CSC

子域名劫持

漏洞报告

执行摘要

全球各地的企业都依赖互联网来开展各种活动——网站、电子邮件、认证、IP 语音 (VoIP) 等等。互联网是企业遭受外部攻击的一部分，需要予以持续监控，以防范来自网络犯罪的攻击和欺诈。域名系统 (DNS) 本质上是互联网的电话簿，而 DNS 记录管理是最糟糕的管理任务之一。而这也是 20 多年来，DNS 的不同所有者、供应商，以及政策导致的历史遗留问题，当然，也与管理员对删除任何不确定的记录的恐惧息息相关。想要详细且全面地掌握名下所有数字资产，并确定哪些为关键的、功能性的或是冗余（因而不再需要）的资产，对各企业来说都是一项重大挑战。更糟的是，纵观 CSC 托管的数以千计的域名组合，有五分之一的 DNS 记录处于容易遭受子域名劫持的状态。

主要亮点

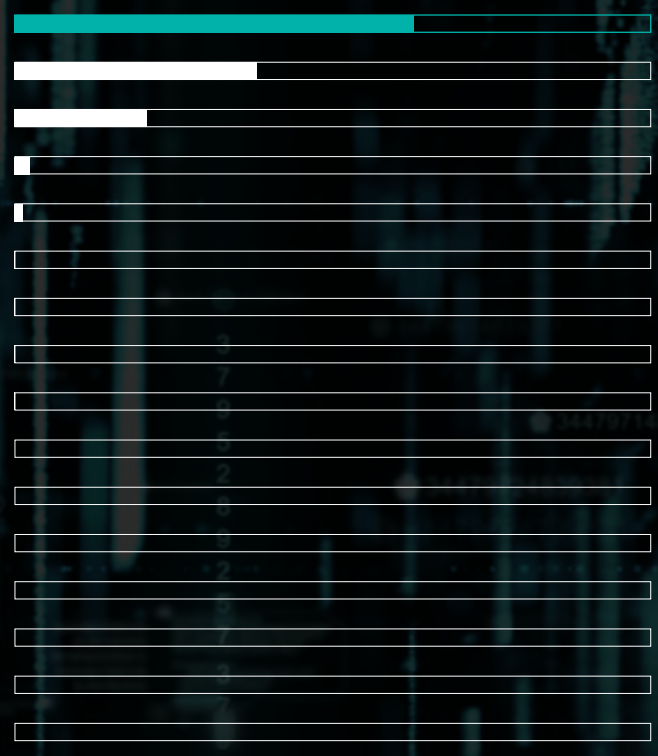
CSC 分析了数据库中 600 多万份 DNS 记录，并通过查看指向云端基础架构的 A 记录和 CNAME，进一步筛选至仅剩 440,000 多份 DNS 记录。这些记录有可能遭受子域名劫持入侵。我们之所以这样做，旨在了解企业子域名管理的现状。从这些 440,000 份 DNS 记录中，我们发现，许多企业都容易遭受子域名劫持。

有 21% 的 DNS 记录指向不解析的内容；这可能会使各企业容易遭受子域名劫持。

有 63% 显示错误状态代码，例如“404 未找到”或“502 错误网关”。许多配置了 DNS 记录的域名都返回了错误响应。

高达 38% 显示为“内部服务器错误”，表明这些企业需要改善其 DNS 管理任务和网络卫生。

已分析的 DNS 记录


不解析的区域 62.87%
内部服务器错误 38.12%
未找到 20.78%
错误请求 2.41%
服务不可用（通常是暂时的） 1.30%
错误网关 0.11%
网关超时 0.10%
无内容 0.03%
消失 0.01%
协商循环引用 0.00%
需要升级 0.00%
无法处理实体 0.00%
不可接受 0.00%
负载平衡问题 0.00%
网络连接超时错误 0.00%
冲突 0.00%
解析的区域 37.13%
永久重定向 20.10%
未经授权 5.71%
确定 4.68%
禁止 3.49%
暂时重定向 2.87%
由于 http/1.1 而暂时重定向 0.14%
永久重定向 (RFC 7538) 0.10%
成功 0.03%
不允许使用的方法 0.00%
用户定义的资源错误 0.00%
需要代理身份验证 0.00%
100.00%

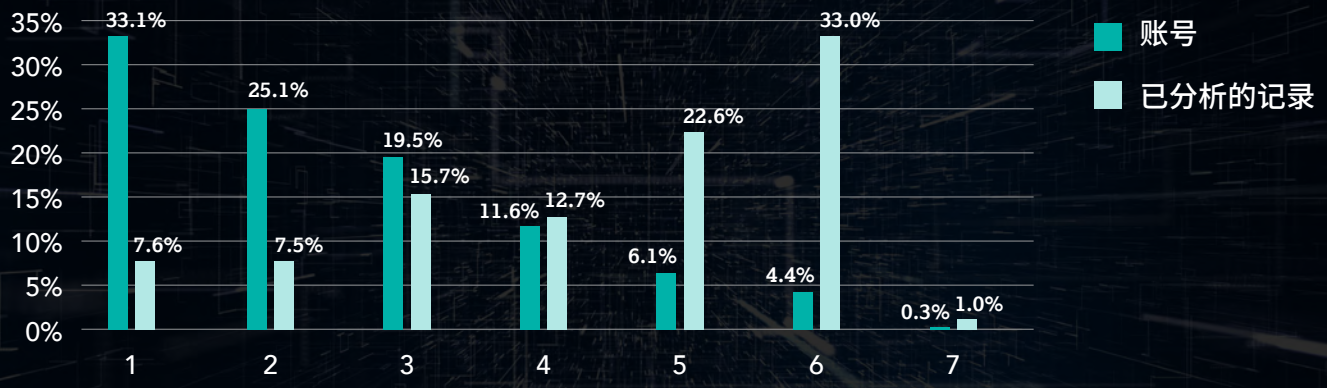
风险因素：使用云端服务提供商的盛行

在所有已分析的记录中，**超过 82%** 主机托管于云端服务提供商。

这个百分比反映的趋势是，在过去几年内，企业不再使用传统的内部数据中心，而外包给云端服务提供商。使用云端服务提供商使这些公司能够运用新技术，从而更具韧性和动态，也更具成本效益。但与以前相比，企业如今需要管理更多 DNS 记录，因此也面临更多风险。

风险因素：拥有较大规模域名组合的企业对服务提供商实施分散管理

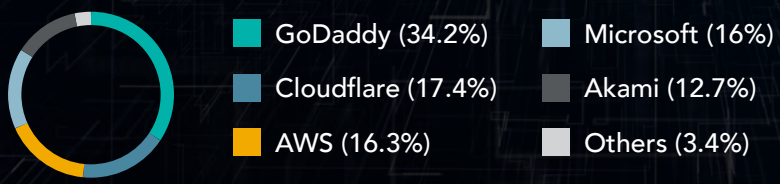
所使用的服务提供商数量



58% 所分析的企业似乎在将子域名整合至一至两个云端服务提供商方面做得更好，但他们拥有的域名组合往往规模较小，因而更易于管理。

相反，在该研究中分析的企业中有 11% 使用了五个或以上的云端服务提供商。这些企业占所分析的全部 DNS 记录的一半以上，有些甚至有规模庞大的域名组合，其中每家企业都有数以千计份记录。这表明，有着庞大域名组合的企业可能未集中管理其云端服务提供商，因此带来的挑战就是，这些企业难以适当地监督所有 DNS 记录。

所使用的云端服务提供商的分布情况



在所有已分析的 DNS 记录中，有 96% 以上分布于五家规模最大的云端服务提供商——GoDaddy、Cloudflare®、AWS、Microsoft® 和 Akamai。Cloudflare®, AWS, Microsoft® und Akamai.

利用子域名监控规避网络威胁

拥有多元化品牌组合和国际业务的大型组织，通常对其数字足迹的规模毫无概念。数字记录随着时间推移而积累。这使得保持网络卫生成为了严峻挑战。

如果对数字记录及其管理缺乏适当的监督，各企业只会累积“噪音”，使简单的网络卫生和整理变得更加复杂，从而可被网络罪犯轻易利用。这种不指向内容的非活跃区域累积现象被称为“悬空 DNS”，而且是子域名劫持的风险。悬空 DNS 为网络钓鱼、恶意软件和勒索软件等其他网络攻击打开了方便之门。这些攻击可能导致品牌声誉受损，失去消费者信任，以及带来更具破坏力的数据泄露和安全漏洞。不了解每个域名来历的管理员不愿意删除这些遗留的记录——他们担心这些记录可能与关键基础实施相关联，一旦删除会无意间使业务瘫痪。

要详细掌握其所有数字资产，并确定哪些为关键、功能性或冗余（因而不再需要）的资产，对各企业来说都是一项挑战。DNS 记录整理是企业管理最差的任务之一。这是由 20 多年来 DNS 的所有人、政策和供应商改变所致，当然，也由对删除企业不确定的任何记录的内在恐惧所致。

此外，子域名劫持是现存的众多域名安全威胁之一。其中包括域名与 DNS 劫持、域名阴影和缓存中毒。这些威胁通常作为触发攻击，以发起更为恶劣的网络钓鱼和勒索软件攻击，以及商业电子邮件泄露 (BEC)、电子邮件欺骗，甚至数据泄露。

我们建议所有企业都采用子域名监控解决方案。这种解决方案不仅在检测到您的 DNS 记录发生变更时发出警示，还向您提供情景知识，以便您能做出信息充分的决策，采取适当的措施，以杜绝子域名劫持。

在此处了解更多关于 CSC 子域名监控解决方案的内容。

CSC是深受福布斯全球2000强和全球最佳品牌100强®企业信赖的安全和威胁情报提供商，业务领域专业且全面覆盖企业域名、域名系统(DNS)、数字证书管理、数字品牌，以及防欺诈保护。随着全球各企业加大安全状况方面的投资，CSC可以帮助他们了解已知的网络安全疏忽问题，并帮助他们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，避免遭受灾难性的收入损失以及因违反《通用数据保护条例》(GDPR) 等政策而面临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。

DBS04172023