CSC

加强DNS安全的6种方法

加强DNS安全的6种方法

域名系统（DNS）从最初单纯的互联网时代到现在变得日益重要。当时，早期的互联网用户主要为政府或教育机构工作，其信任这些机构，甚至完全不会考虑安全性问题。由于在线社区规模很小，互联网的普及率低，因此DNS的重要性尚未得到广泛理解，也没有受到保护。

时至今日，您可以看到由此产生的各种问题。最近的网络攻击突显了不法分子用来拦截和操纵公司合法网络流量、收集凭证或电子邮件地址之类的信息以及实施其他恶意活动（例如网络钓鱼）的特定技术。在某些情况下，不法分子会使用免费的数字证书（验证要求低）来提高欺诈的可信度，使品牌和客户面临的问题更加复杂。消费者对犯罪分子可以访问和窃取其个人信息感到不胜其烦，数据泄露也会损害全球众多公司的声誉，影响公司利润。同时存在的还有分布式拒绝服务（DDos）攻击突然爆发的问题，这种攻击通常旨在通过DNS削弱在线业务。

对于企业而言，其利害关系很简单：没有有效的DNS意味着无法运营网站或开展互联网业务。如果DNS失效，尝试访问网站的客户将无法到达目的地。员工也将无法发送或接收公司的电子邮件。如果公司依靠VoIP拨打和接听电话，则访问将被切断。如果DNS出现故障，公司将不得不使用固定电话和移动设备来联系客户。最后，远程员工无法通过虚拟专用网络访问系统，必然会使公司在急需人手时出现人手短缺。

CSC深知强大安全的DNS基础设施与域名和数字证书管理的结合非常重要，因此选择与NeuStar®合作，该公司运营一个全球最大、最值得信赖的DNS网络20余年，并建议采用六种方法来增强DNS安全。*

**本文档基于Neustar的《Neustar增强DNS安全性的五种方式》编制。*

1 利用多层保护缓解DDoS攻击

批量DDoS攻击的规模已经激增，当今的攻击速度已超过1 Tbps。记录中规模最大的一些攻击主要针对DNS。

针对DNS的DDoS攻击有多种类型

DNS放大是众多攻击方法中的一种。在此攻击中，攻击者利用因特网上大量的开放式DNS服务器，以伪造的目标IP来响应所有小型查询。然后，被攻击目标会接收到更多DNS响应，从而迅速超过网络容量。目的：通过耗尽网络容量来阻止合法的DNS查询。

攻击的另一种常见类型是DNS泛洪，其针对的是托管特定网站的DNS服务器。这些攻击尝试消耗服务器端的资产，例如内存或中央处理器（CPU），并带有大量用户数据报协议（UDP）请求，这些请求是通过在受感染的僵尸网络机器上运行脚本生成的。

多层DDoS保护

为了防御所有类型的DNS攻击，请使用提供多层DDoS保护的解决方案。

DNS节点应配备DDoS缓解设备，以不断监视格式错误的流量以及来自高于正常流量的可疑位置的流量。在许多情况下，缓解只发生在局部。

如果攻击规模特别大，恶意流量会自动重新路由到缓解网络，这是一个完全独立的专用基础设施。这样可以限制对目标名称服务器IP造成任何潜在损害。将影响隔离后，一个全天候的安全运营团队就可以自由采取更积极的对策。

2 通过分段隔离名称服务器

在整个行业中，高度可扩展的DNS已成为一种基于云的服务，拥有成百上千的客户（每位客户都有多个域），这些客户聚集在单个网络上并共享一个名称服务器。

这让您有更多机会去感受别人的痛苦。如果您使用第三方DNS提供商的服务，则其网络上的大多数攻击都不会针对您，而是针对共享由您的提供商分配的名称服务器的域。

隔离DDoS攻击的影响是很明智的选择

选择将DNS网络分成若干段的DNS提供商，每个段都有一个仅由一小部分客户共享的名称服务器公告。由于共享主机名和IP地址的客户减少，因此您感觉到连锁反应的几率大大降低。

这里打个比方，想象一下，在一个有一万人的大厅里，一个人大声尖叫着跳起来，没人能听到他的声音。现在想象同样的情况，但是只有20个人。尖叫的影响便仅限于这20个人。假设该尖叫者是DDoS攻击，则当尖叫（攻击）开始时，名称服务器分段和DDoS缓解策略会立即将整个房间移至隔音区域，移走表现正常的其他成员，然后先使尖叫者闭嘴再把其他人带回来。您可以看到，只有20个人时，受尖叫影响的人更少，更容易找到攻击来源。

无论您还是他人受到攻击，都会受到保护

这种方法使单个名称服务器公告可以从DNS网络迁移到DDoS缓解网络，而不会显著延迟查询解析。您的DNS提供商应该能立即为遭受攻击的人员提供有效的缓解，并防止对仍在DNS网络上的客户产生任何附带影响。

使用云端提供的DNS服务时，位于分段的名称服务器公告上是保护DNS流量的有效方法。

3 使用非开源解析器

DNS解析器（响应域名请求的服务器）用于确保将用户路由到正确的站点。用于管理DNS的最常见的软件应用程序是伯克利因特网名称域（BIND）。1983年，BIND由加利福尼亚大学伯克利分校开发，至今仍然占据全球名称服务器实施方案的绝大部分。目前，BIND的源代码为开源代码，并完全在公共域中，因此很容易被恶意黑客利用和攻击。

避免解析器威胁

CSC之所以选择与Neustar合作，是因为几年前其就解决了这个问题。其开发了专有代码，并委托第三方安全审核员寻找漏洞。其未发现攻击者可以远程利用的漏洞，无论是窃取受限特权还是妨碍目录解析。

除了支持标准的DNS规范和注释请求（RFC），其还改进了解析器，以扩展DNS功能，同时提供额外的冗余和安全性。大多数旧版DNS服务器实施方案永远都无法实现这一点。

4 部署DNS安全扩展（DNSSEC）

当DNS服务器帮助互联网用户找到所需站点时，它们会相互查询。为了加快速度，服务器将结果缓存一段指定的时间。如果在资源记录超时之前存在相同名称的查询，则服务器将提供缓存的答案，而不是查询另一台计算机。

DNS缓存中毒可用于域欺骗攻击

虽然这可以提高效率，但也会引起缓存中毒。当DNS服务器（通常受到犯罪分子攻击）为DNS请求提供错误答案时，就会发生这种情况。用户被引入要求提供个人信息或激活恶意软件的虚假网站。

为什么会这样？在许多情况下，DNS服务器不会验证从其他服务器收到的响应是否与原始查询相关。服务器会缓存不良信息，并将其传递给遭入侵计算机的DNS客户端。

保护的关键是DNSSEC

DNSSEC是一组用于验证DNS响应的安全扩展，利用一系列公钥和私钥组合对信息资源签名，从而实现安全保护。其工作原理是提供一个公钥，让用户的解析器能够确认DNS答案与加密版本匹配。所有事务均已签名，使攻击者无法简单地伪造数据包。

更简单地说，DNSSEC通过防止缓存中毒、域欺骗攻击和其他严重威胁来保护DNS进程。请确保已打开此功能。

DNSSEC采用率

根据我们过去几年的CSC网络安全报告，我们发现在不同行业的大型跨国公司中，DNSSEC的采用率低得惊人，仅介于0%到5%之间。

5 通过专用DNS网络提高弹性

正如一句古老的安全谚语所言，您的总体实力取决于最薄弱的环节。所以，如果您可以通过消除薄弱环节来增强自己的实力，情况是否会有所不同呢？通过减少对公共互联网连接的依赖，私有网络实质上消除了DNS事务的中间也是最危险，且绝大多数DDoS攻击和DNS缓存中毒尝试都发生的部分。请询问您的提供商是否提供此附加服务。

专用网络具有三个主要优点：

更低延迟

在某些情况下，即使DNS正常运行，其他互联网连接问题也可能导致DNS性能下降，从而带来糟糕的用户体验。由于DNS流量无需建立常规的互联网连接，因此专用网络可以提供快速高效的在线体验。

更高安全性

当前使互联网无法访问的DDoS攻击（通过物联网增强）将很快成为过去。提供商网络内用于DNS解析的专用网络可将DDoS攻击和缓存中毒尝试等外部威胁降至最低。

更高可靠性

如果发生DDoS攻击或严重网络中断，查询将继续在部署DNS的专用网络内解析。这种弹性可确保查询网站和其他重要在线资产的用户获得卓越的互联网体验。

6 识别重要数字资产的安全盲点

公司需要能够识别其关键业务域名，并对其进行持续监控以确保它们受到适当的安全保护。

我们发现没有人能帮助公司做到这一点，因此开发了CSC Security Center℠，这是一个智能平台，它可了解重要域名及其所在DNS基础设施中的威胁，并向企业发出风险警告。

这种独特的方法改变了保护域名和DNS的方式，并可帮助公司更好地识别安全盲点。具体而言，CSC安全中心可帮助客户：

识别哪些域名为任务关键型，并需要100%的DNS运行时间保证

识别当前所有的DNS提供商并评估与厂商相关的任何安全风险

识别任何缺失的安全功能（这种缺失会增加DNS缓存中毒、域名或DNS劫持、域名阴影、DDoS和网络钓鱼的风险）。

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