2024 年 年域名安全报告

简介

过去五年，CSC 每年都会率先报告福布斯全球企业 2000 强的域名安全状况。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。

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。我们的理念是提高大家对于这些威胁的认识，分享域名安全最佳实践，从而改善所有企业的域名安全状况。

CSC 发布年度域名安全报告迎来第五个年头，值此之际，我们对分析福布斯全球企业 2000 强域名安全状况的不懈努力进行了回顾。今年恰逢 CSC 成立 125 周年，我们会继续致力于提升人们对数字空间中公司外部网络风险以及采取强有力的域名安全措施必要性的认识。

重要研究结果摘要

尽管突出的网络攻击事件数量增加，但医疗设备与服务行业的域名安全排名却出现下降

今年，在按行业划分的域名安全性方面，医疗设备与服务企业的变化最为显著，排名从 2023 年的第 5 位下降了 7 位，在 2024 年名列第 12 位。相反，技术硬件与设备公司则从 2023 年的第 13 位上升了 8 位，在 2024 年排名第 5。

80% 模仿全球 2000 强品牌名称的注册网络域名（即同形文字域名）由第三方持有，并不属于这些品牌

我们发现，80% 的同形文字（外观相似的虚假）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，42% 有 MX 记录（即电子邮件交换记录），而 2023 年这一比例为 40%。MX 记录可用于发送网络钓鱼电子邮件或拦截电子邮件。

全球 2000 强企业中，有 107 家公司的域名安全分数为零

在全球 2000 强企业中，5% 的企业未部署任何推荐的域名安全措施，因此风险级别最高。根据我们对关键域名安全措施采用情况的分析，如果一家企业的域名安全分数为零，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。

自 2020 年以来，注册局锁的使用率增长了 7 个百分点，但总体采用率仍然较低，仅为 24%

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。

自 2020 年以来，DMARC 采用率增长了 32 个百分点

2023 年，反网络钓鱼工作组 (APWG) 报告了近 500 万次记录在案的网络钓鱼攻击，使 2023 年成为网络钓鱼最严重的一年。攻击频次的加剧推高了基于域名的消息认证、报告和一致性 (DMARC) 的采用率，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。

域名生态系统存在于外部攻击面之上

随着 AI 技术愈加成为网络威胁的助力手段，各种攻击也在不断增加。这使域名安全成为了公司最高级别网络风险评估中重要的一环，公司的域名生态系统成为此类评估中不可或缺的元素，也是切实存在的可能遭受攻击的漏洞，如图 1 所示。被入侵或劫持的合法域名或恶意域名注册均可用于实施图 1 所示的所有攻击。

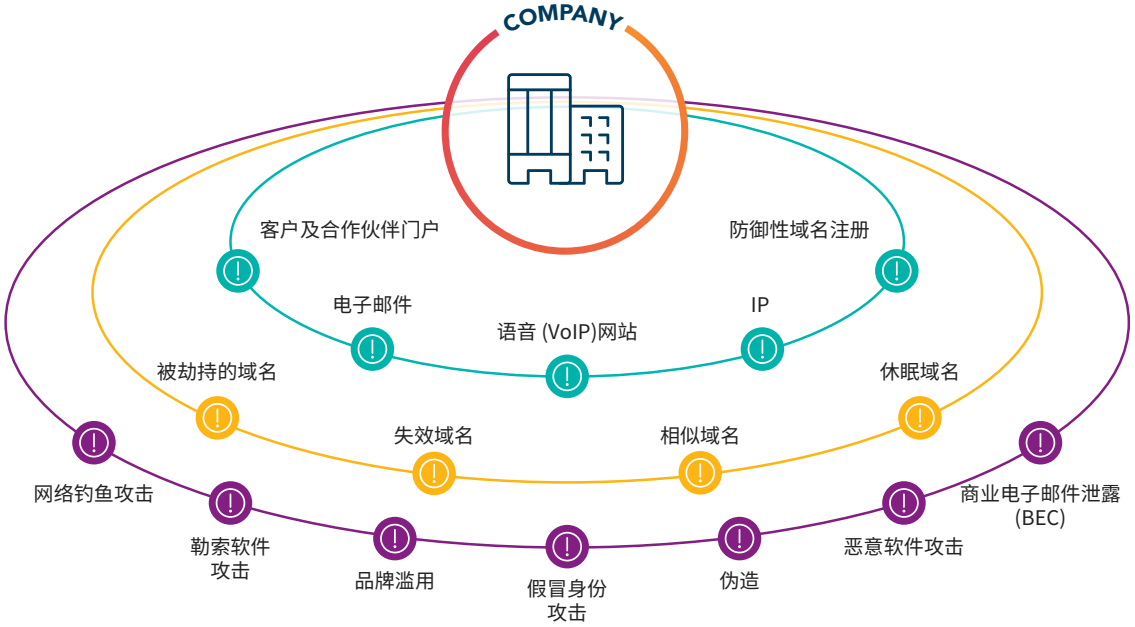


图 1：域名生态系统体系

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)、客户门户、提供商应用等。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。随着网络风险不断提高，各个企业和网络保险公司在量化风险和降低其破坏能力方面面临着更大的挑战。这意味着域名是企业网络安全状况的关键要素，因为互联网和域名对企业基础设施和业务连续性至关重要。

遭到入侵或劫持的合法域名

网络犯罪分子会破坏任何未加保护的域名。企业应采用分层防御的深度防御策略来防止域名劫持。

被劫持的子域名

对于子域名劫持这种攻击方式，网络犯罪分子会通过控制不再使用的合法子域名来托管恶意内容，以针对公司进行网络钓鱼或恶意软件攻击。他们会利用被目标公司遗忘的域名系统 (DNS) 记录（悬挂 DNS），以指向其自己的内容。

休眠域名

网络犯罪分子可能会注册并持有品牌域名，使其处于闲置状态，以备在网络钓鱼或恶意软件攻击中使用这些域名。休眠域名通常会逃脱初始检测，因为它们不符合任何为发动攻击而注册的域名的判断指标，例如通常会引发警报的活跃 MX 记录。

恶意域名注册

域名诈骗组合伎俩和同形文字假冒域名层出不穷，很容易被网络钓鱼者和恶意第三方利用。这些虚假域名注册的目的是利用消费者对目标品牌的信任，发起令人信服的网络钓鱼攻击，或进行其他形式的数字品牌滥用。

新近失效的品牌域名被第三方重新注册

企业可能会因为成本压力而选择放弃之前注册的防御性域名。网络犯罪分子会趁机而动，立即出于恶意目的重新注册这些域名。他们会不断寻找可用的品牌域名，并以此作为武器。

研究结果与分析：全球 2000 强企业采用域名安全措施的情况

在这项分析中，CSC 介绍了全球企业 2000 强对五大关键域名安全措施的采用情况，即：DMARC、DNS 冗余、注册局锁、证书认证机构授权 (CAA) 记录和域名系统安全扩展 (DNSSEC)。然后，我们按照行业和地区对采用率进行了深入分析。

趋势（2020-2024 年）

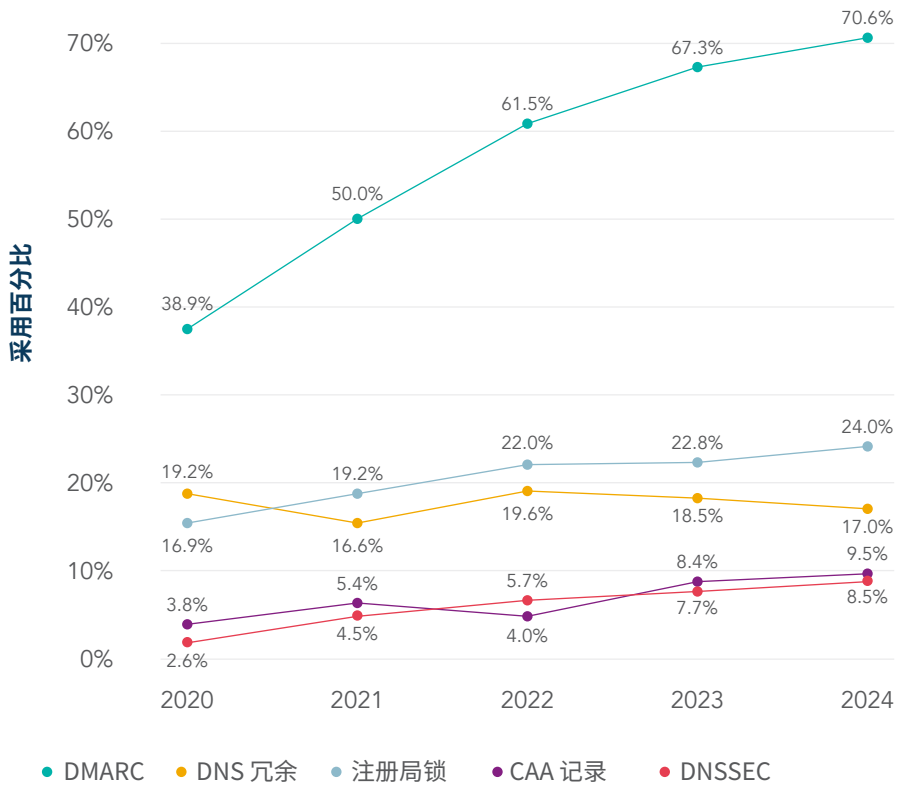


图 2：全球 2000 强企业对五大关键域名安全措施的采用情况（2000 - 2024 年）

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 的采用率从 2020 年的 39% 迅速上升到 2024 年的 71%（图 3），这并不令人意外。

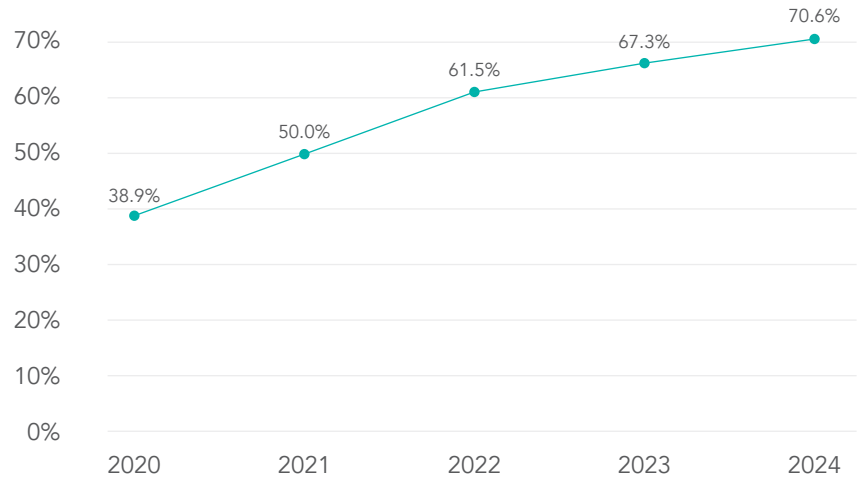


图 3：2020-2024 年 DMARC 采用率

另一个推动 DMARC 采用率提高的因素或许还与电子邮件客户端越来越多地采用品牌信息识别指标 (BIMI) 有关，这使得品牌标志得以在经过验证的电子邮件中展示。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 。

注册局锁采用率平稳缓慢增长

企业对注册局锁的采用率从 2020 年的 17% 增长到 2024 年的 24%。我们还发现，2024 年，在使用企业级注册商的公司中，有 45% 也更频繁地使用了注册局锁。随着加强网络安全的压力日益增大，越来越多的注册商开始为其域名扩展提供锁定功能，以实现端到端域名事务的安全性，从而减少人为错误和第三方风险。

公司的域名组合不断变化，因此，CSC 使用了预测性建模算法来评估域名的 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。

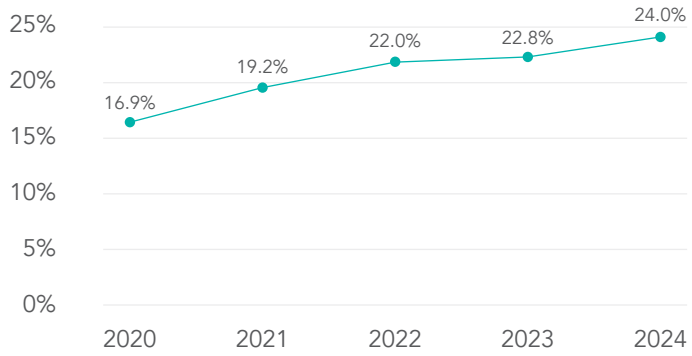


图 4：2020-2024 年注册局锁采用率

DNS 冗余、DNSSEC 和 CAA 记录等安全措施存在不一致问题

尽管部署 DNSSEC 的公司比例仍然很低 但在过去五年中已增加了两倍，从 2020 年的 3% 增加到了 2024 年的 9%。DNSSEC 的工作原理是为 DNS 查询和响应提供身份验证和数据完整性，从而防止网络犯罪分子将互联网流量重定向到网络钓鱼网站等恶意网站。

出人意料的是，今年 DNS 冗余再次下降了 1%，使得今年优先考虑采用 DNS 冗余措施的公司比例低于 2020 年。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。

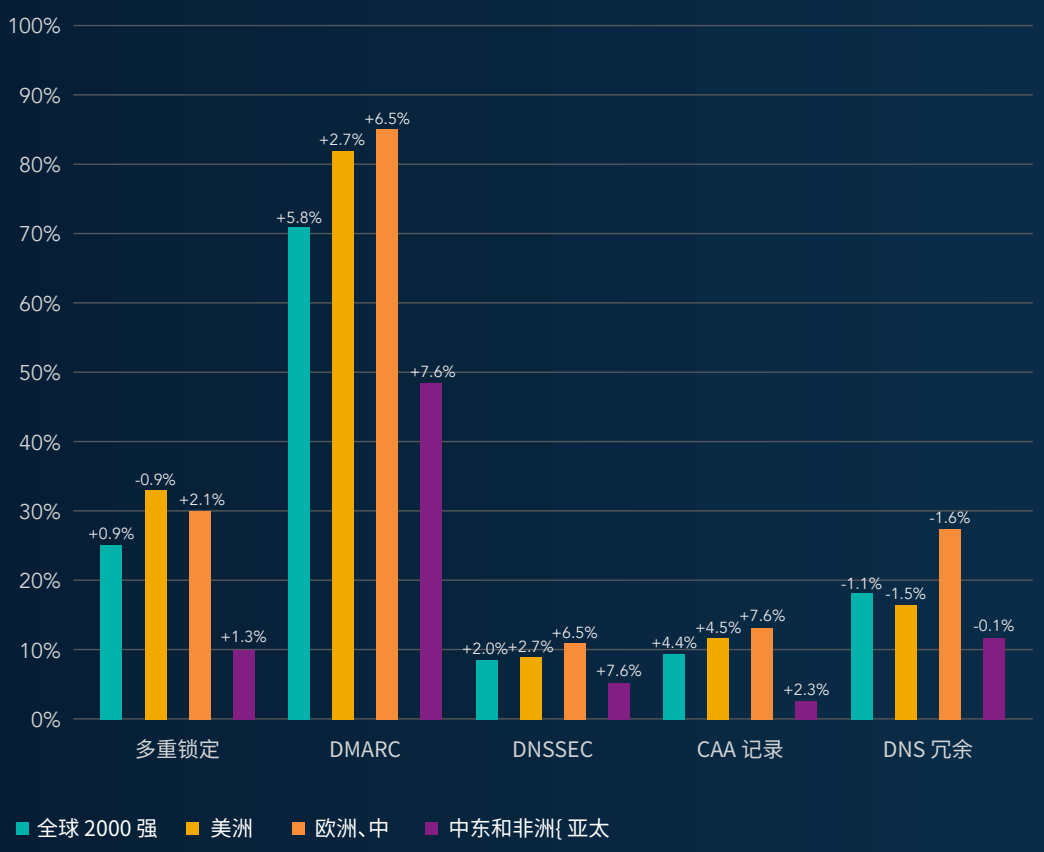
最后，CAA 记录的采用率从 2020 年的 4% 上升到了 2024 年的 10%。CAA 记录允许公司指定一个特定的证书认证机构 (CA)，作为其公司域名的唯一数字证书认证机构。此举可防止网络罪犯使用未授权的证书认证机构获取新数字证书，这会导致他们的请求失败，同时公司也会收到相关的警报。

我们还发现，2024 年，在使用企业级注册商的公司中，有 45% 也更频繁地使用了注册局锁。

2024 年域名安全措施采用情况

按地区

2023 年至 2024 年期间，欧洲、中东和非洲地区的域名安全措施采用率增长最快。



相较于上一年的增幅/减幅百分比

图 5：按地区划分的域名安全措施采用率

按行业

2024 年，医疗保健行业排名下降 7 位。

行业划分	2024 年排名	2023 年排名	
科技硬件与设备	5	13	↑
医疗设备与服务	12	5	↓

在福布斯全球企业 2000 强涉及的 26 个行业中，医疗设备与服务行业的排名下降了 7 位，跌出了之前的前五名。排名从 2023 年的第 5 位下降到 2024 年的第 12 位，与今年针对医院和医疗保健系统的网络攻击显著上升形成鲜明对比，特别是考虑到医疗保健行业目前是 勒索软件攻击最频繁的目标。[1] 2024 年，医疗保健行业已经报告了 280 起网络安全事件，这占“美国 2024 年网络安全事件的 24%，使医疗保健行业高于其他所有行业。”[2]

科技硬件与设备上升 8 位，排名第 5。对于科技公司来说，进入前五名无疑是有利的，这些公司的采用率增长可能与它们自 2020 年 SolarWinds 遭受重大供应链攻击以来一直在实施的安全措施有关。

表现最佳的行业

- 商业服务与用品
- IT 软件与服务
- 媒体
- 零售
- 科技硬件与设备

表现最差的行业

- 建筑
- 食品、饮料和烟草
- 食品市场
- 材料
- 石油和天然气业务

2024 年按注册商类型划分的域名安全措施

在本报告中，我们根据全球企业 2000 强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。

很多公司都存在一个误区，认为所有注册商都别无二致，然而，消费级注册商的首先考虑的可能并不是域名安全，甚至不提供域名安全措施，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 。

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。

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。

选择企业级功能的企业采用域名安全措施的比例更高

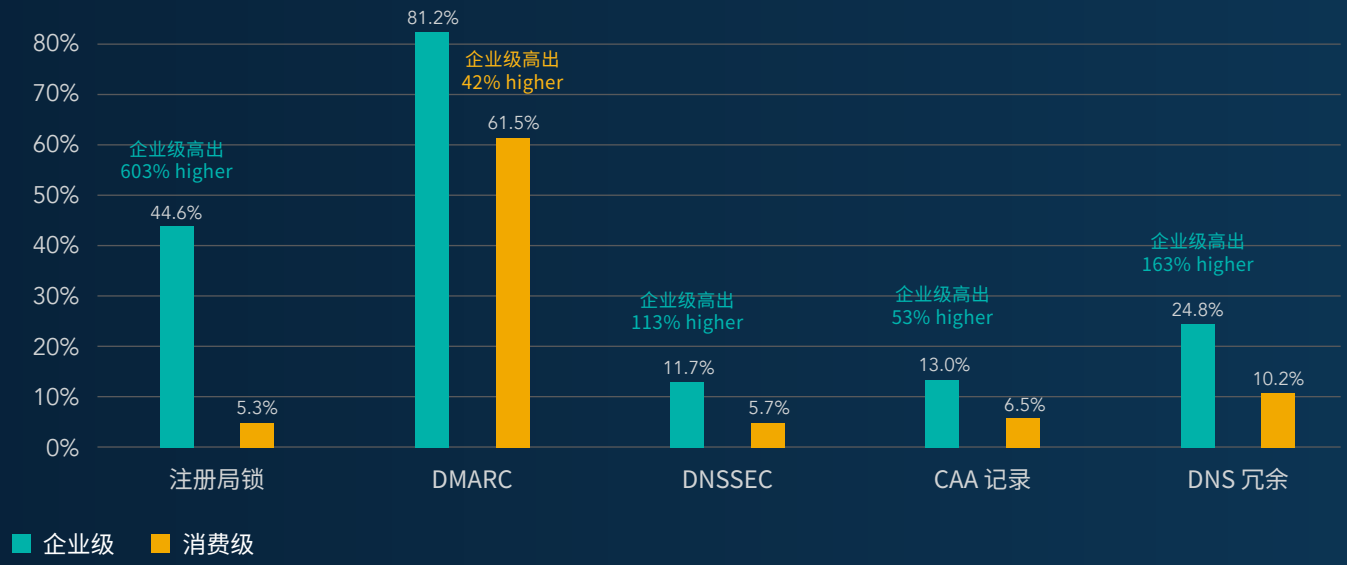


图 6：安全措施的成熟度水平——企业级 (EC) 与消费级 (CG) 注册商的对比

域名安全状况

CSC 根据企业域名安全风险等级，对扩展的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（多重锁定）
- CAA 记录
- DNS 冗余
- DNSSEC
- 发件人策略框架 (SPF)
- 域名密钥识别邮件 (DKIM)
- DMARC

域名安全风险等级

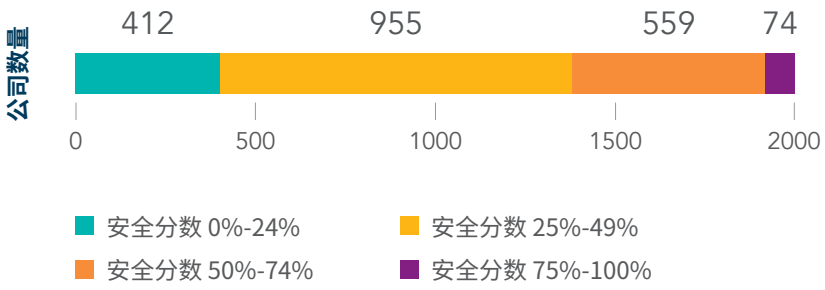


图 7：全球 2000 强企业的域名安全分数和相关域名安全风险等级

68% 的全球 2000 强企业实施的安全措施不到上述推荐措施的一半。

表现最佳的公司

只有一家公司的得分是 100%，而且去年的得分也是 100%。在满分 8 分中，有 12 家公司获得了 7 分。

表现最差的公司

107 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。这些第三方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。这些都会给受影响的品牌带来收入损失、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。

我们特意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

域名诈骗伎俩

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

图 8：域名诈骗常见伎俩

.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

c → e	0 → 0	m → n	l → I	m → rn
g → q	E → 3	S → 5	B → 8	l → 1

图 9：.COM 域名中常见的同形文字（模糊匹配）

80% 的同形文字域名由第三方所有

在第三方所有的域名中：

42% 在 2024 年有 MX 记录，而在 2023 年，这一比例为 40%。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？

48% 指向广告、按点击付费的广告或用于域名停放。

33% 指向不活跃的网站。

2% 指向可能损害品牌声誉和客户信心的恶意内容

17% 解析到与品牌持有人无关的活跃网站。

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

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	19.9%
多元化金融	7.2%
IT 软件与服务	7.2%
建筑	6.4%
保险	6.3%
石油和天然气业务	6.2%
公共事业服务	6.1%
资本货物	5.5%
耐用消费品	5.3%
商业服务与用品	5.0%
交通运输	4.9%
材料	4.7%
零售	4.6%
科技硬件与设备	4.2%
药物和生物技术	3.5%
食品、饮料和烟草	3.4%
医疗设备与服务	3.4%
电信服务	3.0%
半导体	2.9%
化学品	2.6%
航空航天与国防	2.0%
酒店、餐厅与休闲	1.7%
家庭与个人用品	1.7%
食品市场	1.5%
贸易公司	1.2%
媒体	1.1%

域名安全洞察：从 2024 年奥运会期间域名激增中汲取的经验教训

与其他全球大型活动一样，2024 年 7 月在巴黎举行的奥运会同样遭受了诈骗犯的数字威胁，他们试图通过假冒商品、虚假门票、欺诈性流媒体网站和网络钓鱼攻击来利用奥运会的全球影响力。为减少此类数字威胁，监控全球域名生态系统（包括相似域名、取消注册、重新注册或新注册的域名）应成为任何企业安全态势和品牌在线战略的首要任务。各企业应特别警惕休眠域名，即哪些尚未被用作攻击武器，但有迹象显示其正在形成攻击基础架构的域名。

要点

通过调查，我们发现有 8857 个不重复的第三方域名包含“Olympics”或“Paris 2024”等相关关键词（见图 10）。我们的分析研究了 2023 年 8 月 1 日至 2024 年 8 月 13 日期间的域名活动，包括新注册、取消注册和重新注册。从图 10 中可以看出，在奥运会于 7 月 26 日开始和 8 月 13 日结束期间，新注册活动明显激增。在仍处于已注册状态的域名中，49% 处于休眠状态，没有关联活跃的网站。不过，在这些域名中，25% 有 MX 记录，8% 绑定了 SSL 证书。

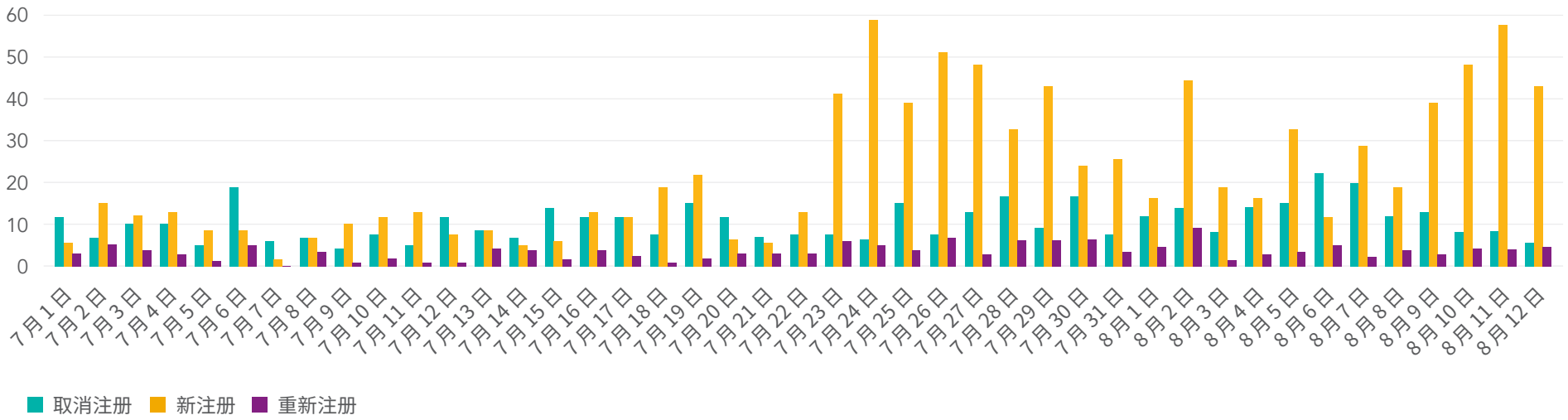


图 10：2024 年 7 月 1 日至 2024 年 8 月 1 日（共 60 日）的域名注册趋势

重要启示

持续实时监控这些域名至关重要，因为休眠域名随时可能被用作攻击武器。通过跟踪恶意域名，企业可以防患于未然，提前发现潜在的风险因素。

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公司的网络安全状况、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。

如果公司尚未对域名加以保护，应该立即在整个全球域名生态系统中进行搜索，包括通用顶级域名和国家代码顶级域名。诸如 CSC 的 3D 域名安全和维权解决方案等高级监控服务，除了可以检测基本的精确匹配、通配符和错别字，还可以检测到更广泛的域名变体。此外，企业还需要与能够打击各种威胁的提供商合作，这些威胁包括网络钓鱼网站、恶意软件下载器、误植域名、欺骗性搜索引擎优化网站、社交媒体门户、移动应用商店和销售假冒产品的网络市集。

查看 CSC 的主动性和防御性安全措施清单，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 是值得信赖的优选安全和威胁情报提供商，深受福布斯全球企业 2000 强和全球最佳品牌 100 强 (Interbrand®) 企业的青睐，专注于域名安全和管理以及数字品牌和欺诈防护业务。随着全球越来越多的公司加大投资力度完善安全状况，我们的 DomainSec℠ 平台可以一展身手，帮助这些公司了解他们存在的网络安全漏洞并且保护其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，防范针对其在线资产和品牌声誉的网络威胁载体，从而避免遭受严重的收入损失。CSC 还提供在线品牌保护（将在线品牌监控和维权活动相结合），多维度审视防火墙外针对特定域名的各类网络威胁。欺诈防护服务可在攻击的早期阶段打击网络钓鱼，使我们的解决方案更加完善。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。

联系我们

cscdbs.com/cn

[1]npr.org/sections/shots-health-news/2024/09/17/nx-s1-5111590/cyberattacks-ransomware-health-care-federal-response

[2]tebra.com/theintake/practice-operations/medical-news/the-major-cyberattacks-that-have-affected-healthcare-systems-in-2024

DBS12122024