DNS篡改/劫持攻击检测调研报告

学号：2019e8018661041 姓名：李侗格

一、DNS篡改/劫持

DNS篡改/劫持/重定向（以下均称为DNS劫持），是一种DNS攻击类型，在这种攻击中，DNS查询被错误解析，以实现用户无法访问目标网站或将用户重定向到恶意站点的目的。

为了实现DNS劫持，攻击者要么在用户计算机上安装恶意软件，接管路由器，要么拦截或侵入DNS服务器。DNS劫持可用于广告的投放(攻击者通常显示不需要的广告以产生收入)或网络钓鱼(显示用户访问的网站的虚假版本并窃取用户数据或凭据)。除了恶意攻击者，许多互联网服务提供商(ISP)会使用DNS劫持，来接管用户的DNS请求，用于收集统计数据，或返回广告。一些政府也会利用DNS劫持进行审查，将用户重定向到政府授权的网站。

DNS劫持或DNS重定向有四种基本类型[3]：

（1）本地DNS劫持-攻击者在用户的计算机上安装特洛伊木马恶意软件，并更改本地DNS设置以将用户重定向到恶意站点。

（2）路由器DNS劫持-许多路由器存在默认密码或固件漏洞。攻击者可以接管路由器并覆盖DNS设置，从而影响连接到该路由器的所有用户。

（3）中间人DNS攻击-攻击者拦截用户和DNS服务器之间的通信，修改或构造虚假的DNS响应，以使用户法访问目标网站或将用户重定向到恶意站点。

TCP/IP体系通过序列号等多种方式避免仿冒数据的插入，但入侵者如果通过监听客户端和DNS服务器的对话，就可以猜测服务器响应给客户端的DNS查询ID。攻击者可以通过推测到的ID来构造虚假的DNS响应数据包。攻击者在DNS服务器之前将虚假的响应交给用户，从而欺骗客户端去访问恶意的网站。假设当提交给某个域名服务器的域名解析请求的DNS报文包数据被截获，然后按截获者的意图将一个虚假的IP地址作为应答信息返回给请求者。原始请求者就会把这个虚假的IP地址作为它所要请求的域名而进行访问，这样他就被欺骗到了别处而无妨连接想要访问的那个域名

（4）更改DNS服务器记录-攻击者可以入侵DNS服务器，并更改DNS记录以将DNS请求重定向到恶意站点。

在这里介绍一种更改DNS服务器记录的实现方式：使用域名劫持技术，通过冒充原域名以E-MAIL方式修改公司的注册域名记录，或将域名转让到其他组织，通过修改注册信息后在所指定的DNS服务器加进该域名记录，让原域名指向另一IP的服务器，让多数网民无法正确访问，从而使得某些用户直接访问到了恶意用户所指定的域名地址，其实施步骤如下[1]：

步骤（1）：获取劫持域名注册信息：首先攻击者会访问域名查询站点，通过MAKECHANGES功能，输入要查询的域名以取得该域名注册信息。

步骤（2）：控制该域名的E-MAIL帐号：此时攻击者会利用社会工程学或暴力破解学进行该E-MAIL密码破解，有能力的攻击者将直接对该E-MAIL进行入侵行为，以获取所需信息。

步骤（3）：修改注册信息：当攻击者破获了E-MAIL后，会利用相关的MAKECHANGES功能修改该域名的注册信息，包括拥有者信息，DNS服务器信息等。

步骤（4）：使用E-MAIL收发确认函：此时的攻击者会在信件帐号的真正拥有者之前，截获网络公司回馈的网络确认注册信息更改件，并进行回件确认，随后网络公司将再次回馈成功修改信件，此时攻击者成功劫持域名。

二、DNS劫持的现状

2.1.DNS安全事件

2.1.1.DNSpionage[2]

2018年11月27日，思科的Talos研究部门发表了一篇文章，概述了一场被称为“DNSpionage”的复杂网络间谍活动的轮廓。Talos说，DNSpionage的肇事者能够通过劫持这些目标的DNS服务器，从黎巴嫩和阿联酋的一些政府和私营部门实体窃取电子邮件和其他登录凭据，以便将所有电子邮件和虚拟专用网(VPN)流量重定向到攻击者控制的互联网地址。这些DNS劫持还为攻击者获取目标域的SSL加密证书铺平了道路，这使得他们能够解密截获的电子邮件和VPN凭据，并以明文形式查看它们。2019年1月9日，安全供应商FireEye发布了其报告“全球DNS劫持运动：大规模的DNS记录操纵”，该报告对间谍活动的“如何”进行了更多的技术细节。大约在FireEye报告的同时，美国国土安全部(Department Of Home land Security)发布了一项罕见的紧急指令，命令所有美国联邦文职机构保护其互联网域名记录的登录凭据。作为这项任务的一部分，国土安全部公布了DNSpionage活动中使用的域名和互联网地址的简短列表。2019年1月25日安全公司Crowd Strike发布了一篇博客文章，列出了到目前为止间谍活动使用的几乎每个已知的互联网地址(Ab)。

DNSpionage攻击损害了包括阿尔巴尼亚、塞浦路斯、埃及、伊拉克、约旦、科威特、黎巴嫩、利比亚、沙特阿拉伯和阿拉伯联合酋长国在内的50多家中东公司和政府机构的DNS基础设施。这些攻击归咎于伊朗的国家行为，在攻击进行前，一些注册商和DNS服务器的登录信息被泄露。

此次的攻击使用了三种不同的方法来实施DNS劫持攻击。

第一个攻击涉及攻击者使用先前泄露的凭据登录到DNS提供商的管理面板，更改DNSA记录以劫持流量。

第二种形式的攻击使用类似的方法登录到管理面板，但这次会访问受害者的域名注册商帐户，并更改DNSNS记录以劫持流量。

第三种形式是将两者相结合，实现DNS重定向攻击。

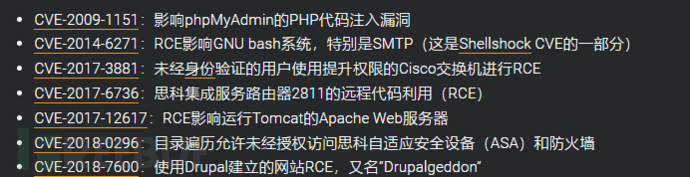
2.1.2.sea turtle[9]

思科Talos团队安全研究人员发现一起针对中东和北非地区的DNS劫持攻击活动，Talos将其幕后组织命名为"海龟"(sea turtle)。该攻击活动最早于2017年1月开始，并持续到2019年第一季度。至少有来自13个不同国家的40个不同组织遭到入侵。

Talos确定了40多个受害者。受害者组织大致分为两类。第一组受害者，我们称之为主要受害者，几乎完全位于中东和北非。这类受害者主要包括如下领域：外交部、军事组织、情报机构、著名的能源组织。第二组受害组织可能会受到攻击，以帮助实现对主要目标的攻击。这些组织遍布世界各地;然而，他们大多集中在中东和北非。这类受害者主要包括如下领域：电信公司、互联网服务商、信息技术公司、登记处等。

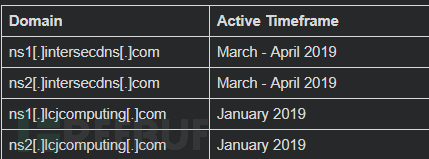
DNS劫持仅仅是攻击者实现其主要目标的手段。根据观察到的行为，思科认为该行为者最终打算窃取凭证以获取对感兴趣的网络和系统的访问权限。为了实现他们的目标，建立了一种控制目标DNS记录的方法。

海龟活动背后的威胁行为者通过利用已知漏洞或发送鱼叉式网络钓鱼电子邮件获得了初始访问权限。Talos认为，威胁参与者利用多个已知的CVE获得初始访问权限或在受影响的组织内横向移动。根据研究，攻击者利用以下已知的漏洞：



之后攻击者将修改目标组织的NS记录，将用户指向恶意DNS服务器，该服务器提供对所有相应DNS查询的响应。目标DNS记录被劫持的时间范围可以从几分钟到几天不等。这种类型的活动可以使攻击者能够重定向任何在全球范围内查询该特定域的受害者。

在2019年期间，观察到以下名称服务器用于支持Sea Turtle活动：



海龟运动背后的威胁行动者已被证明具有很强的能力，因为他们已经能够执行两年多的行动，并且没有被记录其活动各个方面的公开报告所阻止。

近两年的大型DNS劫持攻击都主要采用了更改DNS记录的方法，造成大规模的攻击。

2.2.DNS劫持的学术界研究现状

有关DNS劫持的方法有很多：伪造域名注册人获得解析的控制权；或者采用一些方法，如DDOS攻击、ARP欺骗、DNS缓存投毒等，并更改服务器的域名缓存以劫持域名。

至于对抗DNS劫持的方法，根据有无缓存，可分为目标域名检测和无目标域名劫持。目标域名检测意味着重要的域名应该事先定义，域名和IP地址之间的相应关系放在缓存中。在检测DNS劫持时与缓存中触发比较，以了解是否存在域名劫持。无目标域的检测方法是指检测未存在缓存中的域名劫持[6]。

根据检测和劫持的时间关系可分为两类：劫持前的防范和劫持后的检测。黑客可以通过DDOS攻击、ARP欺骗、DNS缓存中毒等方法实现域名劫持。劫持前的防范是为了防止发生以上事件。在一定程度上，这些方法可以防止域名劫持，但在域名劫持发生后无法工作，因此，这些方法仅限于预防。劫持后的检测根据请求和响应信息来检测是否发生DNS劫持[6]。

根据是否更改基本DNS协议，可分为两类[5]。一种是通过使用该协议来改变基本的DNS协议DNS协议扩展字段加上加密技术，如域名系统安全扩展(DNSSEC)、DNS自适应缓存(ACDNS)等。这些方法可以防御基本攻击但是在大规模部署中有困难，这大大减少了效果。另一种是在不改变DNS协议的情况下，设计一种保护方案不改变协议的攻击方法类型。对于DNS欺骗，Alqahtani[7]等人使用基于IP地址的身份验证而不是域名。Maksutov[8]等人提出了DNS开关来主动检测DNS欺骗攻击。

1. DNS劫持检测的方法

3.1手动检测

被DNS劫持的常见现象：网页加载缓慢，以及网站上通常没有弹出广告的频繁弹出广告，以及告诉您的计算机已感染恶意软件的弹出窗口。虽然这些可能是攻击的常见指标，但不能仅基于它们就确定地识别DNS劫持。可以使用操作系统的终端进行诊断或在线工具可以用来确定是否受到了DNS劫持：

（1）使用ping命令发现DNS劫持的最简单、最有效的方法。

（2）Router Checker恶意软件可以感染您的路由器，使攻击者能够访问路由器管理页，并更改其DNS设置以使用恶意服务器。当这种情况发生时，用户被自动重定向到攻击者的网站。要检查您的路由器是否已被感染，用户的第一步是检查其DNS设置，来自F-Secure实验室的路由器检查器是一个有用的工具，可以验证路由器是否连接到其DNS解析器，以及它是否使用了合法和授权的DNS服务器。

（3）whisDNS。com是一个在线检测的工具，它可以帮助用户公开从用户的设备代表用户的设备发出DNS请求，如果您无法识别它显示的DNS，那么很可能实际上遭受了DNS劫持攻击。

3.2自动化检测

文献[6]提出了一个基于域名与服务器IP对应关系的高速缓存结构来检测DSN劫持的方法。

具体实现细节如下所示：

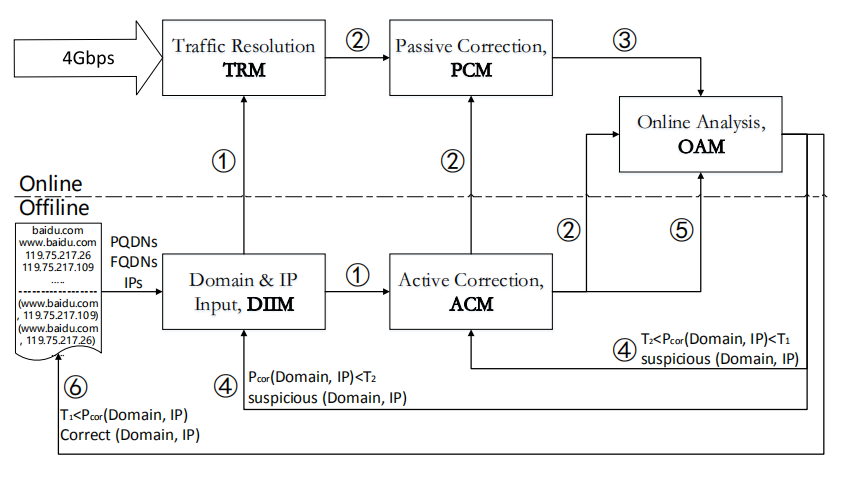
步骤（1）：需要一个经过身份验证的DNS基础数据，其中域名和IP之间的对应关系已经进行了身份验证没有任何劫持。作为DNS认证数据，用于下一步。

步骤（2）：在步骤（1）中的数据的基础上，为本地域名创建域名和IP之间的对应关系作为认证数据缓存。为了实现无目标域名劫持的检测，该缓存数据中的域名应尽可能覆盖一些使用中常见的、可能使用中的域名。如果有新的域名访问，应准备相应的解决方案。

步骤（3）：在步骤（2）中的数据的基础上，由于域名访问的可变性，创建一个动态更新机制。步骤（2）中的数据缓存被动态更新，以删除暂时无用的域名，从而导致数据缓存的消除机制。

步骤（4）;域名访问时，检查步骤（2）中的数据缓存，查看是否在缓存数据中。如果没有，此域名将被放置在挂起的内存区域并继续运行身份验证进程。如果它在缓存中，我们必须检查域名和IP之间的对应关系是否被更改。如果更改，我们将把这种情况视为域名劫持，检测系统还将立即发现并发出警报，等待用户处理。

文献[5]提出了一种部署在局域网网关上的自反馈检测系统(SFDS)，以保护用户不访问错误的网站。具体的流程图如下所示：



SFDS的概述：DIIM接收域和IP字符串并将它们发送到TRM和ACM。TRM解决多协议通信量来匹配这些字符串和最初可疑的输出(域、IP)元组到PCM。ACM将相关网页和证书抓取到PCM。PCM与ACM结合，验证可疑(域、IP)元组，并将验证结果发送给OAM。最后，OAM分析PCM&ACM结果并向用户发送正确的(域，IP)元组。

各部分功能如下：

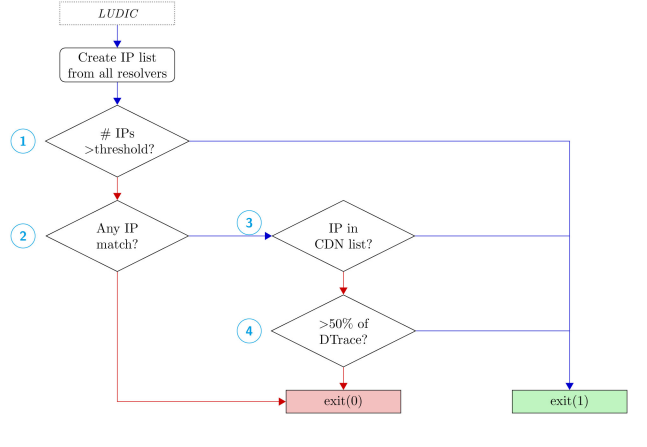
TRM：在解析DNS&SSL&HTTP流量后，将域和IP字符串与SSL中的服务器名称指示(SNI)字段、DNS中的域字段和HTTP中的主机字段进行比较。将只包含域和IP字符串的数据包发送到PCM。

PCM：PCM是被动验证可疑(域、IP)元组的最重要过程。它从TRM接收数据，在线生成网页和证书的指纹，并从ACM接收模板指纹。然后将这些指纹与基于相同域和IP字符串的模板指纹进行比较。PCM向OAM发送经过验证的(域、IP)元组。

ACM：ACM实现了主动抓取、主动查找和主动验证三种功能。主动爬行帮助PCM生成网页和证书的模板指纹。主动验证，利用一些第三方工具来查找和验证更多可疑(域、IP)元组。

OAM：OAM是SFDS工作流程中的最后一步。它的任务是计算每个(域，IP)元组的正确性概率。基于两个不同的阈值(T1，T2)，OAM向不同的模块发送(域，IP)元组。一个(Domain，IP)元组有三个目的地。一是向用户推荐列表，第二是对ACM进行进一步的验证，最后一个是DIIM的下一个工作流。

文献[4]提出了LUDIC系统使用分布式优势点来验证DNS记录。检测域劫持和标识DNS记录正确值的具体流程如下所示：



LUDIC系统由探针，数据库，控制器组成。探针遍布在世界各地，数据库存储查询的域名数据，控制器负责与数据库和客户端进行交互。给定一个使用域foo.bar和值val请求，控制器检查数据库中对应于目标域的探针，检索所有值并计算其返回的响应给客户。例如，如果val是IP地址，控制器将比较探针，为该域报告的IP地址（步骤1和2）。如果超过某个阈值，将报告了相同的IP地址，控制器将其返回给客户端。否则，（步骤3）如果某些值不匹配，控制器将检查目标域是否托管在CDN上。如果目标值不托管在CDN上，那么托管在所有名称服务器上的区域文件应该是相同的。值的不一致将表示良性的错误配置或者攻击。在不一致的情况下，控制器收集探针，从目标域的所有名称服务器的响应中报告，投票选出是否正确，（步骤4）。如果域（目标值所在的域）托管在CDN上，那么不同的响应可能包含不同的ip值。

3.3 部署DNSSEC

Domain Name System Security Extensions (DNSSEC)DNS安全扩展，是由IETF提供的一系列DNS安全认证的机制（可参考RFC2535）。它提供了一种来源鉴定和数据完整性的扩展，但不去保障可用性、加密性和证实域名不存在。DNSSEC依靠数字签名保证DNS应答报文的真实性和完整性。权威域名服务器用自己的私有密钥对资源记录（Resource Record, RR）进行签名，解析服务器用权威服务器的公开密钥对收到的应答信息进行验证。如果验证失败，表明这一报文可能是假冒的，或者在传输过程、缓存过程中被篡改了。 RFC 4033概要介绍了DNSSEC所提供的安全功能并详细介绍了相关的概念。部署DNSSEC可以有效的缓解DNS欺骗及DNS污染攻击。

1. 总结

本次调研主要包括DNS劫持概念、原理、DNS劫持研究现状、DNS劫持检测方法等内容，着重介绍了几篇研究中所使用的DNS劫持检测方法，可以看出目前关于不改变协议情况下的一些DNS劫持检测方法还主要着重于客服端检测，检测方法主要是检测响应DNS数据包是否正常，除了主动检测DNS劫持攻击，还可以通过部署DNSSEC来防御DNS劫持攻击。

1. 参考文献
2. <https://baike.baidu.com/item/%E5%9F%9F%E5%90%8D%E5%8A%AB%E6%8C%81/7657893?fromtitle=DNS%E5%8A%AB%E6%8C%81&fromid=6739044&fr=a>
3. [https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-DNS-hijacking-attacks](https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks) ：A Deep Dive on the Recent Widespread DNS Hijacking Attacks — Krebs on Security
4. [https://www.google.com.hk/amp/s/www.globaldots.com/blog/DNS-hijacking%3fhs\_amp=true](https://www.google.com.hk/amp/s/www.globaldots.com/blog/dns-hijacking?hs_amp=true" \t "_blank)：What is DNS Hijacking and Mitigation Methods
5. Borgwart A, Boukoros S, Shulman H, et al. Detection and forensics of domains hijacking[C]//2015 IEEE Global Communications Conference (GLOBECOM). IEEE, 2015: 1-6.
6. Huang C, Zhang P, Sun Y, et al. SFDS: A Self-Feedback Detection System for DNS Hijacking Based on Multi-Protocol Cross Validation[C]//2019 26th International Conference on Telecommunications (ICT). IEEE, 2019: 238-243.
7. Xue J, Liu Y, Chang P, et al. Design and Implementation of Domain Hijacking Detection System[C]//MATEC Web of Conferences. EDP Sciences, 2015, 22: 01058.
8. A. H. Alqahtani and M. Iftikhar.TCP/IP attacks, defenses and security tools[J]//International Journal of Science and Modern Engineering (IJISME), 2013.
9. A. A. Maksutov, I. A. Cherepanov, and M. S. Alekseev.Detection and prevention of DNS spoofing attacks . 2017:84–87.
10. https://www.freebuf.com/mob/articles/network/201405.html