登录

WSUS MITM远程攻击实战全过程详解

嘶吼roartalk / 2017-06-13 06:01:54 / 浏览数 2964 安全技术 技术讨论 顶(0) 踩(0)

网络攻击（WPAD注入，HTTP / WSUS
中间人攻击，SMBRelay攻击等）是一个非常有用的攻击向量，攻击者可以使用此类攻击尝试以半定向的方式横向扩散，收集证书或升级特权。目前已知的攻击者使用此攻击
2.0是一个很好的例子，可以在野外发现这样的攻击，而这个报道也是一个很好的案例研究。

感谢每天和我一起工作的Jeff Dimmock（@bluscreenofjeff）和Andy
Robbins（@_wald0）的演示和故事，这使得我变得更加熟悉这些技术。学习了Responder后，我把玩了更广泛的功能，如MITMf，它将各种工具组合成一个武器化的平台

https://www.trustwave.com/Resources/SpiderLabs-Blog/Responder-2-0-Owning-Windows-Networks-part-3/

https://www.christophertruncer.com/responder-user-account-credentials-first-come-first-served/

在引用Duqu
2.0报告中的恶意和狡猾的APT操作者的情况下，行动者使用了专门为其工具包构建的一个模块，并且不需要使用公共工具或外部脚本。不幸的是，很长一段时间内，已公开
/中继攻击工具仍然需要你置身于本地局域网才能发起攻击（无论如何...我欢迎你的意见）。2015年初，Kevin
Robertson（@kevin_robertson）发布了 Inveigh，这是一款PowerShell网络攻击工具，它使用原始套接字来实现一些有限的技术，包括LLMNR欺骗，MDNS欺骗和SME
Mudge）对这个话题有一些非常好的主意和想法。

WPAD攻击

让我们退后一步，先学习WSUS MITM攻击的不同组件。Web代理自动发现（WPAD）是Microsoft
Windows客户端自动配置本地代理设置的协议。企业使用协议允许客户端自动定位并使用正确的代理设置来排除不相关的企业网络。发现过程和配置如下：

1. 在DHCP协商期间是否获得了代理配置？
2. 如果没有，解析"wpad.domain.com"并从该服务器获取配置。
3. 如果我们没有得到结果，则使用NetBIOS（NBT-NS）广播来解析名称"WPAD"
4. 如果找到服务器，则使用uri"/wpad.dat（http：// <SERVER> /wpad.dat）从该服务器请求资源，其中将包含代理的设置

由于在NBT-NS回复期间缺乏验证（步骤3），请求的广播域或本地子网中的任何客户端都可以响应并声称"我就是WPAD服务器"。然后，流氓WPAD服务器就可以提供恶意

```
HTTP MITM■iframe■HTA■■■■■■Java Applet■■

HTTP■■■■/■■■■

WSUS■■

...■■■■
```

WSUS MITM

Windows Server Update Services（WSUS）是一种允许公司从集中式Intranet位置，管理和部署更新或修补程序的系统。在 Blackhat USA
2015，安全研究人员Paul Stone（@ pdjstone）和来自Context的 Alex
Chapman 介绍了企业更新在网络上未加密的明显问题。他们明确指出，没有SSL，任何人都可以对更新过程进行中间人攻击，以提供恶意的更新包。顺便说一下，HTTP是

请阅读他们的白皮书进行更多的研究或查看他们的工具
...我不能在这短短的一篇文章中阐明。另外，为了更多关于为什么非加密更新/软件不好的研究，请查看Josh
Pitt的（@midnite_runr） 研究或后门工厂的一些工作。

把它放在一起

好的，所有我在这一点上所做的都是在思考有名的漏洞和攻击策略。当你将工具放在一起并将其武器化在诸如Cobalt
Strike的平台中时，就会提升攻击力，从而可以在本地Intranet范围之外进行MiTM攻击。对于本节，我将假设我们已经从外部获得了初始访问加入域的主机的权限。

免责声明：这是一个演示，显然有大量的约束可以使操作员更改使用的方法或技术。关键是，这些看似先进的技术不仅限于国家赞助的攻击者与定制工具，红均可以有效地

确定可能性

第一步是识别任何WSUS错误配置。在大多数RAT中，我们可以通过查询注册表来确定系统的WSUS设置。接下来我们可以查询Internet
Explorer的当前代理配置。如果WSUS的URL为"HTTP：// <SERVER>"，浏览器设置为自动配置代理，那我们就可以继续！

注册/值：

```
HKLMSoftwarePoliciesMicrosoftWindowsWindowsUpdateWUServer

HKLMSoftwarePoliciesMicrosoftWindowsWindowsUpdateAUUseWUServer
```

HKCUSoftwareMicrosoftWindowsCurrentVersionInternet

SettingsConnectionsDefaultConnectionSettings■■■■■■■■5■■■■■■■■■■■■WPAD■Internet Explorer■■■■■■■■■■■■■

WSUS设置

自动设置选择（第5个字节）

做完这些检查，我们可以使用ARP来定位我们可能想要定位的子网上的另一个主机。

网络弯曲

在使用我们的代理作为WSUS代理的过程中出现了一个明显的问题。幸运的是用Cobalt
Strike的灯塔，我们有反向端口转发的功能。在WPAD中毒攻击期间，我们可以将受害者的浏览器指向我们的“代理”，这只是网络中的一个反向隧道，我们的C2服务器。然后

毒药

一旦隧道准备好了，最后是攻击的时候了。首先，我配置我的恶意有效载荷并启动WSUSpectProxy。WSUSpectProxy接收在其payload.ini文件中定义的自定义负载（如下
user”和“net localgroup”来添加一个后门用户“bob”。

现在是时候使用多个标志来启动Invoke-Inveigh来定义我们希望脚本使用的一些设置了：

-IP <IP OF POISON VICTIM>■■■■■■■■■■■■IP

-NBNS Y■■■■■■NBNS■■

-LLMNR Y■■■■■■LLMNR■■

-HTTP Y■■■■HTTP■■■■■■■■WPAD.dat■■

-SMB N■■■■■■■■■■SMB■■■■■

-StatusOutput Y■■■■■■■■■■■■

-Tool 2■■■■■■■■■■■■■■■■■■■■■Empire■■■■■■■■■■Cobalt Strike■■

-SpooferIPsReply <TARGET IP>■■■■■CSV■■■■IP■■

-WPADAuth■■■■■■■■WPAD■■■■■

-WPADIp <ProxyHost>■■■■rportfwd■■■■■■■■■IP

-WPADPort 8080■rportfwd■■■■■■

该命令将针对目标主机执行WPAD中毒攻击，并提供一个WPAD.dat，将目标浏览器指向我们已经出站的端口转发隧道。该端口将在8080端口上返回我们的C2服务器。

MITM更新

一旦满足MITM条件，更新请求就会被拦截，我的恶意软件包就会被传递给客户端。由于更新至关重要，因此可能会被执行，添加本地用户并允许我们横向传播。

免责声明：将本地用户添加到系统可能会提示，但是可以使用更好的做法，并使演示更容易一些。我建议改进启动方式，启动一个只有内存的代理（可能使用PowerShell）.

不错！我们现在可以访问并且可以使用新添加的用户部署灯塔代理。

修复漏洞

有许多缺陷可以使得这个攻击能够成功，它们应该在任何网络中被修复。这些问题已经确定了很长时间，但是我仍然认为在这个链条中滥用的错误配置缺乏意识和控制。除了

WPAD控制/修复

要修复WPAD错误配置，DNS A或CNAME记录应该添加到名称为“wpad”的内部DNS服务器中，以防止主机进入执行MDNS /
LLMNR广播的步骤。此外，如果不需要该功能，则可以通过GPO取消选中自动设置。

https://technet.microsoft.com/en-us/library/cc995062.aspx

http://tektab.com/2012/09/26/setting-up-web-proxy-autodiscovery-protocol-wpad-using-dns/

WSUS修复

任何更新软件包或软件应始终通过安全连接部署（至少为SSL）。有许多项目专注于通过网络传输的后门软件和应用程序...许多坏人使用这种技术来获得初始访问和横向传播

https://technet.microsoft.com/en-us/library/hh852346.aspx#bkmk_3.5.ConfigSSL

检测

预防控制是一个期望较少的方法，但是随着组织的成熟度的增长，通过安全控制的层次结构，审计和取证能力是必须的。随着组织转向假设违约心态，他们将重点放在预防上

PowerShell v5

PowerShell
v4和v5引入了许多蓝军应该理解的功能。我在这里提到他们特别是因为我在我的攻击链中使用了Inveigh.ps1，但与底层技术的检测并不直接相关，只是武器化向量。有一篇

事件日志

事件日志在大型企业中转发可能很困难。集中收集和收集这些日志所获得的价值不能低估，在我看来，这是完全值得的。在这种攻击链的情况下，似乎添加到集合中的最佳日
windows windowsupdate.log文件。如果你没有收集，则具有"WindowsUpdateClient"和17或19的ID的系统事件日志将显示你下载/安装的更新的名称。比较主机上的日

在这种情况下，DNS日志的集合也是有用的。假设企业组织怀疑通过禁用WPAD正确地修复了WPAD中毒攻击，如果将恶意的或新的工作站引入环境而无需控制或当前工作

WMI事件订阅

我们的团队是WMI在防守上的用途的巨大支持者。你可能已经看到Matt Graeber 最近的一些tweets
，例如，他提供的WMI签名，将提供围绕事件值得监控的警报。ATD的Hunt能力主管Jared
Atkinson开发了一种名为Uproot的工具，它实际上是一种基于代理主机的IDS，使用了WMI事件订阅。

在我们的例子中，可以在"HKEY_USERS <USER-GUID> Software Microsoft Windows CurrentVersion Internet
Settings Wpad"下的网络配置文件子键内的值更改创建WMI事件过滤器的时间。此外，你可以对签名的文件创建或修改wpad.dat文件，该文件暂时放在"<USER
APP DATA> Local Microsoft Windows Temporary Internet Files Content.IE5"中。

如果你有兴趣，请查看Uproot和WmiEvent，并将其作为练习的机会。

结论

虽然我在这篇文章中没有引入任何新的工具，但我的目标是将几个好的工具拼接在一起，展示一个有趣的攻击链，并鼓励创造性的技术。此外，我希望能够引起大家对在大型

本文翻译自：http://www.sixdub.net/?p=623，如若转载，请注明来源于嘶吼： http://www.4hou.com/info/news/5223.html

上一篇：最早的一本Php代码审计书籍 下一篇：Mysql提权(CVE-2016-...
1. 0 条回复
   - 动动手指，沙发就是你的了！