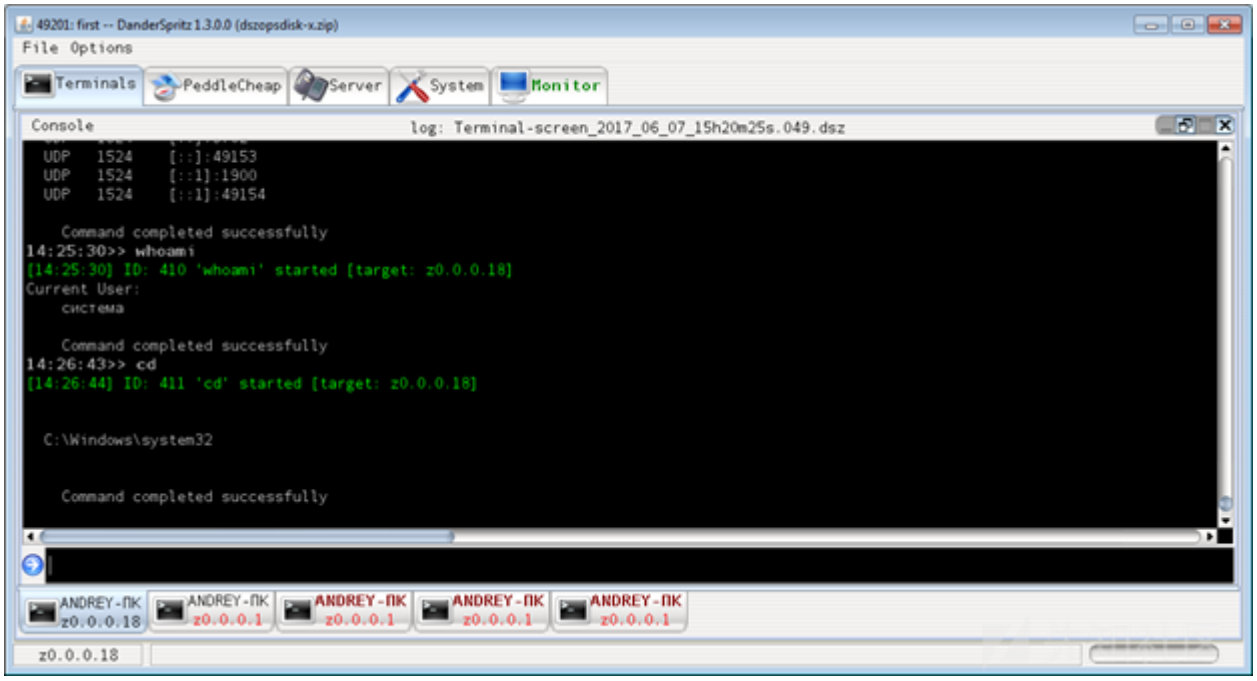
DarkPulsar后门分析

angel010 / 2018-10-20 00:35:09 / 浏览数 2384 技术文章 技术文章 顶(0) 踩(0)

来源：https://securelist.com/darkpulsar/88199/

2017年3月，ShadowBrokers（影子经纪人，是2016年夏季出现的一个黑客组织，发布了包括美国国家安全局的黑客工具在内的数个漏洞）发布了一大堆被窃的数据，其中

DanderSpritz包含的插件可以收集情报、利用漏洞、检查受控的设备；是用Java语言编写的，并提供与僵尸管理面板类似的图形化接口；还有自己的后门和插件。



DanderSprit接口

Fuzzbunch为不同工具提供了一个交互和协作的框架。其中含有不同类型的插件可以用于分析受害者、进行漏洞利用、计划任务等。FuzzBunch框架设置中含有三个文件，分

`%pluginName%-version.fb`

这是框架的实用文件，从XML中复制了header，并包含插件的ID。

`%pluginName%-version.exe`

当FuZZbuNch接受到命令后，可执行文件就会启动。

`%pluginName%-version.xml`

配置文件描述了插件的输入和输出参数，包括参数名、类型和作用描述，这些都以弹窗的形式出现在FuzzBunch中。文件对框架使用性也有一定帮助，因为其支持默认对参数

FuzzBunch分类中含有ImplantConfig，包含通过植入来控制受害者机器的插件。DarkPulsar就是控制被动后门sipauth32.tsp的管理模块，sipauth32.tsp是负责提供远程控

- Burn
- RawShellcode
- EDFStagedUpload
- DisableSecurity
- EnableSecurity
- UpgradeImplant
- PingPong

Burn, RawShellcode, UpgradeImplant, PingPong
可以移除植入，运行任意代码、升级植入，并检查远程机器上是否安装有后门。其他命令的作用并不很清楚，泄露的框架只含有一个管理模块来与DarkPulsar后门进行协作。

在分析管理模块时，研究任意发现了多个用于加密C2与植入之间流量的常数：

```
(TcLog)(v2, 5, "[+] - Performing crypto session setup\n");
v3 = v1[1];
sub_402B70(pbBuffer, 4u);
*&pbBuffer[4] = 0x3BA6814F - *pbBuffer;
v4 = *pbBuffer ^ (0x3BA6814F - *pbBuffer);
v5 = *v1;
*(&v28 + 1) = 4;
HIBYTE(v27) = 5;
*(&v27 + 3) ^= v4;
*(&v28 + 3) = v4 ^ 0xAA64F13D;
v21 = 16;
v20 = 16;
v22 = pbBuffer;
v6 = (*(*v5 + 8))(&v20, &v23);
v7 = v6;
if ( v6 && v6 != 0x90312 )
{
  TcLog(v1[2], 3, "[%s] - CDPProtocolHandler::SendRecv Failed (0x%x)\n",
        "CDPClient::PerformSetupSession", v6);
}
else
{
  v8 = v25;
  if ( (v25 || v23) && v23 >= 16 )
  {
    v9 = *v25;
    v16 = v25;
    if ( *v25 + v25[1] == 0xA13C82E )
```

研究人员认为这些常数应该出现在后门中，因此研究人员对这些常数进行了检测。几个月后研究人员发现了DarkPulsar后门，之后还发现了32位和64位版本。

研究人员发现了大概50个受害者，分别位于俄罗斯、伊朗和埃及，主要感染的是Windows 2003/2008 server。这些目标主要与核能源、电信、IT、航空和研发有关。

DarkPulsar技术细节

DarkPulsar注入是一个动态库，其payload应用在输出函数中。这些函数可以分为以下几组：

1. 系统中两个用来安装后门的函数；
2. 名字与TSPI（Telephony Service Provider Interface电话服务提供商接口）操作相关的函数，用来确保后门在自动运行列表中并可以自动运行；
3. 名字与SSPII（Security Support Provider Interface安全支持提供商接口）操作相关的函数，用来实现主恶意payload。

SSPI和TSPI接口的实现非常简单：由DarkPulsar导出的函数有与接口函数系统的函数名，但其中包含的恶意代码而不是电话服务。

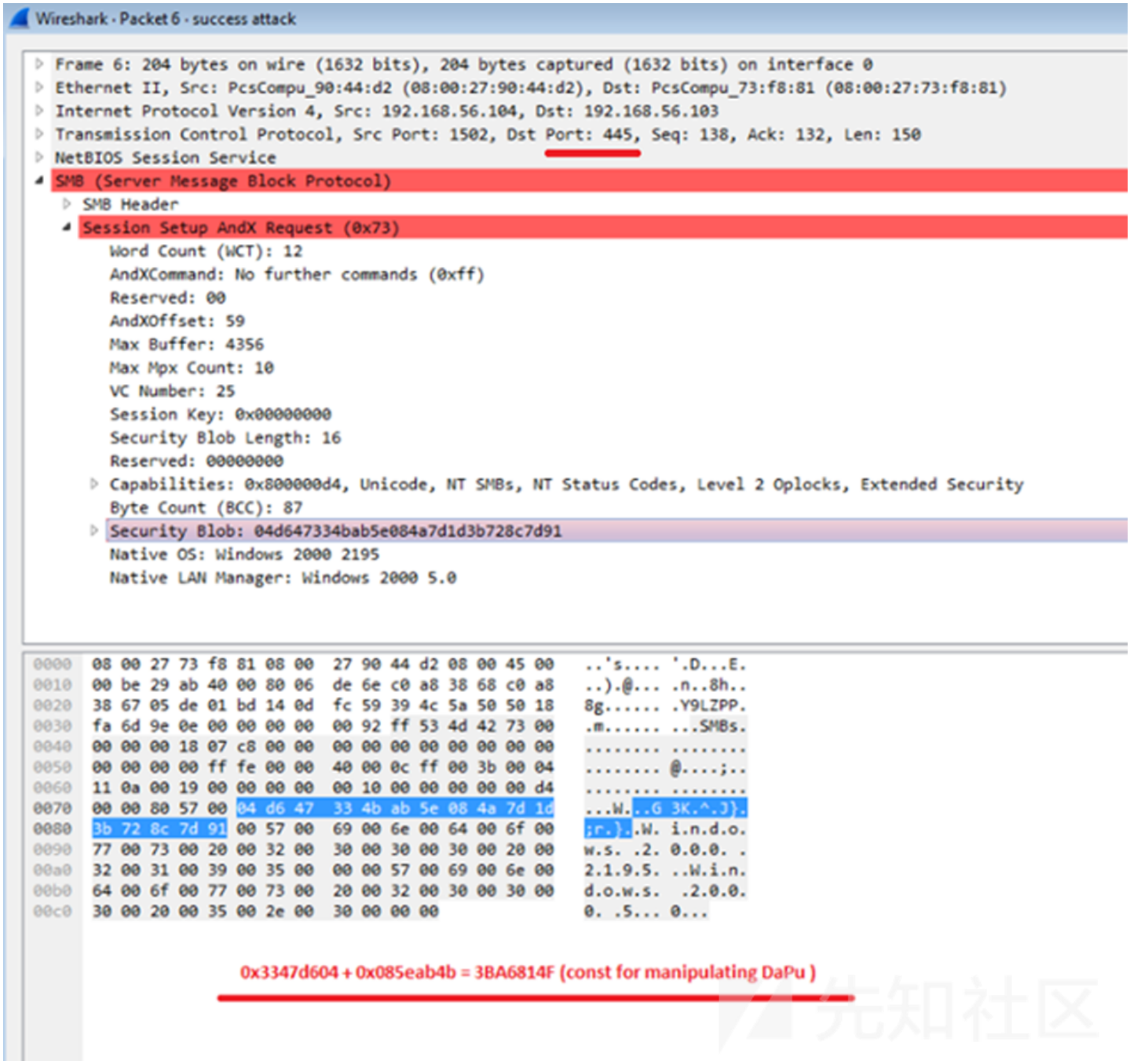
植入是通过无名的导出函数安装在系统中的。以管理权限在其库路径中调用`Secur32.AddSecurityPackage`可以启动后门，`lsass.exe`会以SSP/AP加载DarkPulsar，D

Telephony API (TapiSrv)会与Remote Access Connection Manager (RasMan)服务一起启动在开始时加载，设置`startup`类型为`Automatic`。在加载电话服务提供商的库时，TapiSrv会调用`TSPI_lineNegotiateTSPIVersion`，其中含有

DarkPulsar通过为负责认证的函数`SpAcceptLsaModeContext`安装hook来应用payload。这样的注入出现在`lsass.exe`进程的许多系统认证包中，而且允许Darkpulsar基

- `Msv1_0.dll – for the NTLM protocol,`
- `Kerberos.dll – for the Kerberos protocol,`
- `Schannel.dll – for the TLS/SSL protocols,`
- `Wdigest.dll – for the Digest protocol, and`
- `Lsasrv.dll –for the Negotiate protocol.`

之后，Darkpulsar就获得了将恶意软件流量嵌入系统协议的能力。因为网络活动是根据标准系统流量产生的，所以只会反映在系统进程中，即在不影响正常操作的前提下使用



成功连接到DarkPulsar注入的网络流量

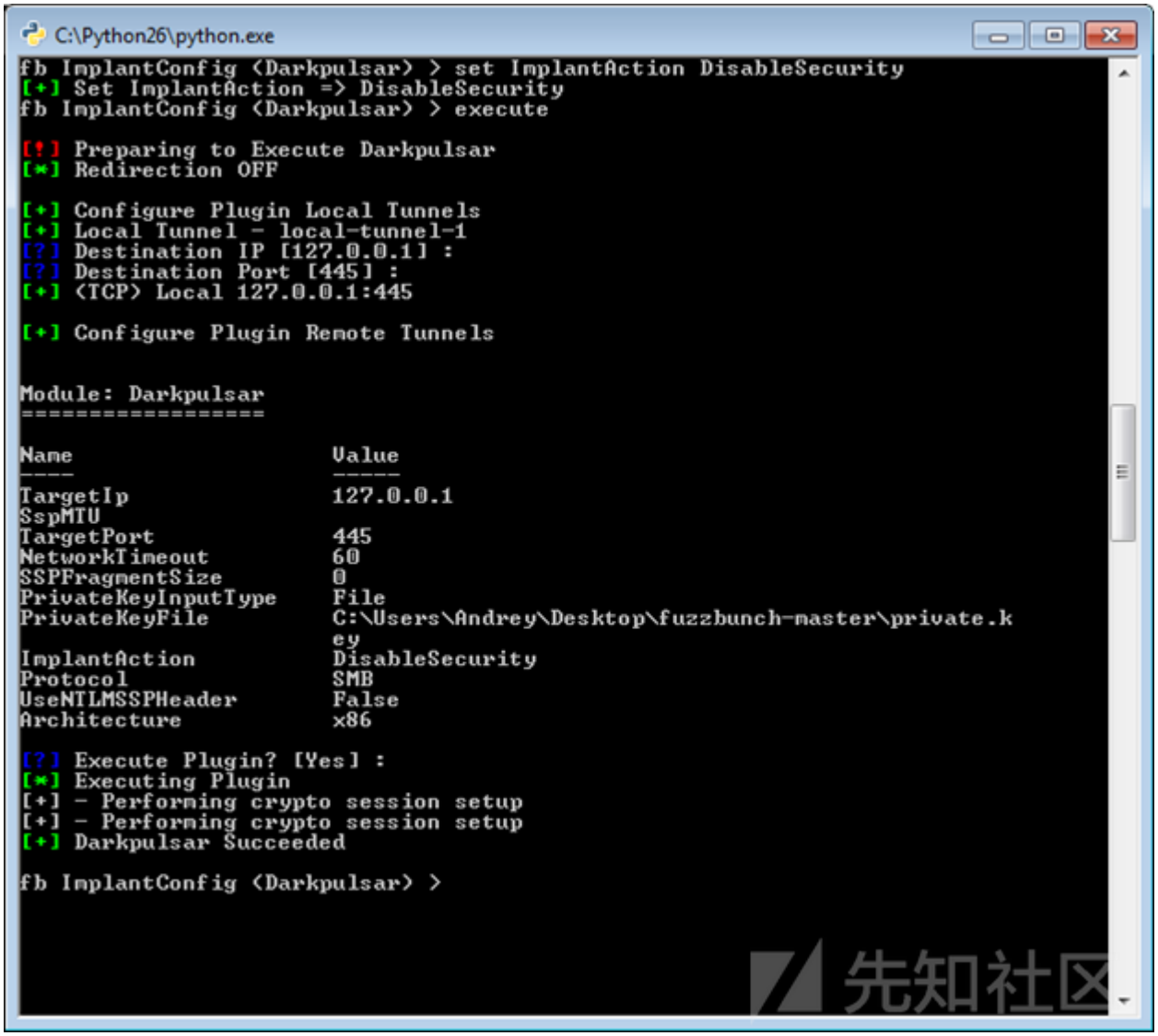
控制认证过程的第二个好处是可以绕过输入用户名和密码来获取对需要认证才可以访问的对象访问权限，此类对象包括进程列表、远程注册表、通过SMB的文件系统。当Da

与DarkPulsar协作

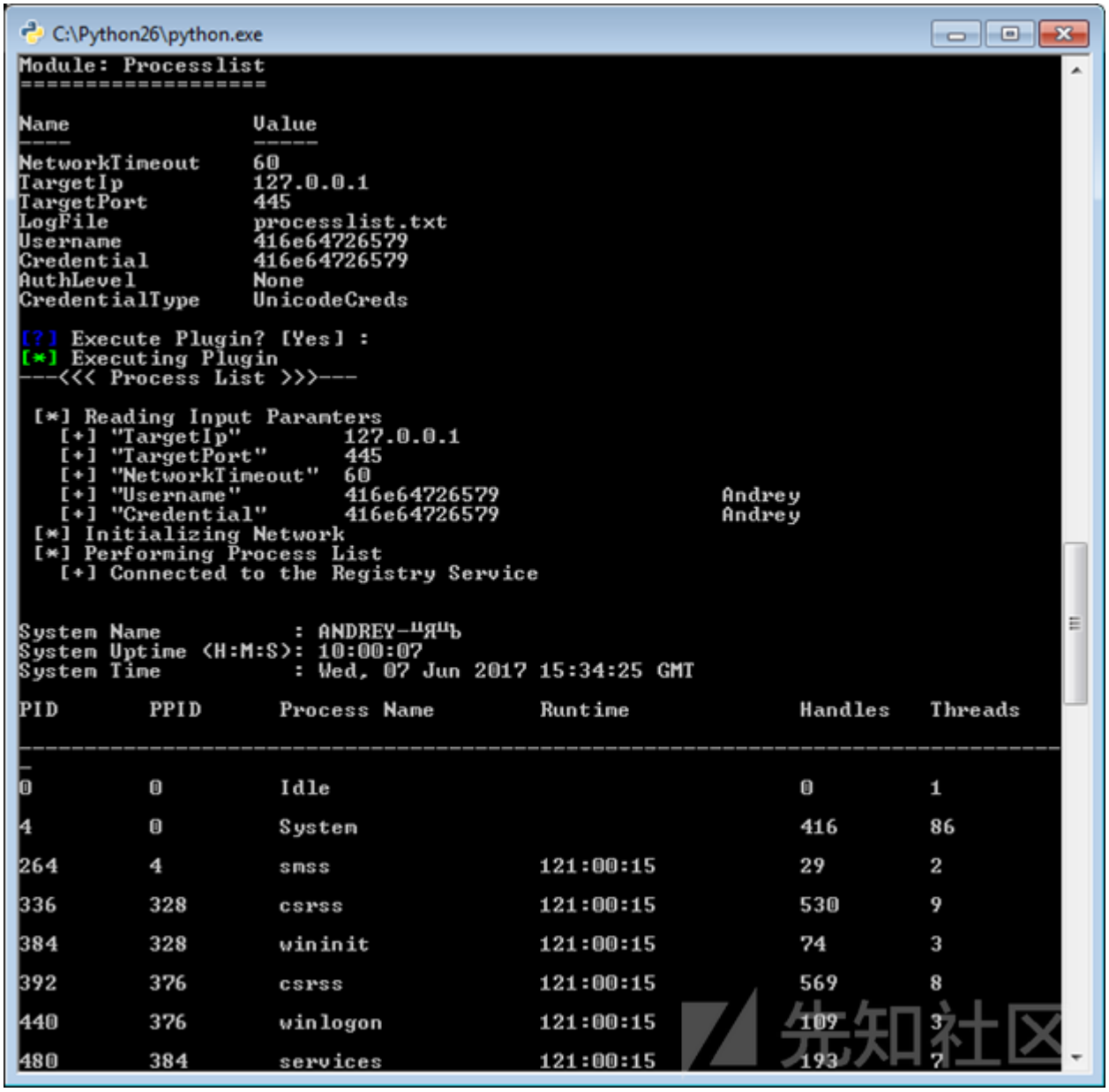
Darkpulsar-1.1.0.exe是遵循`one command – one launch`的管理接口。命令必须在配置文件`Darkpulsar-1.1.0.9.xml`中指定或以命令行参数的形式才能执行，包括：

- 目标机器使用32位或64位系统的情况；
- 传输命令和端口号的协议；
- 用于解密session AES key的私有RSA key。

Darkpulsar-1.1.0并不是为了管理受感染机器的独立程序。而是Fuzzbunch框架的一个插件，该框架可以管理参数和相应的不同组件。下图是Fuzzbunch框架中的`DisableS`



下图是Processlist示例，允许在没有凭证和操作的情况下运行任意插件：



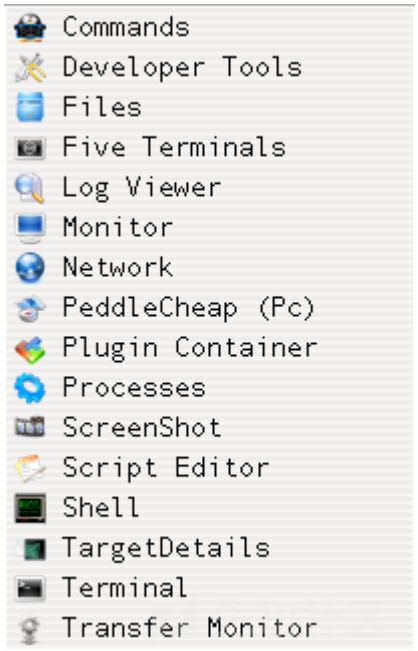
DanderSpritz

DanderSpritz是一个控制受感染机器的框架，与FuZZbuNch不同。DanderSpritz为不同的后门服务，在受害者机器上使用PeedleCheap来启用插件。PeddleCheap是Dan

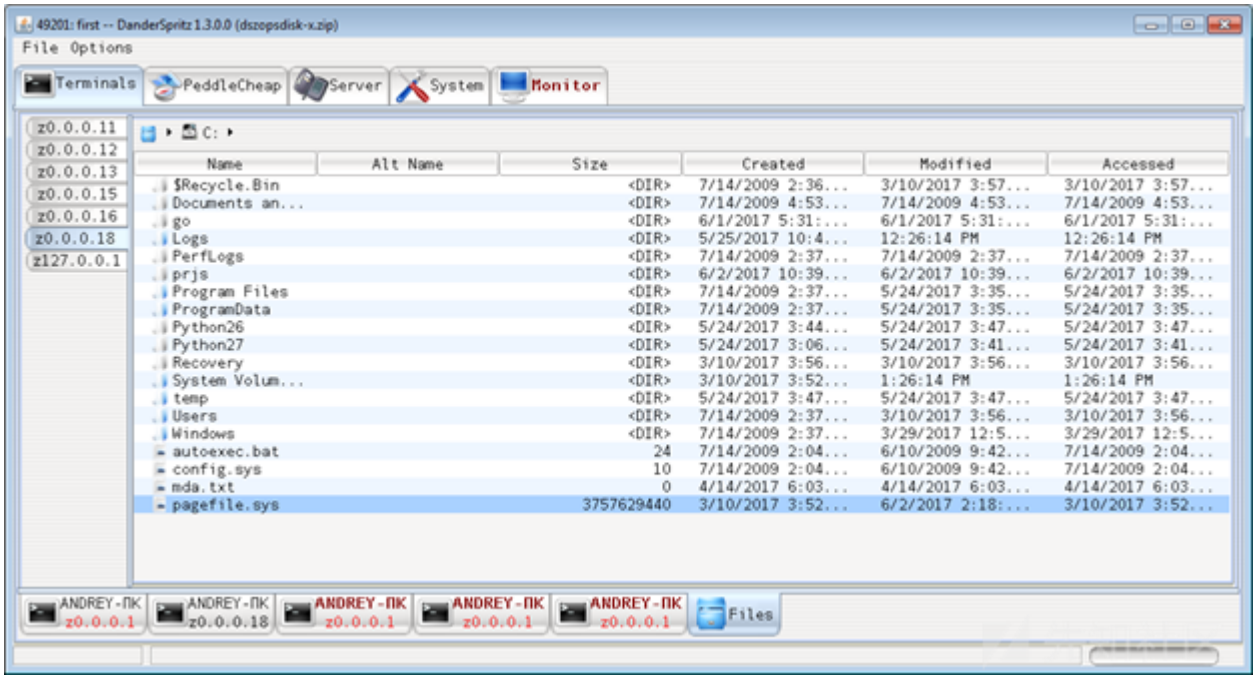
这也就是`EDFStagedUpload`模式的DarkPulsar提供机会来以功能性更强的植入来感染受害者：PCDllLauncher在受害者端应用PeddleCheap植入，DanderSpritz提供用户`DLL Launcher`。

含有PeddleCheap、DarkPulsar、PCDllLauncher插件的完整DanderSpritz使用方案包含4步：

- 通过FuZZbuNch运行命令 EDFStagedUpload来启动DarkPulsar；
- 在DanderSpritz中，运行命令pc_prep (PeedelCheap Preparation)来准备在植入端启动的payload和库；
- 在DanderSpritz中，运行命令pc_old，该命令是用来从Pcdlllauncher等待socket；
- 通过FuZZbuNch 启动Pcdlllauncher，指定payload的路径，payload是用ImplantFilename参数的pc_prep命令准备好了。



DanderSpritz



文件系统插件

结论

FuzzBunch和DanderSpritz框架是灵活的框架，并可以根据其工具扩展功能。每个框架含有用于不同任务的插件，FuzzBunch插件负责监听和攻击受害者，DanderSpritz框

DarkPulsar后门的发现可以帮助理解其在两个框架之间所起的桥接作用。鉴于DarkPulsar驻留和静默的能力，它也是攻击平台的一部分。将恶意流量封装到合法协议中、绕过

IOCs
implant `96f10cfa6ba24c9ecd08aa6d37993fe4`
文件路径 `%SystemRoot%\System32\sipauth32.tsp`
注册表 `HKLM\Software\Microsoft\Windows\CurrentVersion\Telephony\Providers`

https://securelist.com/darkpulsar/88199/

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板