域名安全报告

福布斯全球 2000 强企业

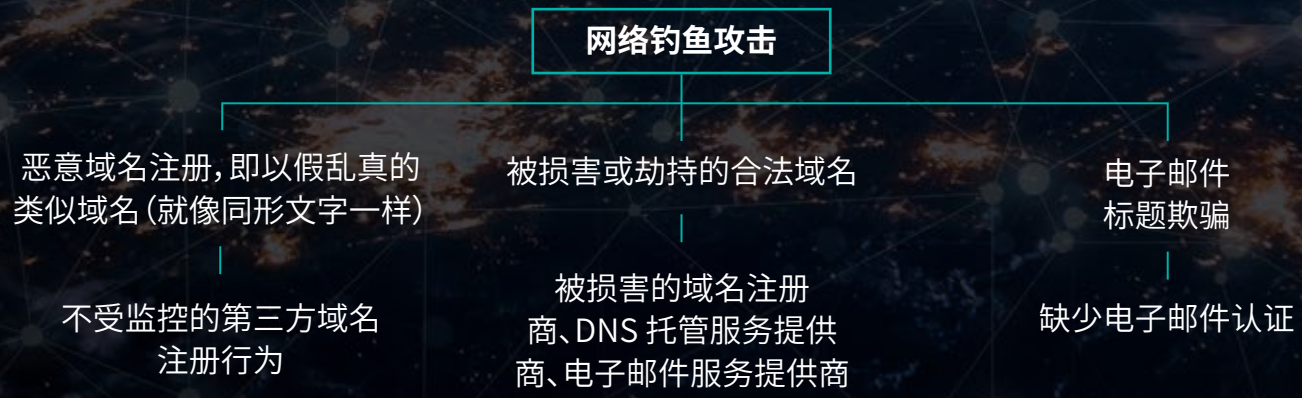
2021

重点摘要

网络犯罪与日俱增，2021 年，众多公司受到的勒索软件攻击、商业电子邮件泄露 (BEC)、网络钓鱼攻击、供应链攻击和线上品牌和商标滥用有增无减。尽管域名网络风险持续增加，但福布斯全球 2000 强企业仍采用相同程度的措施来改善域名安全状况，因而面临更多风险。

域名安全是在早期减轻网络攻击的关键组件——*您的第一道防线*

根据 CISA 的资料，大部分网络攻击（包括勒索软件攻击和 BEC）都始于网络钓鱼。尽管如今因勒索软件导致的损失每年超过几十亿元，但大部分勒索软件保护和响应措施都没有在发生勒索软件攻击的早期充分地化解网络钓鱼风险，因为这些措施不包含抵御最常见网络钓鱼攻击的域名安全措施。既有的研究表明，网络钓鱼攻击最频繁发生在恶意注册、以假乱真的类似域名上或被损害或劫持的合法域名上，或通过电子邮件标题欺骗发起。



理解您的域名面临的网络风险

如果不解决域名安全问题，可能会带来灾难性的风险。不受保护的域名对您的网络安全状况、数据保护措施、消费者安全、知识产权、供应链、收入和声誉构成严重威胁。

CSC 建议密切留意以下适合域名安全的网络风险框架：

域名安全框架

防范可疑和恶意的域名

抵御
电子邮件标题欺骗

防范被损害
域名的活动

主要调研结果

70% 同形文字域名（模糊匹配）——网络钓鱼和品牌滥用中常用的策略——由第三方拥有，并已向消费级注册商注册。在这些域名注册行为中，超过 **60%** 在过去两年内注册，证明这是一种发展迅速的攻击方式。

81% 面临较大的域名和域名系统 (DNS) 劫持风险，因为这些域名没有采用基本的域名安全措施，例如域名注册局锁协议。

57% 都依赖于消费级域名注册商，而这些注册商对抵御域名和 DNS 劫持、分布式拒绝服务 (DDoS)、中间人攻击 (MitM) 或 DNS 缓存中毒的保护措施有限。

只有 **50%** 在把基于域名的消息认证、报告和一致性 (DMARC) 记录用作电子邮件认证方式。

域名安全对减少网络钓鱼的重要性

近期的网络攻击以跨软件平台的关键行业互联供应链为目标。对这些供应链造成一次损害，即可获得指数级回报。由于域名和 DNS 相互关联，所指出的域名安全和域名注册商漏洞可能会使互联网供应链面临其他风险。主动的预防性控制手段可确保基础域名资产安全，并防范上述网络钓鱼攻击方式。必备条件包括：

- **域名注册商标准**，旨在说明使用消费级注册商的大型组织的隐患，防范用于恶意目的（例如网络钓鱼和品牌滥用）的商业实践。
- **整个行业采用域名安全措施**，例如域名注册局锁、DMARC、DNS 托管冗余、DNS 安全扩展 (DNSSEC) 和证书认证机构授权 (CAA) 记录。
- **持续、迅速检测和禁用以假乱真的类似域名**，即模仿品牌，用于网络钓鱼和其他欺诈性活动的域名。

域名安全：
针对全球 2000 强企业的可疑或恶意域名活动

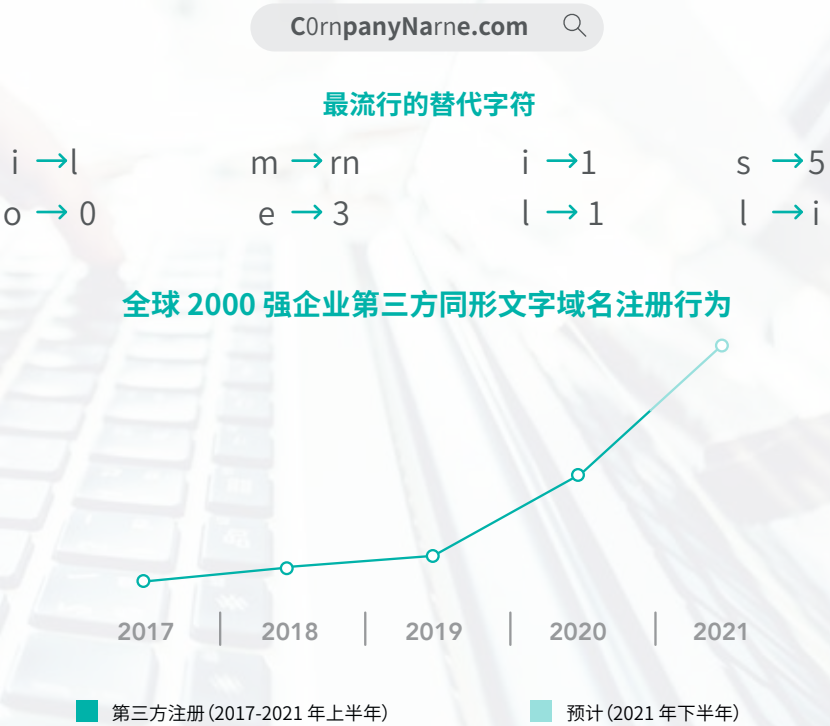
我们识别和分析了某些全球 2000 强企业的域名。这些域名包含具有超过六个字符的品牌名称，由品牌自身拥有[1]。这些可疑或恶意域名注册行为的意图，是利用对目标品牌的信任来发动网络钓鱼攻击或其他形式的数字品牌滥用或知识产权侵权行为，从而导致收入损失、流量分流和品牌声誉受损。

网络钓鱼者和恶意第三方有用之不竭的域名欺骗策略及其组合。

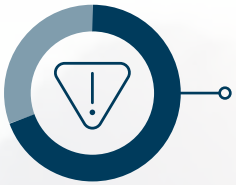
我们选择将域名安全研究的焦点放在以全球 2000 强企业的核心品牌为目标、进行恶意域名注册活动的许多明目张胆的策略上。

.COM 域名的常见同形文字（模糊匹配）

根据对网络钓鱼域名使用行为的密切观察，我们的分析包含了常见的拉丁字符替代字符，例如用 C0rnpanyNarne.com 来仿冒 CompanyName.com。



[1]研究范围仅限于 .COM 扩展名。我们预计能从这些扩展名发现最多第三方注册行为。我们采用保守而有意义的方法，来避免出现任何误报，且分析了具有六个或以上字符的核心品牌。



70% 在包含全球2000强品牌的域名注册中有70% 的域名是由第三方所持有。

在这些第三方拥有的域名中：

60% 在 2020 年至 2021 年上半年期间注册。根据我们的预测，到 2021 年底这个数字可能高达 **68%**。

77% 使用了域名隐私服务，或隐藏了 WHOIS 详细信息。

这证明有人尝试掩盖或隐藏他们的所有权和身份，表明他们可能有一些邪恶的意图。作为一个参考点，当时全球 2000 强企业的合法品牌使用隐私服务或隐藏详细信息的仅占 25%。

43% 配置了 MX（电子邮件）记录。

这些域名中有一半配置了 MX 记录，可用于发送网络钓鱼电子邮件或拦截电子邮件。

在这一分析中，域名注册商与第三方拥有的可疑或恶意注册行为息息相关。

GoDaddy.com, LLC　Namecheap, Inc　PDR, Ltd

目前如何使用这些第三方域名？

指向广告、点击付费网络内容，或被用于域名停放。

Palo Alto 的研究揭示了点击付费域名是如何通过这些服务传播恶意软件的。网络罪犯可将休眠型域名用作一种策略，并在这些域名准备好发起攻击时才启用。

拥有不活跃的网站。

在这些域名中，1/3 没有相关的名称服务器。这可能表明，域名在某个时刻被暂停使用了。

在其余 2/3 中，**57%** 有活跃的 MX 记录。

指向品牌假冒身份和恶意内容，包括网络钓鱼和潜在的恶意软件发送行为。

有害的内容可能损害品牌声誉，削弱客户信心。风险在于，用户可能会接触到含有恶意内容或尝试盗取敏感信息的网站。

建议

从对第三方拥有的这些域名的分析来看，许多域名都具有被用作从事网络攻击的恶意域名的高度倾向。注册者通常隐藏在隐私服务背后或遮盖 WHOIS 来掩盖他们的身份，注册与知名品牌类似、足以以假乱真的域名，以及使用策略来显得合法，从而诱使终端用户点击链接，或信任构成品牌侵权的网站。

我们建议，各公司应制定稳健的域名、网络和网络钓鱼监控计划，并配备应急响应机制，例如网站或域名的关停。这些公司也应制定安全的全方位域名管理策略来注册精准匹配域名，防范各种域名欺骗策略，例如同形文字、模糊匹配、相似域名，以及注册新的通用顶级域名 (gTLD) 和与从事业务和销售活动所在的国家、其他高风险国家与扩展名有关的国家代码域名扩展名。

域名安全分析

福布斯全球 2000 强企业的域名安全举措

本报告中共享的见解完全基于公开可用的数据集，所有这些数据集都很容易被网络罪犯和国家资助的行为体访问，从而促进了DNS 攻击和域名劫持。因此，我们的目的是提高客户对这些威胁的认识，并分享我们的域名安全最佳实践，从而改善所有组织的域名安全状况。在这一分析中，CSC 着眼于全球 2000 强企业对以下概述的域名安全措施的采用情况，然后我们按行业组和地区进行了深入的研究。

在本年度的报告中，我们也分析了与所用域名注册商的类型有关的域名安全采用情况趋势。在所有安全控制手段中，我们观察到，与使用消费级注册商的公司相比，使用企业级注册商的公司更多采用这些控制手段。由于大部分消费级注册商不支持注册局锁功能，所以尤为明显的控制手段是采用注册局锁。

平均而言，与使用消费级注册商的公司相比，使用企业级注册商的公司采用域名安全控制手段的数量要高出两倍。

我们的观察结果基于名列全球 2000 强企业的公司。由于该名单上的公司每年都有变化，2020 年的公司分析与上一年的分析略有不同。

域名注册商供应商

调研结果

在全球 2000 强企业——这些世界上规模庞大的上市公司中，有 57% 的公司没有使用企业级注册商。与消费级注册商相比，由信誉良好的企业级注册商对整个域名组合进行管理，将更有可能采用域名安全标准和最佳实践。

企业级注册商的关键组件：

- ☑ 企业级规模和专业知识，并具有企业专用的域名 DNS 和证书管理服务。
- ☑ 使命和焦点在于网络安全和IP保护。

  不提供：
  - 通过零售网站或零售商服务提供的域名服务
  - 便于知识产权和商标侵权的点击付费、域名颠倒和域名拍卖服务
- ☑ 通过高级服务侧重于域名安全，例如：域名注册 锁、DMARC、DNSSEC、CAA 记录和 DNS 托管冗余。
- ☑ 提供全球和当地的 24x7x365 全天候支持服务，具备全球域名注册功能。
- ☑ 在寻求和验证客户互动行为时实施“了解您的客户”(KYC) 方法。
- ☑ 全球认证的互联网名称与数字地址分配机构 (ICANN) 和注册局。
- ☑ 提供域名、品牌和欺诈监控与维权和关停功能。
- ☑ 提供相辅相成的咨询服务和工具（即 CSC Security Center℠），可加强域名管理和安全，并提供品牌和防欺诈保护。
- ☑ 使用同级别中最佳的操作流程和控制手段，例如强制性书面请求，进行网络安全意识培训，以及采用数据与政策措施。
- ☑ 具有同级别中最佳、视安全为首要使命的操作实践，包括 ISO 27001 认证数据中心、SOC 2 合规和第三方渗透和漏洞测试。

ⓘ 威胁

历史上，消费级注册商经常成为网络攻击的目标。这类注册商因数量庞大，才使品牌滥用和欺诈得以实施。（见上文使用企业级域名注册商的理由。）

注册局锁

按注册商类型划分的使用情况

52% 与企业级注册商合作的公司使用注册局锁

4% 与消费级注册商合作的公司使用注册局锁

调研结果

值得引起警惕的是，只有 19% 的公司将注册局锁作为一种安全措施来使用，这表明全球 2000 强企业中有五分之四的公司在域名安全方面受到严重损害。基于对全球企业持续存在的 DNS 劫持风险，全球 2000 强企业对这种控制手段的采用率非常低。在使用企业级注册商的 43% 全球 2000 强企业中，注册局锁的采用率为 52%，高于使用消费级注册商的公司，后者的采用率为 4%。这表明，所使用的注册商类型影响对域名安全控制手段的采用情况。

威胁

注册局锁可确保端对端域名操作安全，从而减少人为错误和第三方风险。这是一种十分具有成本效益的方式，可使域名免受意外或未经授权修改或删除。未锁定的域易受社会工程策略的影响，这可能导致未经授权的 DNS 更改和域名劫持。*同样，有些域可能保持未锁定状态，因为并非世界各地的每个注册局都提供锁定服务。

DNS 冗余

按注册商类型划分的使用情况

20% 与企业级注册商合作的公司执行 DNS 冗余

13% 与消费级注册商合作的公司执行 DNS 冗余

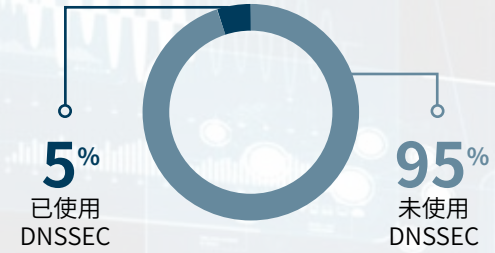
调研结果

仅 17% 全球 2000 强企业对核心域名执行 DNS 冗余（辅助 DNS）。超过 80% 冒着没有辅助 DNS 的风险。如果员工或客户无法访问网站，或在网站上进行交易，即使只有短短几分钟，但辅助 DNS 也可减轻可能导致要付出巨大代价的事件的威胁。

威胁

如果没有 DNS 冗余，则会带来潜在的安全威胁，例如削弱 DDoS 攻击的恢复能力，以及导致运营停止。这些攻击会用大量流量占用您的网络、服务或应用程序，导致真实客户请求无法进入，从而带来收入损失，使声誉受损。

DNSSEC



按注册商类型划分的使用情况

7% 与企业级注册商合作的公司使用 DNSSEC

3% 与消费级注册商合作的公司使用 DNSSEC

调研结果

域名系统安全扩展 (DNSSEC) 是另一种启用 DNS 服务器之间经过身份验证的通信的方法。DNSSEC 的采用率非常低，仅 5%。DNSSEC 可防止 DNS 缓存中毒攻击的发生。这意味着全球 2000 强企业中有 95% 的公司容易受到缓存中毒攻击。

威胁

DNSSEC 是最具成本效益的安全协议之一，如未能部署将导致 DNS 中存在漏洞，包括攻击者对 DNS 查找过程中任意步骤的劫持。由此，黑客可以控制互联网浏览会话，并将用户重定向到欺骗性网站。

CAA 记录

按注册商类型划分的使用情况

8% 与企业级注册商合作的公司使用 CAA 记录

4% 与消费级注册商合作的公司使用 CAA 记录

调研结果

仅 5% 全球 2000 强企业使用证书认证机构授权 (CAA) 记录。CAA 记录允许您指定特定的证书认证机构 (CA) 作为您公司域证书的唯一颁发机构。如果网络罪犯没有使用指定的证书认证机构来获取新的证书，他们的请求不会通过，而您会收到警报，得知有人试图不根据您的 CAA 政策请求新的证书。这是一个强大的合规工具，也是一个强大的安全层。

威胁

一旦网络罪犯获得了一个域名，在很多情况下，他们将能够访问已发布的数字证书。添加 CAA 记录，即可确保只有您选择的供应商才能为您的域名颁发证书，并且是一项重要的技术控制手段，允许执行策略和减轻网络威胁，如被劫持子域名的 HTTPS 网络钓鱼。

电子邮件认证

按注册商类型划分的使用情况

与企业级注册商合作的公司使用 DMARC

与消费级注册商合作的公司使用 DMARC

调研结果

50% 全球 2000 强企业如今在使用基于域名的消息认证、报告和一致性 (DMARC)。DMARC 是一个电子邮件验证系统，旨在保护公司的电子邮件域不被用于电子邮件欺骗、网络钓鱼欺诈和其他网络犯罪。DMARC 本质上提供电子邮件认证，就像 DNSSEC 在 DNS 级别所做的那样。我们也明白，即使执行 DMARC，但如果没有实施 DMARC 拒绝政策，仍会面临网络钓鱼风险。

威胁

进行电子邮件欺骗，使邮件看似发送自 正当的 (实际上并非正当) 来源是一件很容易的事。使用 DMARC、SPF 或 DKIM 验证电子邮件通道，可以最大限度地减少电子邮件欺骗和潜在网络钓鱼的发生率。

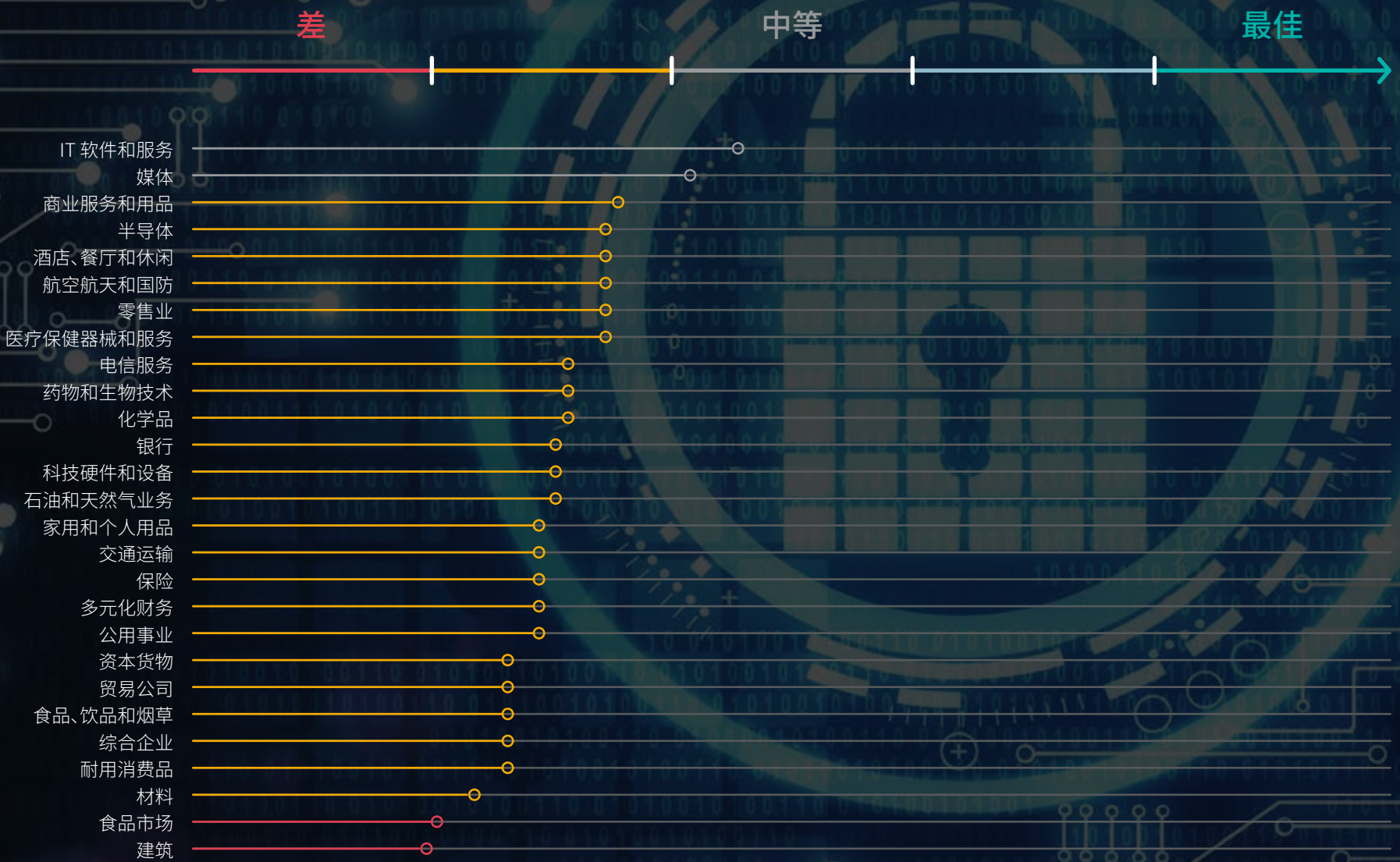
按行业组划分的域名安全控制手段采用情况

受新冠肺炎影响，某些行业发现自身备受关注。这些行业是医疗保健器械和服务业、药物和生物技术业、化学品业以及家用和个人用品业。过去一年半内，人们对以上这些行业的需求有所增加，因而使这些行业成为网络罪犯的主要目标。这些行业仍处于风险缓解成效量表的中下部分，令人十分担忧。在这四个行业中，医疗保健器械和服务业对 DNSSEC 的采用率极低，而家用和个人用品业的采用率则为 0%。同样，如果没有适当采用 CAA 记录，则被损害的域名可能会对自身使用数字证书，让人看起来合法，且不被该品牌察觉。同样，平均而言，在这些行业内，仅有四分之一的组织采用注册局锁，而注册局锁可防范域名劫持和对DNS的未经授权变更。鉴于这些行业内有32-48%的公司在使用消费级注册商，而这类注册商没有将DNSSEC、注册商锁或 CAA记录用作其标准，所以就算这三种协议的采用率低，或许也不足为奇。因此，这些公司可选择与企业级域名注册商合作，从而受益。

石油和天然气业近期也成为了焦点，尤其是美国能源公司 Colonial Pipelines 受到勒索软件攻击后。这次攻击使该公司关闭了5,500英里州际燃料管道。路透社评论称：“这次事件是有报道以来最具破坏性的数字勒索行动之一，引起了大众对美国能源基础设施在面对黑客时如此不堪一击的关注。”从事石油和天然气业的公司应认真看待这件事——尤其是，我们的统计数据显示，在全球2000强企业中，石油和天然气业处于成效量表的下半部分。在从事该行业的公司中，仅 4% 使用DNSSEC，有 10% 则使用注册局锁。

在采用域名和 DNS 安全措施方面，银行业仍喜忧参半。换言之，作为按理来说是网络钓鱼攻击首要目标的行业，DMARC（电子邮件认证协议）的采用率为 49.7%，仍低得令人忧心。

风险缓解成效量表


差
中等
最佳
IT 软件和服务
媒体
商业服务和用品
半导体
酒店、餐厅和休闲
航空航天和国防
零售业
医疗保健器械和服务
电信服务
药物和生物技术
化学品
银行
科技硬件和设备
石油和天然气业务
家用和个人用品
交通运输
保险
多元化财务
公用事业
资本货物
贸易公司
食品、饮品和烟草
综合企业
耐用消费品
材料
食品市场
建筑

建议

域名安全是大部分网络安全策略中缺失的一环。为您的域名执行同级别中最佳的安全措施，有助于在早期防范网络钓鱼攻击、BEC 和勒索软件攻击。许多业内专家都强调，维持良好的网络健康十分重要。域名安全是各公司不足之处的主要例子。域名安全在网络钓鱼攻击中发挥预防性作用，这样也能防范 BEC 攻击、假冒身份欺诈、勒索软件攻击和其他众多威胁。

从事各行各业的所有公司，尤其是如今因新冠肺炎而面临更大风险的公司，应从与企业级提供商合作开始，为域名安全采用多层次深度防御措施。CSC 推荐以下四大策略：

- **采用**深度防御措施来进行域名管理
- **确认**您的域名注册商的商业实践没有助长欺诈和品牌滥用行为
- **持续监控**域名空间和关键数字渠道，如市场、应用程序、社交媒体和电子邮件，防止品牌滥用、侵权、网络钓鱼和欺诈
- **实行**全球维权，包括关停和先进的网络封锁技术

采用深度防御措施来进行域名管理

- 为了消除第三方风险，除了评估您的域名注册商的安全性，技术和流程，也需要评估您的DNS管理服务提供商。
- 通过以下方式保护关键域名、DNS 和数字证书：
  - 执行双重验证
  - 监控 DNS 活动
  - 使用安全措施，例如域名注册局锁、DNSSEC、DMARC、CAA 记录和 DNS 托管冗余

持续监控域名空间和关键数字渠道，如市场、应用程序、社交媒体和电子邮件，防止品牌滥用、侵权、网络钓鱼和欺诈

- 利用网络钓鱼监控和由浏览器、合作伙伴、ISP 和 SIEM 组成的欺诈封锁网络
- 识别域名和 DNS 欺骗策略，例如同形文字（模糊匹配和 IDN）、相似域名、关键字匹配和同音异义词
- 识别网络内容上的商标和版权滥用行为
- 通过市场监控，保护您的品牌免受在线市场滥用
- 追踪相关社交媒体渠道中所有提及品牌的情况
- 监控主要应用程序商店
- 查找耗费您流量并损害您品牌的广告

确认您的域名注册商的商业实践不会助长欺诈和品牌滥用行为

消费级域名注册商通常有以下问题：

- 为域名抢注和拍卖提供域名市场交易功能，并向出价最高者出售包含商标的域名
- 域名颠倒和鼓吹注册包含商标的域名
- 通过包含商标的点击付费类网站的域名赚钱
- 频繁泄露数据，导致 DNS 攻击、网络钓鱼和 BEC

实行全球维权，包括关停和先进的网络封锁技术

- 使用对知识产权侵权和欺诈行为的多种维权行动：
  - 第一类维权行动包括在市场上下架，暂停显示社交媒体页面，使移动应用程序下架，下达停止令，删除欺诈性内容，以及全面缓解威胁载体
  - 第二类维权行动包括暂停使用注册商层面的域名和无效的 WHOIS 域名，并发出欺诈警报
  - 第三类维权行动包括统一域名争议解决规则和统一快速暂停程序、域名收购、深入调查和测试购买
- 使用各种技术上和法律上的维权手段，并按具体案例选择最适合的方法

按安全措施划分的行业采用率

高采用　低采用

企业级域名注册商

酒店、餐厅和休闲	75%
家用和个人用品	68%
商业服务和用品	65%
媒体	64%
IT 软件和服务	61%
化学品	57%
零售业	56%
药物和生物技术	56%
航空航天和国防	54%
半导体	53%
医疗保健器械和服务	52%
资本货物	47%
交通运输	47%
食品、饮品和烟草	47%
耐用消费品	46%
保险	45%
科技硬件和设备	42%
银行	38%
综合企业	38%
电信服务	36%
贸易公司	35%
多元化财务	35%
公用事业	35%
石油和天然气业务	28%
建筑	24%
材料	22%
食品市场	22%

注册局锁

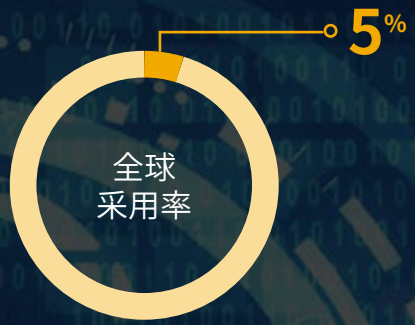
IT 软件和服务	48%
媒体	40%
航空航天和国防	33%
商业服务和用品	33%
半导体	28%
电信服务	28%
零售业	27%
化学品	27%
药物和生物技术	27%
医疗保健器械和服务	25%
耐用消费品	24%
资本货物	23%
酒店、餐厅和休闲	21%
家用和个人用品	21%
多元化财务	20%
交通运输	19%
科技硬件和设备	19%
保险	18%
食品、饮品和烟草	16%
银行	14%
综合企业	13%
公用事业	11%
石油和天然气业务	10%
材料	9%
食品市场	6%
建筑	6%
贸易公司	3%

高采用　低采用

DNS 冗余

交通运输	28%
石油和天然气业务	25%
银行	23%
IT 软件和服务	23%
航空航天和国防	21%
贸易公司	21%
电信服务	20%
化学品	20%
半导体	19%
保险	19%
零售业	18%
多元化财务	17%
酒店、餐厅和休闲	17%
食品市场	16%
资本货物	14%
耐用消费品	13%
材料	12%
商业服务和用品	12%
媒体	12%
家用和个人用品	12%
公用事业	11%
药物和生物技术	11%
食品、饮品和烟草	10%
建筑	9%
综合企业	9%
科技硬件和设备	8%
医疗保健器械和服务	7%

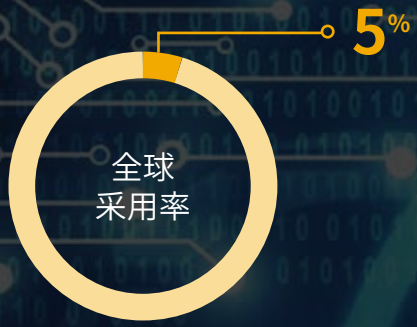
DNSSEC



IT 软件和服务	14%
航空航天和国防	13%
媒体	12%
银行	9%
半导体	9%
多元化财务	6%
公用事业	6%
商业服务和用品	6%
保险	4%
电信服务	4%
石油和天然气业务	4%
资本货物	4%
耐用消费品	3%
贸易公司	3%
药物和生物技术	3%
建筑	2%
化学品	2%
科技硬件和设备	2%
酒店、餐厅和休闲	0%
医疗保健器械和服务	0%
零售业	0%
交通运输	0%
家用和个人用品	0%
食品、饮品和烟草	0%
综合企业	0%
材料	0%
食品市场	0%

高采用　低采用

CAA 记录



媒体	16%
IT 软件和服务	13%
石油和天然气业务	13%
银行	9%
商业服务和用品	8%
电信服务	8%
综合企业	6%
公用事业	6%
多元化财务	6%
化学品	5%
科技硬件和设备	5%
医疗保健器械和服务	5%
酒店、餐厅和休闲	4%
交通运输	4%
保险	4%
材料	3%
零售业	3%
药物和生物技术	3%
耐用消费品	2%
资本货物	2%
建筑	1%
食品、饮品和烟草	1%
半导体	0%
航空航天和国防	0%
家用和个人用品	0%
贸易公司	0%
食品市场	0%

DMARC

IT 软件和服务	74%
医疗保健器械和服务	73%
半导体	72%
媒体	64%
酒店、餐厅和休闲	63%
零售业	60%
药物和生物技术	60%
石油和天然气业务	59%
综合企业	56%
电信服务	56%
科技硬件和设备	56%
食品、饮品和烟草	54%
公用事业	54%
商业服务和用品	53%
航空航天和国防	50%
银行	50%
材料	47%
家用和个人用品	47%
交通运输	46%
保险	46%
多元化财务	43%
贸易公司	41%
化学品	41%
耐用消费品	38%
食品市场	38%
资本货物	37%
建筑	28%

CSC 是企业域名、域名系统 (DNS)、数字证书管理以及数字品牌和欺诈防御领域值得信赖的供应商，位列福布斯全球2000强企业和全球最具价值100大品牌®。随着全球公司加大安全性方面的投资，CSC可以帮助他们了解存在的已知安全盲点，保护域名、DNS和数字证书。CSC的专有安全解决方案可保护公司在线资产免受网络威胁，避免重大经济损失、品牌声誉受损，或因不遵守《通用数据保护条例》(GDPR)之类的政策而受到重大经济处罚。我们还提供在线品牌保护（在线品牌监控和执行活动的结合），采用全面的数字资产保护方法，并提供欺诈防御服务来抵御网络钓鱼攻击。

CSC 提供的研究和主编

Vincent D' Angelo, 公司发展和战略联盟全球总监
Stephanie Mitchell, 市场部经理
Quinn Taggart, 全球品牌安全高级顾问
Letitia Thian, 市场部经理
Sue Watts, 全球营销主管

cscdbs.com/cn

DBS09172021