CSC

在当今网络安全态势下如何管理域名

CSC 洞见白皮书

目录

紧跟 AI 发展步伐，大力管理网络风险 3

域名已成为网络攻击发起的根据地 3

与企业级注册商合作所带来的价值 7

选择消费级注册商所存在的风险 11

利用分层式的纵深防御战略，抵御合法域名遭受入侵后带来的风险 12

未遭受黑客攻击的合法子域名为何也会被劫持 13

在线品牌保护是必要的网络安全措施 14

利用创新方式降低在线网络风险 15

紧跟 AI 发展步伐，大力管理网络风险

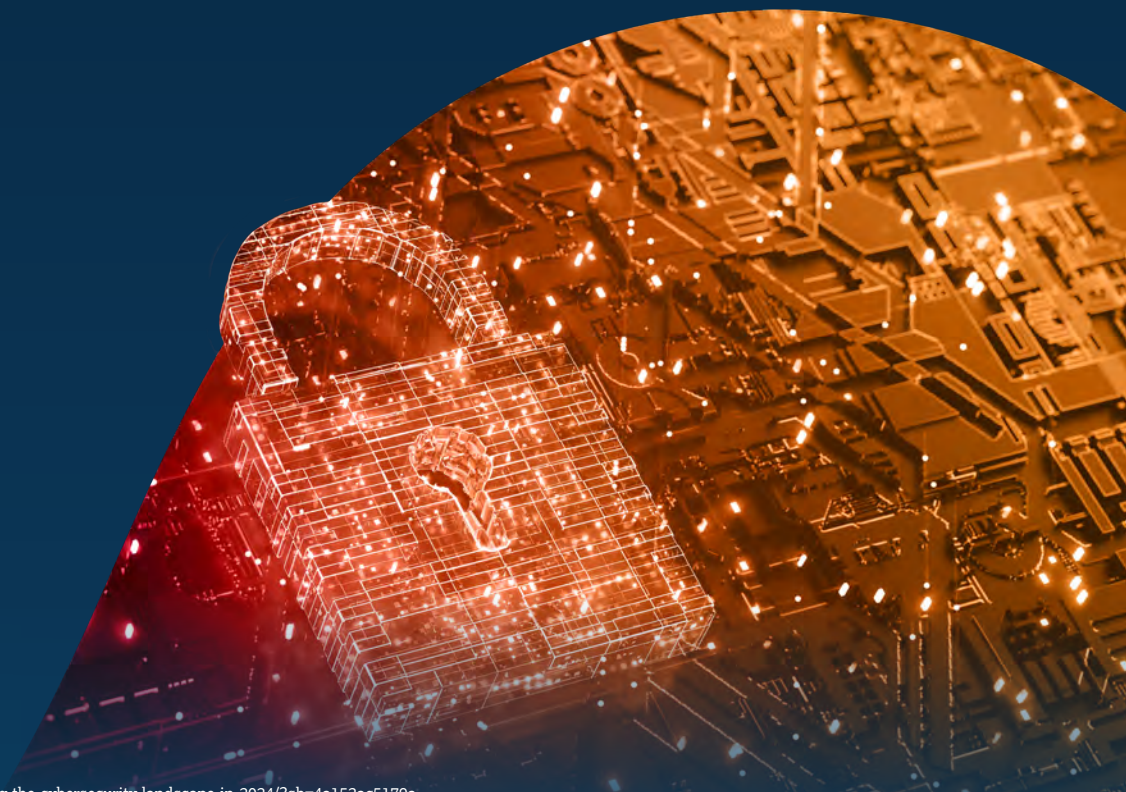
随着人工智能 (AI) 的发展以及网络威胁日益复杂，无论是公司还是个人，都需要加大力度防范关键网络风险。有些因素能够让攻击者在更短的时间内造成更大的伤害，但也同样能够支持制定更好的网络防御策略。[1] 最近对 AI 技术的一项 Splunk 研究[2]显示，虽然70% 的安全高管相信 AI 给攻击者带来更多的好处，但其中仍有 35% 已在试验利用这项技术来实施网络防御。

与此同时，这也不全是坏消息。最近的一份 Goldman Sachs 报告表明，生成式 AI 有可能会使国内生产总值 (GDP) 增长 7%，对任何单项技术来说，这都是相当重大的影响。在针对性攻击中，网络不法分子仍然会使用生成式 AI 来实现更高的复杂性和更快的部署速度。不法分子还能利用生成式 AI 来编写个性化、针对性的网络钓鱼电子邮件，并且做到没有拼写错误且语法正确，使它们变得更难检测。暗网上目前提供了 FraudGPT 等 AI 工具，使不法分子能够实施更为复杂、社交工程化的深度伪造攻击，更快速地操纵攻击对象的情绪或信任度。

域名已成为网络攻击发起的根据地

网络钓鱼攻击、商业电子邮件泄露 (BEC) 和社会工程引发了更复杂的攻击，例如恶意软件和勒索软件等，但首席信息安全官 (CISO) 们并没有更多地关注其企业的域名和网络中存在的外部攻击面，这着实令人惊讶。他们花了很多时间来增强自己的网络，却没注意到周围环境已经发生了变化。许多 CISO 都不知道其企业的域名注册商是谁，更不清楚他们能否提供适当的企业级安全防护。

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、提供商应用程序等。互联网是企业外部攻击面的一部分，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，在量化网络风险以及降低其破坏能力方面，各个企业和网络保险公司面临的挑战愈加严峻。这使得域名成为企业网络安全态势的关键要素，因为互联网和域名在业务基础架构和业务连续性方面有着举足轻重的地位。



1. forbes.com/sites/emilsayegh/2023/12/19/navigating-the-cybersecurity-landscape-in-2024/?sh=4a152ac5179a
2. splunk.com/en_us/form/ciso-report.html

“域名决定着重要业务功能的运行，而对任何企业来说，其所处的生态系统都应该被视为外部攻击面的一部分。在当今的环境中，域名和子域名有可能会被直接入侵（劫持）或恶意注册，这意味假冒品牌会以冒牌网站的形式，出于恶意目的仿冒某个品牌，例如，发起 BEC 攻击或网络钓鱼和恶意软件传播攻击。让许多人感到意外的是，任何人都可以注册域名，只要该域名可用就行。所以，如果您不注册使用自己品牌的域名，或者不使用同形符号和其他策略来保护您的品牌，网上就总会有欺诈分子企图利用您的品牌及其建立的信任感来获利。这会转而使您的收入和声誉面临风险，更不用说对消费者安全问题所造成的影响了。”

首席技术官 Ihab Shraim，
《CSC 的数字品牌服务》，摘自 Safety Detectives 访谈

企业及其域名可能会受到几种方式的攻击：

入侵域名或劫持子域名

网络不法分子会入侵任何未实施安全保护的域名。在针对此类攻击提供保护时，公司应该从分层式的纵深防御开始着手。首先，公司需要通过保护域名组合（可能包含公司收购的多个品牌）和域名系统 (DNS) 在线足迹来保护品牌网络形象。

创建具有欺诈性的恶意域名

虽然有些国家/地区在批准注册域名后缀时，会要求提供注册商标、注册公司或在当地经营，但有一件事需要警惕，那就是任何人都可以注册任何域名。这些虚假域名注册的目的在于利用消费者对目标品牌的信任，发动令人信服的网络钓鱼攻击、其他形式的数字品牌滥用或知识产权 (IP) 侵权。这会导致收入损失、流量分流，并使相关企业的品牌声誉受损，同时让欺诈者从中获利。通过各种组合及同形符号，网络钓鱼者和恶意第三方可以轻松利用不计其数的域名欺诈战术。

第三方重新注册近期失效的品牌域名

有些公司会防御性地注册至关重要的域名，以防止其品牌遭受在线欺诈。在完成注册之后，这些企业有时会因成本压力或品牌发展不力而任由这些域名失效。网络不法分子等的就是这个时机，他们会立即重新注册相同的域名并将其用于恶意目的。他们一直在寻找可用的品牌域名，并将之化为自己的攻击武器。

休眠的域名

有些网络不法分子可能会注册并持有品牌域名，也许是托管持有或停放页面，或者是显示“网站 正在建设中”消息，其意图是将这些域名卖回给目标企业。他们可能还会策划更大规模的恶意活动，如网络钓鱼或恶意软件攻击。如果自最初注册之日起，休眠域名成为攻击武器的时间已超过六个月，就被称为“潜水域名”。休眠域名通常能够逃脱初始检测，因为它们并未直接包含为发起攻击而注册的域名的任何特征，例如，通常会引起高度警惕的活动 MX 记录。这为网络犯罪分子留下了充足的空间，使他们能够组织起更复杂、更有针对性的攻击活动，从而产生更具破坏性的后果。

除了留意域名的年限之外，还需要积极监控域名注册是否与之前发现的威胁接近，并查看是否存在某种注册模式。注册模式很难一眼辨别，但如果您的域名注册商在其专有数据和各种顶级域名 (TLD) 中实施了 AI 和机器学习技术，则可以在各个 IP 地址中发现此类模式。还有一点也非常重要，那就是观察您的域名活动中是否存在模仿行为。我们的意思是：在您的品牌正在为新产品或服务注册一系列新域名时，会不会有第三方也在这样做呢？

域名的外部攻击面

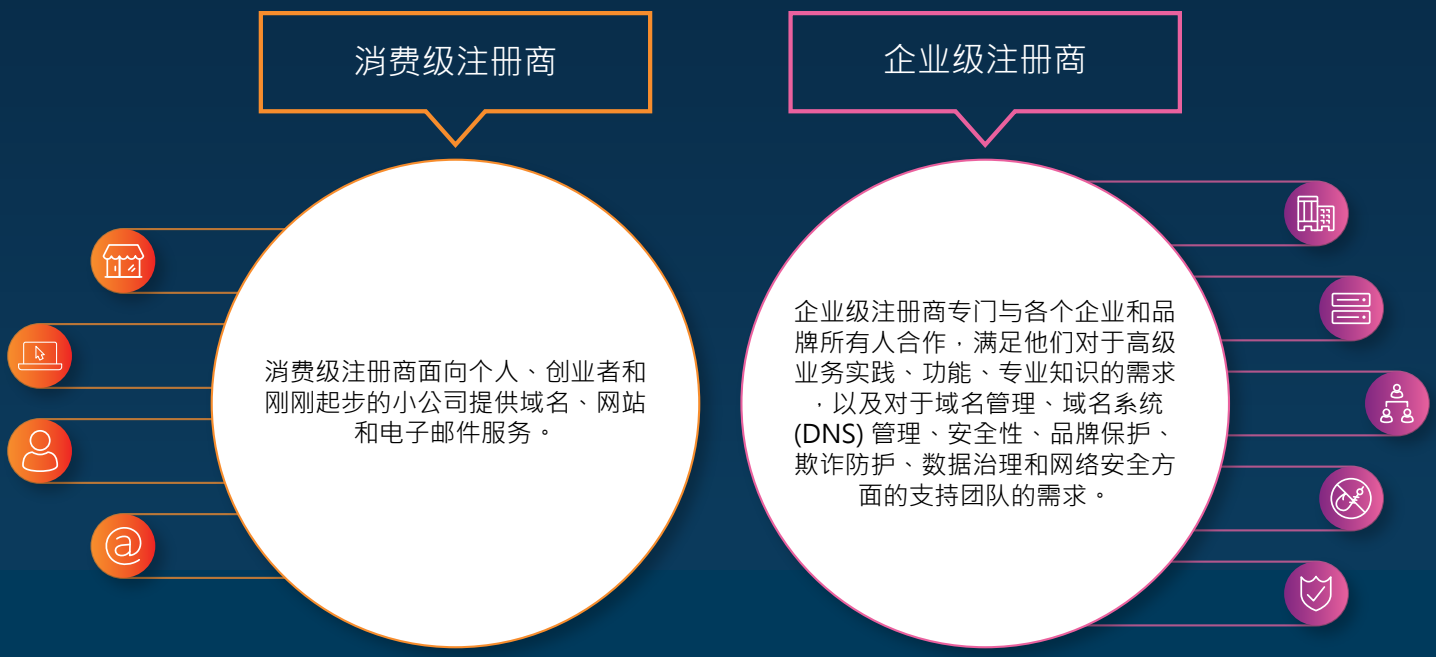
大多数网络安全风险对企业领导者来说都是必备的常识，例如：防止数据泄露、身份和漏洞管理、访问控制、数据保护、被盗凭据以及需要对社会工程策略保持警惕等。但在日常网络安全保护方面，显然许多团队都不知道是谁在负责企业的域名安全。域名经常会用于营销和品牌计划，因此，有些安全团队可能会认为保护在线域名是营销或法律部门的责任。如果企业不太熟悉他们的域名注册商，就很可能不知道注册商运用的策略以及为品牌化、商标化域名所采取的安全措施。

遗憾的是，攻击者有渠道知晓企业在线业务的增长，这导致他们对攻击已暴露的企业域名特别感兴趣。如果企业的安全态势不能得到增强，他们将会陷入到风暴的中心。他们的前路上将遇到各种域名和 DNS 攻击，并面临着潜在的财务和声誉损害风险。CSC 最近的《域名安全报告》对福布斯全球 2000 强公司进行了分析，发现有将近四分之三的企业所实施的域名安全措施仅占全部措施的不到 50%。基于这一见解，再加上许多企业对其域名注册商普遍缺乏了解，表明域名安全往往被搁置一旁，部分原因可能在于内部责任不明。

与企业级注册商合作所带来的价值

域名注册商一般分为两类：消费级和企业级。消费级注册商在全球所有注册商中占比超过 99%，主要面向个人、企业主和创业者，在其起步初期为他们提供域名、网站、电子邮件服务。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。

消费级对比企业级



企业级注册商在安全方面毫不妥协

- ICANN 和注册授权
- 全面了解您的所有域名、DNS 的数字证书提供商
- 书面授权请求（绝对不会以电话方式）
- 遵守《数据和通用数据保护条例》(GDPR)
- 注册转让锁定策略

- ISO 27001 授权数据中心
- SOC 2® 合规性
- 第三方渗透和漏洞测试
- 定期安全检测，包括 SQL 注入和 XSS

- 了解您的客户 (KYC) 身份验证
- 海外资产控制办公室 (OFAC) 筛查
- 在全球以本地语言提供全天候 24 小时内部支持
- 定期开展网络安全人员培训

最合适的做法是使用企业级提供商，他们大力投资于人员和流程，并且在技术当中充分考虑了安全性。任何人都可以宣传说自己的服务能够满足当今全球企业的需求，公司自身有责任做好功课，了解第三方提供商之间的差异。他们需要了解自己选择的提供商是否契合他们在企业整体安全态势以及合规性和风险问题上做出的决策。

企业级注册商在保护您的域名组合时应采取的七个步骤

与数字证书组合的管理一样，域名管理也可能会非常复杂。通过采取这些步骤，您将能够控制关键的公司资产，并减少品牌所面临的安全威胁。

1

就像使用公钥基础架构 (PKI) 来管理数字证书一样，在同一个管理系统中管理全球域名组合可以实现一致的流程，并保护公司运营所依赖的资产。

集中化

2

一旦所有域名资产都实现了集中化，您就可以通过许多应用程序编程接口 (API) 来享受自动化的便利，类似于数字证书的管理。域名组合 API 应该包括各种选项，例如：

自动化

- 域名组合报告
- 针对新注册的域名可用性检查
- 域名注册及订单模板功能（可完成大量后缀的注册）
- 域名服务器和 WHOIS 联系人更新
- DNS 记录检索和名称修改
- URL 转发管理
- 报告 10 种与域名相关的安全事件，以方便审核或执行安全信息和事件管理 (SIEM) 服务提供商集成
- 数字证书管理，包括预订、续订、检索、重发和撤消证书；针对所有预订和更新操作提供状态检查

3

如果选择的提供商了解每个域名所在的不同司法管辖区，能确保您的数据保持最新并遵守所在国家或地区的法规，将会非常节省时间。

合规性

4

将域名和 DNS 集成在一起以快速安全地进行更改，这一点非常重要。

集成

5

每家公司都各不相同，可能需要采用不同的设置。这可能意味着您的域名使用非常分散，或者是按业务单位分段。如果采用的系统可以由不同的群体进行管理，则需要进行一定程度的调整，以使正确的用户能够访问正确的信息。此外，公司还需要浏览并理解关于其域名组合的复杂数据。企业需要在安全、可靠和功能丰富的环境中快速访问数据，这样才能分析大量信息并制定数据驱动型决策。需要定期审核的报告包括：

- 活跃域名状态——了解是否在将域名解析到内容
- 品牌字符串数量——了解域名组合中呈现了多少个不同的品牌
- 国家/地区——了解品牌在全球的业务覆盖情况

灵活性

6

每年都有越来越多的新域名推出，您需要确保自己的企业针对潜在威胁做出正确的注册决定。如果能有一支战略顾问团队来支持保护您的品牌，将会极有助益。他们可以帮助解答一些重要问题，例如：

不断变化的环境

- 域名数量是否合适，或者是否应该考虑延长防御性注册以抵御更多风险？
- 是否部署了端到端工作流程，以利用威胁情报来抵御基于域名的攻击？
- 如何确定应该在何处注册域名？
- 如果不注册，会存在哪些风险？
- 如何在企业内部集中进行沟通并注册域名？

7

没有哪家公司可以注册完某个域名的所有变体，所以需要部署一种有效的域名监控解决方案，从而发现何时有第三方在利用您的品牌名称。

监控

与企业级注册商合作，评估欧洲 NIS2 网络安全指令对您的域名和 DNS 的影响

简介：

「 “在 2024 年 10 月 17 日之前，委员会应该会通过实施法案，针对与以下各方相关的安全措施制定出具体的技术和方法要求，其中包括 DNS 服务提供商、TLD 域名注册商、云计算服务提供商、数据中心服务提供商、内容交付网络提供商、托管服务提供商、托管安全服务提供商、在线市场提供商、在线搜索引擎和社交网络服务平台提供商以及可信任服务提供商。” [3]

为何实施：

“2016 年推出的欧盟网络安全规则已通过 NIS2 指令进行了更新，并于 2023 年生效。该规则使现有的法律框架实现了现代化，以应对日益增长的数字化和不断变化的网络安全威胁格局。通过将网络安全规则的范围拓展到新的行业和实体，它进一步提高了公共和私营实体、主管当局和整个欧盟的复原力和事件响应能力。” [4]

3. nis-2-directive.com/NIS_2_Directive_Article_21.html#:~:text=By%2017%20October%202024%2C%20the,service%20providers%2C%20content%20delivery%20network
4. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

选择消费级注册商所存在的风险

各家公司都希望能够削减成本，而剔除域名组合可能会被视为一个很容易达成的目标。这种做法也许能够短期解决问题，但可能会导致域名受到不法分子攻击的长期风险，使真正品牌收入被抽走，同时还会造成其他损害。

域名安全应该成为网络安全的一个重要分支，这样才能在网络上保护品牌的安全，而对于消费级域名注册商来说，这并不一定是首要任务。[5] 对消费级注册商的信任往往只是一种误解，因为他们的设计通常不会将域名安全视为优先事项。这种错误的信任可能会影响一家公司的整体安全状况。

很多公司都存在一个误区，认为所有注册商都别无二致

消费级注册商与其客户之间的关系偏向于交易性质，不会像企业级提供商那样开展全面深入的评估。消费级注册商无法提供抵御域名欺诈、域名和 DNS 劫持攻击、子域接管和网络钓鱼攻击等数字风险的解决方案。有些消费级注册商的业务实践可能会在无意间对品牌造成损害。其中一些还经营着域名市场，将品牌化或商标化域名卖给出价最高的人，或者进行域名转向并怂恿注册商标化域名，造成误植域名的情况激增。虽然这些做法不会对企业造成直接损害，但它们会鼓励品牌滥用或注册混淆性的相似域名，并可能将其用于恶意目的。

我们都听过一种说法：“你最强大的地方,就是最薄弱的地方。” 每家企业都会依赖于一系列提供商和供应商，而复杂的一系列供应商和工作流程会增加供应链攻击的风险。供应链攻击是一种网络攻击，当攻击者通过可以访问您的系统和数据的第三方合作伙伴入侵您的系统时，就会发生这种攻击。网络安全状况最差的供应商通常会成为攻击目标。

虽然攻击目标是您的提供商，但同样会影响到您。过去的两年里，曾经发生过一些值得注意的供应链攻击事件。重要的是确保任何企业的域名注册都安全无虞，没有被入侵的风险。域名注册商应由一个团队进行审查，该团队应充分了解域名注册商在公司整体安全态势中所扮演的角色。务必对供应商的被入侵记录进行监控。注重安全的域名注册商最终可以减轻安全团队的一些负担，并使公司能够发现其域名所面临的威胁，以避免对其品牌造成重大损害。

“正如 2 月 16 日发布的 2022 年 10K 文件所述，自 2020 年以来，该公司每年都会被同一伙网络攻击者入侵一次，最近一次发生在去年 12 月。同样值得一提的是，该公司也曾是早期网络入侵的对象。GoDaddy® 发生的后果是一回事，但更值得注意的是，这些入侵事件导致该公司 100 多万用户的数据被泄露。” [6]

——Dark Reading, “GoDaddy 长年遭受入侵对数以百万计的客户来说意味着什么”

5. cpomagazine.com/cyber-security/the-glaring-gap-in-your-cybersecurity-posture-domain-security/
6. darkreading.com/cyber-risk/what-godaddy-years-long-breach-means-millions-clients

利用分层式的纵深防御战略，抵御合法域名遭受入侵后带来的风险

为了抵御网络攻击的风险，可以将纵深防御原则运用到域名安全上。纵深防御方法最初是作为一种军事战略提出的，其目的在于保护目标资产。针对域名安全，它提供了多层安全对策的协调使用。

任何人都可以宣传说自己的服务能够满足当今全球企业的需求，每家公司都必须花时间来了解第三方提供商之间的差异。企业需要了解自己选择的提供商是否契合他们在企业整体安全态势，以及关于知识产权侵权和商标法的顾虑。

1

寻找企业级的域名注册商

在涉及到域名生态系统时，域名注册商的选择可能会影响负责某些领域工作的同事，例如：网络安全和 IT、法律（总法律顾问）、风险和合规（首席风险官）以及网络钓鱼攻击、在线欺诈和品牌滥用。若想妥善管理公司的域名组合，您必须选择一个能够大力投资保护自身系统的提供商。

2

仅与能够确保安全访问您的域名管理平台的注册商合作

域名安全纵深防御方法的第二层是确保您的注册商对域名和 DNS 管理系统实施安全访问。注册商应该要求自己的所有客户都通过双重身份验证。他们还应该提供 IP 验证和联合 ID，使其客户能够登录他们的网络，并确知他们在自己的域名管理平台上实施了安全的身份验证。

3

确保所有用户权限都已得到控制和管理

在与注册商合作时，务必要确保他们提供了精细的权限级别。注册商应该允许您访问并管理用户访问及权限。他们应该提供对权限提升的监测能力，包括在出现变化时发生通知。万一遭受网络攻击，此功能将显得特别重要。如果攻击者设法获取了注册系统的访问权限，就会创建一个新用户或更改现有用户的权限，从而造成损害。

4

利用高级域名安全功能

纵深防御方法的第四层是在单个域名级别应用高级安全功能。在确定了相关的域名之后，就应该对其应用适当的控制。首先是注册局锁定（即在注册局层面锁定域名），这会禁用将注册商自动关联到注册局。这意味着不手动输入密码就无法更改 DNS，而该密码必须经过授权联系人验证才能解锁域名。这是一种非常安全、有效的方法，可以确保在没有适当授权的情况下无法更改重要域名的 DNS。

未遭受黑客攻击的合法子域名为何也会被劫持

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，数字记录不断增加，导致遵循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。

“数字记录会随着时间的推移而积累，如果管理员不了解每个域名的历史情况，在删除遗留记录时就会犹豫不决，担心这些记录与关键的基础架构有关。这种不指向任何内容的非活跃 DNS 区域记录的积累被称为‘悬空 DNS’，它们存在子域名劫持的风险，攻击者可以控制不再使用的合法子域名来托管自己的欺诈或恶意内容。”

Mark Flegg，SC Media 全球安全服务主管，
“如何确保 DNS 记录不会变成安全危害”

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。不法分子会利用不执行验证检查的云提供商来托管内容，请求先前使用过的区域目的地，并开始将 Web 用户引流到这些全部加载了其非法内容的子域名，而且不必入侵企业基础架构或第三方服务帐户。例如，ZDNet 曾报道，一家全球性计算公司被攻击者劫持，并将其子域显示为扑克赌场。

通过利用悬空 DNS 记录，可以给其他网络攻击（例如网络钓鱼和恶意软件传播）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。位于澳大利亚的 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此类攻击。DNS 记录管理必须成为当今网络安全做法的一部分。20 多年来，某些公司一直面临管理不当的风险，他们通过不同的责任人、政策和供应商来管理其 DNS。如果在发生并购后需要删除任何内容，将使这种情况变得更加复杂，因为就连责任人都不能确定这些内容是什么。

CSC 的《子域名劫持漏洞报告》审查了 44 万多条 DNS 记录，发现超过 21% 的 DNS 记录指向的是无法解析的内容，导致许多公司都很容易遭受子域名劫持。 此外，还有超过 27.7 万 (63%) 条记录显示错误状态代码，例如 “404 未找到” 或 “502 错误网关” 。由于长期以来存在不同的责任人、政策和供应商，DNS 记录整理一直都是最常被忽视的任务之一。数字记录会随着时间的推移而积累，如果管理员不了解每个域名的历史情况，在删除遗留记录时就会犹豫不决，担心这些记录可能与关键的基础架构有关。悬空 DNS 存在子域名劫持的风险。子域名劫持是指攻击者控制了不再使用的合法子域名，用于托管自己的欺诈或恶意内容。这会给其他网络攻击带来可乘之机，例如网络钓鱼、恶意软件和勒索软件攻击。

21%

的 DNS 活跃子域名记录无法解析，这使公司很容易遭受子域名劫持。

在线品牌保护是必要的网络安全措施

恶意注册域名往往是全面发起针对性网络钓鱼或 BEC 活动的前兆，与其配合行动的可能还有危害极大的可下载恶意软件。为了防范这些初始攻击活动，企业需要妥善处理域名环境的现状，消除负责这一环节数字品牌计划的各团队间的脱节问题。安全团队必须积极地对其域名和品牌进行在线监控，以降低 Web 域名利用其品牌名称（或某个版本）开展欺诈活动的可能性。

确保域名安全是防范网络钓鱼攻击的首要任务。

公司需要更好地了解攻击者，他们可能正在注册或重新注册试图冒充其在线品牌的相似域名。这种洞察力可以帮助公司在发生安全事件时及时发现，并采取应对措施。

根据以往的经验来看，许多公司并不了解挑战的深度以及在线侵权活动渠道数量的增长。公司投入大量时间和金钱打造值得信赖的品牌，但如果遭受网络犯罪的侵害，这一切都可能变得毫无意义。公司保护其品牌的最佳方式是实施在线品牌保护计划，将在线监控与维权活动相结合以清除欺诈内容。补充性解决方案也有助于打造更全面的方法，例如与浏览器提供商、互联网服务提供商 (ISP) 和其他 SIEM 合作组建阻断网络，以阻止欺诈性网站接触到互联网用户，使用这些方法来跟踪和修复侵权者的活动时，还应同时运行一个确保域名管理安全的程序，使品牌所有人能够管理和保护自己的官方域名组合。

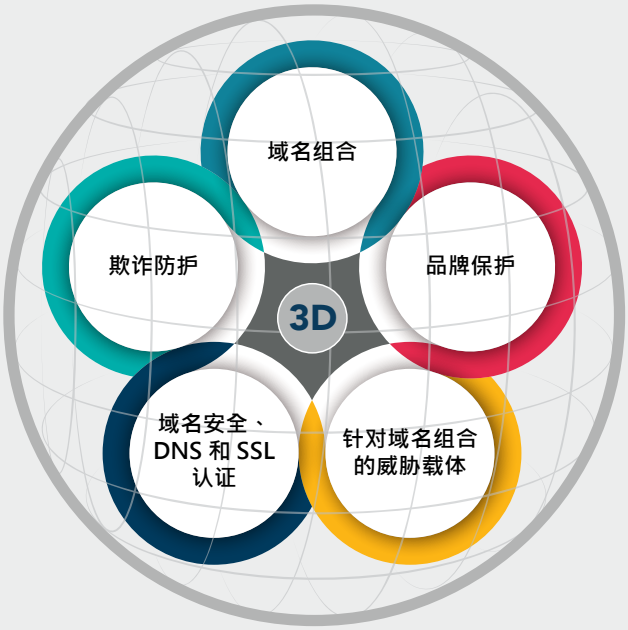
利用创新方式降低在线网络风险

作为一家服务于全球知名品牌的优秀企业级域名注册商，CSC 正在推动域名生态系统发生变革。CSC 相信，域名安全情报拥有强大的力量。

DomainSec 平台

DomainSec℠ 是 CSC 率先推出的一种为品牌域名生态系统提供安全保护的整体化方法。它是市面上极具创新性的企业域名管理和安全解决方案，同时结合了新一代在线品牌保护和欺诈防护功能。通过将来自这些解决方案的数据整合到一个平台，CSC 可以提供大幅改善的网络安全保护，

以增强企业的安全态势。我们可以帮助品牌完善其 Zero Trust 安全模型，而不仅仅是保护周边环境。这一同类首创的平台使用专有技术，同时结合机器学习、人工智能和群集技术，利用先进的指标来提供极具洞察力的安全情报。



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 简介

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 2000 强企业和百大全球最佳品牌 (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 DomainSecSM 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（在线品牌监控与维权活动相结合），对防火墙外针对特定域名的各种威胁进行多维度观察。欺诈防护服务可以在攻击的早期阶段对抗网络钓鱼攻击，进一步完善了我们的解决方案。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。

联系我们

cscdbs.com/cn