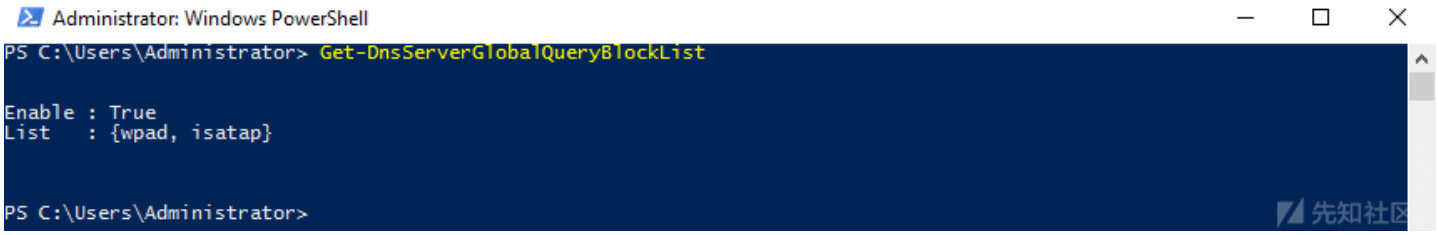
ADIDNS 安全研究：绕过 GQBL 限制解析 WPAD 域名

angel010 / 2018-12-14 15:46:00 / 浏览数 3216 技术文章 翻译文章 顶(0) 踩(0)

2018年6月，作者发布了如何利用adidns的文章，文章主要涵盖攻击和防御的相关技术。本文分析另一个与域名解析有关的默认设置问题。

WPAD

Web Proxy Auto-Discovery (WPAD，web代理自动发现)是LLMNR（链路本地多播名称解析）和NBNS（网络基本输入/输出系统 (NetBIOS) 名称服务器）欺骗的常见目标。WPAD是通过ADIDNS增加的最明显的记录。认证的用户可以增加这一记录，因为它默认是不存在的。如果用户为WPAD增加了记录，就可以 query block list,GQBL）中默认含有WPAD和ISATAP。

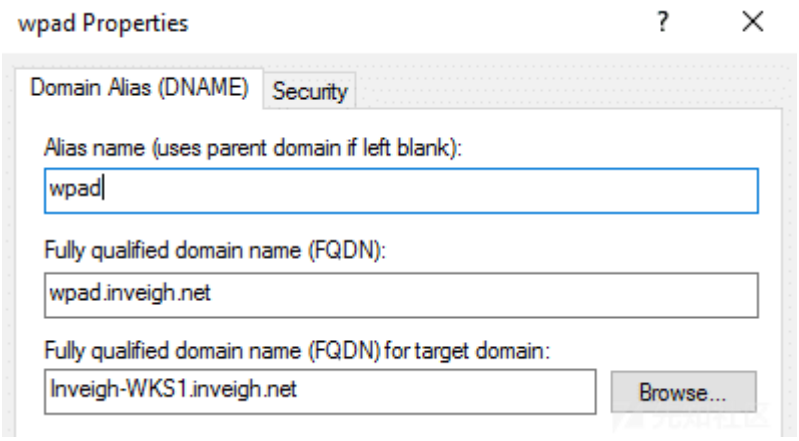


主流的Windows DNS服务器不会应答与GQBL中主机列表匹配的域名查询。所以，GQBL经常是不工作的。

绕过GQBL

研究人员在测试wildcard record（通配符记录）中发现，Windows DNS服务器会忽略GQBL并通过通配符应答WPAD的请求。研究人员只通过动态更新来增加记录。因为*字符在动态更新中并不能准确工作，所以研究人员决定找一个可以与

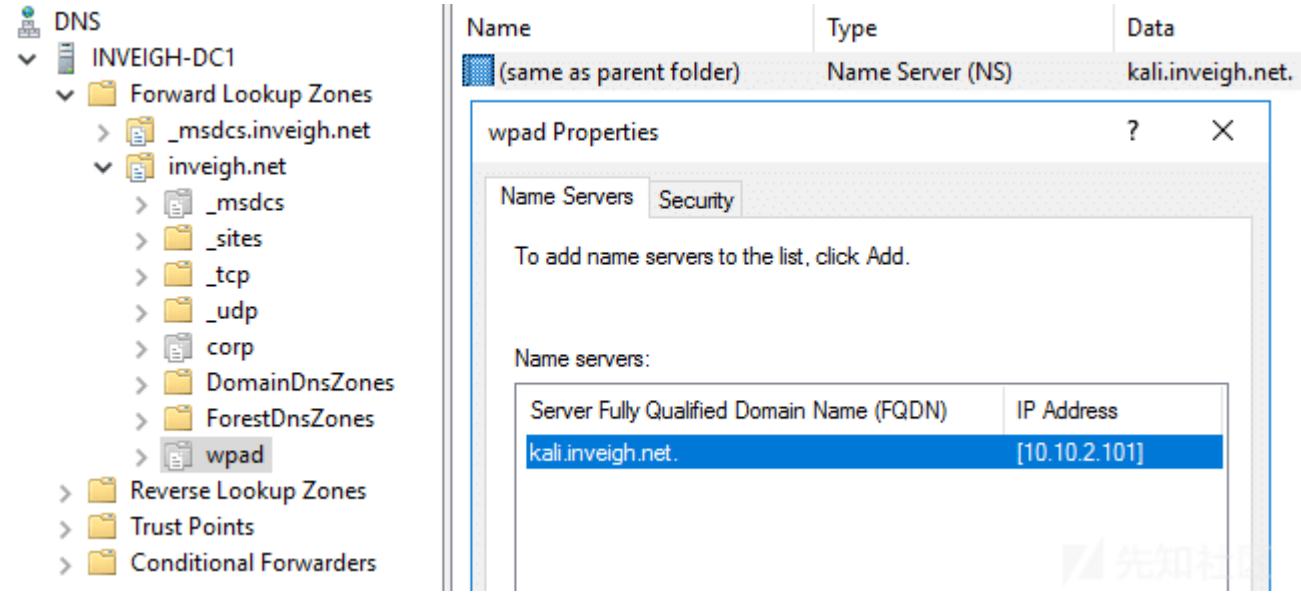
第一个方法就是通过DNAME记录。如果有WPAD的DNAME记录，Windows DNS服务器会解析WPAD。



一般情况下，DNAME记录并不会解析与真实记录匹配的请求。DNS服务器只会应答与主机映射的域名的请求，比如`host.wpad.inveigh.net`。在这个例子中，`wpad.in`

但研究人员发现Windows DNS服务器在满足特定条件的情况下会应答DNAME记录根的请求。记录需要与GQBL列表中的主机相匹配，而GQBL需要开启。考虑到WPAD，默认开启的GQBL会让情况变

但DNAME记录还是不能动态更新。所以研究人员尝试寻找其他的方法，即在WPAD子域名中添加NS记录。

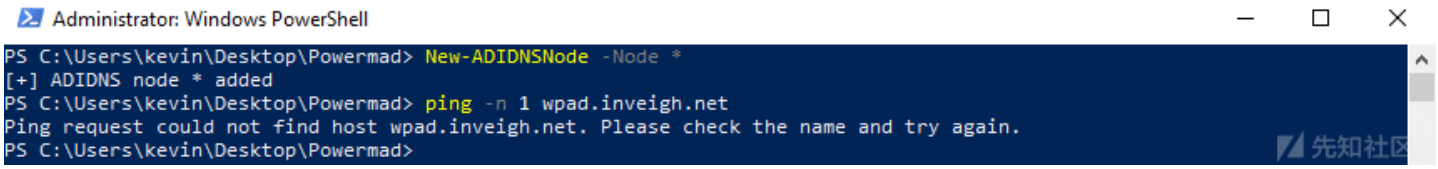


该方法稍微有点复杂，因为它需要NS记录指向研究人员控制的DNS服务器。Kali系统中的DNSchef是一种简单的设置DNS服务器来提供应答接收的请求的方法。

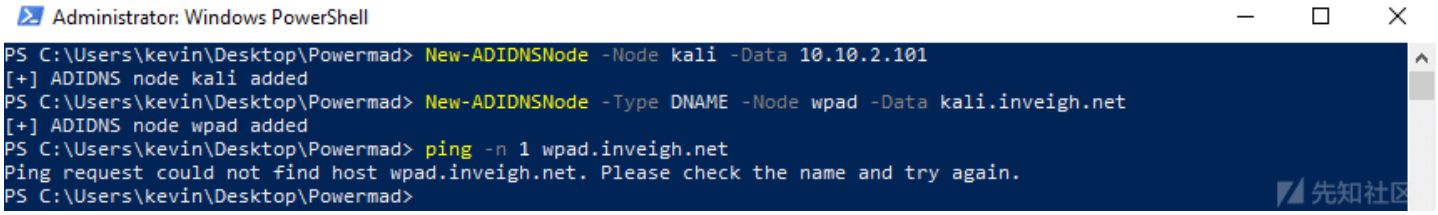
但这种方法也不能动态更新。这三种方法实现过程都有点复杂。

CVE-2018-8320

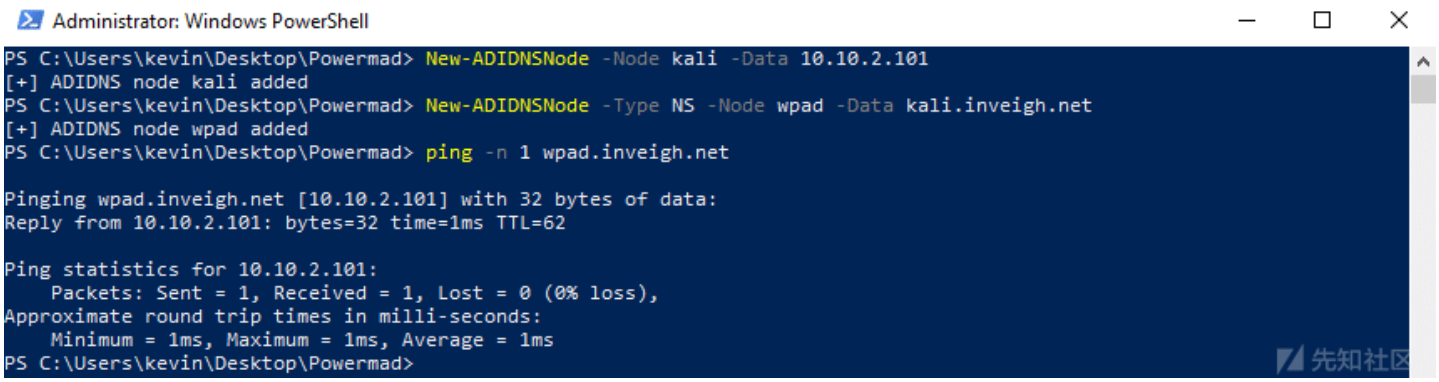
研究人员将三种GQBL绕过的方法通告给了微软，微软为该GQBL漏洞分配CVE编号为CVE-2018-8320。



通配符记录不再解析GQBL列表中主机的请求。



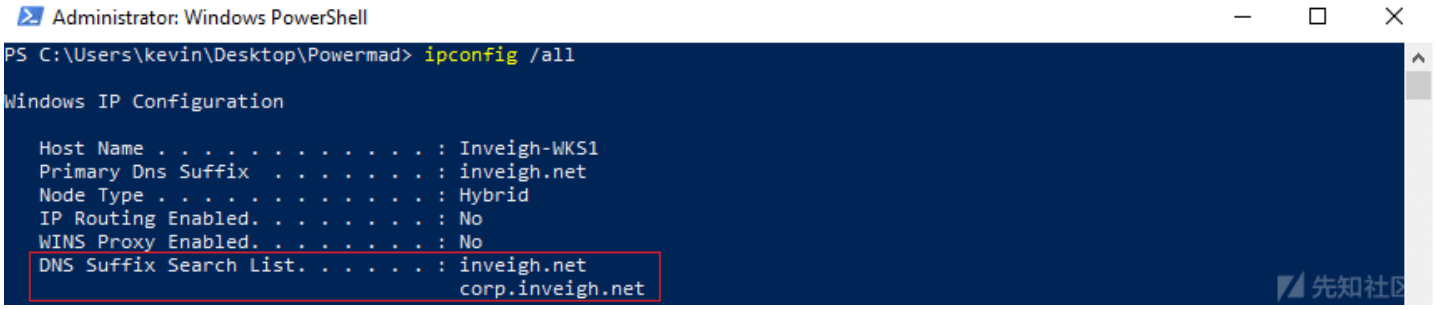
DNAME记录不再解析GQBL列表中主机的请求。



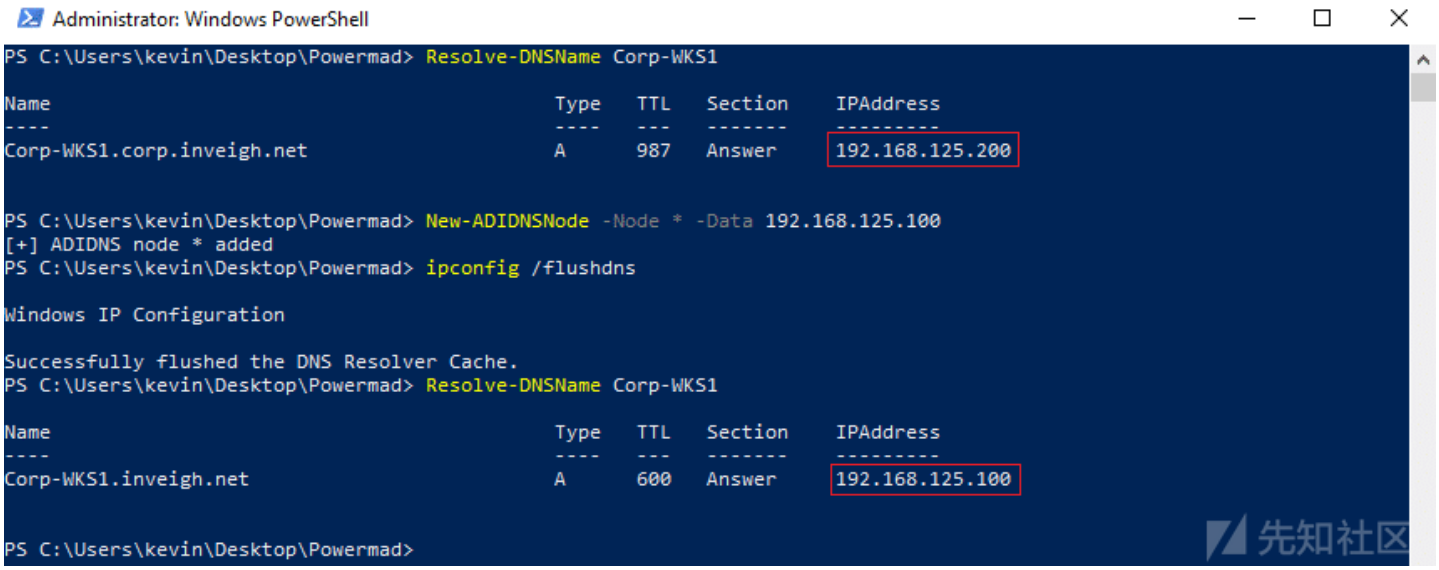
NS记录仍然可以绕过GQBL。

域名后缀搜索顺序

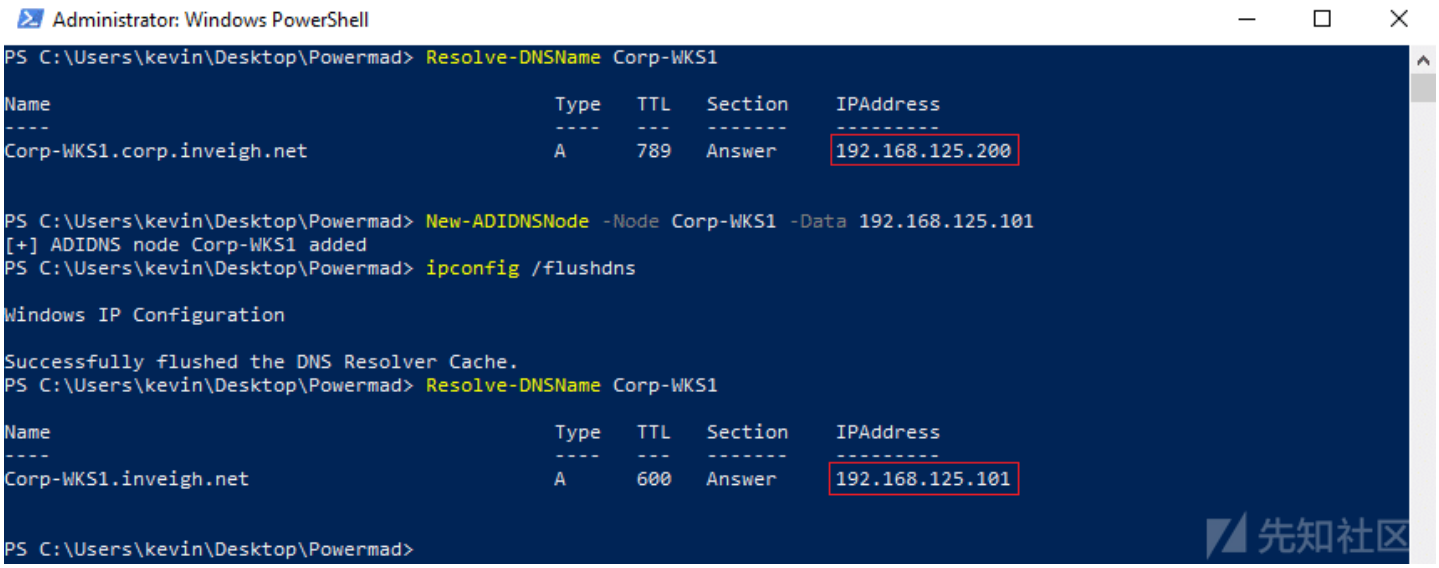
研究人员推荐管理员控制的通配符记录作为防御ADIDNS通配符攻击和LLMNR/NBNS欺骗的方法。许多研究人员指出当多个域名后缀通过组策略被分配给搜索列表时，通配



在进行了一些测试后，研究人员确认他们是对的。当匹配的有效记录存在时，更高域名后缀区域的通配符可以防止有效的非完全适当的请求降到较低的域名后缀中。



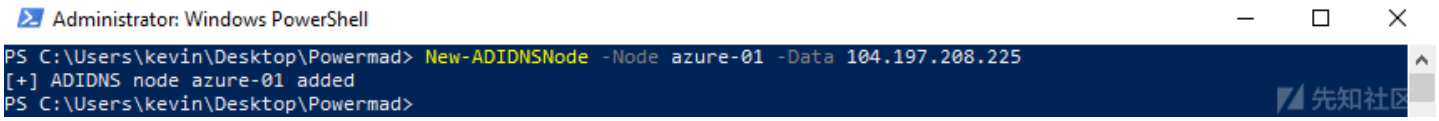
这一行为导致了一种全新的攻击方法，即攻击请求已有记录的请求。如果可以在zone中增加记录作为后缀，那么就可以在低优先级的域名后缀中攻击有效的主机。对目标主



DNS后缀在执行通配符攻击时会被考虑到。如果找到一条有多个DNS后缀的搜索列表，通配符攻击可以导致注入失败。

通过钓鱼进行ADIDNS攻击

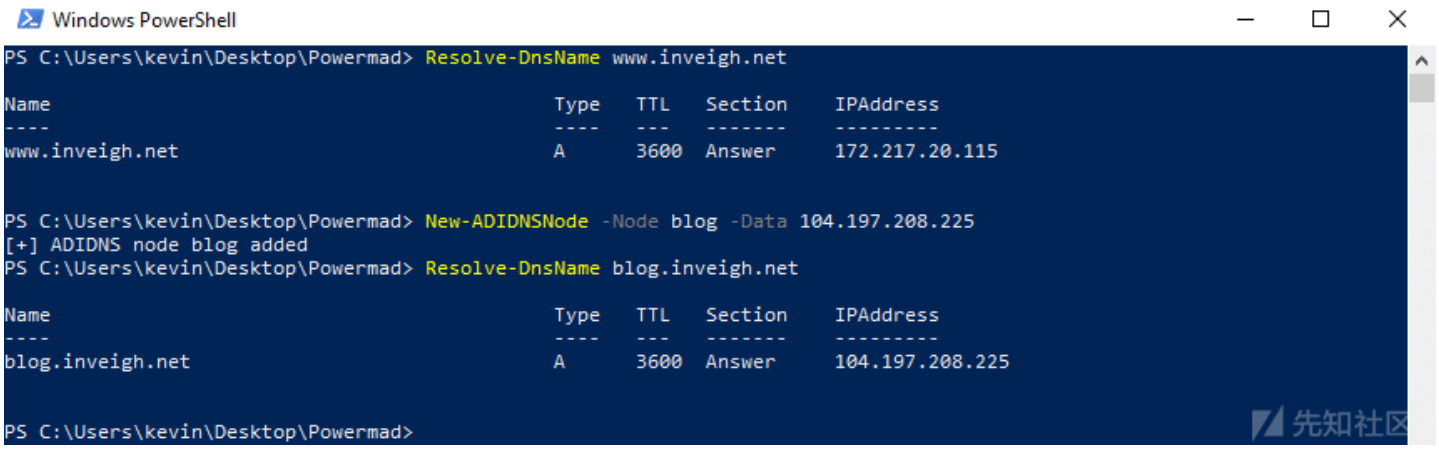
研究人员认为ADIDNS攻击很容易通过钓鱼攻击进行传播。只有一个AD连接的钓鱼目标需要执行payload来增加记录，该记录可以发送流量到远程攻击者控制的系统中。这



上面是用powershell工具增加指向公有IP的记录的例子。对于真实的钓鱼攻击，可以使用更加合适的payload。
这是另一个NS记录用于攻击的例子。一旦设置了NS记录，可以通过自己的DNS服务器来增加额外的记录到受控的子域名中。

Domain Borrowing

当企业的内部AD域名与其公有域名匹配时，来自边界外的ADIDNS攻击就显得更有意思了。在该攻击场景中，用户可以使用公有域名的可信来进行内容过滤。



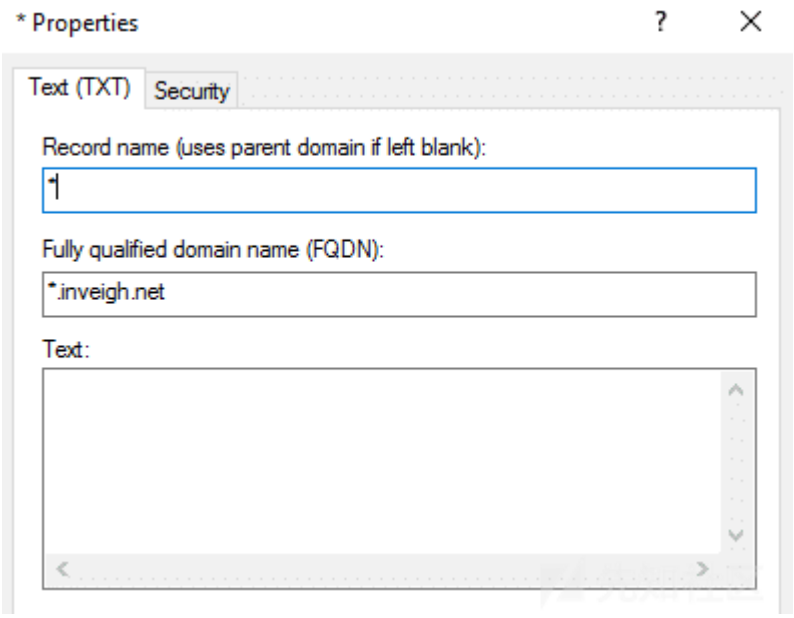
但这也有一定的限制，就是只能影响使用目标ADIDNS作域名解析的资源。但是在设置HTTPS的可信证书方面会比较麻烦。

C2和数据窃取技术

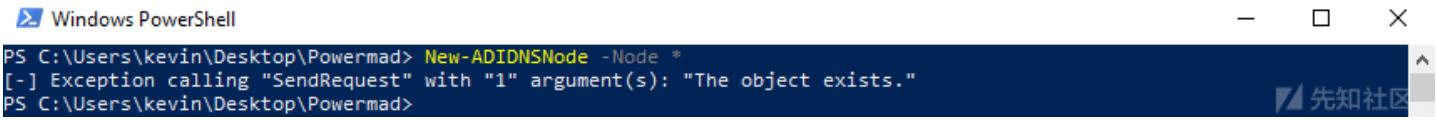
文章Command and Control Using Active Directory中提到可以将AD用作C2信道。那么ADIDNS可以吗？当增加了dnsNode对象后，认证的用户从创建开始就会得到完全的控制。dnsNode对象也含有大量可写的属

ADIDNS防御

前面提到，如果用户使用含有多个DNS后缀的搜索列表，管理员控制的通配符A记录可能会带来一些问题。作为一个备选方法，用户可以无法解析域名请求的记录类型来创建



因为所有的记录类型都保存在dnsNode对象中，增加任意形式的通配符记录可以防止非授权用户增加名为*的dnsNode。但非解析的通配符记录无法作为应对LLMNR和NBN



锁定zone权限是缓解认证用户ADIDNS攻击的最彻底的方法。根据设置，用户可能可以利用DHCP中的特定DNS动态更新账户。这允许用户移除Authenticated Users的Create all child objects权限。

许多域名解析攻击都是通过非完全有效的域名请求进行的。这类用户生成的请求很难消除。
https://blog.netspi.com/adidns-revisited/

上一篇：AWD二进制运维工具-AutoAW... 下一篇：手机ClickFraud应用的安全...

1. 0 条回复
   - 动动手指，沙发就是你的了！