辅助DNS服务的案例

改进的安全策略可保护您的在线资产

它可能发生在您身上

2016年10月21日，众所周知的托管域名系统（DNS）提供商遭受大规模分布式拒绝服务（DDoS）攻击。这次攻击不仅中断了DNS提供商的可用性和服务，而且附带损害还蔓延到了许多知名品牌，这些品牌的网站和应用程序也遭受间歇性中断。

攻击发生之后，人们清醒地认识到，任何人都无法避免DDoS威胁的困扰，尤其是对其DNS的威胁。但同样令人担忧的是，大部分人都认为受影响的公司没有做错任何事情。其采取了许多顾问当时建议的措施，也就是将DNS委托给托管服务提供商。但事实证明，没有进行备份是一个致命的错误。

10月21日的攻击标志着DDoS攻击未来的组合方式将发生根本改变。这次攻击是使用Mirai Botnet恶意软件发起的，该恶意软件由非典型的联网设备组成，例如安全摄像机、DVR和家用路由器。组合在一起之后，被劫持的设备形成了一种危险而威力强大的高容量武器。Mirai Botnet以前所未有的规模发动了毁灭性的DDoS攻击。而且由于其有效性，僵尸网络预示着攻击将带来严重的后果。

但最重要的是，这次攻击为企业对DNS的新要求提供了宝贵的教训。具体而言，企业不应冒险地将全部在线业务托管在一项DNS服务上。仅依靠一个DNS提供商的组织遭受了依赖于单个故障点的现实后果。如果这些公司在多个服务之间分配了DNS，那么其网站、应用程序和其他在线资产就不太可能出现故障，即使在攻击高峰期也是如此。

使问题更加复杂的是当今网络犯罪的演变速度。用于限制网络攻击的可靠策略在不到六个月的时间里就可以淘汰了。对于DNS攻击尤其如此，因为犯罪分子认识到攻击DNS漏洞可以造成破坏。

本文档基于Neustar®的《辅助DNS服务的案例》编制。

通过采用新技术并修改其当前的安全策略，企业能够以最低的成本和最少的精力来有效地改善其DNS安全状况。

深入探讨DNS困境

在当今的互联网时代，企业安全主要集中在保护在线边界（如网络边界）上。这样做的理由是，如果您可以阻止恶意软件和不良代理进入网络，就可以保护您的数据和业务。但是，网络犯罪分子非常顽固且适应性强。一扇门关上后，他们会发现一扇新开的窗户。因此，网络犯罪分子很快就会发现他们可以通过攻击负责在线内容呈现的协议——DNS来影响和破坏组织。

尽管DNS很重要，但多年来，人们只有在发生安全事件后才会想起它。它被认为是用于路由请求的公共协议，但是它本身并不被视为安全漏洞。这一切都随着拒绝服务（DoS，以及后来的DDoS）攻击而改变。通过向DNS服务器发送大量请求，网络犯罪分子可以无限期关闭组织的网站和应用程序。而且，由于网站和应用程序的可用性与DNS有着千丝万缕的联系，安全性问题因此很快就由事后考虑因素变成当务之急。

要攻击DNS服务器，首先需要获取其物理地址。托管自己的域名系统会将DNS地址暴露给任何人，即使他们只具备一点点互联网技能。例如，有一定互联网技能的用户可以在不到30秒的时间内发现不受保护的DNS地址。因此，安全顾问开始倡导组织使用外部DNS提供商以更加安全和有效的方式处理其DNS请求，这并不足为奇。

权威DNS的适当安全状态

为保护其权威DNS服务，组织可采取的最重要措施就是同时实施主DNS解决方案和辅助DNS解决方案。在MiraiBotnet出现之后，行业分析机构（例如Gartner）建议组织部署辅助DNS服务以提高性能和安全性。

辅助DNS服务不应与冗余DNS提供商混淆。这不是说制定B计划，以防A计划失败。而是制定更智能的A计划，以有效地在两个受信任的网络之间分配DNS流量。这种策略不仅可以防止您的品牌遭受单一的DDoS攻击，而且可以通过在两个网络之间分配负载来提高DNS冗余性。

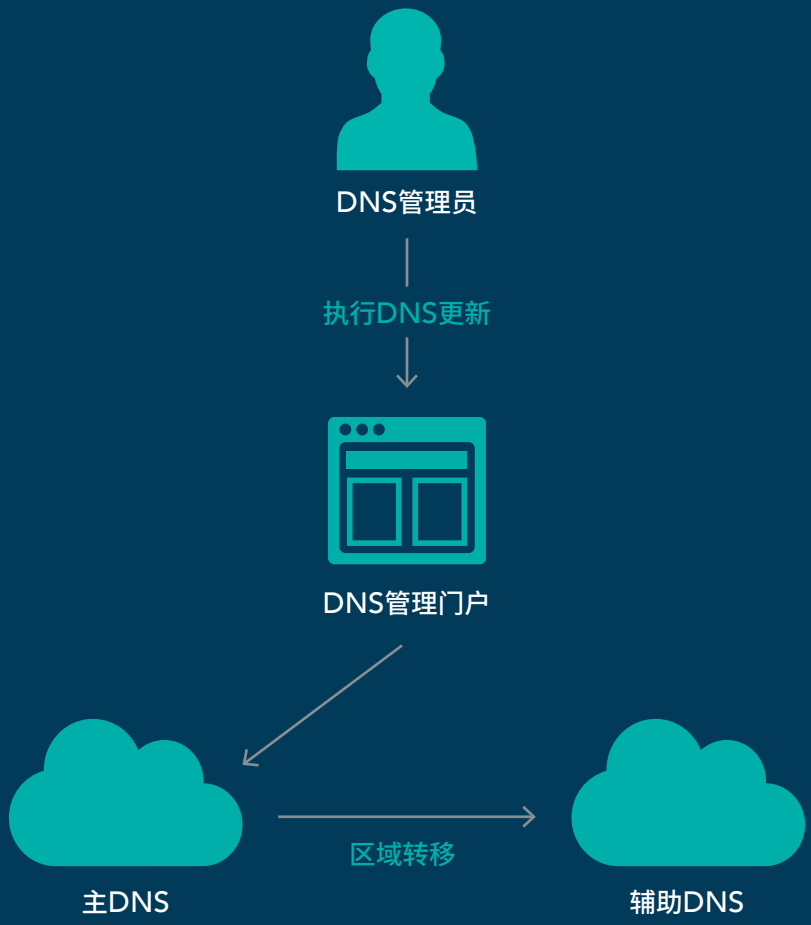
寻找辅助托管DNS服务是增强DNS安全性的第一步。其次是选择一个DNS提供商，为其托管的DNS网络提供专用的内部DDoS缓解服务。随着越来越多的互联设备加入互联网并为更多和更广泛的僵尸网络大军创造潜力，对于组织而言，部署单独的DDoS保护层变得合理。更妙的是，如果您可以“隐藏”DNS，使其不会通过气隙网络直接暴露于互联网，则可以大大减少针对DNS的攻击数量。

权威DNS的增强安全态势包括：

- 主要和辅助的托管DNS服务
- 选择为其DNS网络提供专用内部DDoS缓解服务的提供商
- 隐藏DNS系统以免其直接暴露于互联网的能力

主DNS和辅助DNS的工作方式

1. DNS管理员登录到DNS管理门户
2. DNS管理员更新DNS记录
3. 通过DNS网络更改传播
4. 辅助DNS将收到更新通知，
   并执行区域转移以接收更新的记录



通过受信且安全的合作伙伴加倍打击DNS攻击

俗话说：“您的安全性取决于最薄弱的环节”。请与为您提供所需安全性的提供商合作。CSC是当今市场上极注重安全性的企业级域名、DNS和数字证书提供商。我们执行安全策略以确保系统的安全性，而且我们的员工经验丰富并经过缓解威胁的培训，从而能够全天候保护客户的数字资产。我们安全态势的重要组成部分是选择合适的合作伙伴并与之合作。

CSC之所以与Neustar合作，是因为它是一家企业级提供商，能够提供在当今数字环境下驱动DNS所需的可用性、可扩展性和安全性。Neustar在建立高级DNS安全解决方案方面投入了巨资，以保护组织免受各种类型的威胁。借助我们的域和数字证书管理服务以及CSC安全中心[SM]，CSC可使其客户安全地管理其防火墙外的所有数字资产，这些资产可能受到DNS缓存中毒、域名或DNS劫持、域名阴影以及DDoS、恶意软件和网络钓鱼的威胁。

获取有关CSC安全中心和我们的DNS管理服务如何帮助您缓解网络威胁的更多信息。

CSC通过暴露存在于域名、DNS和数字证书等基本互联网资产中的盲点，为在安全性方面进行重大投资的公司提供支持。。通过利用我们专有的安全解决方案，CSC可使公司数字资产免受网络威胁，避免发生重大经济损失、避免品牌声誉受损，或由于不遵守GDPR之类的政策而受到重大的经济处罚。除了互联网资产，CSC还保护受假冒网站、欺诈行为和知识产权侵权行为侵害的在线品牌，并帮助监控和缓解这种情况，提供相关执法和咨询服务来保护众多全球知名品牌。如需了解更多信息，请访问cscdigitalbrand.services/cn。

cscdigitalbrand.services/cn