CSC

2022

域名安全报告

主要研究结果摘要——2022 年有何新进展?

过去三年,CSC 每年都在报告福布斯全球 2000 强公司的域名安全状况。今年,我们看到一些公司在安全方面有所提升,但也仍有部分公司依然面临着相当大的域名安全风险。我们的宗旨在于,提高客户对这些威胁的认识,分享我们的域名安全最佳实践经验,从而改善所有企业的域名安全状况。

近 3/4 的全球 2000 强企业,面临的安全威胁风险高得惊人

近四分之三的全球 2000 强企业仅实施了不到一半的域名安全措施。CSC 研究了八项关键安全措施,并据此得出了每家公司的平均得分。得分越高,安全系数越强。

45% 与企业级注册商合作的企业也使用注册局锁

注册局锁可确保端到端域名操作安全,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的修改或删除。而使用消费级注册商的企业仅有5%部署了注册局锁。而未锁定的域名极其容易受到社交工程策略的影响,这可能导致未经授权的 DNS 更改和域名劫持。

75% 的模仿全球 2000 强品牌名称(同形文字)的域名注册,由第三方持有

在 75% 由第三方(而非全球 2000 强品牌所有人)拥有的同形字(虚假)域名中,2022年有82%的企业使用隐私保护措施遮盖了自己的 WHOIS 或所有者的详细信息,而2021 年则为77%,这表明有更多公司在使用 WHOIS 隐私保护措施。

<5% 执行其他保护性域名安全措施方面的增长量

各公司均在绞尽脑汁设法获得其能承担的网络保险费率的资格,而域名安全与其他网络开支相比则是成本相对较低的解决之道。鉴于不部署域名安全措施的风险有可能导致网络钓鱼或勒索软件攻击,以及许多其他网络威胁,我们表达过希望看到更多公司执行其中某些安全措施,例如注册局锁、域名系统 (DNS) 冗余、DNS 安全扩展 (DNSSEC) 和证书认证机构授权 (CAA) 记录。

23% 的 DMARC 方面增长量(其为最高增长量)

反钓鱼工作小组 (APWG) 的最新数字显示,网络钓鱼攻击的次数创下新高,自 2020 年以来增长了十倍——因此,说它助推了各公司基于域名而采用的消息身份验证、报告和一致性(DMARC),也就不足为奇了。—DMARC是一种电子邮件验证系统,旨在保护公司的电子邮件域名不被用于欺骗、网络钓鱼欺诈和其他网络犯罪。

随着零信任安全模型成为最佳的防御性安全策略，2022 年已然向公众告知了将域名安全包含在内有多重要

零信任模型须延伸至业务系统、应用程序和设备之外，且把作为实际漏洞的公司域名生态系统纳入至图 1 所注的攻击内。以下两种域名安全威胁被用于启动下列所有攻击。

图 1

拥有全球业务的企业极其依赖互联网开展各类活动——网站、电子邮件、认证、IP 语音 (VoIP) 等等。互联网是企业易遭受外部攻击的一部分，需要予以持续监控，以防范网络犯罪攻击和欺诈。随着网络风险持续增加，各企业和网络保险公司在确定这些风险的数量和化解其伤害的能力方面面临着巨大的挑战。差不多每一天，我们都在被告知着有关供应链攻击、勒索软件和网络钓鱼攻击的新进展，此外，在需要覆盖什么范围以及如何阻止它们方面，还增加了更多层次的复杂性。

具有定义的域名安全

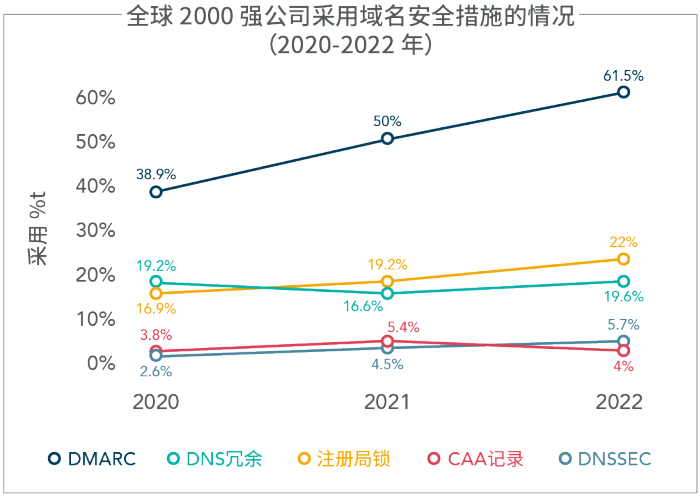
CSC使用多层次的方法管理域名安全。首先也是最重要的，是确保域名组合的安全，来保障品牌的在线曝光安全，这可能由多个品牌收购和在线DNS足迹组成。其次，我们针对网络品牌的威胁载体进行监控和分析，并采取相应的维权行动。最后，我们以防火墙背后的内部数据集来补足其他两个数据集，以全面了解品牌的安全状况。

本报告研究了全球 2000 强公司的安全状况，而福布斯每年都会更新其榜单（每年都有新公司上榜，一些之前上榜的公司在之后可能无法进入前2000名）。本报告中发表的见解完全基于公开的数据集。这些数据集通过经由机器学习、人工智能和深度搜索技术提供支持的独一无二专有数据湖来管理。

研究结果和分析

在本研究分析中，CSC首先 研究了全球 2000 强企业对下述域名安全措施的采用情况，然后再按照行业和地区进行深入的分析。

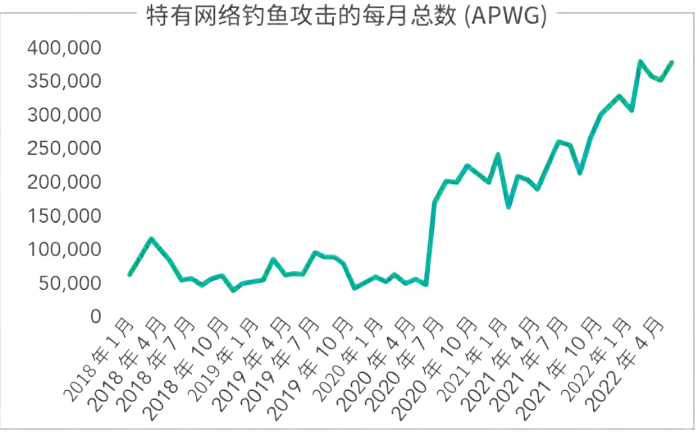
采用域名安全措施的趋势（2020-2022 年）



两年内，DMARC 的使用几乎翻了一番

鉴于有关网络钓鱼攻击的（包括其攻击量和复杂程度的增加）所有新闻报道，DMARC 的使用率从 2020 年的 39% 飙升至 2022 年的 62%，也就不足为奇。

反钓鱼工作组 (APWG) 的最新数据显示，网络钓鱼攻击的次数比以往任何时候都高，其中在 2022 年第一季度，已识别的特有网络钓鱼攻击的季度总数首次超过 100 万次，且每月有 600 多个不同的品牌受到攻击。



而如今，验证标记证书 (VMC) 要求设置 DMARC，来验明安全套接 (SSL) 证书，这也是推动 DMARC 增长的原因。此外，Apple 在 9 月公布了品牌信息识别指标 (BIMI)，并称其 iOS 16 和 macOS 的电子邮件客户端将为业界致力打击品牌欺骗和假冒身份的努力提供支持。支持 BIMI 的发件人必须严格符合电子邮件身份验证标准，包括使用 DMARC 安全标准。

使邮件看似发送自正当（实际上并非正当）的来源，以此进行电子邮件欺诈，是一件很容易的事情。尽管使用 DMARC 对电子邮件渠道进行身份验证可以最大程度地减少电子邮件欺骗和潜在的网络钓鱼，我们依然明白，如果没有执行 DMARC 拒绝策略，即便落实了这种控制措施，也仍然会带来网络钓鱼风险，所以，在执行过程中包含这种策略也是必须的。

注册局锁、DNS 冗余、DNSSEC 和 CAA 记录等安全措施在持续而缓慢地增长

启用注册局锁的公司从 2020 年的 17%，增长至 2021 年的 19% 和 2022 年的 22%。注册局锁可确保端到端域名操作安全，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的修改或删除。但有些域名依然可能保持在未锁定状态，因为并非世界各地的每个注册局都提供锁定服务。

在过去的三年中，部署 DNS 冗余和 DNSSEC 的企业数量略有增加。由于 DNS 是企业核心基础设施的关键组件，所以有更多政府机构呼吁 DNS需具备一定的柔韧性。但由于各公司需要通盘规划其日益增加的成本和资源配置，所以即便 DNS 的采用率增长情况与各组织日益面临的加强措施的压力一致，我们亦仍未看到更高的采用率。

最后，CAA记录的使用率在 2020 年至 2021 年期间略有提升，但在 2022 年又略有下降。CAA 记录允许企业指定特定的证书认证机构 (CA) 作为其企业域名证书的唯一颁发机构。这样可以防止网络罪犯使用非指定的证书认证机构来获取新证书。他们的请求会失败，公司会收到警报。但许多公司仍没有充分利用这项安全控制措施，因为他们通常难以全面了解掌控相关要求，尤其是在他们使用多家域名、DNS 和 SSL 提供商时。

按注册商类型划分的 2022 年域名安全措施

在这份报告中，我们对全球 2000 强企业所使用的域名注册商的域名安全措施采用趋势进行了分析。

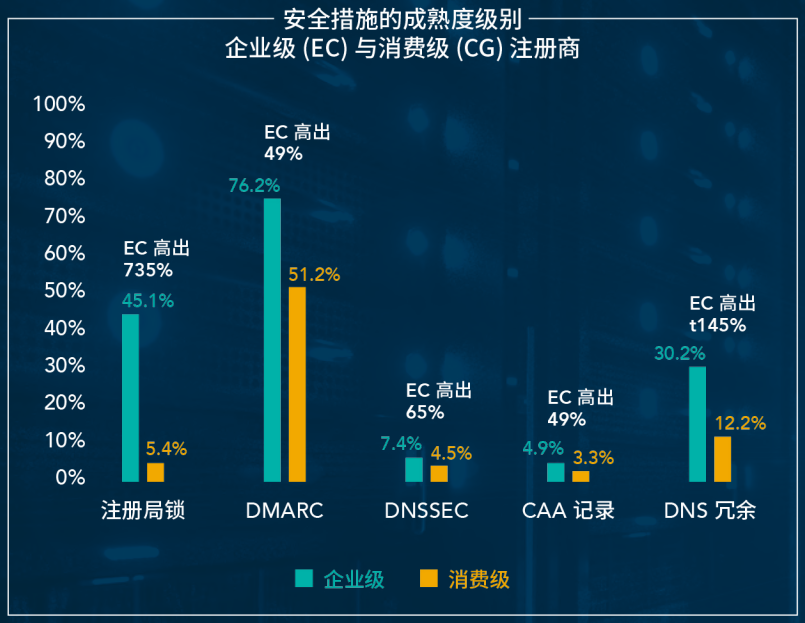
消费级注册商：

消费级注册商专门为个人用途、企业家和初创小公司提供域名服务、网站和电子邮件服务。

企业级注册商：

企业级注册商专业从事与各企业和品牌所有人合作，在域名和 DNS 管理以及安全、品牌和防欺诈保护、数据治理和网络安全方面提供其所需的高级业务实践、能力、专业知识和支持人员。

依赖企业级注册商实力的企业，其采用域名安全措施的比率更高。



许多企业误认为所有注册商都一样，因此对消费级注册商投注了错误的信任和期望。而实际上这类注册商可能不是为了域名安全而设计的，这可能会影响公司整体的安全状况。这在注册局锁的采用方面尤为明显，因为大部分消费级注册商都不支持注册局锁功能。

在 2021 年末，SecurityScorecard 研究了使用企业级注册商和消费级注册商的公司的网络评级。他们的研究结果显示，由企业级域名注册商管理域名的公司，其整体网络安全评级高出半个或整个字母等级。

了解更多：

- 域名安全始于您的注册商
- 您网络安全的短板取决于您供应商的实力
- 在域名注册商生态系统中，供应商选择至关重要

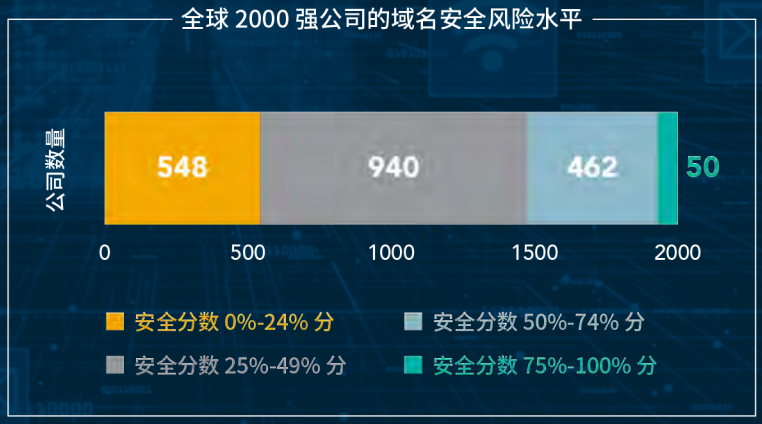
总体域名安全状况

CSC 根据企业的**域名安全风险等级**，对八项主要安全措施的重要性进行分组，为每家企业计算出一个平均分。该平均分构成了企业的安全分数，分数越高，表明安全状况越稳固——这也意味着公司遭受域名安全威胁的风险越低。

主要域名安全措施

- 企业级注册商
- 注册局锁（多重锁定）
- CAA 记录
- DNS 冗余
- DNSSEC
- SPF
- DKIM
- DMARC

近 3/4 的公司执行的域名安全措施不足全部措施的一半



表现最佳的五大行业

- IT 软件与服务
- 商业服务与用品
- 酒店、餐厅与休闲
- 媒体
- 航空航天与防务

表现最佳的公司

6 家公司的安全分数得分最高，且对域名安全措施的采用率也最高。

其中 2/3 的公司为美国公司。

表现最差的五大行业

- 耐用消费品
- 食品市场
- 建筑
- 贸易公司
- 材料

表现最差的公司

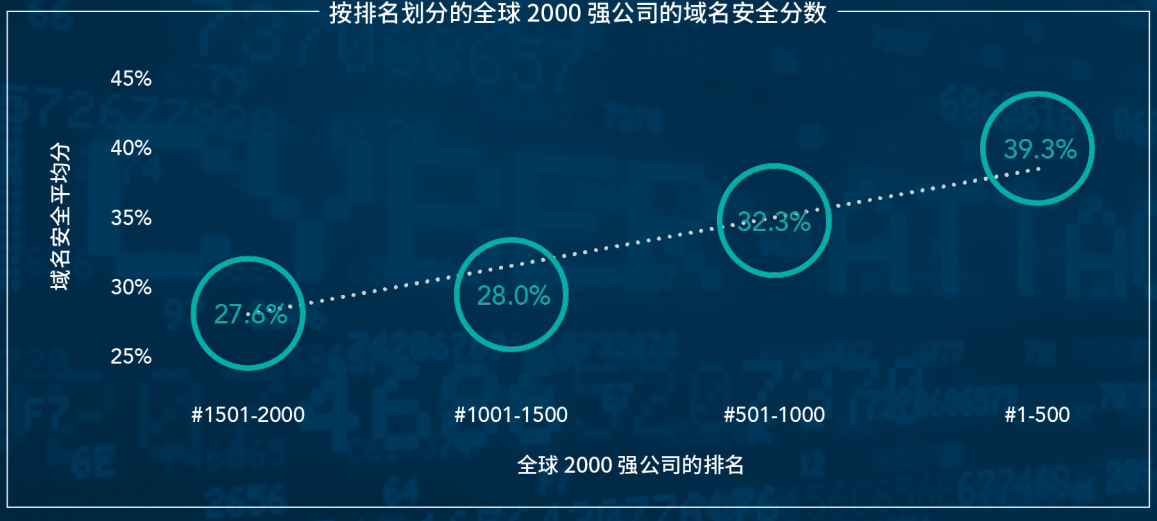
137 家公司的域名安全分数为零分

这些公司主要位于亚太地区，它们占据零分公司的 **82%**

表现最差的行业，即食品市场、材料和建筑，因缺乏域名组合安全措施，而面临的网络攻击风险最高。供应链问题与这三个行业已经在应对的各种材料、劳动力和分销问题交织在一起，带来了更多问题。耐用消费品也位列表现最差的五大行业内，其中包括各汽车公司。值得注意的是，鉴于物联网 (IoT) 已成为新车内更个性化功能的一个重要组成分，这些公司如今的网络安全状况也变得更稳健。这些公司需要规避更多潜在的威胁。

域名安全分数与全球 2000 强公司排名的关系

一家公司在全球 2000 强中的排名越靠前，其域名安全状况越佳。



针对全球 2000 强企业的可疑或恶意域名活动

我们识别和分析了包含全球 2000 强公司品牌名称的超过六个字符的域名，而这些品牌本身并不拥有这些域名。这些虚假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，从而导致品牌造成收入损失、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和组合方式。

我们有意关注常见的同形文字，因为它们是威胁发起者使用的最恶劣攻击方法之一。

域名欺骗策略

模糊匹配

cscg1obal.com　cscgl0bal.com

同形文字 – 国际化域名 (IDN)

ćscglobal.com　csçglobal.com

相似域名

cscglobal.jp　cscglobal.ec

关键字匹配

cscglobalcovid.com　covidcscglobal.ar　covid19.com

同音异义词（同音字符串）

siesiglobal.com　cscclobol.com

.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

C0rnpanyNarne.com

最流行的替代字符

i → l	m → rn	i → 1
s → 5	o → 0	e → 3
l → 1	l → i	w → vv

75% 超过 75% 的同形字域名由第三方所有。这与 2021 年的研究结果一致。

在第三方所有的域名中：

82% 在 2022 年掩盖了他们的 WHOIS 或所有权详情，而 2021 年为 **77%**，这表明逐渐有更多公司在使用隐私保护措施。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。

48% 在 2022 年配置了 MX 记录。2021 年则为 **43%**。MX 记录可以被用来发送网络钓鱼电子邮件或拦截电子邮件。

第三方域名作何用途？

46% 指向广告、按点击付费的广告，或被用于域名停放。

41% 拥有不活跃的网站。

5% 被指向恶意内容。有害的内容可能损害品牌声誉，削弱客户信心。其风险在于，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。

8% 解析与品牌持有人无关的活跃网站。

域名注册商大多数与第三方的虚假域名注册活动有关：

GoDaddy® | Namecheap™ | PDR LTD

可疑和恶意域名：目标是谁？

虚假域名注册针对的行业排名

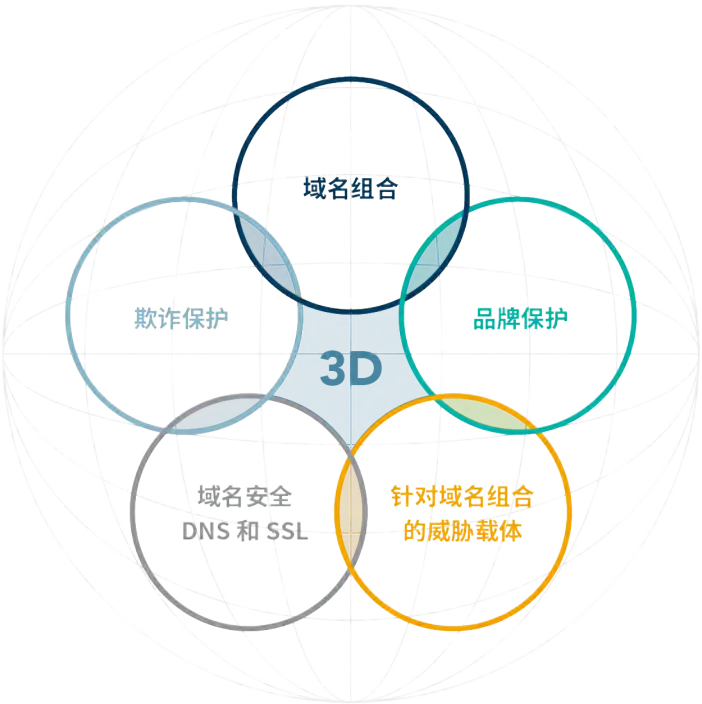
行业	虚假域名威胁占总数的百分比
银行	10.0%
IT 软件与服务	7.0%
商业服务与用品	5.5%
耐用消费品	5.4%
医疗保健器械与服务	4.6%
多元化财务	4.6%
药物和生物技术	4.6%
电信服务	4.5%
交通运输	4.2%
保险	4.1%
石油和天然气业务	3.9%
建筑	3.7%
材料	3.5%
食品、饮品和烟草	3.5%
零售业	3.2%
化学品	3.2%
科技硬件与设备	3.2%
酒店、餐厅与休闲	3.0%
资本货物	2.8%
公用事业	2.7%
航空航天与防务	2.5%
家庭与个人用品	2.1%
贸易公司	2.0%
综合企业	2.0%
媒体	1.8%
半导体	1.7%
食品市场	0.4%

CSC 的 DOMAINSEC℠ 平台简介

CSC 的 3D 域名安全与维权解决方案通过运用旗下 DomainSec 平台强大的功能打造而成。

DomainSec 是 CSC 发明的一款软件即服务 (SaaS) 网络安全平台，是业内首个保障和维护品牌域名生态系统的全套解决方案。该平台使用专有机器学习深度搜索（MLDS）技术，结合了机器学习、人工智能与归集合并技术以识别重要的泄露指标。

DomainSec 将 CSC 域名管理，域名安全与品牌保护和欺诈防护解决方案融入一个平台——这意味着我们不仅能提供效果呈指数级提高的保护，还能帮助各企业优化零信任安全模型，突破安全保障的局限。



结论

公司如若不对域名安全风险采取应对措施，后果将不堪设想。未受保护的域名对网络安全状况、数据保护措施、消费者安全、知识产权、供应链、收入和声誉均会构成重大威胁。我们可以预期，公众对这些问题的意识将会提高，网络保险提供商将开始要求客户对其域名防御策略和方法的质量和严谨性负责。

各企业需要在零信任框架内建立分层的安全模型，以搭建稳健的企业安全形态，将业务面临的风险降至最低。如前文所述，该方法的组成包括与企业级注册商合作，对暴露面（包括域名和 DNS）的可见性，以及对那些视企业的线上曝光为目标的威胁手段进行分析的能力。

请获取我们的域名安全建议，使您的域名和品牌免遭网络威胁和欺诈。

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方面值得信赖的安全与威胁情报提供商，是福布斯全球 2000 强企业和全球最具价值 100 大品牌® 的首选。随着全球各企业加大安全状况方面的投资，CSC 可以帮助企业了解已知的网络安全疏忽问题，并帮助企业保护在线数字资产和品牌。企业可以凭借 CSC 的专有技术来增强自身的安全状况，防范针对在线资产和品牌声誉的网络威胁载体，避免因违反《通用数据保护条例》(GDPR) 等政策而遭受灾难性的收入损失以及数额巨大的经济罚款。CSC 还提供线上品牌保护 (在线品牌监控和维权活动的结合)，采用全面的数字资产保护方法，并提供欺诈防护服务来抵御网络钓鱼攻击。CSC 成立于 1899 年，总部位于美国特拉华州威尔明顿市，在美国、加拿大、欧洲和亚太地区设有办事处。CSC 是一家全球性公司，通过聘请相关领域的专家，可与世界各地的客户开展合作。请访问 cscdbs.com/cn.

本研究由 CSC 的以下人员编写：

IHAB SHRAIM	首席技术官
VINCENT D'ANGELO	全球总监，战略联盟与合作伙伴
ELLIOTT CHAMPION	产品总监，全球品牌和域名
QUINN TAGGART	安全高级顾问，全球品牌安全
FERNANDO CEVALLOS	产品总监，全球反欺诈和威胁情报

DBS11142022