利用新的 DNS 缺陷
黑客能够发起大规模 DDoS 攻击

（2020-5-21）

以色列的网络安全研究人员披露了有关影响 DNS 协议的新缺陷的详细信息，该缺陷可被利用来发起放大的大规模分布式拒绝服务（DDoS）攻击，以使所针对的目标网站崩溃。

被称为 NXNSAttack 的攻击，利用 DNS 委派机制的缺陷，迫使域名递归解析服务器向攻击者针对的权威服务器发出更多 DNS 查询，从而通过激活大规模的僵尸网络可能导致在线服务中断。

安全研究人员发现：在典型的域名解析过程中，交换的 DNS 消息数量较之实际的需求高得多，主要表现为对具体域名服务器 IP 地址的主动域名解析请求的并发访问数量。

安全研究人员证明：这种行为模式造成域名解析服务的瓶颈，可能用于对递归域名解析服务器器和域名权威服务器发起毁灭性的攻击。

在 NXNSAttack 攻击模式被披露后，运营互联网基础设施（提供域名解析服务）的主要公司，包括 PowerDNS（补丁 CVE-2020-10995），CZ.NIC（补丁 CVE-2020-12667），Cloudflare，谷歌，亚马逊，微软，甲骨文（Dyn），Verisign 和 IBM Quad9，已对其软件进行了修补，以解决该缺陷（或漏洞）。

NXNSAttack 攻击模式

当客户端欲查询与域名关联的 IP 地址（例如，www.google.com），通过域名递归解析服务器与多个授权域名服务器按层次结构顺序迭代通信，并将域名解析结果返回给客户端。

域名递归解析服务通常是客户所属的运营商（ISP）隐式提供，或是公共 DNS 服务器，如 Cloudflare（1.1.1.1）或 Google（8.8.8.8），取决于客户端配置。

如果域名递归解析服务未保存（或无法找到）客户端查询域名的 IP 地址，则将请求传递给授权域名解析服务器，并委托进行层次结构顺序的迭代通信。

这个分层域名解析过程直至提供所查询域名的 IP 地址，使得客户端的用户能够访问相应的网站。

安全研究人员发现，利用大量且并非实际需要的域名查询请求可以欺骗域名递归解析服务器，迫使其不断地将大量数据包发送到目标域，而不是合法的授权域名服务器。

为此，攻击者必须拥有一台权威域名解析服务器，而通过购买一个域名就可以轻松实现。这样，攻击者可以冒充权威域名服务器，并伪装响应对域名的查询。

NXNSAttack 的攻击原理是，向易受攻击的域名递归解析服务器发送被攻击者控制的域名（例如"attacker.com"）查询请求，该服务器会将域名查询转发到攻击者控制的权威服务器（图 1）。

攻击者控制的权威服务器响应域名查询的返回结果，是已被控制的虚假服务器或子域名，而指向被攻击受害者的域名。

然后，虚假服务器将域名查询请求转发到所有不存在的子域，从而导致受害者站点的流量激增。

已经证明，这种放大攻击可以使域名递归解析服务器交换的数据包数增加1,620 倍，不仅使得域名递归解析服务器无法处理正常的域名查询请求，而且过量（放大）的虚假域名查询请求造成目标域被“淹没”（泛洪攻击），而崩溃（图 2）。

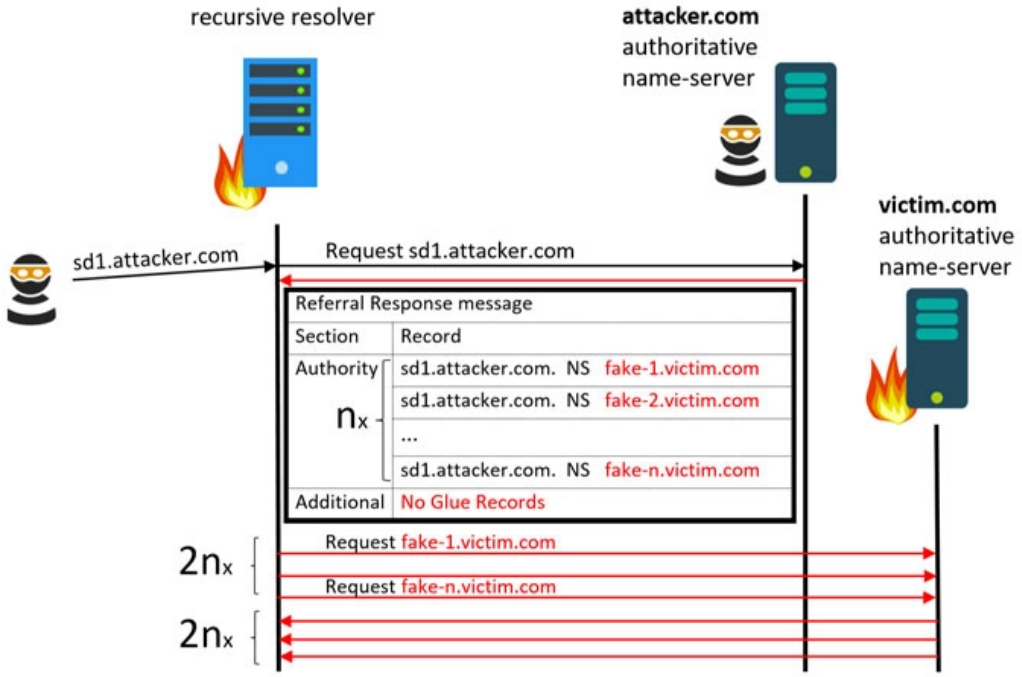
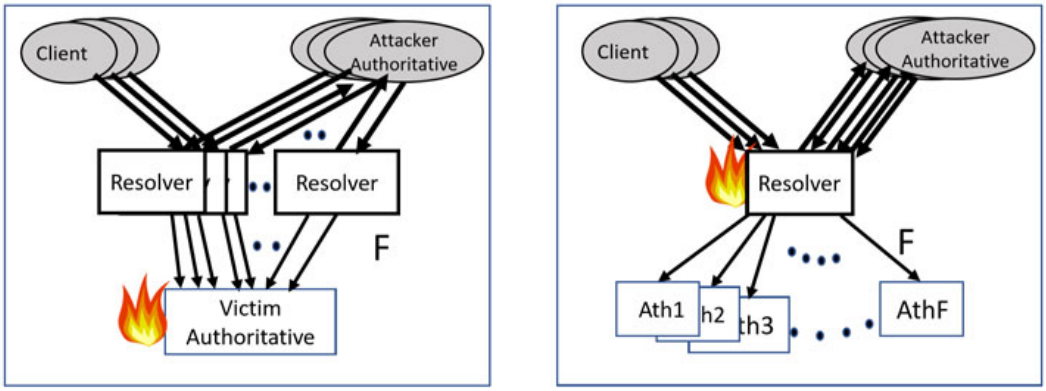


图 1 NXNSAttack 攻击模式



NXNSAttack targeting the authoritative server (a) and the recursive resolver (b)

图 2 NXNSAttack 攻击造成的“双效应”

（a） 攻击权威域名和目标域

（b） 域名递归服务器被拥塞

而且，使用 Mirai 等僵尸网络，可以进一步扩大攻击范围。

安全研究人员指出，事实上，由攻击者控制以及获取大量客户和大量权威域名服务器，既容易又便宜（代价小）。

安全研究人员强调，研究的最初目标是分析域名递归解析服务器的效率及其在不同攻击模式下的性能。但是，发现了一个新的，而且极其高危的缺陷或漏洞，即 NXNSAttack。

新 NXNSAttack 攻击的关键要素是 ：

（1）拥有或控制权威名称服务器的便利性，

（2）向域名递归解析服务器请求不存在的域名查询，

（3）以放大的域名请求泛洪破坏 DNS 结构中的容错机制及快速响应的能力。

强烈建议：网络管理员将其域名解析服务器的软件更新到最新版本。

备注：互联网系统联盟（ISC）的 DNS 软件 BIND 是“事实上的标准”（de facto standard）。目前发布的版本：

版本	状态	发布时间	停止维护时间
9.17.1	开发	2020-4	待定
9.16.3	目前稳定	2020-5	待定
9.14.12	即将停止维护	2020-5	2020-5
9.11.19	目前稳定	2020-5	2021-12

此外，请注意，目前第二次 DNS“执行日”（Flag Day）正在进行测试，重点是强制性支持 DNS 查询请求的 TCP 传输模式，因而 DNS 解析服务软件和系统设置将有重大改变。