当域名安全遇到供应链短缺

cscdbs.com/cn

重点摘要

CSC 的最新研究表明，伪造者借助 2022 年的婴儿配方奶粉的短缺情况，利用假冒的品牌域名针对消费者进行诈骗。主要研究结果显示，与婴儿配方奶粉相关的域名注册数量激增，这些域名利用受信赖的品牌名诱导消费者。**84%** 的这些网站域名是自 2021 年以来创建的假冒网站，例如，由并非品牌所有人的第三方所持有。这对消费者以及拥有这些品牌的公司来说，在产品安全、网络钓鱼攻击、财务困境和数据外流方面，都是真正的潜在隐患。除了婴儿配方奶粉市场，我们还发现模仿半导体行业芯片制造商的相同类型的假域名注册。**95%** 的 2021 年以来注册的品牌域名都是由并非品牌所有人的第三方所持有。

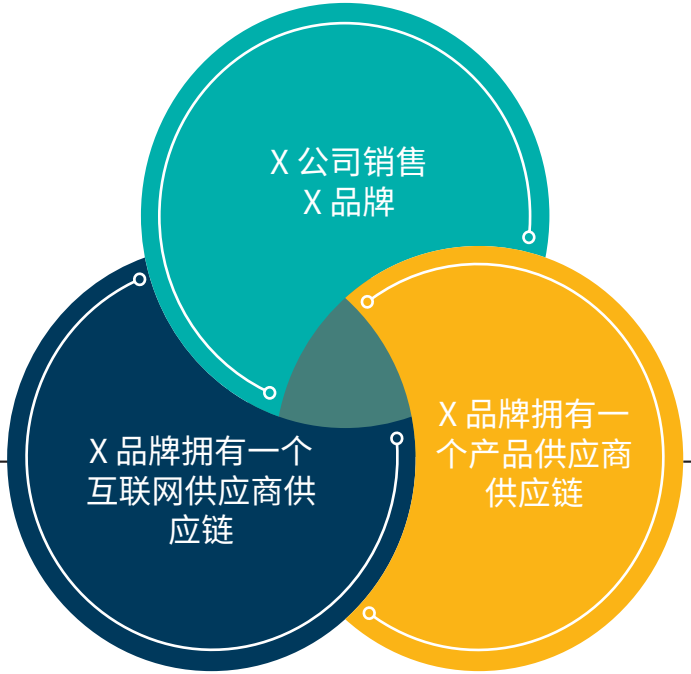
最后，相当多的公司缺乏域名安全卫生，这会让他们面临更大的域名安全风险，这也说明这个问题在关键基础设施领域普遍存在。如果发生对云提供商或域名注册商的大规模攻击（即域名系统 (DNS) 劫持或分布式拒绝服务 (DDOS) 攻击），或发生对社会工程的攻击亦或网络钓鱼攻击，域名安全卫生可以让企业在应对这些风险时有更强的抵御能力。

域名安全与供应链的联系

在过去的两年里，我们都面临着供应短缺问题，而短缺的竟然是那些我们以前根本想象不到会缺货的商品。各企业的管理团队都在纳闷："哪些因素是我们应该注意，实际上却毫无察觉的？"有一个重要的企业风险因素仍然没有引起重视——品牌网站域名注册安全。

正如我们在最近的供应链攻击中所看到的，比如 **Colonial Pipeline** 和 **JBS Foods**，通过单点破坏对一家公司进行攻击，有可能会破坏由互相连接的公司和产品、合作伙伴、供应商和客户所构成的整个网络，从而可以为攻击者创造指数级的回报。由于域名和 DNS 之间天然的关联性，对域名注册商或云计算提供商进行单点攻击，或使用假冒域名进行网络钓鱼攻击，就可以突破互联网供应链而延伸到产品和基础设施供应链中。

网络欺诈涉及虚假域名注册以及对云计算提供商、域名注册商和 DNS 主机托管提供商的攻击。



示例：

婴儿配方奶粉的短缺是一个线下品牌关注的问题，但网络安全风险加剧了这一情况的恶化。

CSC 的最新研究表明，遭遇供应链短缺的公司和消费者所面临的风险在增加

假冒域名是互联网欺诈最常见的手段，这可能会给品牌所有人造成收入损失、品牌声誉受损、消费者安全问题以及品牌所有人的其他网络安全顾虑。CSC 注意到，随着供应链短缺等全球性和社会性事件的发生，企图利用这些事件的域名注册现象也相应增加。2022 年 1 月，基于网络罪犯以同样的手法利用疫苗相关品牌和健康组织品牌，CSC 发布了**关于与 COVID 相关的欺诈性域名激增的研究**。

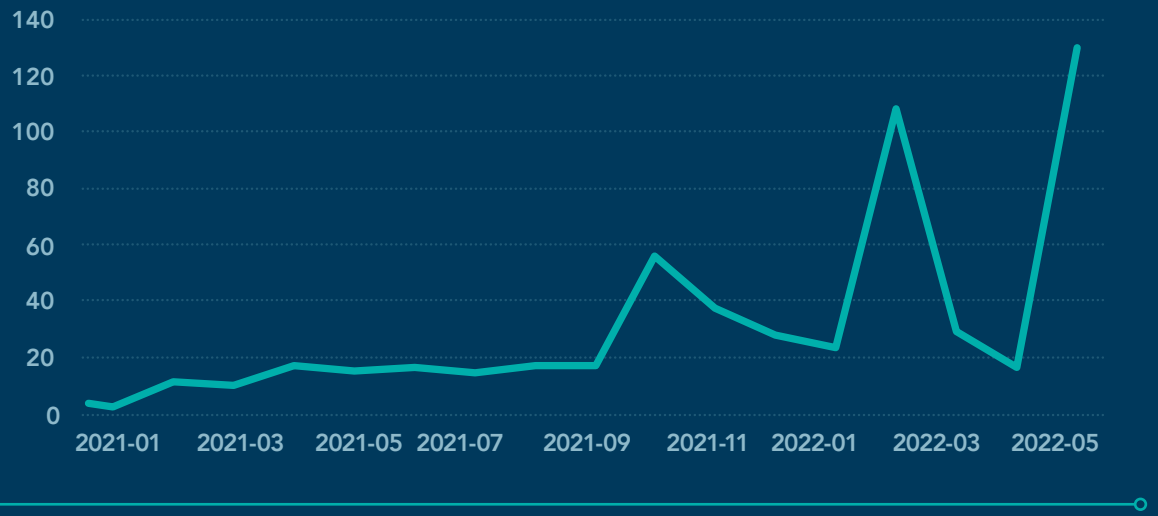
“

CSC 的研究团队评估了含有顶级婴儿配方奶粉和半导体品牌名称的域名。结果与先前研究一致，2021 年至 2022 年 5 月期间发生的假冒域名注册激增。

主要研究结果：
婴儿配方奶粉短缺

CSC 评审了包含前五大婴儿配方奶粉品牌名称或其他相关搜索词的域名，如婴儿奶、配方奶粉和婴儿食品。

与婴儿配方奶粉相关的第三方域名的每月注册数量（品牌和关键字）



84%

的域名归第三方所有*

**根据我们对第三方域名的定义，这些域名不归属于品牌所有人，并且是假冒的。*

93% 使用了域名隐私服务，或隐藏了 WHOIS 详细信息。

这证明有人试图掩盖或隐藏其所有权和身份，表明他们可能有一些邪恶的意图。

26% 配置了 MX（电子邮件）记录。

有 MX 记录的域名可以被用来发送网络钓鱼电子邮件或拦截电子邮件。

在分析中与虚假注册关联最大的域名注册商：

- GoDaddy.com, LLC
- Sav.com, LLC
- 成都西维数码科技有限公司

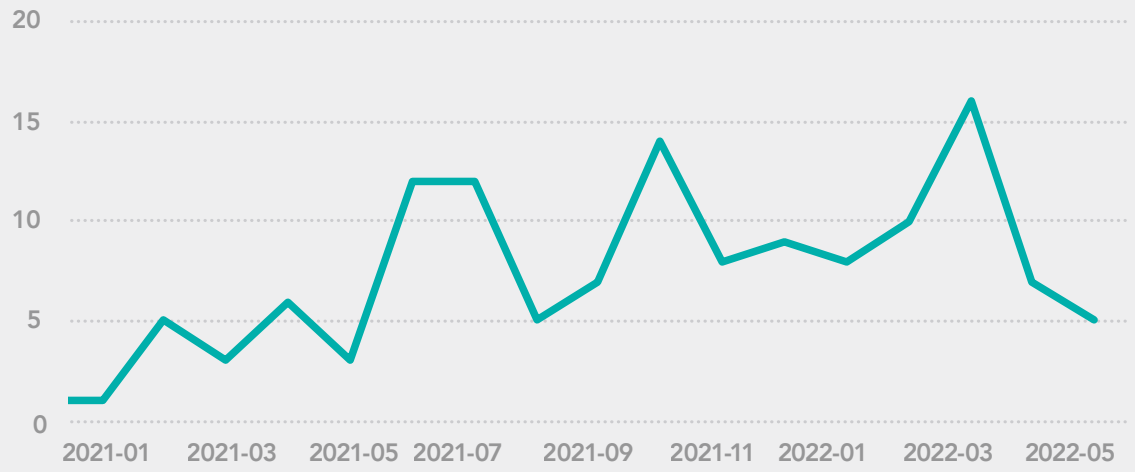
在分析中与虚假注册关联最大的 DNS 主机托管域名：

- domaincontrol.com（提供商 GoDaddy）
- bodis.com（提供商 Bodis）
- registrar-servers.com（提供商 NameCheap）

主要研究结果：半导体短缺

CSC 勘测了包含前六大半导体品牌名称或其他相关搜索词的域名，如半导体和电子芯片。

与半导体芯片相关的第三方域名的每月注册数量（品牌和关键字）



95%

的域名归第三方所有*

**根据我们对第三方域名的定义，这些域名不归属于品牌所有人，并且是假冒的。*

79% 使用了域名隐私服务，或隐藏了 WHOIS 详细信息。

这证明有人试图掩盖或隐藏其所有权和身份，表明他们可能有一些邪恶的意图。

44% 配置了 MX（电子邮件）记录。

有 MX 记录的域名可以被用来发送网络钓鱼电子邮件或拦截电子邮件。

在分析中与虚假注册关联最大的域名注册商：

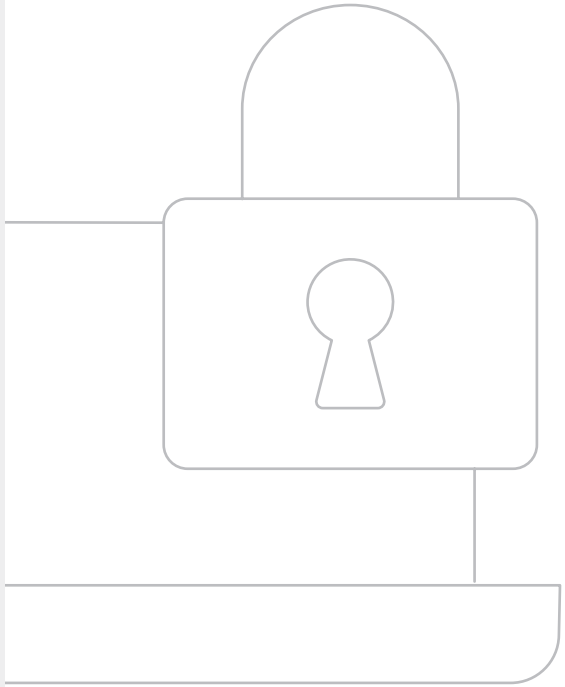
- GoDaddy.com, LLC
- Namecheap Inc.
- Dynadot LLC

在分析中与虚假注册关联最大的 DNS 主机托管域名：

- domaincontrol.com（提供商 GoDaddy）
- registrar-servers.com（提供商 NameCheap）
- hichina.com（提供商 Alibaba）

域名安全和网络卫生

利用域名安全，除了保护您的公司免受虚假域名注册的影响外，还必须具有前瞻性并使用关键的安全控制措施作为保障域名安全卫生的一部分。CSC 建议采用**深度防御的方法**，并结合以下高级安全措施：



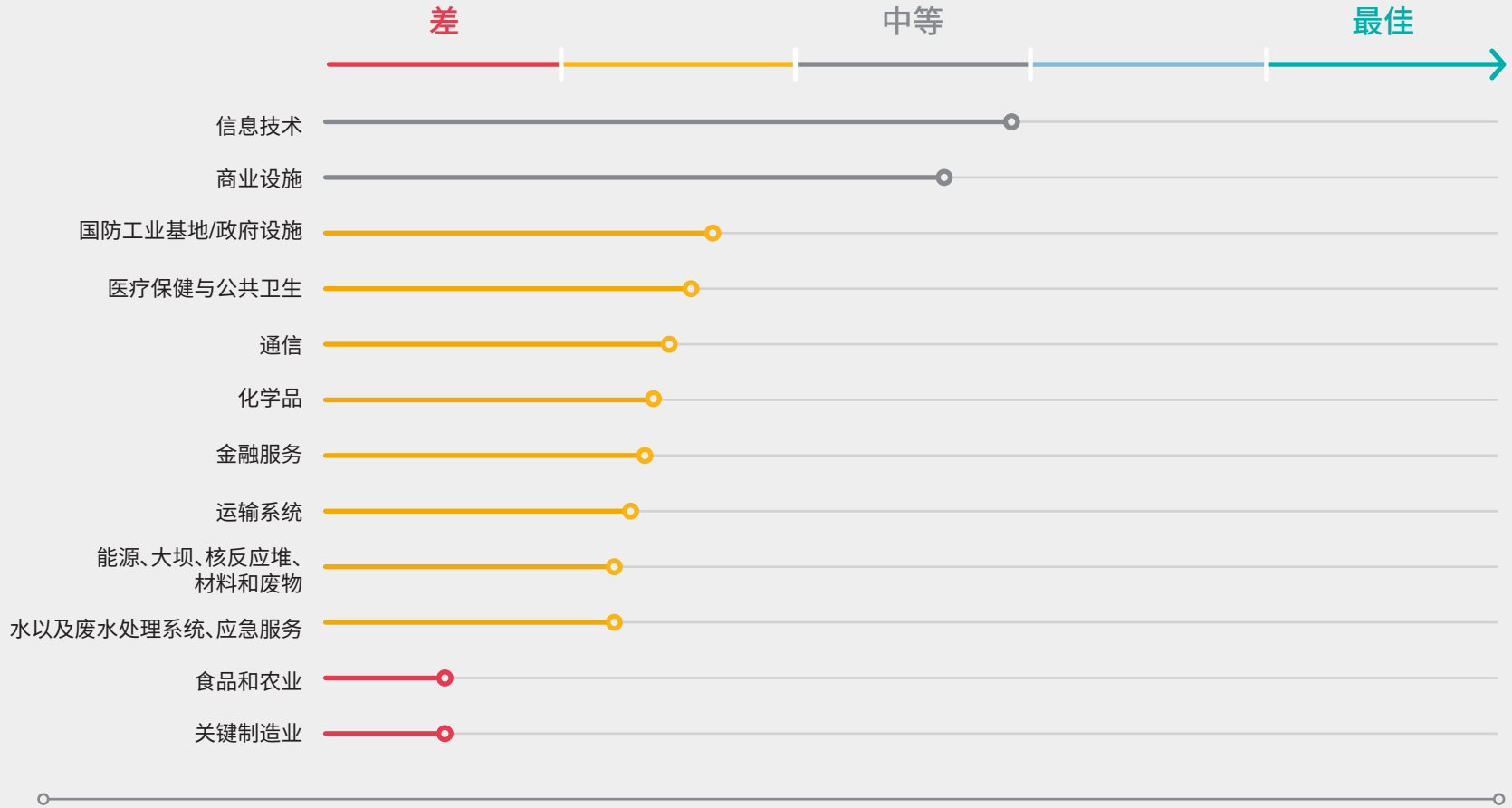
CSC 的域名安全卫生措施

域名安全措施	目的
DNS 主机托管冗余	缓解停机和遭受 DDoS 攻击。
域名系统安全扩展 (DNSSEC)	防止黑客控制互联网浏览会话，旨在将用户重新引导至欺骗性网站。
发件人策略框架 (SPF)	可减少垃圾邮件、诈骗和网络钓鱼的电子邮件认证标准。
基于域名的消息身份认证、报告与一致性 (DMARC)	
域名密钥识别的邮件 (DKIM)	
多重锁定	将注册局和注册商级别的锁与 WHOIS 锁相结合，以防止 DNS 记录的未授权更改以及域名劫持。
证书认证机构授权 (CAA) 记录	确保只有经授权的证书认证机构才能颁发证书。
使用企业级注册商	专业从事与各企业合作，在域名和 DNS 管理以及全、品牌和防欺诈保护、数据治理和网络安全方面提供其所需的高级业务实践、能力、专业知识和支持人员。

了解关键行业情况的大局

利用**域名安全报告**中的数据，我们研究了福布斯全球 2000 强企业，并将相关行业领域与 16 个 **CISA 关键基础设施领域**之一相对照。然后，我们观察到上述八个域名安全卫生迹象，按照这些关键基础设施领域对域名安全措施的实施情况进行排名。

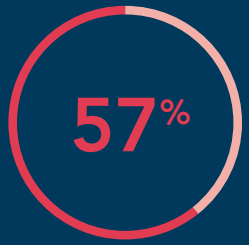
风险缓解成效量表



这些最新的研究结果为半导体和婴儿配方奶粉所属的行业——关键制造业以及食品和农业，所面临的更大的潜在问题提供了背景，也表明了域名安全状况仍然不容乐观，而且几乎没有改善。

CSC 的域名安全报告：福布斯全球 2000 强企业对全球最重要的商业领域的域名安全状况进行了更深入的分析。

81% 面临着更大的域名和 DNS 劫持风险，因为这些域名没有采取基本的域名安全措施，例如域名注册局锁。



57% 都依赖于消费级域名注册商，对抵御域名和 DNS 域名劫持、DDos、中间人攻击 (MitM) 或 DNS 缓存中毒的保护措施有限。

50% 使用 DMARC 记录作为电子邮件认证方法。

风险导致病急乱投医，因此必须予以纠正

买家在缺货时会不惜一切代价去设法买到其所需的东西。品牌和域名行业必须保持警惕，从而确保消费者访问的是安全和经授权的域名。薄弱的域名安全状况并不是新的挑战，但它正在成为前沿核心问题，需要在战略上予以更多重视。各公司需要在互联网上彻底搜索以找到并处理任何可能会削弱或损害其品牌信誉并将其终端消费者引入欺诈性活动的蛛丝马迹。这些风险是可以避免的，消费者通过网络搜寻其所需商品，但却不幸落入网络罪犯魔爪，这种现象必须要加以制止。必须要实施更完善的域名安全措施，商业界必须接纳并采用广泛的域名安全标准。

品牌已经在数字化转型、品牌保护和网络安全风险缓解方面进行了大量投资。然而，由此产生的域名和 DNS 内部的系统性风险正在导致供应链漏洞、网络钓鱼、欺诈（即勒索软件和商业电子邮件泄露）、品牌滥用和伪造等现象。提供关键基础设施的各公司需要更多地展示其改善自己安全状况的行动能力。域名安全是其中的一部分，也是一种系统性商业风险。

此外，网络保险行业也应当评估这些风险。对于很多公司而言，网络保险的保费和核保经历正在发生变化，保险公司开始关注能够影响保险政策的新指标。在这些指标中所反映的薄弱域名安全状况可能会对这些公司产生长期影响。当涉及到域名安全时，无所作为是不可取的。CSC 认为现在急需制定更广泛的域名安全标准以及针对与 DNS 日常活动和行为有关的政策或法规。

要了解更多有关如何确保您的企业在保护自己的信息，请访问：

我们的供应链博客文章中的域名安全建议

CSC

CSC 是企业域名、域名系统 (DNS)、数字证书管理以及数字品牌和欺诈防御方面值得信赖的提供商，位列福布斯全球2000强企业和全球最具价值 100 大品牌®。随着全球公司加大安全性方面的投资，CSC 可以帮助他们了解存在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。公司可以凭借 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（在线品牌监控和执行活动的结合），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**。

Vincent D' Angelo, 公司发展和战略联盟全球总监

Quinn Taggart, 全球品牌安全高级顾问

Sue Watts, 全球营销主管

David Barnett, 品牌监控咨询负责人

cscdbs.com/cn

DBS07062022