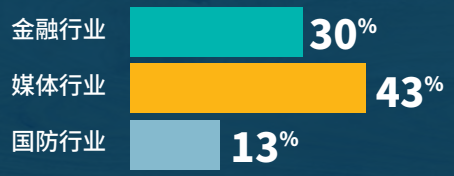
域名安全控制措施：国防工业 vs 媒体行业 vs 金融行业

CSC的之前两份报告主要关注金融和媒体行业。本期报告的关注重点是全球国防工业承包商，看起来这些公司在采用各种域名安全防护措施（特别是注册局锁定、企业级域名注册商、企业级DNS托管提供商和DMARC）方面进展缓慢。正如CSC之前所指出的，这些控制措施中的大多数是由行业领导者推荐的。

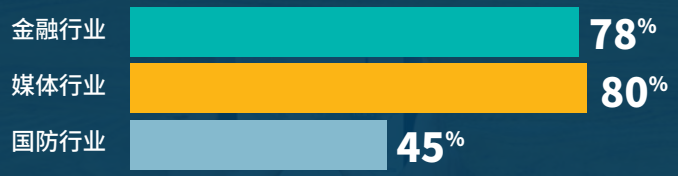
企业级域名注册商



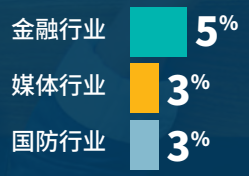
注册局锁定启用



企业或内部DNS



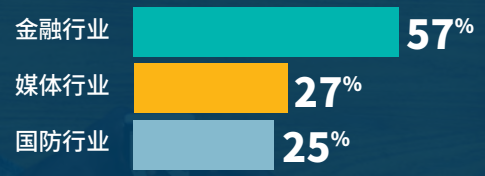
DNSSEC 启用



处处皆加密

数字证书类型（EV或OV）

DMARC 启用



此外，并不是所有的安全措施都代价昂贵，特别是与单次数据泄露所造成的后果相比；然而，我们发现国防行业对基本安全措施的采用程度依然不足以应对呈逐年上升趋势的网络威胁。令人苦恼的是，最简单、安全、可以解决整体域名安全问题并提振用户信心的技术，对各公司来说似乎最难实施。

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

截至2019年第二季度，超过55%的钓鱼网站拥有数字证书，使得向用户提示其所访问的网站是否安全不再取得应有的效果。钓鱼网站使用“HTTPS”域名，从而使其看起来更合法，以欺骗互联网用户，并利用互联网安全功能对付消费者，允许危险分子窃取个人身份数据和账户凭证。

网络钓鱼攻击

2019年第二季度的钓鱼网站数量为182,465个，比上季度稍有增加。然而，2019年上半年的网络攻击总数比2018年下半年明显增加25%。

受灾严重的行业

软件即服务（SaaS）和电子邮件、在线支付服务、银行和金融机构仍然是2019年第二季度网络钓鱼攻击所针对的三大行业。

来源: APWG 2019年第二季度网络钓鱼活动趋势报告，

钓鱼网站常用的顶级域名

传统顶级域名(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。

Type of TLD:

传统gTLD | ccTLD | 新gTLD

↑ / ↓ 排名变化　　+ / - 数量变化

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

来源: APWG 2019年第二季度网络钓鱼活动趋势报告

所有组织都面临危险

新闻例证

美国

消减DNS基础设施篡改

美国国土安全部网络安全和基础设施安全局跟踪了一系列篡改事件，并向联邦机构发布紧急指令，要求它们采取必要行动（比如审计DNS记录）并确保门户访问安全以减少DNS劫持事件。

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

针对已公布报告中提及的域名系统攻击发出警告

互联网名称与数字地址分配机构（ICANN）向所有组织发出警告，要求它们采取最佳实践和措施（如DNSSEC和注册局锁定）以保护各自的系统不受针对DNS的恶意活动破坏。

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

深入研究最近肆虐全球的DNS劫持攻击

KrebsOnSecurity研究了构思精巧且广为蔓延的DNS劫持攻击活动以探查其源头和破坏程度，得出的结论表明：由于关键的互联网基础设施提供商发生数据泄露，全球多个国家的政府机构受到影响。

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

情报机构调查美国政府IT承包商数据泄露事件

一家为20多个联邦机构服务的IT承包商因为受到隐藏在电子邮件附件中的恶意软件攻击而发生数据泄露事件，这种恶意软件攻击破坏电子邮件通信和可访问受影响机构数据库的凭证。

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

英国

持续存在的DNS劫持风险和消减建议

英国国家网络安全中心发布的一份报告指出，大规模全球DNS劫持活动仍然肆虐多个地区和行业，并针对注册商、域名服务器和网络应用程序安全提出风险消减建议。

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

保加利亚

整个国家被黑

保加利亚国家税务机构遭到网络攻击，使这个总人口为700万的国家中的500万公民的个人信息和财务记录外泄。

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

厄瓜多尔

在厄瓜多尔，几乎每个人都是数据泄露的受害者

厄瓜多尔国内约2000万人（包括该国总统）的详细个人信息，连同政府登记处和其它机构的数据，都被曝光在当地一家承包商的服务器上。

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

澳大利亚

ACSC为政府和关键基础设施部署DNS防护措施

澳大利亚网络安全中心（ACSC）正在为地方政府和关键基础设施试点一项DNS防护措施。

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

建议

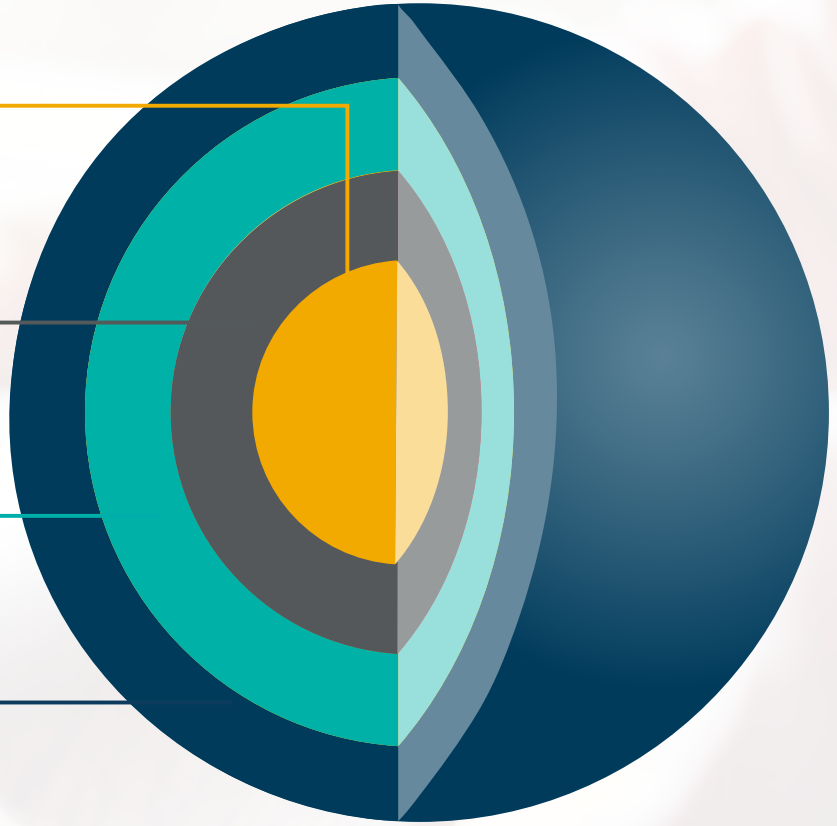
深度防御(DiD)方法

为业务关键型域名采用高级安全技术
多重锁定、DNSSEC、HTTPS、DMARC、CAA记录

控制用户权限
升级权限和通知的可见性

确保安全门户访问
IP验证、双重身份认证
和统一身份管理

企业级提供商
系统、员工、策略、流程



CSC

CSC可以查找域名、DNS和数字证书等基础互联网资产内部存在的盲点，为在网络安全领域进行重大投资的公司提供支持。CSC独有的安全解决方案可保护公司的数字资产免受网络威胁，帮助它们避免难以承受的收入损失、品牌声誉受损，或者因为违反欧盟通用数据保护条例（GDPR）这样的政策法规而受到严厉的经济处罚。除了互联网资产，CSC还保护被冒牌网站、网络欺诈和IP违例等行为所侵犯的在线品牌，帮助监控和消减这些攻击行为，提供执行和咨询服务以保护众多全球主流品牌。更多信息请访问 ***cscdigitalbrand.services/cn***。

参考文献:

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