使用企业级域名注册商对整体安全评级的影响

SecurityScorecard.com
info@securityscorecard.com
©2021 SecurityScorecard Inc.

214 West 29th St., 5th Floor
New York, NY 10001
1.800.682.1707

SecurityScorecard CSC

执行摘要

包括勒索软件攻击和商业电子邮件泄露 (BEC) 在内的大多数网络攻击都是从网络钓鱼开始的。
在勒索软件攻击的早期阶段，网络钓鱼充当着踏脚石。尽管目前每年因勒索软件造成的损失高达数十亿美元[1]，但大多数勒索软件保护和响应措施并不能充分化解网络钓鱼风险。

既有的研究表明，网络钓鱼攻击最频繁发生在恶意注册、以假乱真的类似域名上或被损害或劫持的合法域名上，或是电子邮件欺骗上。与企业级域名注册商合作，可能有助于抵御这些风险。

域名注册商的选择是组织整体安全状况的一个指标。

SecurityScorecard所做的研究表明，组织对域名注册商的选择与公司的网络安全评级息息相关。选择企业级域名注册商 (ECR) 进行域名管理的组织的总分要比选择消费级域名注册商 (CGR) 的组织平均高出至少半个到一个字母等级。

企业级注册商的属性

共有两种类型的域名注册商：消费级注册商和企业级注册商。消费级注册商专注于个人或小企业使用的域名服务、网站和电子邮件。尽管 CGR 本身不怀恶意，但他们通常并不提供域名安全功能和控制措施，也不注重知识产权保护。

企业级注册商以网络安全和知识产权保护为使命和关注点，会通过高级服务和工具来重视域名安全。此外，他们不会通过零售网站或点击付费、域名虚构和域名拍卖服务来提供域名服务，此类方法可能导致知识产权和商标侵权。

需要留意的企业级注册商的主要特征如下：

- 整个企业的规模和专业知识，并具有企业专用的域名 DNS 和证书管理服务。
- 高级服务，例如域名注册局锁、DMARC、DNSSEC、CAA 记录和 DNS 主机冗余。
- 全球和当地 24x7x365 全天候支持能力，具备全球域名注册能力。
- 在寻求和验证客户互动行为时实施《了解您的客户》(KYC) 方法。
- 提供域名、品牌和欺诈监管与维权和关停能力。

评价福布斯全球 2000 强企业的域名安全

《2021 CSC 域名安全报告》显示，尽管全球 2000 强企业普遍向现代化企业和运营转变，但网站域名仍未得到充分保护，岌岌可危。2021 年，众多公司面临着更多的勒索软件攻击、商业电子邮件泄露、网络钓鱼攻击、供应链攻击以及线上品牌和商标滥用。尽管网络风险与日俱增，但福布斯全球 2000 强企业所采取行动的水平却仍未改变。

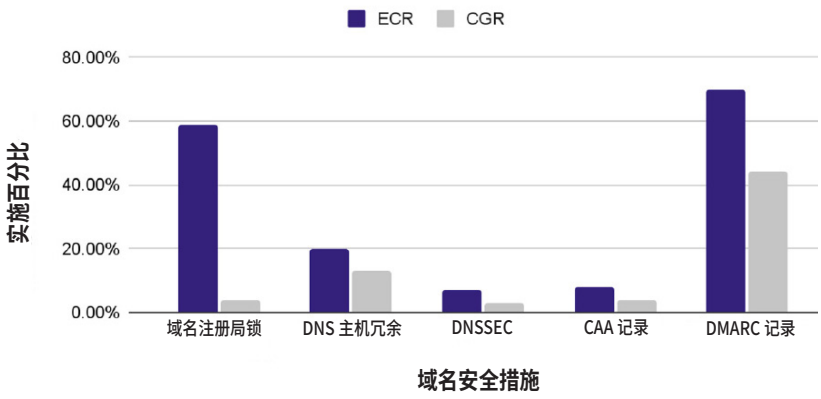
该报告的调研结果突显了福布斯全球 2000 强企业面临的域名安全风险：

- **70% 的同形文字域名**（模糊匹配）一网络钓鱼和品牌滥用中常用的一种策略一由第三方拥有，并已向消费级注册商注册。
- **60% 的此类域名注册行为**都发生在近两年中，证明这是一种越来越多的攻击方式。
- **81% 的公司面临更大的**域名和域名系统 (DNS) 劫持风险，因为这些域名没有采用基本的域名安全措施，例如域名注册局锁协议。
- **57% 的公司都依赖于消费级域名注册商**，而这些注册商对抵御域名和 DNS 劫持、分布式拒绝 服务 (DDoS)、中间人攻击 (MitM) 或 DNS 缓存中毒的保护措施有限。
- **仅 50% 的公司在使用 DMARC。**

该研究还比较了 ECR 组和 CGR 组的域名安全措施实施情况，从而印证了上述调研成果。

福布斯 2000 强企业域名安全措施实施情况

ECR 组与 CGR 组对比



使用企业级域名注册商可在整体 SecurityScorecard 评级方面提升半个到一个字母等级

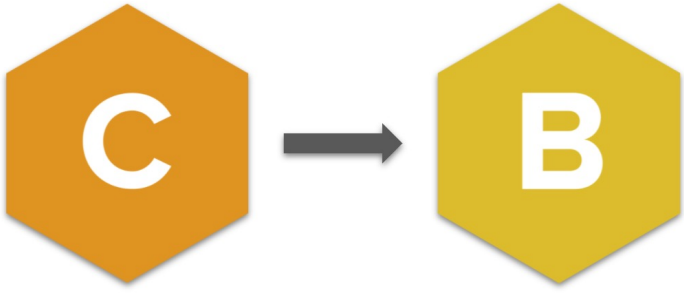
安全评级强调了优先考虑域名安全的需求

SecurityScorecard 分析了其平台中 50,000 家最受关注公司的安全评级，调研成果不断证实优先考虑借助值得信赖的企业级域名注册商保障域名和 DNS 安全的需求。选择企业级注册商进行域名管理的公司的总分比使用消费级注册商的公司平均高出至少半个字母等级。在我们的分析中，这种选择会产生总分为“C”还是“B”的差别。

SecurityScorecard 的研究证实，域名注册商的选择是一个关键决定，常被忽视，但肯定能增强组织的整体安全状况。

量化企业级域名注册商对组织整体安全评级的影响

在 SecurityScorecard 分析的 50,000 家组织中，使用消费级注册商的组织的平均 SecurityScorecard 评级为 76.92。使用企业级域名注册商的组织的平均 SecurityScorecard 评级为 81.73，产生了 5 分的平均优势。将 ECR 组与 CGR 组之间的差异可导致从“C”提升到“B”的整个字母等级优势。



DNS 运行状况尽管是一个重要的评分因素，但被确定为排名最低的风险因素得分

SecurityScorecard 平台考核了多个 DNS 配置设置，例如 OpenResolver 配置，以及是否存在建议配置，包括 DNSSEC、SPF、DKIM 和 DMARC。

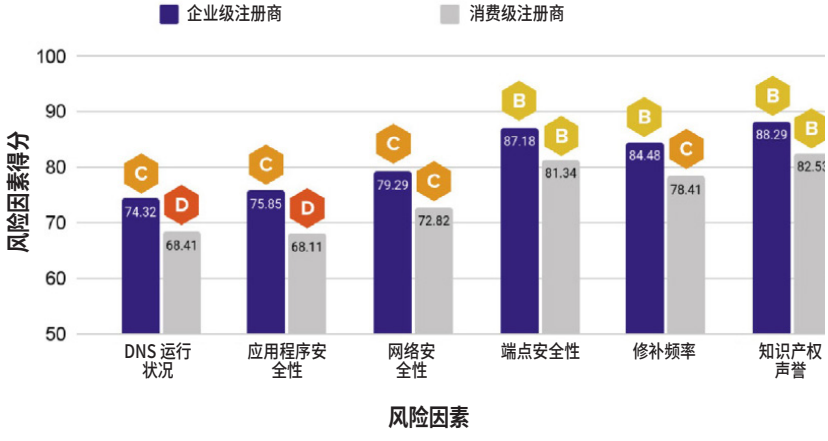
尽管 DNS 运行状况在 SecurityScorecard 的评分算法中是一个重要的评分因素，但所分析的公司平均 DNS 运行状况分数为 71.36（C 字母等级）。因此，DNS 运行状况是我们分析的所有因素分数中排名最低的因素分数。ECR 组的平均 SecurityScorecard DNS 运行状况因素分数为 74.32，CGR 组为 68.41，二者之间接近 6 分的平均优势差距。这导致两个组出现从 C 到 D 的整个字母等级优势。

DNS 运行状况影响其他关键风险因素

我们的研究还表明，ECR 组和 CGR 组在应用程序安全、网络安全、端点安全、修补频率和知识产权声誉等其他因素分数方面存在 5 分以上的差距，导致在几个因素分数方面产生整个字母等级优势。

平均风险因素得分

ECR 与 CGR 对比



该分析表明，采用主动的域名安全措施，有助于改善 DNS 运行状况并提高其他因素分数，从而提高整体安全评级。

CSC和SecurityScorecard：建立在网络风险防范基础之上的联盟

安全评级的全球领导者 SecurityScorecard 与 CSC 达成战略联盟，以向其客户提供域名安全见解。通过采取十分明智且主动的措施来防御域名和 DNS 攻击，各组织和网络保险公司可以更精准地找出潜在的网络风险、品牌网络钓鱼滥用和泄露，防患于未然。

尽管域名安全需要高级安全措施和操作协议等深度防御方法，但从 SolarWinds 等公司遭受的攻击对供应链造成的影响来看，您选择的注册商类型也十分重要。查看 DNS 安全的传统方法更多地着重于 DNS 韧性、解决方案和相关 DDoS 保护。如今常被忽略的一个 DNS 运行状况的关键部分是，攻击者如何操纵域名和 DNS，来对企业及其客户进行恶意攻击。

域名安全的三大支柱

CSC 从三个方面专注于域名安全：

1. 确保合法域名和与其关联的 DNS 不会在您的域名注册商或 DNS 主机服务提供商环节遭到入侵（DNS 劫持、域名劫持、子域名劫持）。
2. 监控和停用恶意第三方域名。
3. 确保使用电子邮件认证来防御电子邮件欺骗。

CSC 域名安全最佳实践

所有行业的所有公司 - 尤其是如今因新冠病毒而面临更大风险的公司 - 都应从与企业级域名注册商合作开始，采用多层次深度防御方法来确保域名安全。

CSC 推荐四项关键策略：

1. 采用深度防御方法进行域名管理。
2. 确认您的域名注册商的业务实践不会助长欺诈和品牌滥用行为。
3. 持续监控域名和 DNS 空间以及关键数字渠道，如市场、应用程序、社交媒体和电子邮件，防止品牌滥用、侵权、网络钓鱼和欺诈。
4. 实行全球维权，包括关停和先进的网络封锁技术。

结论

远程工作政策的实行导致勒索软件扩散和安全挑战层出不穷，所以对于负责网络安全风险缓解和线上品牌保护的人来说，选择信誉良好的域名注册商已成为至关重要的决定。选择一家优先考虑安全、数据管控和全球支持的企业级注册商，对于保护组织的品牌和客户安全十分重要。

SecurityScorecard和CSC 已达成合作，从选择域名注册商开始，提供关于因缺少域名安全措施所带来的安全风险的培训，并缓解这些风险。

结束语

在此处注册，以获取免费的 SecurityScorecard 企业许可证，从而监控您自己的组织和最多五位供应商。

在此处注册，以获取免费的 CSC 域名安全审计。

[1] https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=75f066bf71c6

资源

完整的最佳实践列表：

《CSC 2021 域名安全报告》

CSC 博客

《建立现代网络风险管理团队的五个步骤》

《完美记分卡：从您的董事会获取网络安全 A 级评价》

SecurityScorecard 博客

关于 CSC

CSC 是企业域名、域名系统、数字证书管理以及数字品牌、欺诈和网络钓鱼防御领域值得信赖的提供商，是福布斯全球 2000 强企业和“全球最具价值 100 大品牌®”的首选。我们使用专有安全解决方案帮助各公司抵御其线上资产面临的网络威胁，帮助他们避免灾难性的收入损失、品牌声誉损害或数额巨大的罚款。
我们还提供兼具线上品牌监控和维权服务，采用全面方法来保护数字资产。请访问 cscdbs.com，以详细了解我们的域名管理、安全、品牌保护和欺诈防护服务。

关于 SecurityScorecard

SecurityScorecard 通过持续的非侵入式监管，帮助企业获取对其安全状况及其第三方安全状况的运营掌控。该公司的安全方案着重于像黑客那样从外部视角识别漏洞。SecurityScorecard 的专有 SaaS 平台在关键数据点的广度和深度方面无与伦比，其中包括众多风险类别，如应用程序安全、恶意软件、修补频率、网络安全、黑客网络通信、社交工程和已泄漏的信息。

如要接收包含贵司当前分数的电子邮件，请访问 instant.securityscorecard.com。

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.com
@security_score

SecurityScorecard 总部
214 West 29th St., 5th Floor
New York, NY 10001