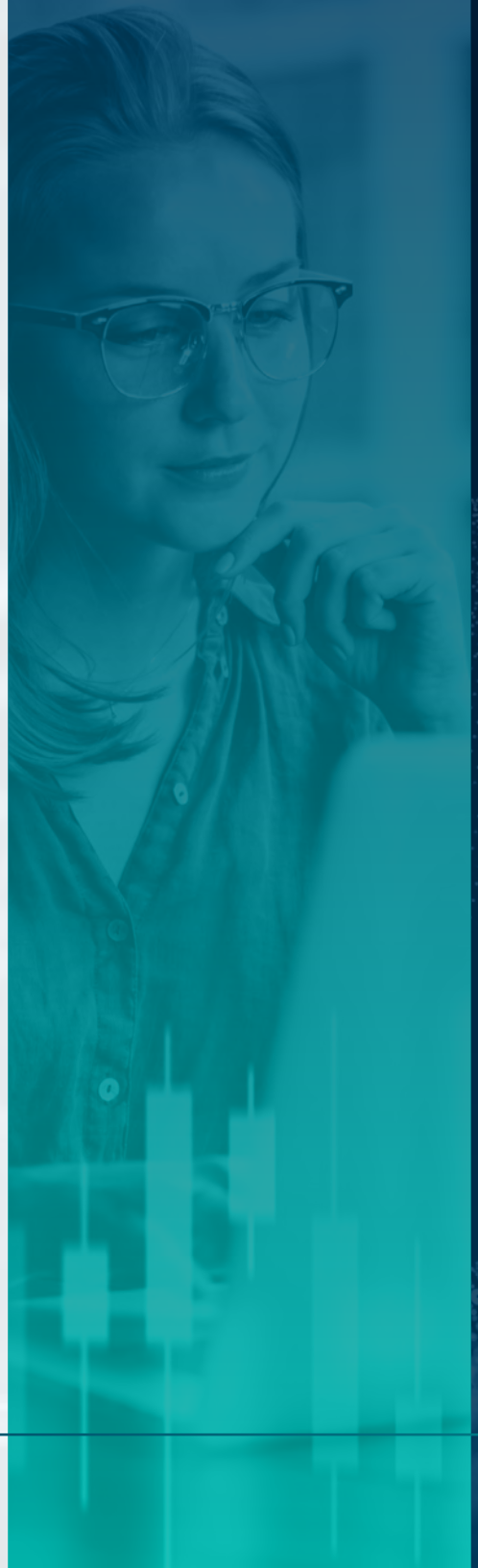


2023 域名安全报告

过去四年，CSC 每年都会率先报告福布斯全球 2000 强企业的域名安全状况。今年，我们看到部分企业更加重视安全问题，但仍有很大比例的企业依然存在相当大的域名安全风险。我们的理念是提高对这些威胁的认识，分享域名安全最佳实践。

我们分析了全球 2000 强企业为降低公司防火墙之外的域名生态系统中的网络风险而采取的域名安全措施，以及第三方对线上品牌造成的潜在滥用与侵权事件。

重要研究结果摘要

第三方注册了 43% 的 .AI 域名

很多企业要么还没有考虑过购买自有品牌的 .AI 域名，要么就发现此类域名早已被一些精于此道的网络惯犯抢注。2023 年涉及 .AI 域名后缀域名争议案件同比增长 350%，充分证明了这一现状。

21% 的子域名 DNS 记录指向无法解析的内容，这使公司易受到子域名劫持

CSC 分析了我们数据库中的 600 多万条域名系统（DNS）记录，并审视了指向云基础架构的 A 记录和 CNAME，进一步筛查出 44 万多条有可能遭受子域名劫持的 DNS 记录。

79% 模仿全球 2000 强品牌名称的注册域名（即同形文字域名）由第三方持有

79% 的同形文字（虚假）域名由第三方而非全球 2000 强品牌所有者持有，在这些域名中，有 40% 的 MX 记录可能会用于未来的网络钓鱼攻击。

使用企业级注册商的企业中，46% 的企业还使用了注册局锁

注册局锁支持端到端域名事务的安全性，可减少人为错误，降低第三方风险。这是一种颇具成本效益的域名保护方法，可防止域名被意外或未经授权的修改或删除。而在使用消费级注册商的企业中，仅有 7 % 部署了注册局锁。(参见企业级与消费级注册商。)

112 家企业的域名安全评分为 0%

在全球 2000 强企业中，6% 的企业未部署任何推荐的域名安全措施，风险极高。根据我们对关键域名安全措施采用情况的分析，如果一家企业的风险水平为 0%，即表明其未采取任何措施，因此域名安全威胁处于最高风险水平。

基于域名的消息认证、报告和一致性 (DMARC) 增长 6%，是过去四年中增速最快的一年

自 2020 年以来，基于域名的消息认证、报告和一致性 (DMARC) 的采用率上升了 28%，这是一种电子邮件验证系统，旨在保护企业电子邮件域名，避免被用于诈骗和网络钓鱼欺诈。

2023 年域名安全成为引人关注的商业现象

随着人工智能 (AI) 赋能的网络安全日渐盛行，相应的攻击也随之增加，这使域名安全评估已成为一些公司最高级别网络风险评估流程中的重要一环。以下三种域名安全威胁被用于实现下列各种攻击。

遭到入侵或劫持的合法域名

恶意域名注册，比如同形文字域名

劫持的子域名

域名安全定义

全球企业的各种事务都要依靠互联网实现，包括网站、电子邮件、身份验证、IP语音 (VoIP) 等。互联网是企业外部受攻击面的一部分，需要持续进行监控，以防范网络犯罪和欺诈。随着网络风险不断加大，各个企业和网络保险公司在量化风险以及降低其破坏能力方面，面临的挑战愈加严峻。几乎每天，我们都会了解到关于供应链攻击、勒索软件和网络钓鱼攻击的新发展态势，我们需要花费更多时间和精力，才能全面获悉这些威胁并采取相应措施进行应对。

CSC 利用专有技术，采用分层式方法管理域名安全。首先，这涉及到通过保护域名组合（可能包含企业收购的多个品牌）和 DNS 在线足迹来保护品牌网络形象。其次，我们会监测和分析以线上品牌为攻击目标的威胁载体并开展维权活动。

什么是子域名劫持？

子域名劫持是指网络罪犯控制一个不再使用的合法子域名，并在其中加载自己的恶意内容，针对目标公司发动网络钓鱼攻击或恶意软件攻击活动。他们可能会巧妙地利用被目标公司遗忘的 DNS 记录，指向其自己的内容。

新出现的威胁：子域名劫持

21% 的 DNS 活跃子域名记录无法解析，这使公司易受到子域名劫持。

CSC 观察了指向主要云基础架构的 A 记录和 CNAME，分析了我们数据库中的 600 多万条 DNS 记录，并确定了超过 44 万条活跃的子域名记录。这些记录可能造成不法分子实施子域名劫持。我们开展这项调查的目的是了解企业子域名管理现状，以及这对公司整体安全状况的影响。

如何主动检测子域名劫持？

1. 对现有 DNS 区域文件进行全面审核，并查询每一条记录。
2. 确定应处于活跃状态的域名及其相应的子域名。
3. 实施持续监控，具体方法是定期扫描 DNS 活跃记录、捕捉任何状态变化，并立即向 SOC 24x7x365 全天候当值团队发出告警。
4. 在发现非法网站时，立即采取维权行动，并使用互联网屏蔽功能来阻止有害的在线内容。

如何避免您的合法子域名被不法分子劫持？

拥有多元化品牌组合和国际化业务的大型企业往往并未认识到其分布在全球的数字化足迹究竟有多庞大。随着时间的推移，数字化记录不断增加，导致坚守网络安全习惯成为一项艰巨的挑战。长久以来，企业一直通过与云提供商进行外包合作的方式获得使用新技术的机会，但 DNS 记录的增加（远超以往）以及日渐复杂的环境都会增加企业面临的风险。如果未对数字记录进行适当的监督和日常监控，企业就会积累“噪音”，导致原本简单的网络安全习惯复杂化，容易给网络罪犯留下可乘之机。

网络罪犯会扫描各种基础架构，例如云和公共服务，包括搜索指向某品牌不再使用的 Web 服务的 DNS 区域记录。不法分子会在不执行验证检查的云提供商处托管内容，请求先前使用过的区域目的地，并开始将 Web 用户引流到这些加载了其非法内容的子域名，而且完全不必入侵企业基础架构或第三方服务账户。据 ZDNet 报道，不法分子劫持了微软®的子域名，以宣传扑克赌场。

这种不指向任何内容、不活跃的区域的积累就称为“悬空 DNS”，会给企业造成子域名劫持风险。

这会给其他针对品牌的网络攻击（例如网络钓鱼和恶意软件攻击）带来可乘之机，进而给企业带来多种负面后果：收入损失、数据泄露、消费者信心丧失，以及因安全漏洞而造成的品牌声誉受损。总部位于维也纳的 IT 安全咨询公司 Certitude Consulting 近期在 Security Week 上发表了一份研究报告，其中警告称：数以千计的实体极易遭受这些攻击。

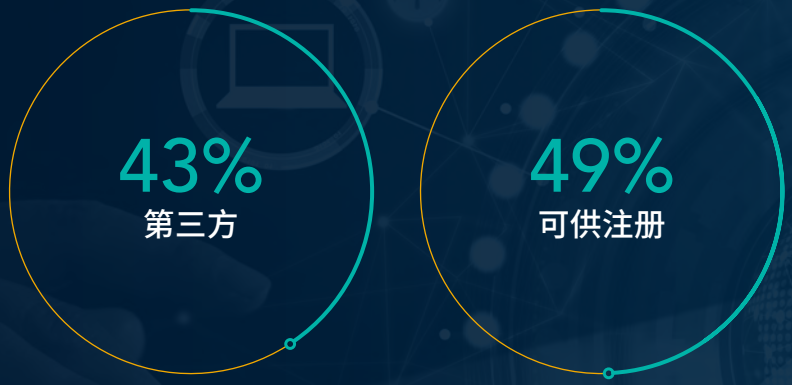
DNS 记录的管理必须纳入到当今的网络安全习惯之中。20 多年来，企业一直面临着 DNS 记录管理不善的风险，因为他们利用不同的所有人、策略和供应商来管理 DNS，如果有兼并和收购，情况还会进一步复杂化。此外，所有人不敢删除自己不确定的内容，担心会引起不必要的问题。

子域名劫持已成为当今诸多域名安全威胁之一，与域名劫持、DNS 劫持、域名阴影和缓存中毒并列。这些威胁往往会给进一步的网络攻击创造条件，使不法分子能够发动更恶劣的网络钓鱼和勒索软件攻击、商业电子邮件泄露 (BEC) 或数据渗漏攻击。

敬请阅读我们的《子域名劫持漏洞报告》或联系 CSC，了解更多信息！

第三方注册了 43% 的 .AI 域名

很多企业要么还没有考虑过购买自有品牌的 .AI 域名，要么就发现此类域名早已被一些精于此道的网络惯犯抢注。



随着人工智能 (AI) 技术的普及，科技领域发生了翻天覆地的变化。.AI 域名注册量的大幅增长印证了这样的变化，体现出人们对于 AI 技术的广泛使用与热情。CSC 始终立足这一趋势的前沿，积极主动地为客户出谋划策，帮助客户了解制定 .AI 域名注册和维权战略的重要性[1]。

此外，2023 年涉及 .AI 扩展名的域名争议案件数量大幅增加。截至 2023 年 9 月，此类案件的数量已经远超往年。2023 年，这种案件的同比增幅达到 350%，总数已超过先前四年的总和，凸显了提高警惕性和加强监管的必要性[2]。

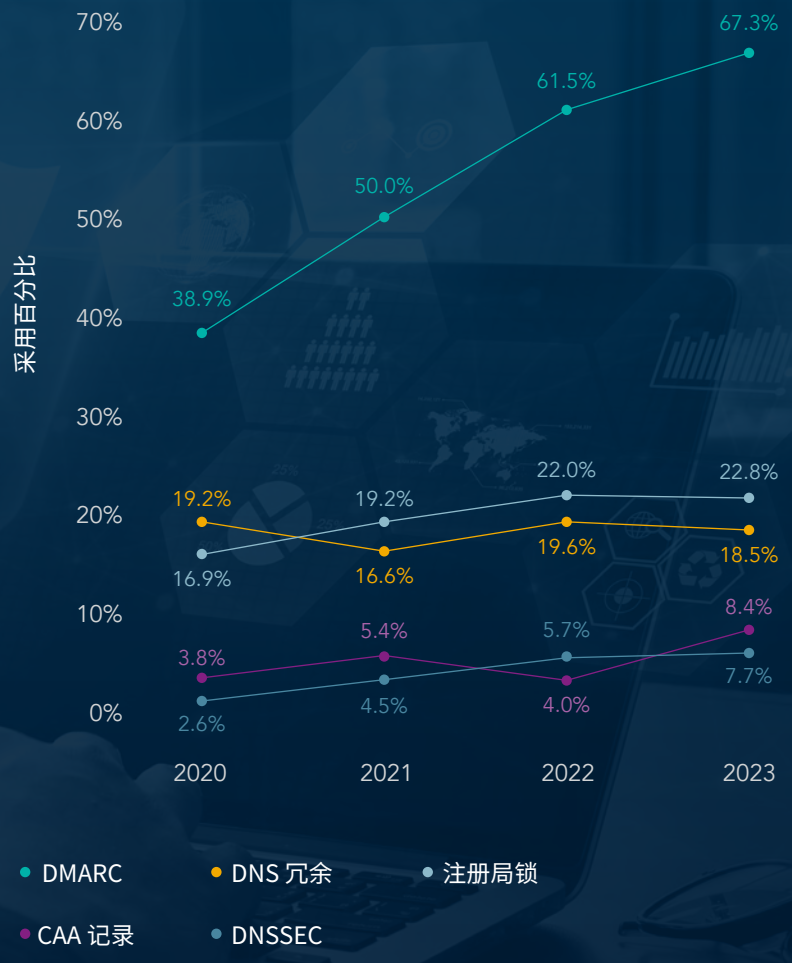
在全球 2000 强企业中，第三方注册或侵权的总体比例达到 43%。在已注册 .AI 品牌域名的企业中，84% 的相应域名注册在第三方名下。49% 的此类域名处于可注册状态。诸如银行业、多元化金融业以及 IT 软件和服务业等特定行业使用 .AI 域名的比例最高。

各国政府正在加强对 AI 工具的监管，企业也在不断开发和采用 AI 系统与流程。这一趋势表明，.AI 域名的需求量可能会进一步增加。此外，Google® 近期决定将 .AI 域名视为通用顶级域名，而不是以往的国家代码，突显出对于 AI 的全球重要性的认可[3]。

.AI 域名注册量的增长还预示着更加广阔的技术前景。AI 技术不断渗透到日常生活的方方面面，我们必须谨慎和高瞻远瞩地应对相关责任与挑战。

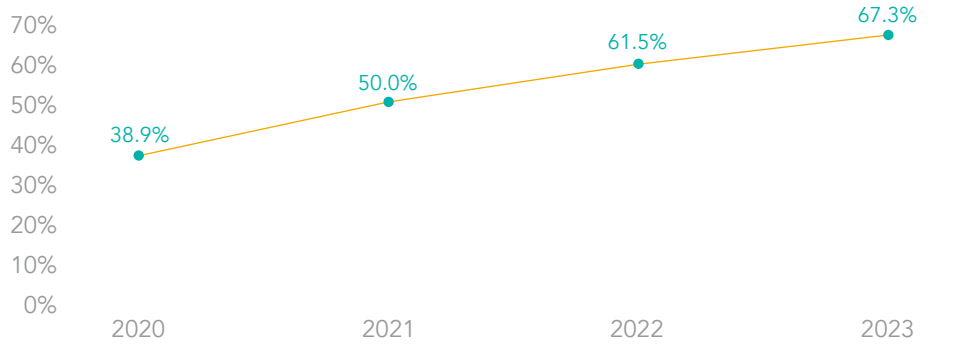
今年，涉及 .AI 后缀的域名争议案件数量增加了 350%。

全球 2000 强企业采用域名安全措施的情况 (2020 - 2023 年)



DMARC 见证最快增长

鉴于网络钓鱼攻击的各种报道频频登上头条，攻击数量和复杂程度与日俱增，DMARC 的使用率从 2020 年的 39% 迅速上升到 2023 年的 67%，这并不令人意外。



APWG 最新发布的数据表明，2022 年的网络钓鱼攻击创下新纪录，有记录的攻击超过 470 万次，2022 年第四季度，BEC 攻击平均造成的损失为 132.559 美元。自 2019 年初以来，网络钓鱼攻击的数量每年增幅都超过 150%，近年来每季度发生的网络钓鱼攻击都超过 100 万起，每月受到攻击的品牌（仅统计非重复品牌）约为 600 个。

每月的独立网络钓鱼攻击总数 (APWG)

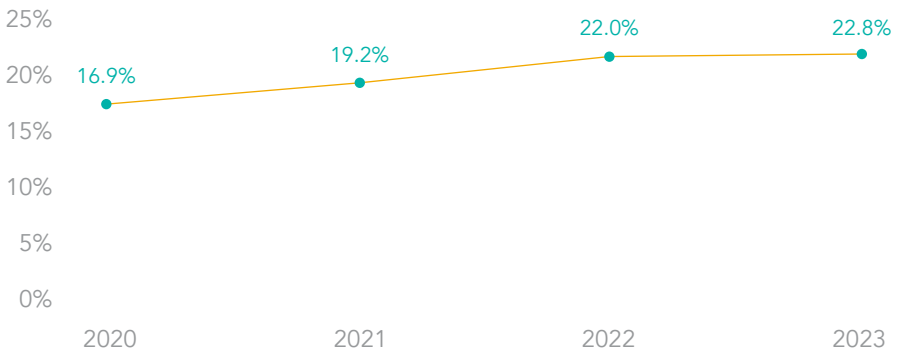
推动 DMARC 增长的因素还有电子邮件客户端越来越多地采用品牌信息识别指标 (BIMI)，允许在经验证的电子邮件中展示品牌标识。DMARC 是设置 BIMI 的安全前提条件，两者协同配合，基于电子邮件域名验证公司身份的真实性。

注册局锁的应用略有增长，但全球 2000 强企业的风险依然居高不下

部署注册局锁的企业（即注册局锁采用率）从 2020 年的 17% 增加到 2023 年的 23%。我们还观察到，在使用企业级注册商的企业中，46% 的企业还使用了注册局锁。随着政府机构进一步强调加强网络安全、杜绝域名系统滥用风险，越来越多的注册商为了应对监管和行业压力，开始为其域名扩展提供锁定功能。注册局锁支持端到端域名事务的安全性，可减少人为错误，降低第三方风险。这是一种颇具成本效益的域名保护方法，可防止域名被意外或未经授权的修改或删除。然而，有些域名可能依然未被锁定，因为并非全球各地的每一个注册局均提供锁定服务。

公司的域名组合不断变化，为此，CSC 使用预测性建模算法，评估域名的 20 多个属性，以确定该域名是否对公司运营和线上品牌具有关键的商业意义，并就应锁定的重要域名提出建议。

注册局锁

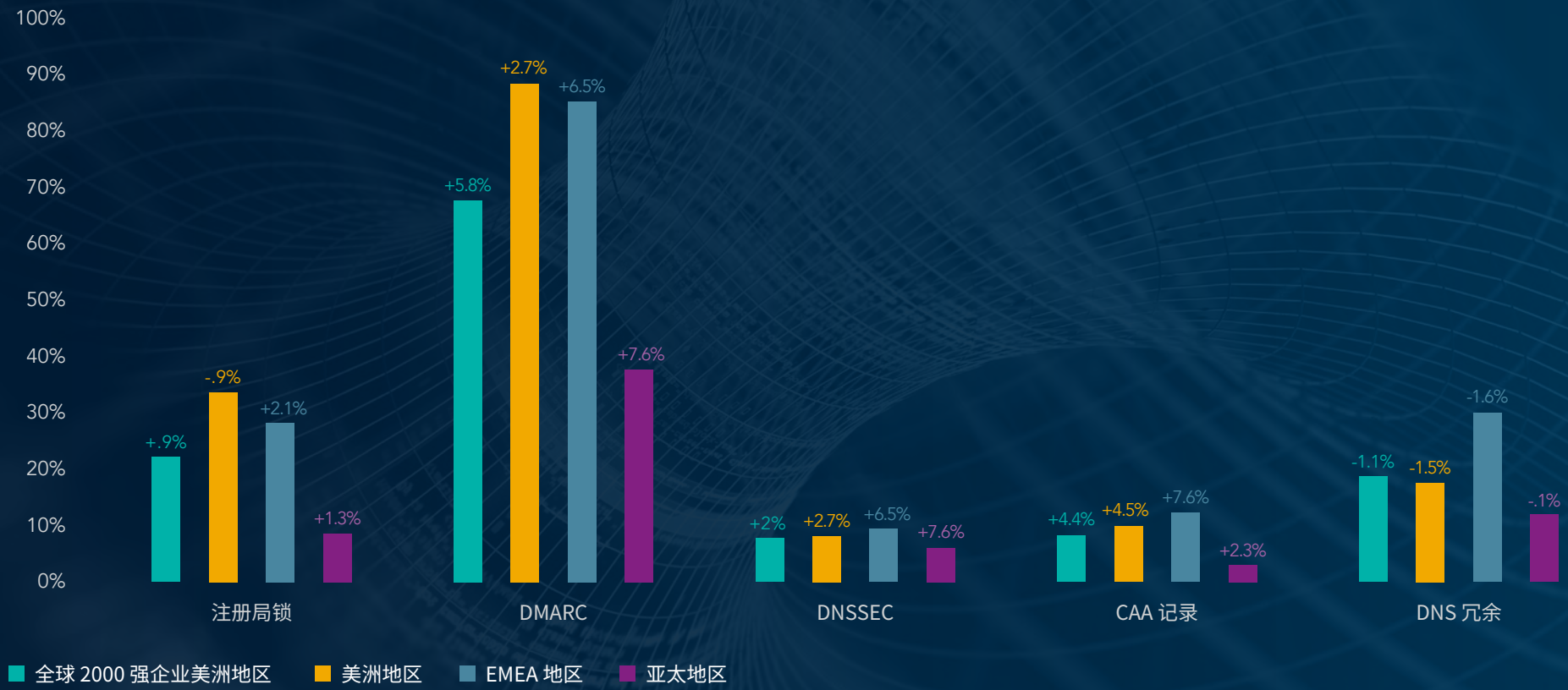


DNS 冗余、DNSSEC 和 CAA 记录等安全措施存在不一致问题

尽管部署域名系统安全扩展 (DNSSEC) 的公司依然还是少数，但在过去三年中，部署比例增加了一倍多，从 2020 年的 3% 增加到 2023 年的 8%。令人惊讶的是，尽管越来越多的政府机构呼吁提高 DNS 的抗风险能力，DNS 的冗余度却比去年下滑 1%，降至 19%。DNS 冗余对任何企业的核心基础架构来说都是重要组成部分，但我们发现，这种安全措施的采用率在下滑，原因可能是企业面临不断增加的成本和资源分配压力，需要合理筹划。

最后，证书认证机构授权 (CAA) 记录的使用率从 2020 年的 3.8% 增加到 2023 年的 8.4%。CAA 记录允许公司指定一个特定的证书认证机构 (CA)，作为其公司域名的唯一证书认证机构。此举可防止网络罪犯使用非指定的证书认证机构获取新证书，这会导致他们的请求失败，同时公司也会收到相关的警报。然而，很多公司仍未充分利用这种安全控制措施，因为他们通常难以全面掌控相关要求，这在他们使用多家提供商的域名、DNS 和安全套接 (SSL) 服务时表现尤甚。

2023 年按地区划分的域名安全措施



+/- 相较于上一年的增幅/减幅百分比

2023 年按注册商类型划分的域名安全措施

在本报告中，我们根据全球 2000 强企业使用的域名注册商类型，对域名安全措施的采用趋势进行了分析。

消费级注册商：

消费级注册商面向个人、创业者和刚刚起步的小公司提供域名服务、网站和电子邮件。

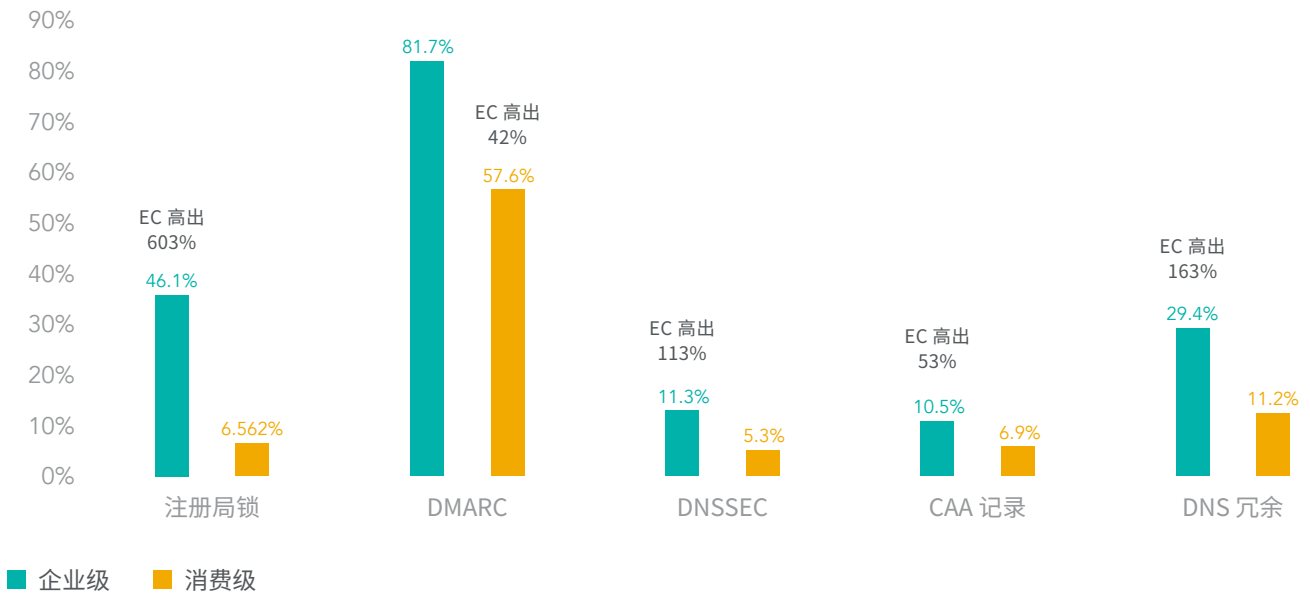
企业级注册商：

企业级注册商专门与各个企业和品牌所有人合作，满足他们对于高级业务实践、功能、专业知识的需求，以及对于域名管理、DNS 管理、安全性、品牌保护、欺诈防护、数据治理和网络安全方面的支持团队的需求。

很多公司都存在一个误区，认为所有注册商都别无二致，但是，消费级注册商的首要目标可能并不是保证域名安全，一旦误选了消费级注册商，企业的整体安全状况可能会受到不利影响。这一点在采用注册局锁方面尤为明显，因为大多数消费级注册商都不支持注册局锁。

依赖企业级功能的企业采用域名安全措施的比例更高

安全措施的成熟度水平，企业级 (EC) 与消费级 (CG) 注册商的对比



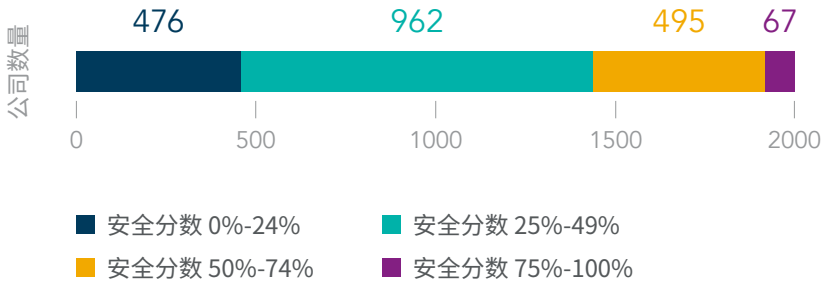
整体域名安全状况

CSC 根据企业域名安全风险等级，对八项主要安全措施的重要性进行分组，并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，表明企业的安全状况越稳固——这也意味着企业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
- CAA 记录
- DNS 冗余
- DNSSEC
- SPF
- DKIM
- DMARC

域名安全风险等级



72% 的公司实施的安全措施不到上述所列措施一半

表现最佳的行业

- IT 软件与服务
- 媒体
- 商业服务与用品
- 酒店、餐厅与休闲
- 医疗设备与服务

表现最佳的公司

- 只有两家公司取得了最高安全分数，对域名安全措施的采用率达到了最高值 100%。

表现最差的行业

- 公共事业服务
- 贸易公司
- 食品市场
- 建筑
- 材料

表现最差的公司

- 112 家公司的域名安全分数为零。
- 这些公司主要位于亚太地区，该地区的公司占零分公司的 87%。

针对全球 2000 强企业的可疑或恶意域名活动

我们确定并分析了不是由全球 2000 强企业持有但包含这些企业品牌名称中超过 6 个字符的域名。这些虚假域名注册的目的是利用人们对目标品牌的信任，发动网络钓鱼攻击、其他形式的数字品牌滥用或知识产权侵权，从而导致收入损失、流量分流及品牌声誉的下降。

网络钓鱼者和恶意第三方可以使用不计其数的域名诈骗战术和组合方法。

我们有意地关注了常见的同形文字，因为它们是威胁发起者使用的最恶劣攻击方法之一

域名诈骗策略

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
关键词匹配	cscglobalcovid.com | covidcscglobal.ar | covid19.com
同音异义词 (soundex)	siesiglobal.com | cscclobol.com

.COM 域名中常见的同形文字（模糊匹配）

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

C0rnpanyNarne.com

最常见的替代字符

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

超过 79% 的同形文字域名由第三方所有

在第三方所有的域名中：

87% 在 2023 年掩盖了他们的 WHOIS 或所有权详情，而在 2022 年，这一比例为 82%。这种增加可能是有意为之，也可能是为遵守《通用数据保护条例》(GDPR) 等隐私政策而进行的修改。但尝试掩盖或隐藏所有权和身份的做法更多地指向恶意注册，尤其是在第三方持有的域名中。

40% 在 2023 年配置了 MX 记录，而在 2022 年，这一比例为 48%。MX 记录可用于发送网络钓鱼电子邮件或拦截电子邮件。

第三方域名会被用于何种目的？

36% 指向广告、按点击付费的广告或用于域名停放。

49% 指向不活跃的网站。

1% 指向可能损害品牌声誉、损害客户信心的恶意内容。

14% 解析到与品牌持有人无关的活跃网站。

最近，Instagram 在 2023 年 7 月推出了 Threads，该品牌已经感受到了第三方域名注册的影响，其中一些域名被用于冒称具有附属公司关系以及滥用品牌标识和假冒品牌等。

了解详情： 全新 CSC 研究发现，Instagram Threads 日渐成为欺诈和品牌滥用重灾区

可疑和恶意域名：目标是谁？

行业	虚假域名威胁占总数的百分比
银行	13.1%
建筑	5.4%
石油和天然气业务	4.5%
多元化金融	4.2%
材料	4.2%
IT 软件与服务	4.1%
公共事业服务	3.6%
商业服务与用品	3.5%
保险	3.5%
资本货物	3.4%
耐用消费品	3.3%
零售	3.2%
化学品	2.8%
药物和生物技术	2.6%
交通运输	2.4%
科技硬件与设备	2.2%
食品、饮料和烟草	2.1%
电信服务	1.9%
医疗设备与服务	1.9%
半导体	1.7%
酒店、餐厅与休闲	1.2%
航空航天与国防	1.1%
家庭与个人用品	1.0%
贸易公司	0.9%
媒体	0.9%
食品市场	0.8%

与第三方持有的虚假域名注册活动关联度最高的域名注册商：

- GoDaddy®
- Namecheap™
- Network Solutions

结论

如果公司不解决域名安全问题，将可能造成灾难性的风险。未受保护的域名会对网络安全状况、数据保护、消费者安全、知识产权、供应链、收入和声誉构成重大威胁。

我们的研究表明，与全球 2000 强企业相关的 .AI 域名中，43% 被第三方注册。2023 年，涉及 .AI 域名扩展的域名争议案件数量同比增长 350%，而未能确保 .AI 域名安全的公司现在会发现，自己的 .AI 域名已被很多精于此道的网络惯犯抢先注册。

作为对战略性域名注册工作的补充，企业需要在零信任框架内使用分层安全模型，从而实施域名安全措施，建立稳健的企业安全状况，并将业务风险降至最低。与企业级注册商建立合作关系必不可少，这样不仅可以监测暴露面（包括域名和 DNS），分析针对公司网络形象的威胁载体的能力，还可以获得支持抵御解决方案和维权行动的资源。

查看 CSC 的防御性和主动性安全措施清单，使用多层次、深度防御的域名安全方法，保护您的域名和品牌。

下载我们的域名安全检查清单。

CSC DOMAINSEC 平台简介

CSC 的 3D 域名安全和维权解决方案依托 CSC DomainSec℠ 平台的强大技术精心打造。DomainSec 是由 CSC 创建的“软件即服务”(SaaS) 网络安全平台，也是业内优秀的整体化方法，旨在保护和捍卫品牌域名生态系统。它运用专有机器学习深度搜索 (MLDS) 技术，整合了机器学习、人工智能和归集合并技术，用以确定主要入侵指标。

DomainSec 将 CSC 的域名管理、域名安全整合到一个平台之中，辅以品牌保护和欺诈防护解决方案，因此可以提供卓越的保护，将保护范畴拓展到安全边界以外，帮助企业完善其零信任安全模型。

CSC 是值得信赖的安全和风险情报提供商，为福布斯全球 2000 强企业和全球 100 强品牌® 提供域名安全解决方案，包括安全域名组合管理、域名系统 (DNS)、数字证书管理以及数字品牌保护和欺诈防护。随着全球企业加大安全状况投资，不断地努力保护外部攻击面，CSC 可以帮助企业了解其域名安全风险，以及如何将其与零信任模型协调一致。企业可以凭借 CSC 的专有技术来增强自身的安全状况，防范针对其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（线上品牌监管和维权活动的结合），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，我们通过聘用所服务行业的业内专家，可为世界各地的客户提供服务。请访问 cscdbs.com/cn。

[1]CSC博客《.AI 域名来袭，域名组合新成员——先人一步采用新域名，你准备好了吗？》(AI You Ready? A Domain to Add to Your Portfolio—Before Someone Else Does.) cscdbs.com/blog/ai-you-ready-a-domain-to-add- to-your-portfoliobefore-someone-else-does/

[2]DNDisputes.com, “AI: Domain Name Dispute Cases with AI Extension” dndisputes.com/case/domain/extension/ai/

[3]Search Engine Land, “Google now treats .ai domains as generic top-level domains” searchengineland.com/google-now-treats-ai-domains-as- generic-top-level-domains-427770

CSC10122023