# 论文简介

## 论文题目

MitM Attack by Name Collision：Cause Analysis and Vulnerability Assessment in the New gTLD Era

## 背景

* DNS系统
  + 域名管理和授权：DNS根区的结构和内容由Internet Assigned Numbers Authority (IANA)决定，实际的域名管理和维护由Root Zone Maintainer (RZM)负责
  + 域名注册：二级域名（SLD）注册过程由三个角色参与，顶级域（TLD）注册表操作员、注册服务商和注册者。注册者申请注册，注册服务商将信息提供给TLD注册表操作员，由他在WHOIS数据库中添加相应记录
  + 域名解析：一般由网络提供商提供，解析器查询DNS域标签层次结构后的名称服务器，获取相应的IP地址或NXDomain响应
  + The New gTLD Program：新通用顶级域计划，为了增强竞争和增多消费者选择，ICANN启动了新通用顶级域计划，在2015/08/25前的不到2年的时间内，超过700个新的通用顶级域域名被授权。
* 内部DNS名称空间

内部DNS名称空间（Internal DNS Namespace）有助于控制对内部机密信息的访问，并且可以在任何外部网络连接中断的情况下运行，是很多公司的常见做法。

要创建内部DNS名称空间，内部名称服务器需要提供定制的内部域区域文件，并且解析器配置为查询这些内部服务器，而不是公共名称空间中的DNS服务器。

为了方便起见，管理员在配置内部域时采用的是那些未被授权的公共名称空间中的TLD字符串，他们当时默认这些TLD永远不会被授权。

* WPAD (Web Proxy Auto-Discovery)

WPAD是为浏览器和操作系统设计的自动发现web代理配置文件的协议，使代理服务器相对于用户来说是透明的。代理服务器主要用来连接Internet（互联网）和Intranet（内部网络）。默认的WAPD配置文件名为wpad.dat，采用proxy auto-config（PAC）格式编写，用PROXY （IP）：（port）指定代理服务器的IP和端口。

WPAD 可以借助 DNS 服务器或 DHCP 服务器来查询代理自动配置(PAC)文件的位置。如果本地DHCP支持WPAD，可以通过向其发送DHCPINFORM消息获取代理配置文件；否则只能采用DNS WPAD，浏览器通过域名形式获取服务器中的wpad.dat文件。

常用的浏览器和操作系统都支持WAPD，有些甚至将WPAD设置为默认配置。表1列举了已知的浏览器和操作系统支持的版本，以及是否为默认配置。

表1 支持WPAD的常见浏览器和操作系统

|  |  |  |  |
| --- | --- | --- | --- |
| Supported OSes | | Verified versions | Enabled |
| and browsers | | for DNS WPAD | by default |
| Browser | Internet Explorer | 6–11 | Yes |
| Chrome | 43 | No |
| Firefox | 12, 33 | No |
| Safari | 8 | No |
| OS | Windows OS | XP, Vista, 7, 8, 8.1, 10 | Yes |
| Ubuntu | 12.04, 14.04 | No |
| Mac OS X | 10.10 | No |

## 威胁和漏洞

* 攻击原理

如图1所示，由于内部DNS名称空间泄露，造成内部DNS域名和Internet的DNS域名冲突。当用户在内部网络之外使用终端设备时，由于终端配置的原因，终端会尝试获取WPAD配置文件，由于以前在内部网络使用的TLD在Internet中是非法的，所以DNS根服务器会返回NXD消息以说明找不到相关DNS查询记录，而随着新通用顶级域计划的实行，这些内部网络域在Internet中得到授权，因此攻击者可以通过简单的注册相应的域名，使受害终端得到攻击者提供的代理配置文件，从而受害终端将通过攻击者的代理服务器访问外部网络，攻击者可以监听流量获取机密信息，甚至篡改流量。

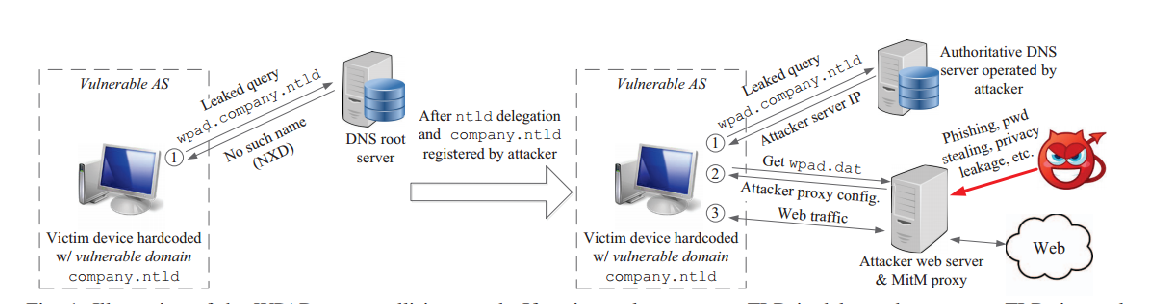


图1 基于名称冲突的中间人攻击过程

* 攻击严重性

由于很多浏览器采用了WPAD协议，而且是在浏览器启动时就自动开启的，所以这一中间人攻击具有很高的隐蔽性，而且攻击过程中的DNS请求和查询都是合法的，所以不需要伪装，同样可以欺骗DNSSEC。

另外，攻击者并不需要猜测那些易受攻击的脆弱域，这完全可以通过嗅探本地网络的查询记录和分析一些权威机构收集的DNS查询的流量获得。

* 造成域名冲突原因

由于新通用顶级域计划，原本默认不会被授权的在内部DNS名称空间使用的域名现在被授权可以在公共DNS名称空间使用，并且由于用户终端的配置问题，内部DNS名称空间查询被泄露到了公共DNS系统中，从而造成了域名冲突。

* 内部DNS名称空间泄露原因

通过DNS根服务器的流量分析得出，造成内部DNS名称空间查询泄露的主要源头是家用网络，表2展示了美国泄露查询最多的12个自制域的类型，这12个自制域泄露了85%的内部DNS查询，其中的12个是家用网络，还有两个是类家用网络。表3是表2的A1自制域的泄露查询类型，可以看出在家用网络中泄露的域名后缀基本都是公司网络的而不是家用网络的。

表2 美国泄露查询最多的12个自制域

|  |  |
| --- | --- |
| AS code name | Home access network related |
| A1 | Yes |
| A2 | Yes |
| A3 | Yes |
| A4 | Likely |
| A5 | Yes |
| A6 | Yes |
| A7 | Likely |
| A8 | Yes |
| A9 | Yes |
| A10 | Yes |
| A11 | Yes |
| A12 | Yes |

表3 泄露最多的域名后缀

|  |  |  |  |
| --- | --- | --- | --- |
| Domian suffix string | Query% | Home network related | Corporate network related |
| (defense contractor) .master. | 0.28 | No | Unclear |
| corp.local. | 0.26 | No | Yes |
| (marketing).local. | 0.22 | No | Yes |
| root.local. | 0.21 | Unclear | Unclear |
| (manufacture).inc. | 0.15 | No | Yes |
| (town name).local. | 0.14 | No | Yes |
| prod.dca. | 0.13 | No | Yes |
| (consulting).local. | 0.13 | No | Yes |
| us.local. | 0.13 | Unclear | Unclear |
| (real estate).local. | 0.12 | No | Yes |
| (computer).lan. | 0.11 | No | Yes |
| (bank).ubc | 0.11 | No | Yes |
| datacenters.ww. | 0.11 | No | Yes |
| (marketing).intraxa.. | 0.10 | No | Yes |
| Root.corp. | 0.09 | No | Yes |

由此可以假设造成内部DNS查询泄露的原因是在外部网络进行内部DNS查询，如在公司使用公司内部网络的DNS系统，而回到家后继续使用这种配置，就会将公司内部网络DNS名称空间查询泄露到公共网络的DNS系统中。

本文通过实验验证了这种可能性，实验通过在宿主主机中开启一些主流的操作系统，并提供了三种网络环境，其中两种是不同域名后缀的DHCP网络，第三种是蜂窝网络的共享网络，结果发现这些主流操作系统在网络配置方面存在的漏洞如表4所示，这些漏洞造成设备错误地在外部网络执行内部DNS查询。第一个漏洞是在windows下手动配置计算机的域，这一配置将会覆盖DHCP的配置，从而在外部网络依然执行内部的DNS查询，这一漏洞在每个Windows版本中都存在。第二个漏洞是域搜索列表的配置，如果列表中公司内部网络的域后缀在前，则会先被查询，这也会造成查询泄露，这一漏洞在Window，Mac OS和Ubuntu中都存在。第三个漏洞是针对Windowss Vista，实验发现当从一个域配置网络切换到没有域配置的网络时，域不会被重置，所以当使用Windows Vista的计算机连接到外部网络时可能就会造成内部查询泄露。

表4 主流操作系统在网络配置方面的漏洞

|  |  |
| --- | --- |
| OS configuration | Affected OSes |
| Set Windows PC domain | Windows XP/Vista/7/8/8.1/10 |
| Hardcode domain search list | Windows XP/Vista/7/8/8.1/10, Mac OS X, Ubuntu 12.04 |
| Change from a network with domain to a network without domain | Windows Vista |

## 攻击效果

到本文发表前为止，还没有切实的证据表明这种攻击的存在，但是确实发现了一些可疑的注册行为。本文指出了这种攻击的潜在威胁，并呼吁建立一套主动防御体系来防御这种攻击。

图2显示了A和J根服务器在2015/1到2015/7间发出的NXD流量，可以看出WPAD协议的查询量排在第4位，图3显示这些WPAD协议查询的NDX响应中的流行的新顶级域，可以看到有大量的终端的WPAD协议在查询这些新顶级域的子域，这就使得这种攻击存在潜在的可能性和风险性。

本文定义了高度脆弱域概念（HVDs），HVDs具有两个特点：高持续性，即被频繁查询的域名；高查询量，即被大量用户查询的域名。调查发现已经有10%的高度脆弱域名被注册，这使得这种攻击随时都有可能发生。

0

1e+07

2e+07

3e+07

4e+07

5e+07

6e+07

7e+07

www

10

\_ldap

wpad

b

lb

db

r

dr

isatap

venueproxy

\_kerberos

0

1

2

3

4

5

Average daily query #

Average daily query %

图2 首标签的NDX查询

0

5000

10000

15000

20000

25000

30000

35000

40000

45000

.global

.ads

.group

.network

.dev

.office

.prod

.hsbc

.win

.world

.one

.sap

.site

0

0.05

0.1

0.15

0.2

0.25

0.3

0.35

0.4

Average daily query #

Average daily query %

图3 WPAD协议的新gTLDs的NDX查询

* 防御措施

本文从三个方面给出了推荐的防御策略，以及预估的有效性和部署难度。

* 从新的通用顶级域注册角度看，本文给出的建议是对那些高度脆弱域的注册进行审查，一种简单的方法是禁止高度脆弱域的子域注册，但是这在实施上难度很大，因为对于一个新的顶级域平均需要阻止7449.3次注册，处理量很大。
* 从自制域角度看，由于大多数的查询泄露来自极少数的自制域，所以在这些自制域内可以设置一个黑名单，这些黑名单中记录的是高度脆弱域，在收到查询请求时过滤掉这些高度脆弱域的请求，从而达到阻止查询泄露的目的，图4显示当有大量的自制域设置了黑名单确实可以有效地阻止查询泄露，可以看出当自制域超过500时，过滤的WPAD查询超过了80%。
* 从终端用户角度，本文提出造成内部查询泄露的主要原因是终端设备的配置问题，因此作者提出如果不在内部网络中使用WPAD协议则禁用WPAD服务；另外公司或其他团体应该停止对计算机设备进行硬编码，如禁止手动配置PC domain，以及更新操作系统；最后，作者建议设计一个操作系统级别的守护进程，以根据网络环境来过滤查询，这将是一个长远的防御手段，但是实现难度也是最大的。

0

20

40

60

80

100

0

2000

4000

6000

8000

10000

Filtered WPAD query % CDF

0

20

40

60

80

100

0

100

200

300

400

500

图4 增加黑名单后的过滤的WPAD查询