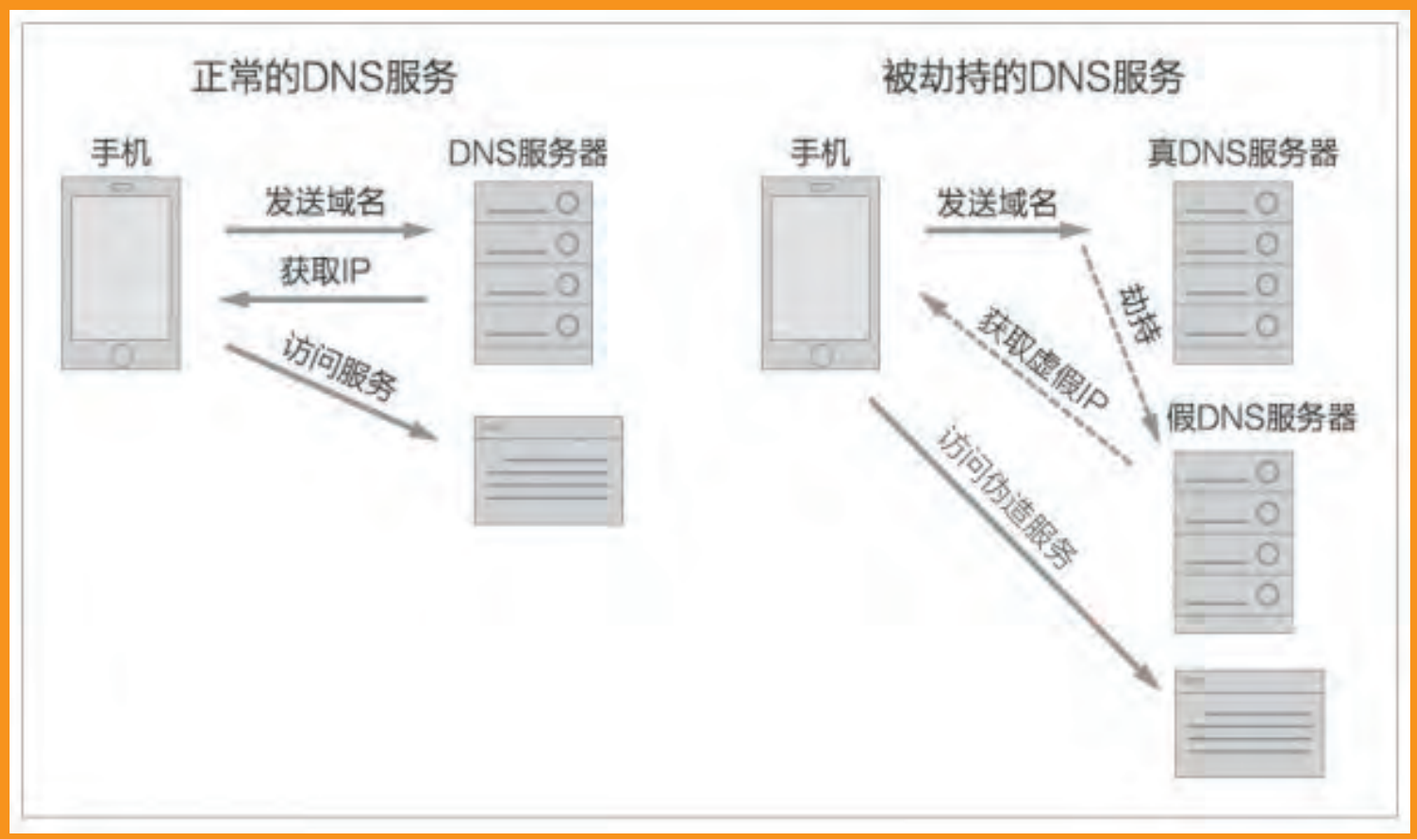
AsiaInfo | 亚信安全

# 如何防护DNS劫持攻击？





要执行DNS劫持攻击，攻击者要么在用户的系统上安装恶意软件，要么通过利用已知漏洞或破解DNS通信来接管路由器。
攻击涉及破坏用户的系统DNS(TCP / IP)设置，以将其重定向到“Rogue DNS”服务器，从而使默认DNS设置无效。

AsiaInfo | 亚信安全

# DNS劫持攻击的类型

**本地DNS劫持攻击**

在本地DNS劫持中，用户的系统现在使用由攻击者控制的DNS服务器。攻击者控制的DNS服务器将网站域请求转换为恶意站点的IP地址，从而将用户重定向到恶意站点。

**路由器DNS劫持攻击**

攻击者利用路由器中存在的固件漏洞来覆盖DNS设置，从而影响连接到该路由器的所有用户。攻击者还可以通过利用路由器的默认密码来接管路由器。

**中间人(MiTM)DNS攻击**

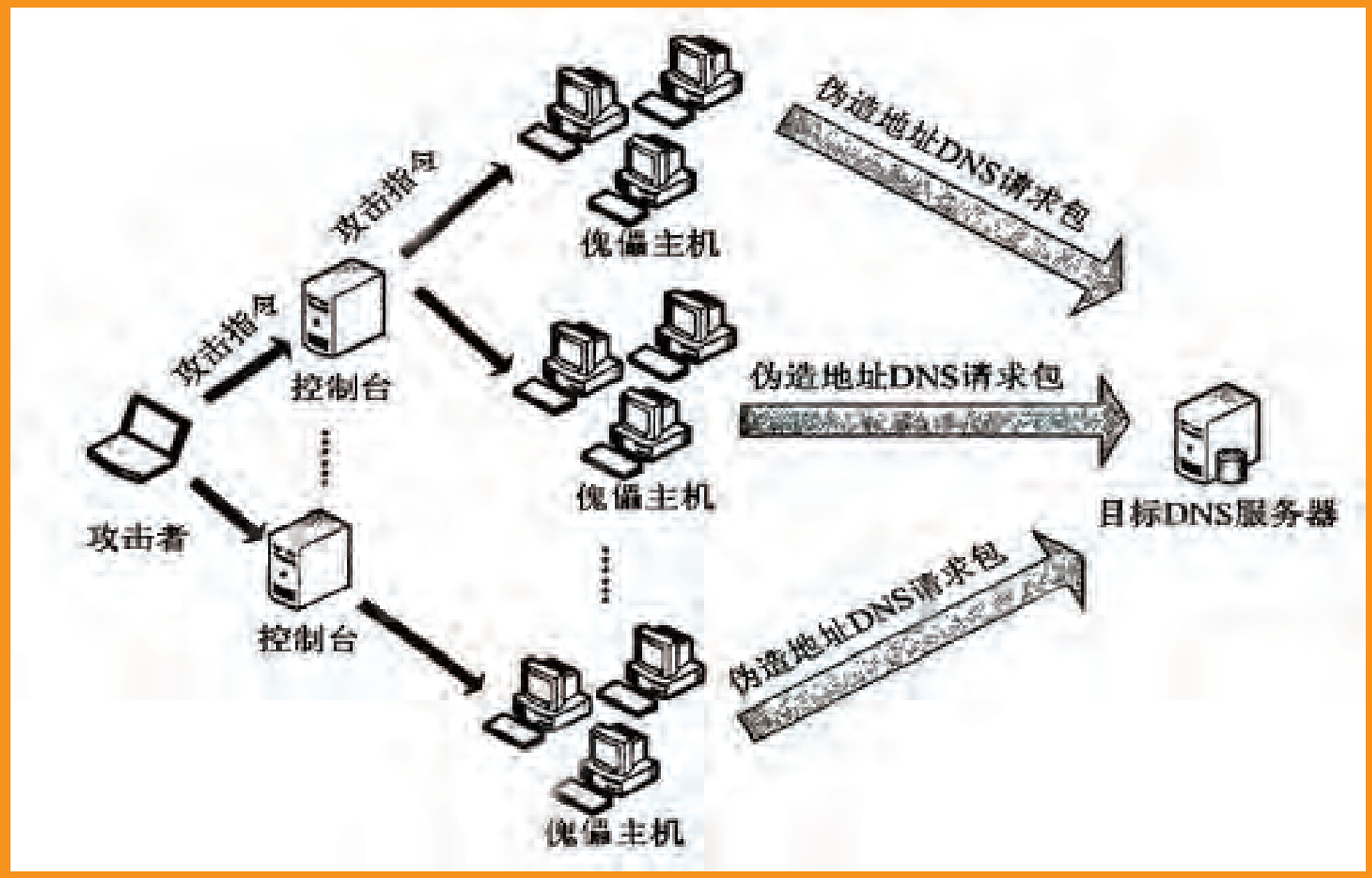
攻击者执行中间人(MiTM)攻击以拦截用户和DNS服务器之间的通信并提供不同的目标IP地址，从而将用户重定向到恶意站点。

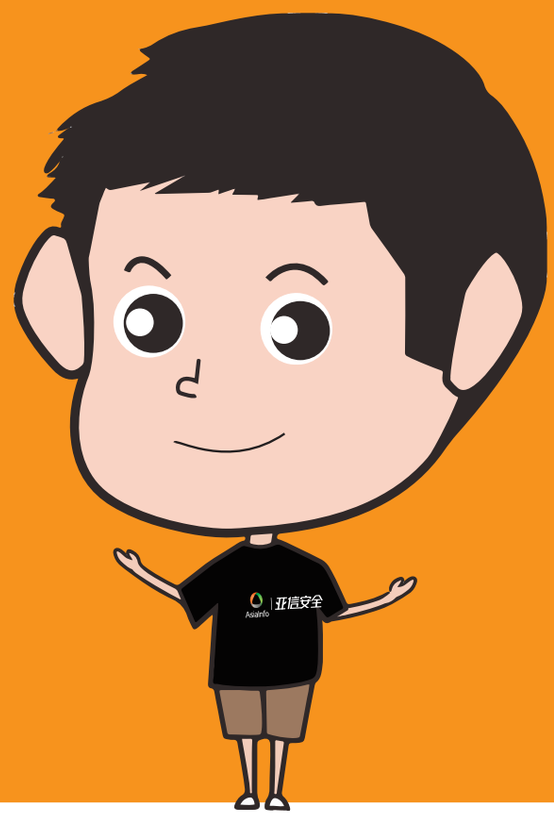
**流氓DNS服务器**

在此攻击中，攻击者可以破解DNS服务器，并更改DNS记录以将DNS请求重定向到恶意站点。

AsiaInfo | 亚信安全

# DNS劫持攻击如何工作?




您的DNS服务器由您的ISP(Internet服务提供商)拥有和控制，您的系统的DNS设置通常由您的ISP分配。当用户尝试访问网站时，请求被引用到他们系统的DNS设置，而DNS设置又将请求重定向到DNS服务器。DNS服务器扫描DNS请求，然后将用户定向到所请求的网站。

但是，当用户DNS设置因恶意软件或路由器入侵而受到威胁时，用户发出的DNS请求将被重定向到由攻击者控制的流氓DNS服务器。这个受攻击者控制的流氓服务器会将用户的请求转换为恶意网站。

AsiaInfo | 亚信安全

# DNS劫持攻击示例

**案例1**

**攻击者使用DNSChanger木马通过恶意广告活动劫持超过400万台计算机的DNS设置，并获得约1400万美元的收入。**

**案例2**

**最近的一个DNS劫持活动在2019年1月已成功定位针对全球组织。这一系列攻击影响了北美、北非和中东的商业实体、政府机构、互联网基础设施提供商和电信提供商。在攻击中，攻击者修改了“DNS A”和“DNS NS”记录，并将受害者组织的名称服务器记录重定向到攻击者控制的域。**

AsiaInfo | 亚信安全

# 如何防止DNS劫持攻击?

安全软件和防病毒程序确保定期更新软件

建议使用公共DNS服务器

定期检查您的DNS设置是否已修改

使用复杂的密码重置路由器的默认密码

使用双因素身份验证修补路由器中漏洞

如已被感染请删除HOSTS文件的内容并重置Hosts File