# 威胁情报分析课程报告

刘婉萍

(四川大学网络空间安全学院，成都 610065)

**摘 要：**本文通过搭建漏洞渗透测试环境，利用ms08\_067漏洞实现攻击机对靶机的远程控制、加载并执行恶意样本。结合漏洞渗透攻击模块源代码解析和Wireshark抓包结果分析攻击的具体过程和利用的漏洞。同时对恶意代码进行静态文件特征分析和动态文件行为分析，并进行拓线查询找到其背后的高级可持续性威胁（ATP）组织，形成最终的威胁情报。

**关键词:** 漏洞渗透 恶意样本 威胁情报

# Threat intelligence analysis course report

LIU Wanping

(College of Cybersecurity，Sichuan University，610065，China)

**Abstract:** In this paper, the vulnerability penetration testing environment is built and ms08\_067 vulnerability is used to realize the remote control, loading and execution of malicious samples by the attacking host to the target host. Combining the analysis of the source code of the vulnerability penetration attack module and the captured packages by Wireshark, we analyze the specific process of the attack and the vulnerability being exploited. At the same time, the static file characteristic analysis and dynamic file behavior analysis of the malicious code are carried out, and the ATP organization behind them is found through the extension line query to form the final threat intelligence.

**Keywords:** vulnerability penetration; malicious sample; threat intelligence

## 1 引言

本文主要模拟漏洞渗透攻击环境，利用ms08\_067漏洞实现攻击机对靶机的远程控制、加载并执行恶意样本。通过对恶意样本的溯源分析，复现攻击过程，拓线查询相关信息，得到最终的威胁情报。

本文第二部分详细介绍攻击过程，第三部分从过程和代码两方面对漏洞进行分析，第四部对样本7进行分析及拓线查询，最后进行总结。

## 2 攻击过程

该部分详细介绍实验攻击过程，包括四个步骤：资产识别、漏洞挖掘、漏洞利用和植入木马。

本实验攻击机为kali Linux，IP地址为192.168.127.133，靶机为Windows XP SP2 Chinese-Simplified(NX)，IP地址为192.168.127.134，关闭防火墙及自动更新。

### 2.1 资产识别

使用nmap扫描整个网段，查看开放的主机列表，从中得到网络资产识别列表只有4台虚拟机设备，如图1所示。

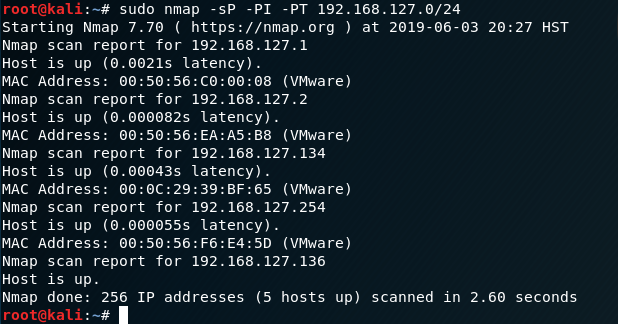


图1 网段内开放的主机列表

### 2.2 漏洞挖掘

得到网段内开放主机列表后，选定192.168.127.134为攻击目标，利用nmap扫描可利用漏洞，选择ms08\_067\_netapi漏洞，如图2所示。

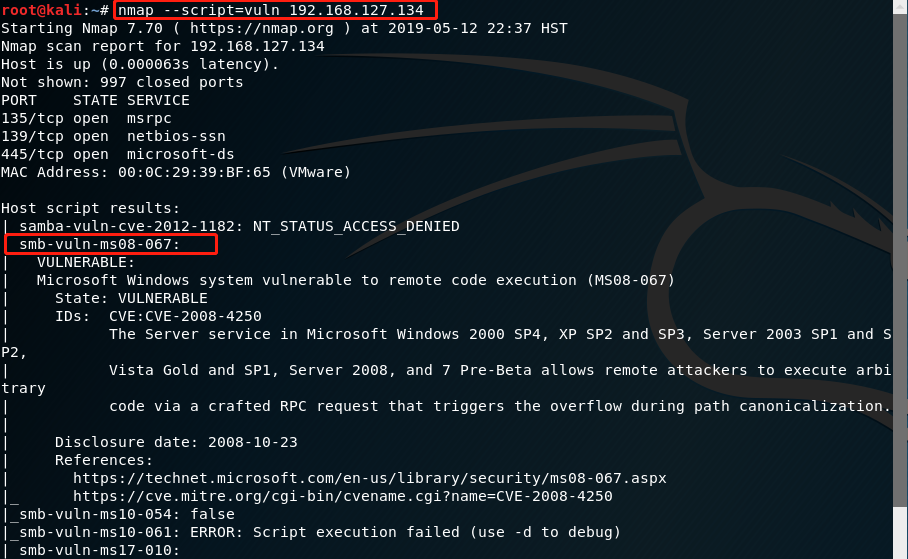


图2 nmap扫描可利用漏洞

在kali机启动metasploit，如图3所示。

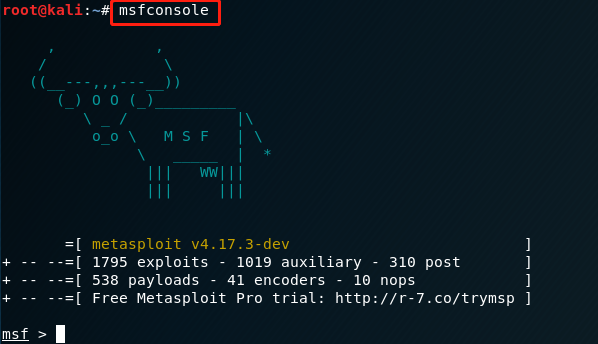


图3 kali成功启动metasploit

查看漏洞的详细信息，如图4所示。可知该漏洞是08年发现的漏洞，等级为Great。

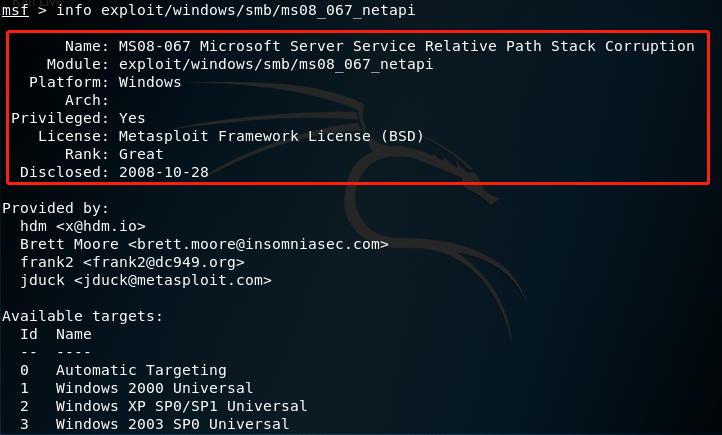


图4 查看漏洞的详细信息

### 2.3 漏洞利用

发现并选定可利用漏洞后，进入该漏洞模块的使用，如图5所示。

F:\有道云笔记\liuyiyihappy@163.com\92b10d6f6b034ed7a86b1dade5f3fc88\clipboard.png

图5 使用该漏洞模块

显示有效的攻击载荷，如shell\_bind\_tcp(基于TCP的连接shell）和shell\_reverse\_tcp(基于TCP的反向连接shell），如图6所示。本实验选定shell\_reverse\_tcp，因为其很稳定。



图6 显示有效的攻击载荷

设置攻击载荷，如图7所示。



图7 设置攻击载荷

查询并设置参数，如图8-9所示。

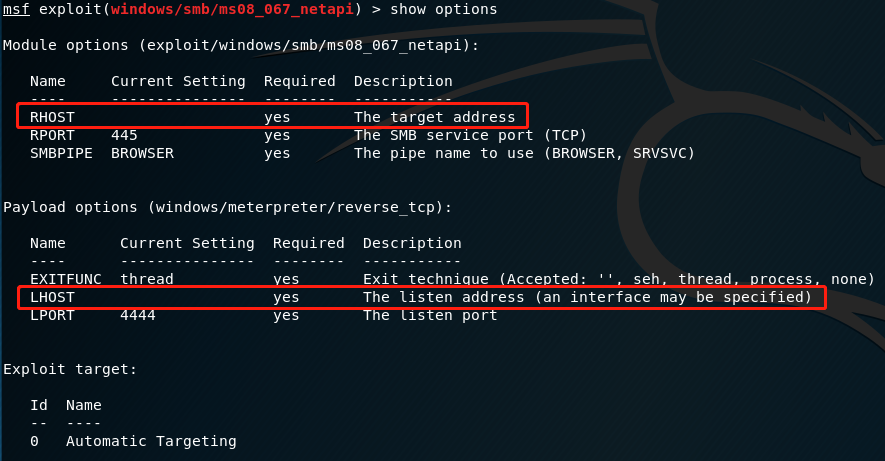


图8 查询需设置的参数

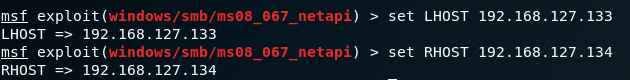


图9 设置参数

查询并设置攻击目标系统类型，如图10-11所示。

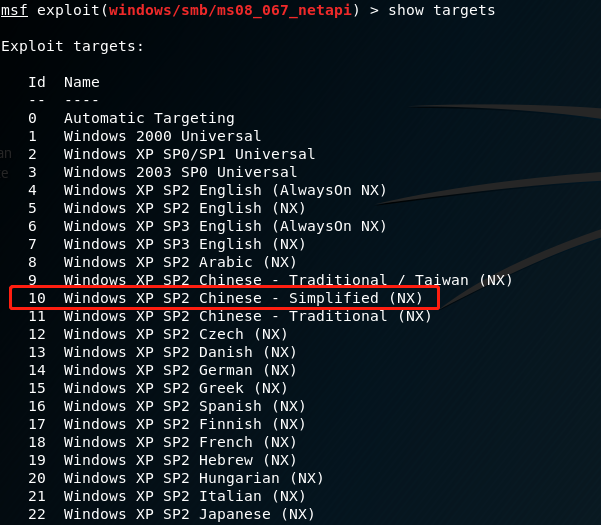


图10 查询攻击目标系统类型



图11 设置攻击目标系统类型

执行攻击，攻击成功，如如图12所示。

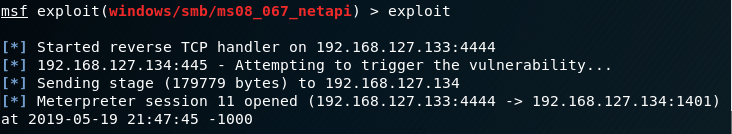


图12 攻击成功

控制会话进行交互，进入目标的shell中，如图13所示。

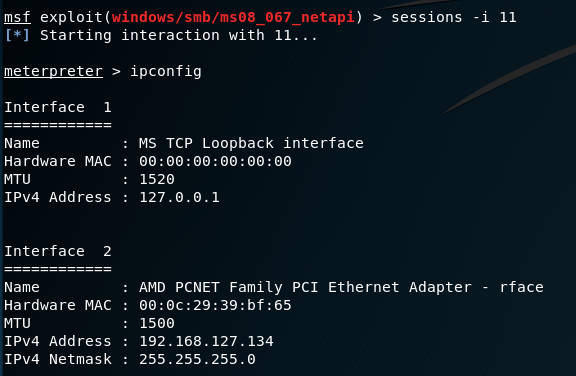


图13 进入目标shell

### 2.4 植入木马

进入目标的shell后，利用upload命令上传恶意代码文件至目标机器，如图14所示。本文选定的恶意代码文件为sample7.exe。

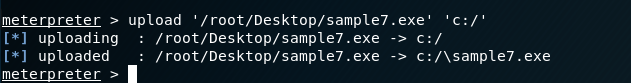


图14 上传恶意代码文件至靶机

在靶机查看确认文件上传成功，如图15所示。

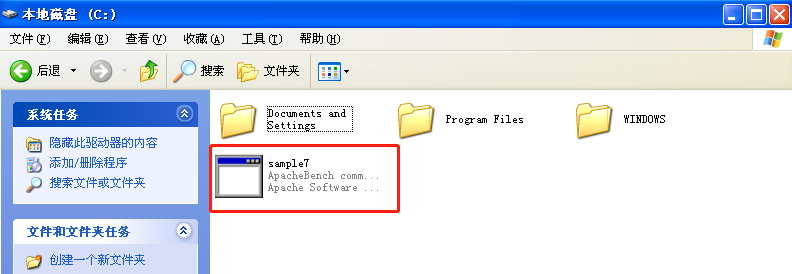


图15 恶意代码文件上传成功

远程控制靶机执行sample7.exe，并显示目标主机进程，如图16所示。

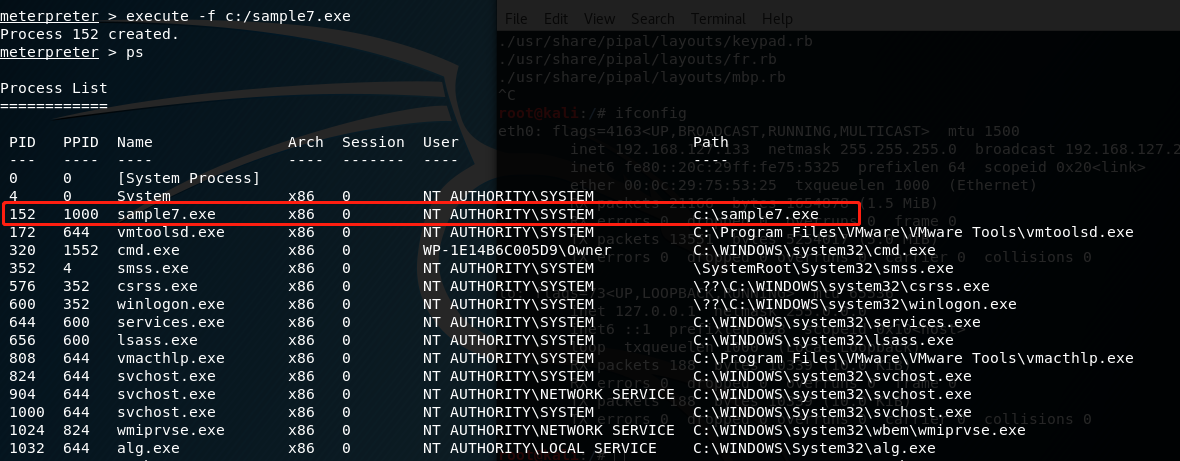


图16 远程执行sample7.exe

至此，已完成整个攻击过程。

## 3 漏洞分析

该部分主要通过对ms08\_067\_netapi漏洞渗透攻击模块源代码解析，结合Wireshark抓包，详细分析对该漏洞的渗透过程。

metasploit框架中，ms08\_067渗透攻击模块对应的源代码文件为ms08\_067\_netapi.rb，整个渗透攻击模块的指令档可分为三个部分：

1. 前提环境准备

原代码如图17所示。此模块包含Metasploit核心库的所有函数，其中的类继承远程渗透类的特性，且此漏洞攻击模块具有非常高的利用等级，稳定性与可用性都非常高，代码将从核心库导入DCERPC和SMB实现模块。

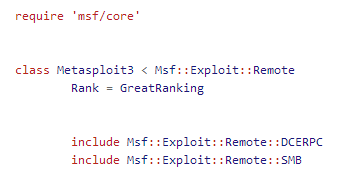


图17 漏洞渗透攻击模块前提环境准备源代码

1. 模块初始化

该部分包括模块描述、引用、默认选项、攻击载荷及目标等，部分代码如图18所示.

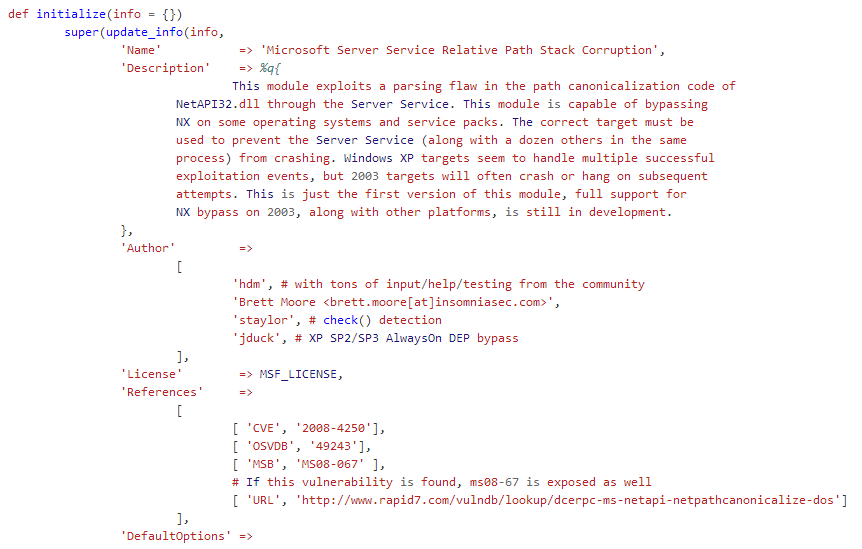


图18 漏洞渗透攻击模块初始化源代码（部分）

1. 功能函数

对于渗透攻击模块来说，exploit操作是必不可少的，exploit函数包含了渗透攻击的整个过程。原代码如图19所示。



图19 漏洞渗透攻击模块功能函数源代码

对源代码进行分析可将exploit函数功能归纳为3步，下面分别进行详细说明。

1. 建立连接

首先与目标主机建立TCP连接，用Wireshark抓包如图20所示。

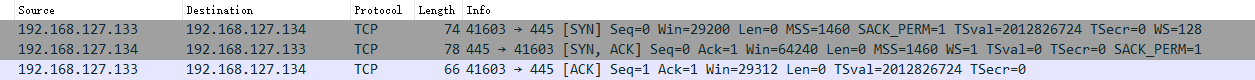


图20 Wireshark抓包建立TCP连接

然后进行SMB回话连接，如果选择自动获取目标模式，则尝试通过SMB协议会话获取目标系统信息。本次实验已指定目标系统，则赋予目标相关的参数值，如图21所示。

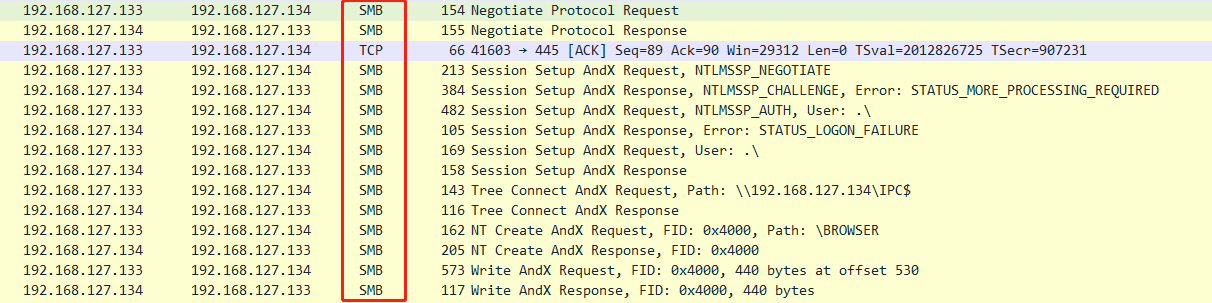


图21 Wireshark抓包进行SMB回话连接

1. 构建恶意路径

在构建恶意路径时，先是初始化一些变量，包括填补字符串pad，服务器名称server以及前缀prefix、路径path等，源代码如图22所示。

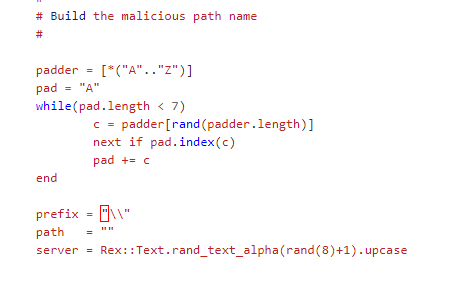


图22 构建恶意路径初始化变量源代码

当渗透目标是Windows XP SP2时，选择分支中对应的代码，如图23所示。其中一些变量的初始化操作位于前面模块初始化中的targets数组中，源代码如图24所示。该部分定义且赋值了变数Ret、Scratch，且由注释可知，变数Ret值对应得是ACGENRAL.DLL中的JMP ESI指令地址，可以猜测这个渗透攻击模块是利用ESI寄存器中指向栈空间的地址，覆盖返回地址，并通过ACGENRAL.DLL中JMP ESI指令进行中转跳转，最终执行栈中的Shellcode。

这里重点分析一下Windows XP SP2分支源代码，如图23所示。函数首先构造内跳转地址的填充字符串jumper，jumper初始化为长度70字节，内容为“A”到“Z”的随机字符串；从第5字节气填充4字节由初始化变数Ret定义的返回地址；从第51字节起填充8字节的空指令和2字节的跳转指令“\xeb\x62”。生成的恶意路径结构path由8个部分构成，其中包括编码的Shellcode、触发漏洞的unicode相对路径“\\..\\..\\”、填补字符串pad、EBP栈基址、RET返回地址、跳转指令块jumper、字符串结尾‘\0’。

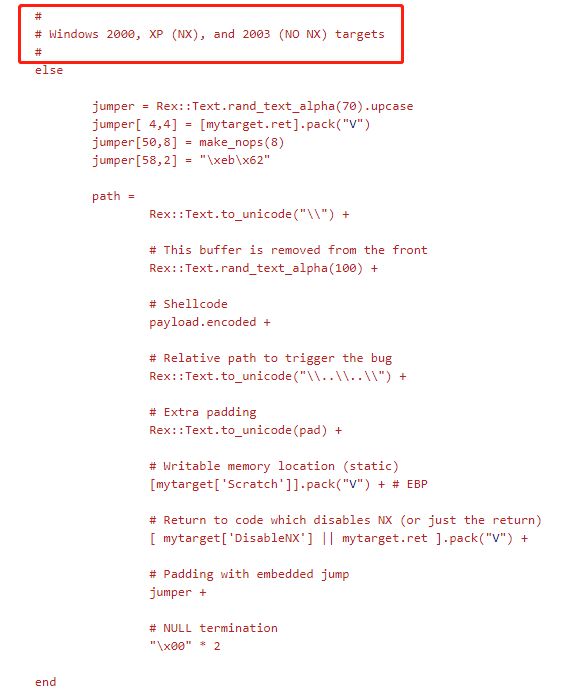


图23 针对Windows xp SP2时构建恶意路径源代码

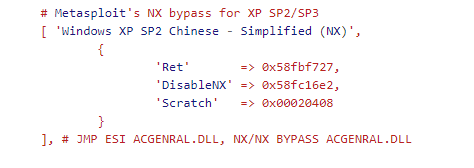


图24 变量的初始化操作源代码

1. 发送数据

当以上构造恶意请求的元素都准备就绪后，接着就是和远程服务器进行“正常”交互，把构造的数据发过去，源代码如图25所示。①首先向远程主机的SMB端口发起RPC请求；②接着将前面准备好的各元素构造成完整的数据包；③将数据表作为内容调用远程主机的RPC接口。

整个发送数据过程用Wireshark抓包如图26所示。查看其中SRVSVC包可进一步看到构造的恶意请求数据特征，如图27所示。



图25 发送恶意请求数据源代码

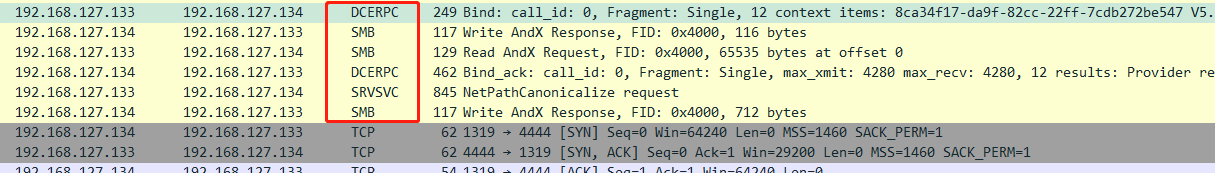


图26 Wireshark抓包显示发送数据过程

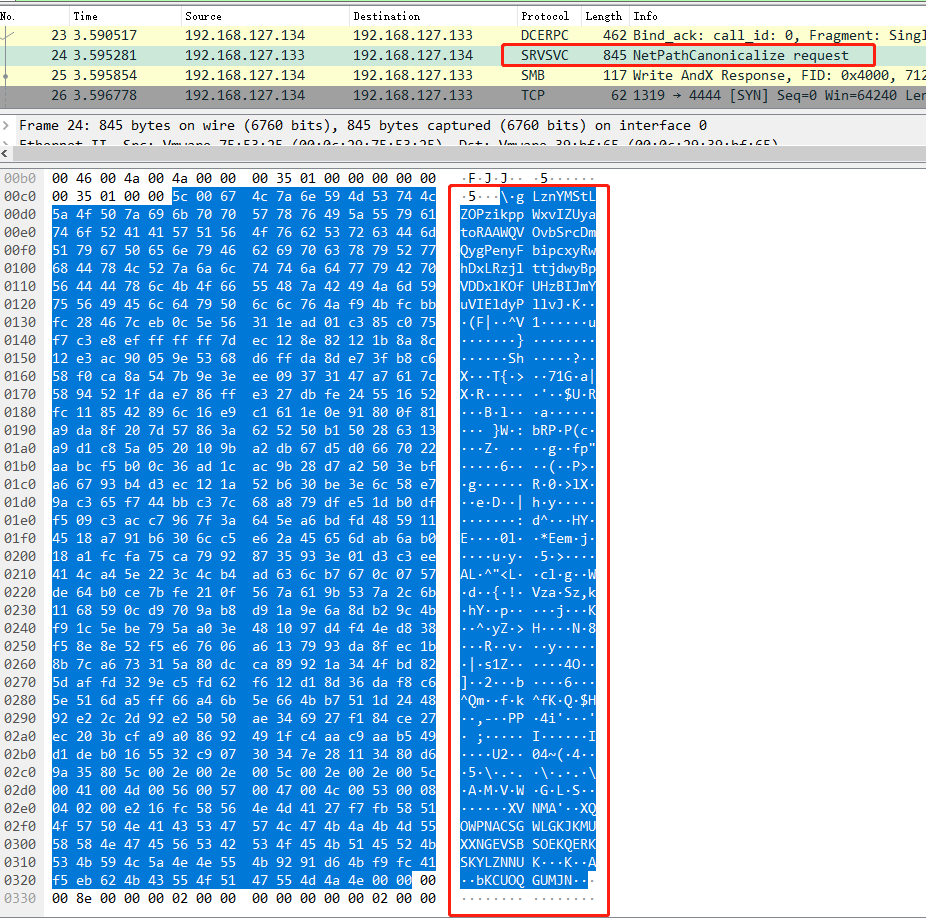


图27 Wireshark抓包显示构造恶意请求数据

## 4 恶意样本分析

主要从静态文件特征和动态文件行为两个方面对恶意样本进行分析。

### 4.1 静态文件特征分析

对恶意代码的静态文件特征分析包括杀毒软件多引擎扫描、Hash值、字符串列表、函数表、文件头信息、壳信息等。

4.1.1 杀毒软件多引擎扫描

利用在线杀毒软件扫描样本7，被认定为恶意代码，还可查看其MD5值、加壳信息等，如图28所示。

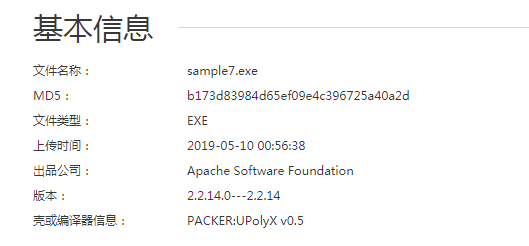


图28 在线扫描信息

4.1.2 PE文件分析

通过使用PE explorer、dependency walker等工具分析得到样本基础信息、dll依赖关系等，如图29所示。但恶意程序加壳处理后，很难得到字符串与函数信息。

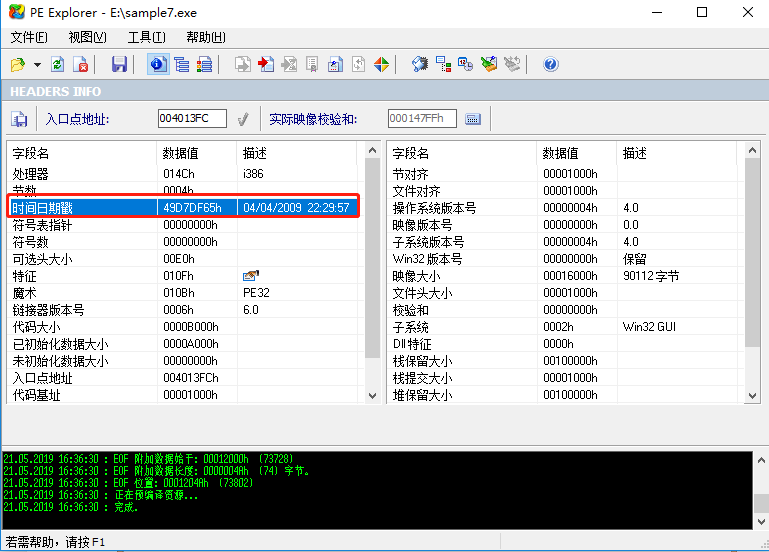


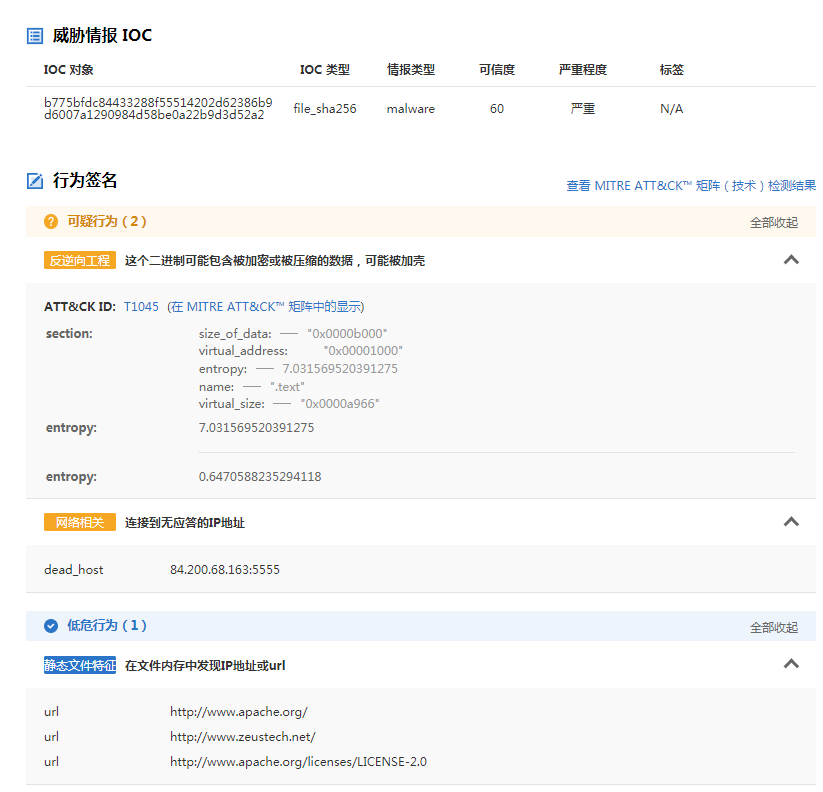
图29 文件头信息

### 4.2 动态文件行为分析

对恶意代码的动态文件行为分析包括在线沙箱分析、注册表比较及进程监控等。

4.2.1 在线沙箱

利用在线沙箱分析样本文件得到信息如图30-31所示。



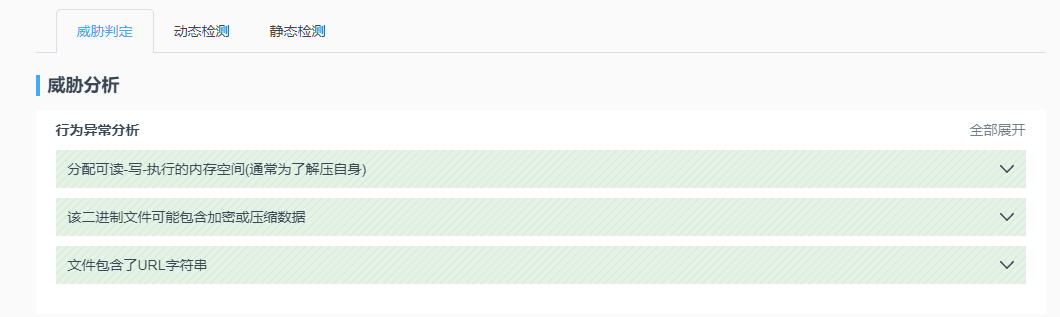


图30-31 在线沙箱分析结果

4.2.2 注册表比较

在靶机使用regshot对比恶意代码运行前后注册表的变化，如图32所示。



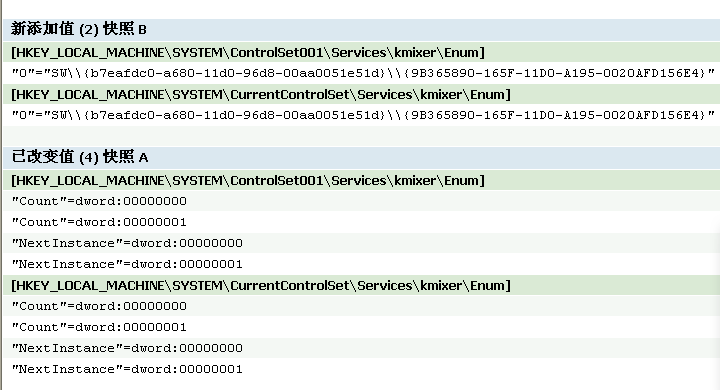


图32 注册表比较

4.2.3 进程监控

在靶机端利用ProcessMonitor监控进程的文件操作、网络连接、注册表操作、进程线程操作等。

通过设置过滤条件，查看该恶意程序无ProcessCreate、RegSetValue等敏感操作，只是对注册表的打开、查询等操作，如图33所示。并发现该程序连接到一个无响应的IP地址：84.200.68.163，进程监控结果如图34所示，Wireshark抓包结果如图35所示。

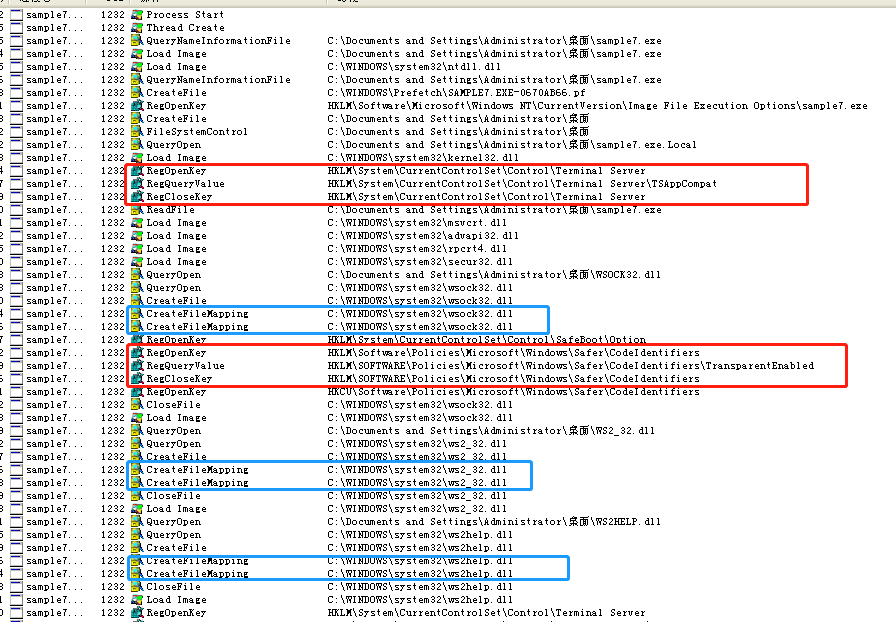


图33 进程监控结果（部分）

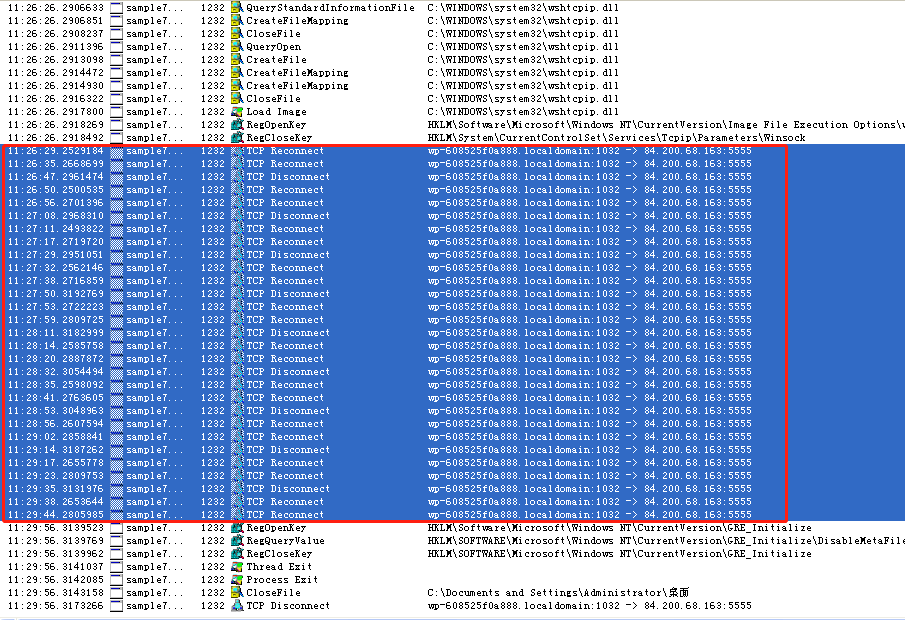


图34 进程监控结果（部分）

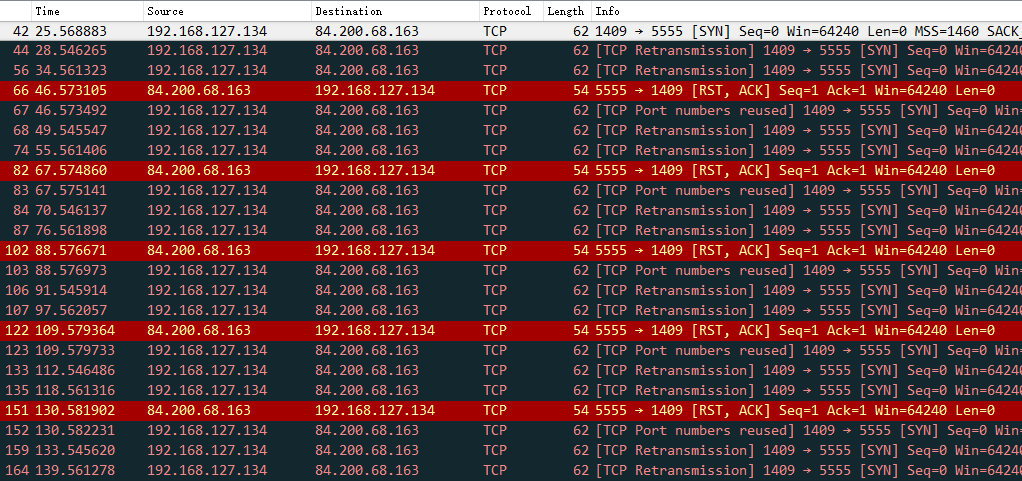


图35 Wireshark抓包结果（部分）

4.2.4 拓线查询

通过查询该恶意程序连接的IP地址，得到与之相关的数据信息如图36所示，可查看该IP地址对应的地理位置、运营商、时区等信息，同时发现与之相关联的威胁情报事件，通过网络查询关于DustySky行动的具体内容。进一步反查域名得到结果如图37所示。

DustySky行动是2016年初由ATP攻击组织Gaza Cybergang发起的针对政府机构的网络间谍活动，该行动主要以中东及北非地区的石油与天然气企业为目标，持续入侵系统并窃取数据。在以色列安全公司ClearSky发布该行动的第一篇报告之后， 该组织短暂停止了一切活动。在2016年4月又开始对以色列一些新目标进行攻击，时间点和图37显示的域名活跃时间保持一致。该组织主要集中150多个不同的目标进行攻击，其中有3/5的钓鱼邮件集中在私人的电子邮件地址 (Gmail、Yahoo、Hotmail)。

Gaza Cybergang前期主要利用恶意钓鱼邮件，如图38所示。邮件内容主要是用希伯来语、阿拉伯语还和英语，邮件包含一个压缩文件（RAR或ZIP），和一个外部链接，甚至会出现 .exe可执行文件或Word文档、视频文件及宏病毒等形式。攻击者往往还会用到一些远程工具，如Poison ivy、Nano Core、 XtremeRAT、 DarkComet 以及Spy-Net。

攻击者通过一切方式绕过基于代码的传统安全方案(如防病毒软件、防火墙、IPS等)，例如C&C服务器（mafy.2waky [.]com）就是伪造和 radaronline.com一样的网站迷惑用户，如图39所示。



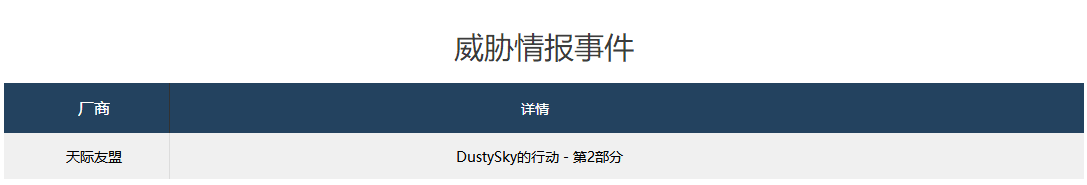


图36 查询IP地址相关信息

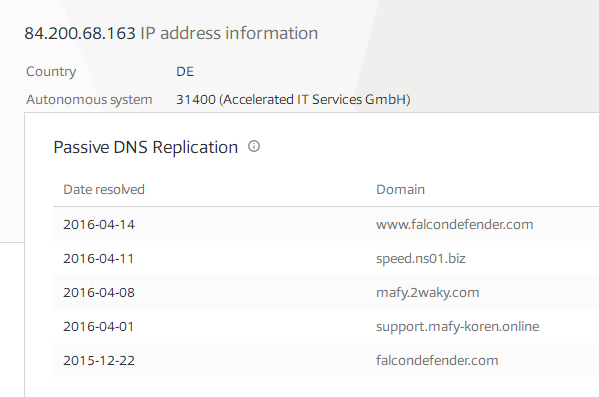


图37 反查域名相关信息





图38 恶意钓鱼邮件

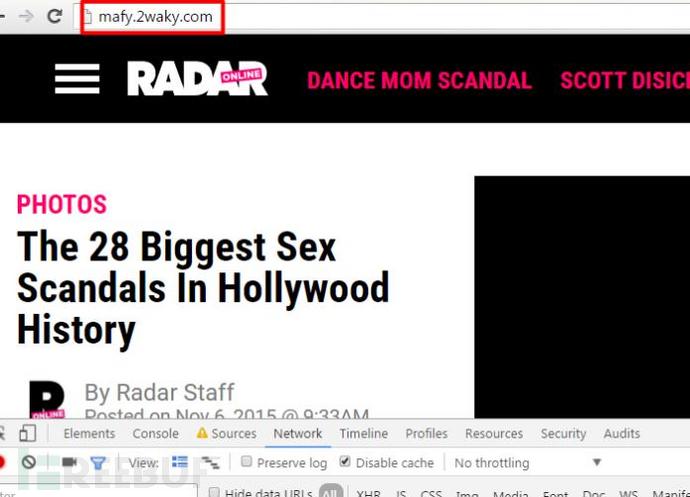


图39 攻击者伪造网站信息

## 5 总结

本文通过模拟漏洞渗透攻击环境，利用ms08\_067漏洞实现攻击机对靶机的远程控制、加载并执行恶意样本。通过对恶意样本的溯源分析，复现攻击过程，拓线查询相关信息，得到最终的威胁情报。但因个人能力水平有限，在对恶意样本静态分析过程中，未能成功将壳脱去，以至于未能对恶意样本源代码进行进一步逆向分析。此外，在拓线时，同源性分析及组织架构相关信息还有待完善。