# 每月热点威胁：DNS 攻击

## DNS 和 DNS 重定向是什么？

**域名系统 (DNS) 是将用户定向至互联网上不同网站和其他位置的核心技术。这种定向就像请图书管理员帮我们找书一样，只不过您要找的不是书，而是特定的网站。**DNS **会检查其记录，然后告知您的计算机网站所在位置。**

DNS **重定向是指，攻击者设法入侵** DNS **进程，篡改通往合法网站的路由，使其通向恶意网站，最终危害其攻击目标。在这种情况下，虽然您请求访问的是特定域的** IP **地址，但** DNS **记录已遭篡改，所以系统会将您定向到篡改后的恶意** IP **地址。**

## DNS 攻击

攻击者可以通过以下方式，设法入侵 DNS 记录并对其进行更改：

- 对 DNS 管理员实施网络钓鱼攻击。
- 入侵 DNS 托管服务。
- 入侵 DNS 请求链上的基础设施。

# 延伸阅读

- DNS 攻击
- DNSpionage 活动对中东发起针对性攻击
- DNSpionage 带出 Karkoff
- DNS 劫持滥用对核心互联网服务的信任
- Sea Turtle 继续活动，寻找新的受害者以实施 DNS 劫持
- 隐蔽通道和不良决策：DNSMessenger 的故事
- 欺骗性 SEC 邮件分发经过演变的 DNSMessenger 变体
- 检测 DNS 数据泄露



07/19

### DNSpionage 攻击

在此攻击中，攻击者首先向 DNS 管理员发送 LinkedIn 网络钓鱼邮件。然后，管理员点击了邮件中的恶意链接，就被重定向至某个恶意 Word 文档。

结果，攻击者就入侵了管理员的计算机，从而得以窃取 DNS 登录信息。

在获得域控制权限后，攻击者将 webmail 服务器重定向至恶意 IP 地址，并注册有效证书以使重定向的域“合法化”。恶意页面模仿 Webmail 界面，以便攻击者继续窃取登录信息。

### Sea Turtle 攻击

Sea Turtle 攻击最终目标与 DNSpionage 相似，即窃取信息，但它幕后的攻击者却是以托管 TLD 服务器的网络基础设施作为入口。在侥幸侵入了 TLD 服务器后，攻击者会修改特定域的名称服务器 IP 地址。

这种方法使攻击者能够更好地控制重定向。通过设置恶意名称服务器，攻击者可选择何时将对特定域的请求发送至合法站点或恶意站点。

Sea Turtle 还会更改 Webmail 服务器记录，从中拦截和窃取所需信息，并且在完成后将目标发送至合法系统。

### Umbrella Investigate

- 通过 Umbrella Investigate，可以查看 DNS 记录以检查合法或不合法的更改。

### Duo 可信访问

- Duo 多因素身份验证可防止在未经身份验证的情况下随意更改 DNS 记录。