登录

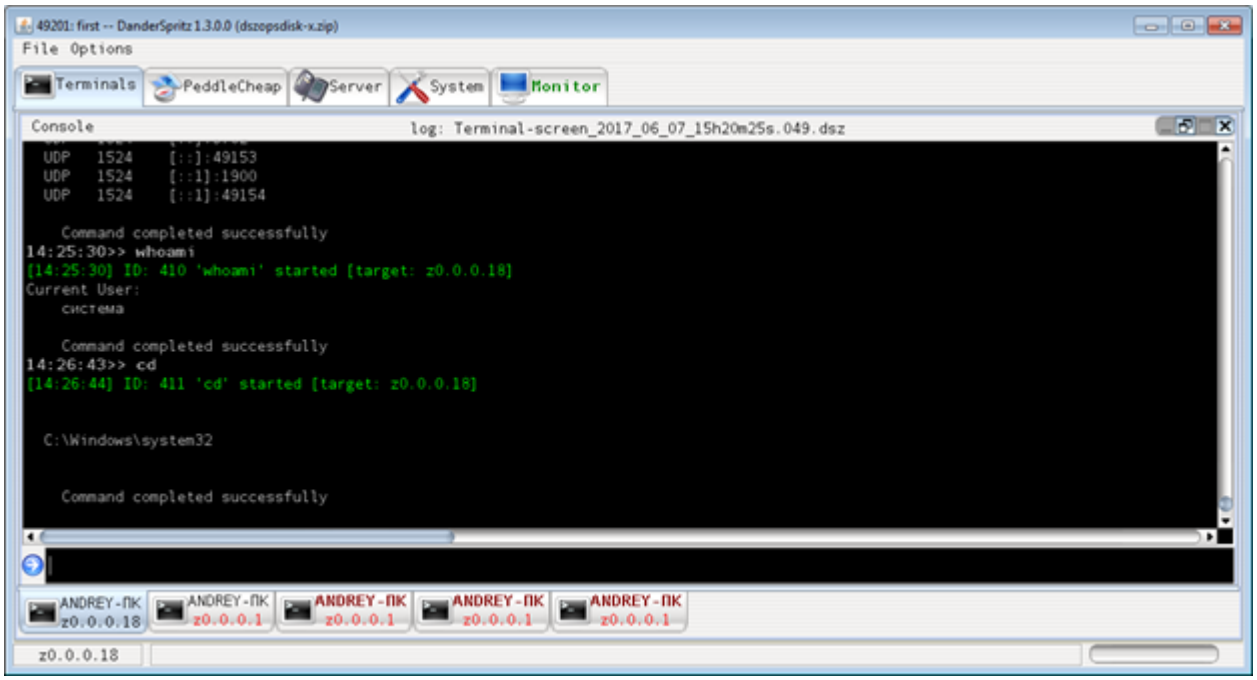
“黑暗恒星”事件分析

s小胖不吃饭 / 2018-10-20 10:36:55 / 浏览数 2408 技术文章 技术文章 顶(1) 踩(0)

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

在2017年3月，ShadowBrokers发表了一大部分被盗数据，其中包含两种构架：DanderSpritz 和 FuzzBunch。

DanderSpritz完全由插件组成，用于收集情报，使用漏洞并检查已经被控制的机器。它是用Java编写的，提供了类似于僵尸网络管理面板的图形窗口界面以及类似Metasplo



在另一方面DanderSprit
接口Fuzzbunch为不同的实用程序提供了一个交互和协同工作的框架。它包含各种类型的插件，用于分析受害者，利用漏洞，计划任务等。FuzzBunch框架的插件集中有三

- %pluginName%-version.fb

这是框架的实用程序文件。 它从XLM复制标头并包含插件的ID。

- %pluginName%-version.exe

当FuZZbuNch收到执行此命令的命令时，将启动此可执行文件。

- %pluginName%-version.xml

此配置文件描述了插件的输入和输出参数—参数名称，其类型和对其负责的描述；所有这些可以在FuzzBunch中显示为提示。该文件也为框架的可用性做出了很大贡献，因

最有趣的Fuzzbunch类别之一称为ImplantConfig，其中包含旨在通过植入后控制受感染机器的插件。DarkPulsar是一个非常有趣的管理模块，用于控制名为”sipauth32.ts

它支持以下命令：

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

Burn，RawShellcode，UpgradeImplant和PingPong移除植入物，运行任意代码，升级植入物并检查后门是否分别安装在远程机器上。
其他命令的目的并不那么明显，更糟糕的是，泄漏的框架只包含管理模块来处理DarkPulsar的后门，而不是后门本身。

在分析管理模块时，我们注意到几个常量用于加密C＆C和植入物之间的流量：

```
(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 )
```

我们认为可能这些常量也应该出现在后门中，因此我们为它们创建了一个检测器。几个月后，我们发现了神秘的DarkPulsar后门。后来我们能够找到32位和64位版本。

我们发现大约50名受害者位于俄罗斯，伊朗和埃及，通常感染Windows 2003/2008服务器。 目标涉及核能，电信，IT，航空航天和R&D研发。

DarkPulsar 技术亮点

DarkPulsar植入体是一个动态库，其有效载荷在导出的函数中实现。这些功能可以分组如下：

1.两个无名函数用于在系统中安装后门。
2.名称与TSPI（电话服务提供程序接口）操作相关的函数，用于确保后门位于自动运行列表中并能够自动启动。
3.具有与SSPI（安全支持提供程序接口）操作相关的名称的函数。它承载了主要的恶意负载。

SSPI和TSPI接口的实现是简洁的：DarkPulsar导出的函数与接口函数的名称相同; 但是，它们包含恶意代码而不是电话服务。

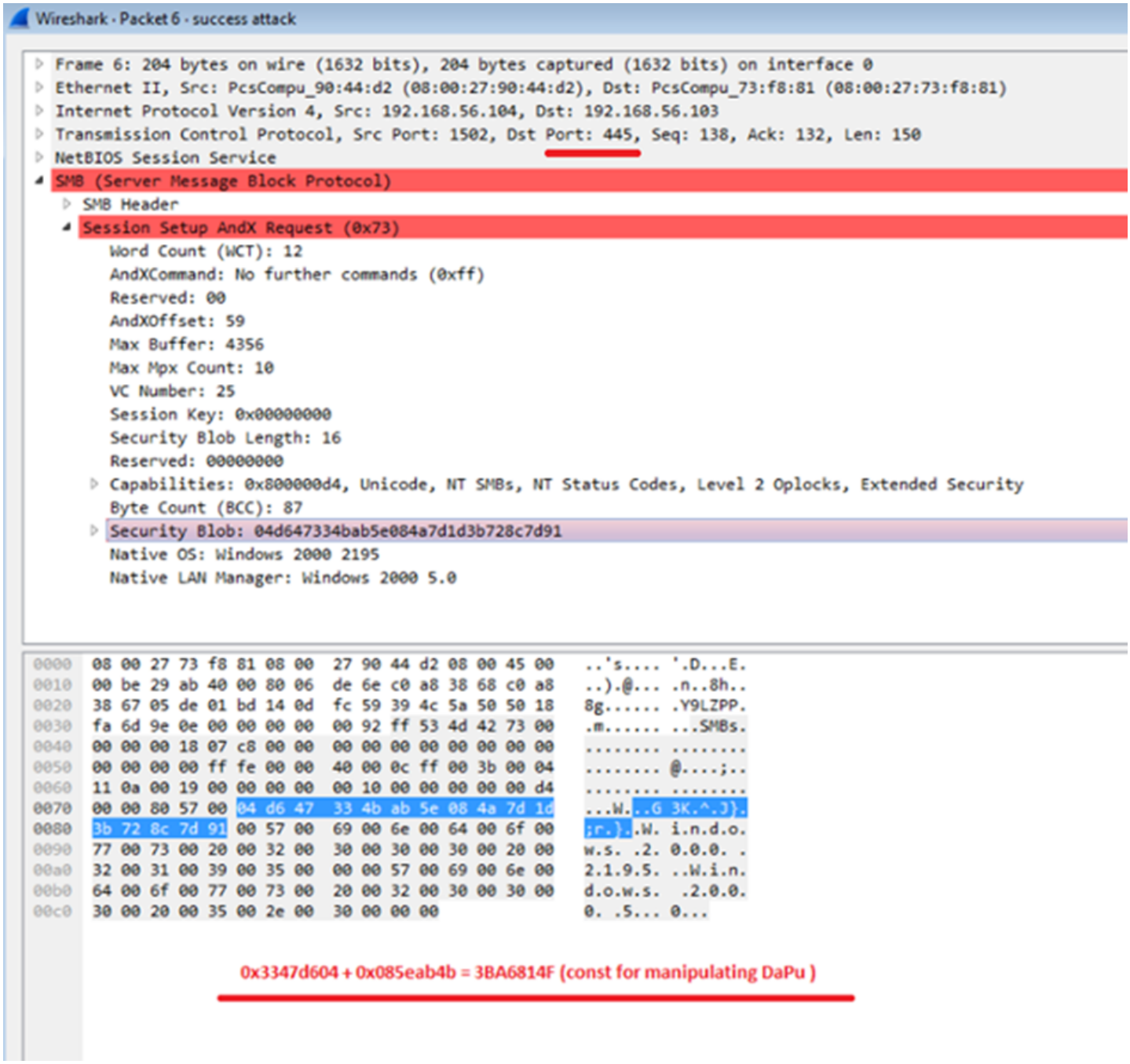
植入物通过无名导出功能安装在系统中。通过调用具有管理员权限的`Secur32.AddSecurityPackage`以及参数中它自己的库的路径来启动后门，导致`lsass.exe`将DarkP
/ AP，并由DarkPulsar初始化后门来调用其导出的函数`SpLsaModeInitialize`。这样，`AddSecurityPackage`用于将代码注入`lsass.exe`。
它还在`HKLM\Software\Microsoft\Windows\CurrentVersion\Telephony\Providers`添加了库名。

这是在远程访问连接管理器（RasMan）服务旁边启动的Telephony
API（TapiSrv）开始加载，将启动类型设置为"自动"。加载由电话服务提供商的库时，TapiSrv调用TSPI_lineNegotiateTSPIVersion，其中包含AddSecurityPackage调用以

DarkPulsar通过为SpAcceptLsaModeContext（负责身份验证的函数）安装钩子来实现其有效负载。此类注入在进程lsass.exe中的多个系统身份验证数据包中生成，并允许

- Msv1_0.dll – 用于NTLM协议，
- Kerberos.dll – 用于Kerberos协议，
- Schannel.dll – 用于TLS / SSL协议，
- Wdigest.dll – 用于摘要协议，
- Lsasrv.dll – 用于谈判协议。

在此之后，Darkpulsar能够将恶意软件流量嵌入到系统协议中。由于此网络活动是根据标准系统图表进行的，因此它只会反映在系统进程中，它使用为上述协议保留的系统端



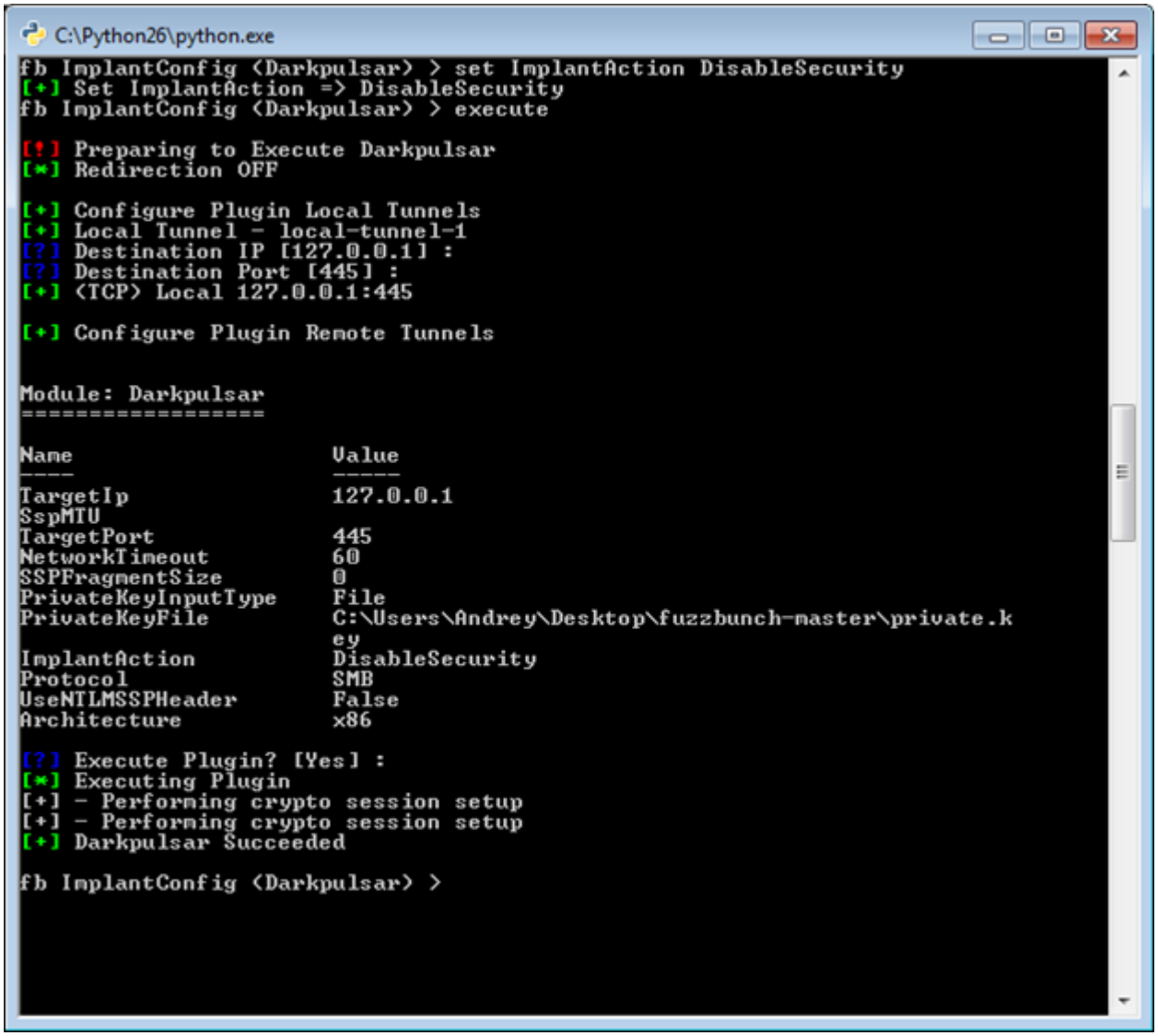
控制身份验证过程的第二个优点是可以绕过输入有效的用户名和密码，以获取对需要身份验证的对象的访问权限，例如进程列表，远程注册表，通过SMB的文件系统。发送D

利用DarkPulsar工作

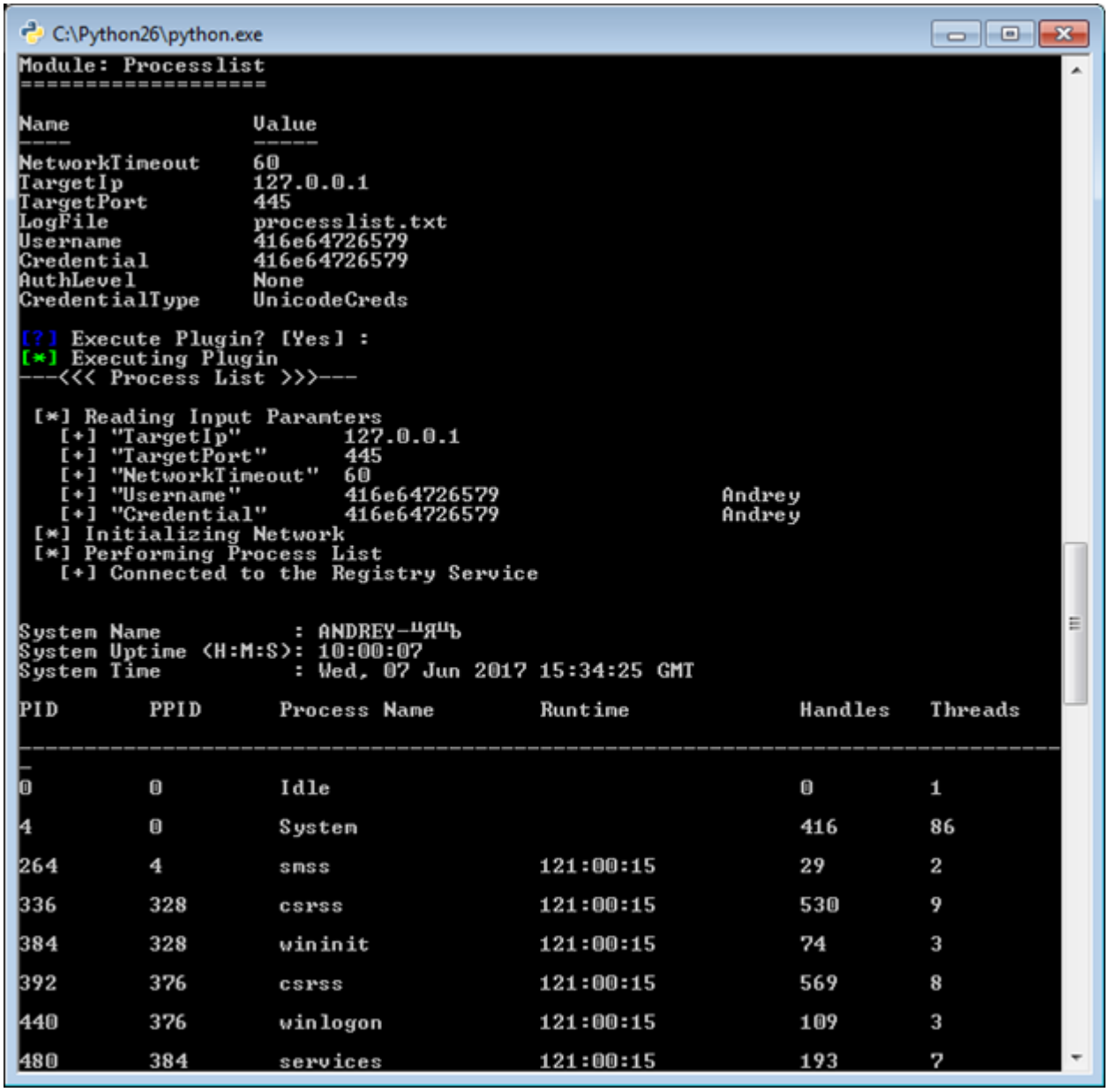
Darkpulsar-1.1.0.exe是在"一个命令-一次启动"原则下工作的管理界面。要执行的命令必须在配置文件Darkpulsar-1.1.0.9.xml中指定或者作为命令行参数指定，至少详细说

- 目标计算机是使用32位还是64位系统；
- 提供命令和端口号的协议（支持SMB，NBT，SSL，RDP协议）
- 私有RSA密钥，用于解密会话AES密钥

Darkpulsar-1.1.0并非是管理受感染机器的独立程序。该实用程序是Fuzzbunch框架的插件，可以管理参数和协调不同的组件。以下是Fuzzbunch中的DisableSecurity命令



下面是DisableSecurity之后的Processlist示例，允许执行任何没有有效凭据的插件，并通过常规系统功能（远程注册表服务）进行操作：



DanderSpritz

DanderSpritz是用于控制受感染机器的框架，与FuZZbuNch不同，因为后者为具有特定功能的后开发阶段提供了有限的工具包，例如DisableSecurity和DarkSeuls的Enabl

DanderSpritz适用于更大范围的后门，在受害者中使用PeedleCheap来启动运营商以启动插件。PeddleCheap是DanderSpritz的插件，可用于配置植入物并连接到受感染的

这就是EDFStagedUpload模式中的DarkPulsar如何通过更实用的植入物为受害者提供感染的机会：PCDllLauncher（Fuzzbunch的插件）在受害者一侧部署PeddleCheap
DLL Launcher'。

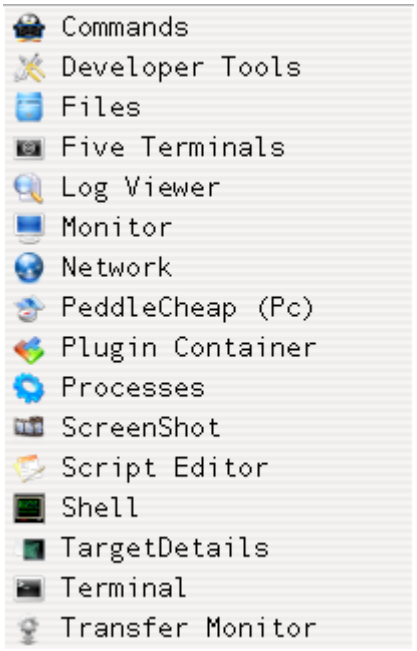
完整的DanderSpritz与通过FuZZbuNch 的 PeddleCheap插件及DarkPulsar和PCDllLauncher插件使用方案包含四个步骤：

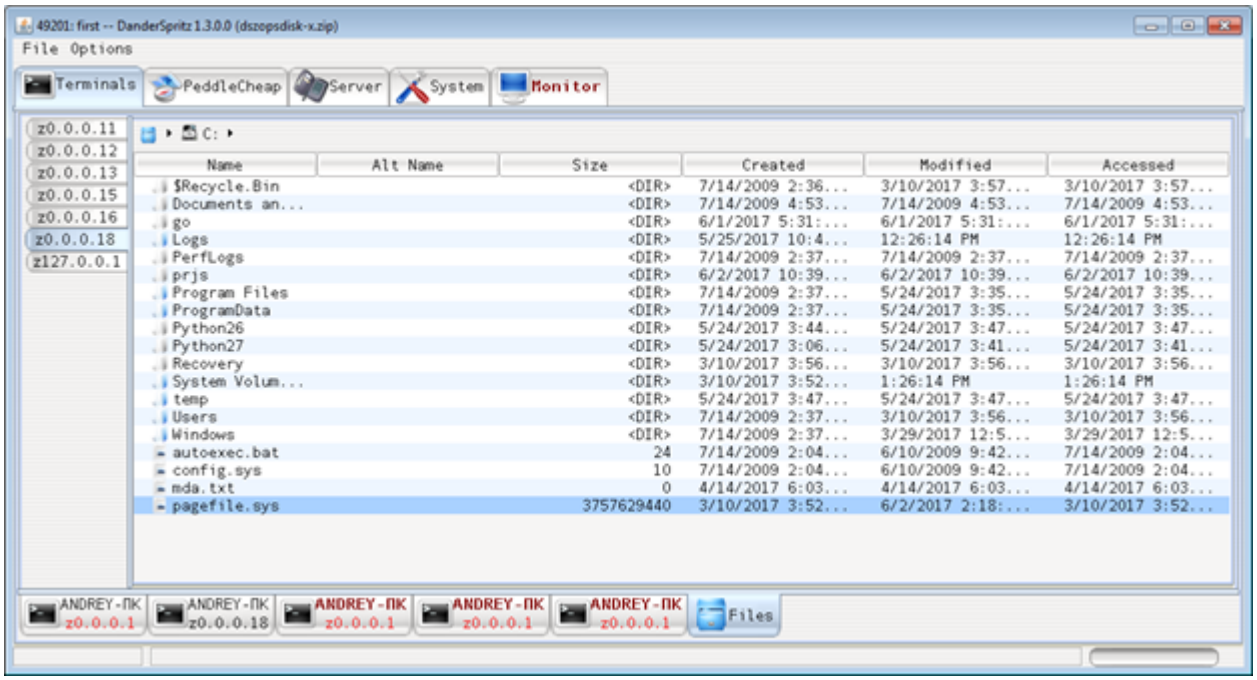
1.通过FuZZbuNch，运行命令EDFStagedUpload以启动DarkPulsar。

2.在DanderSpritz中，运行命令pc_prep（PeedelCheap Preparation）以准备有效载荷和要在种植体侧启动的库。

3.在DanderSpritz中，运行命令pc_old（这是命令pc_listen -reuse -nolisten -key Default的别名）,这会将其设置为等待来自Pcdlllauncher的套接字。

4.通过FuZZbuNch启动Pcdlllauncher并指定使用ImplantFilename参数中的命令pc_prep准备的有效负载的路径。





结论

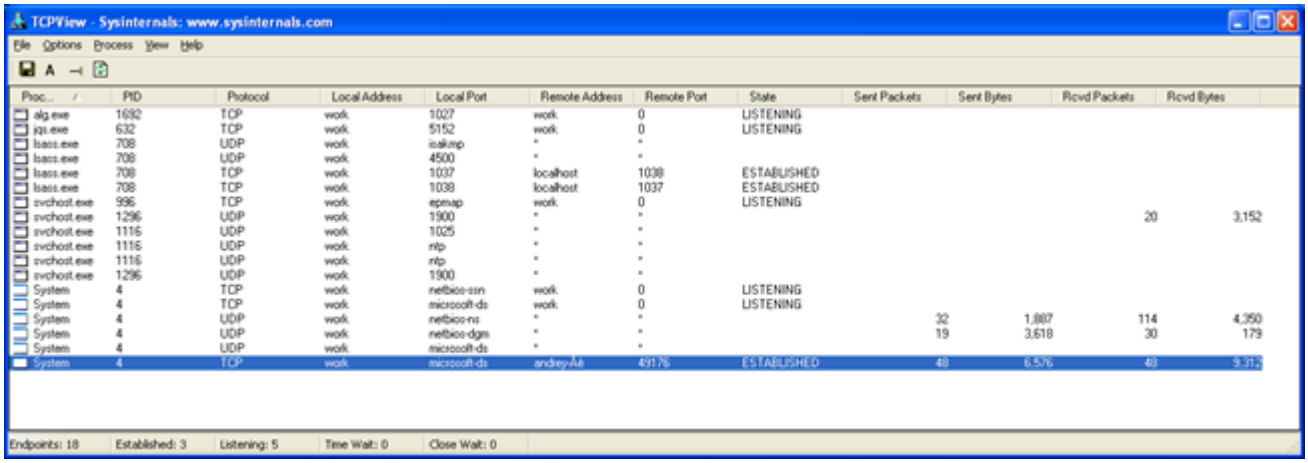
FuzzBunch和DanderSpritz框架旨在提高灵活性，扩展功能并与其他工具兼容。它们都包含一组专为不同任务设计的插件：虽然FuzzBunch插件负责侦察和攻击受害者，但

DarkPulsar后门的发现有助于理解它作为两个泄露框架之间的桥梁的作用，以及它们如何基于DarkPulsar的持久性和隐身性的先进能力，成为同一攻击平台的一部分，这些

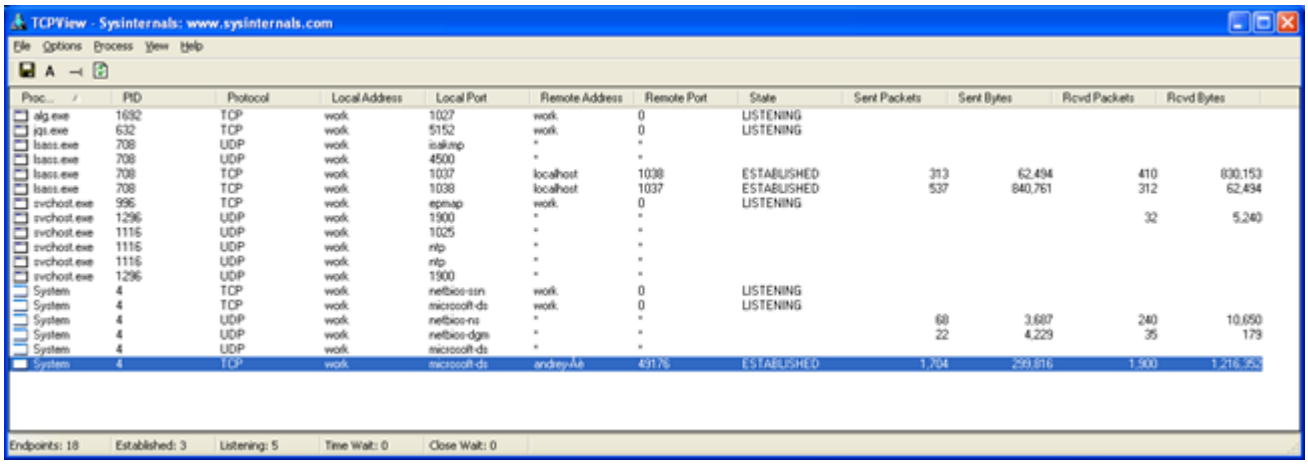
我们的产品可以完全删除与此攻击恶意软件相关的内容。

检测恶意网络活动

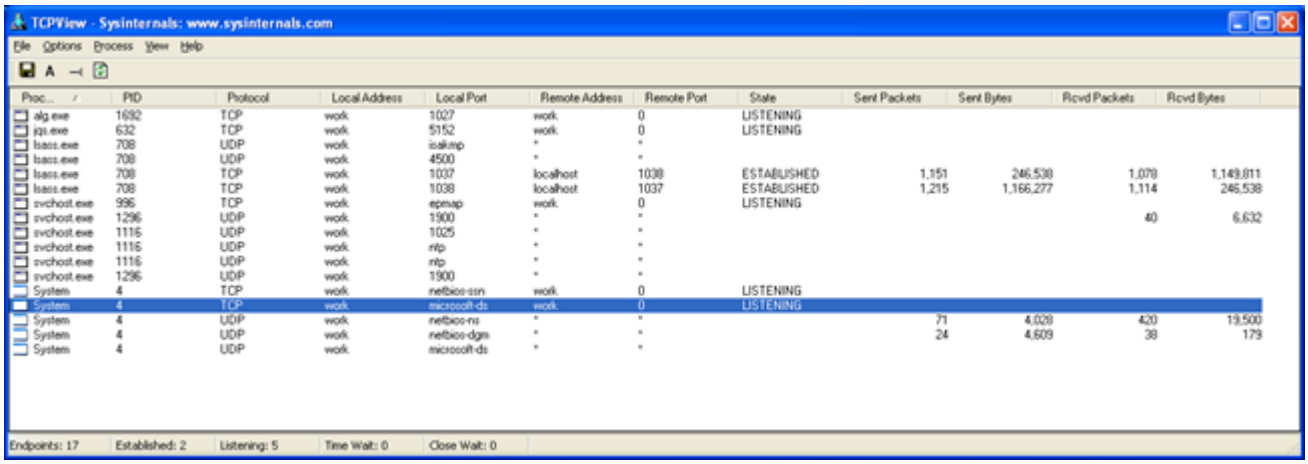
在受感染的计算机中执行EDFStagedUpload时，会建立永久连接，这就是出现通过端口445的流量的原因。lsass.exe中还出现一对绑定套接字：



当DanderSpritz通过PcDllLauncher插件部署PeddleCheap的有效负载时，网络活动会急剧增加。



当终止与受感染计算机的连接时，网络活动将停止，并且只保留lsass.exe中两个绑定套接字的跟踪：



IOCs

```
implant – 96f10cfa6ba24c9ecd08aa6d37993fe4
File path – %SystemRoot%\System32\sipauth32.tsp
Registry – HKLM\Software\Microsoft\Windows\CurrentVersion\Telephony\Providers
```


上一篇：D-Link 850L&645路由... 下一篇：区块链安全—白话parity多签名...

1. 0 条回复
   - 动动手指，沙发就是你的了！

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