

0x00 前言

DanderSpritz是NSA的一款界面化的远控工具，基于FuzzBunch框架，执行Start.jar即可启动。

在实际测试过程中，由于缺少说明文档，遇到的问题有很多，同时一些细节也值得深入研究。所以本文将要帮助大家答疑解惑，分享测试心得，结合木马特点分析防御思路。

0x01 简介

本文将要介绍以下内容：

> 执行pc_prep无法获得回显的原因及解决方法

> Pc同Pc2.2的区别

> level3和level4木马代表的含义及如何使用

> 各类型木马区别

> dll木马利用方式

> Windows单条日志删除功能

> 木马查杀思路

0x02 实际测试

测试环境：Win7 x86

安装如下工具：

> python2.6

> pywin32

> jdk

1、下载fuzzbunch

参考链接：<https://github.com/3gstudent/fuzzbunch>

注：

我fork了公开的fuzzbunch项目<https://github.com/fuzzbunch/fuzzbunch>，并添加了部分内容，解决了一个bug，具体内容会在后面介绍

2、直接运行Start.jar

如图

设置启动参数，Log Directory需要设置成固定格式：c:\logsxxx(xxx任意名称)

否则，会出现报错，如下图

注：

网上的部分分析文章认为应该先用fb.py生成一个日志文件，接着Start.jar指向该目录，其实不需要，只要路径格式正确即可

3、执行pc_prep配置木马

输入pc_prep获得回显，如下图

注：

有很多人在测试的时候发现输入pc_prep无法获得回显，如下图

原因：

fuzzbunch工程下载自如下链接：https://github.com/x0rz/EQGRP_Lost_in_Translation

文件缺失，导致该错误。

正确的下载位置：<https://github.com/fuzzbunch/fuzzbunch>

但是，下载后还需要补全缺失的文件，才能完全正常使用。

我fork了上述工程，并补全了缺失文件，下载我的github即可解决上述问题，地址如下：<https://github.com/3gstudent/fuzzbunch>

补充：

在之前的测试过程中，使用了存在bug的版本，虽然pc_prep无法获得回显，但是使用pc2.2_prep可以生成木马。如下图

可是木马无法回连

猜测原因：

pc相对于Pc2.2版本更高，低版本已经不再使用。

查看ResourcesPc2.2Version.xml，显示：PeddleCheap 2.2.0.2，表示Pc2.2对应的PeddleCheap版本为2.2.0.2。

查看ResourcesPcVersion.xml，显示：PeddleCheap 2.3.0，表示Pc对应的PeddleCheap版本为2.3.0。

注：

PeddleCheap用来操作同木马通信，在DanderSpritz主面板显示

4、木马分类

可选择的木马类型如下：

- 1) – Standard TCP (i386-winnt Level3 sharedlib)
- 2) – HTTP Proxy (i386-winnt Level3 sharedlib)
- 3) – Standard TCP (i386-winnt Level3 exe)
- 4) – HTTP Proxy (i386-winnt Level3 exe)
- 5) – Standard TCP (x64-winnt Level3 sharedlib)
- 6) – HTTP Proxy (x64-winnt Level3 sharedlib)
- 7) – Standard TCP (x64-winnt Level3 exe)
- 8) – HTTP Proxy (x64-winnt Level3 exe)
- 9) – Standard TCP Generic (i386-winnt Level4 sharedlib)
- 10) – HTTP Proxy Generic (i386-winnt Level4 sharedlib)
- 11) – Standard TCP AppCompat-enabled (i386-winnt Level4 sharedlib)
- 12) – HTTP Proxy AppCompat-enabled (i386-winnt Level4 sharedlib)
- 13) – Standard TCP UtilityBurst-enabled (i386-winnt Level4 sharedlib)
- 14) – HTTP Proxy UtilityBurst-enabled (i386-winnt Level4 sharedlib)
- 15) – Standard TCP WinsockHelperApi-enabled (i386-winnt Level4 sharedlib)
- 16) – HTTP Proxy WinsockHelperApi-enabled (i386-winnt Level4 sharedlib)
- 17) – Standard TCP (i386-winnt Level4 exe)
- 18) – HTTP Proxy (i386-winnt Level4 exe)
- 19) – Standard TCP (x64-winnt Level4 sharedlib)
- 20) – HTTP Proxy (x64-winnt Level4 sharedlib)
- 21) – Standard TCP AppCompat-enabled (x64-winnt Level4 sharedlib)
- 22) – HTTP Proxy AppCompat-enabled (x64-winnt Level4 sharedlib)

23) – Standard TCP WinsockHelperApi-enabled (x64-winnt Level4 sharedlib)

24) – HTTP Proxy WinsockHelperApi-enabled (x64-winnt Level4 sharedlib)

25) – Standard TCP (x64-winnt Level4 exe)

26) – HTTP Proxy (x64-winnt Level4 exe)

按平台区分：x86、x64

按文件格式区分：exe、dll

按通信协议区分:Standard TCP、HTTP Proxy

按功能区分：Standard、AppCompat-enabled、UtilityBurst-enabled、WinsockHelperApi-enabled

按Level区分：Level3、Level4

注：

经实际测试，Level代表回连方式

level3表示反向连接，控制端监听端口，等待回连

leve4表示正向连接，目标主机监听端口，等待控制端主动连接

5、木马测试

选择代表性的进行测试

(1) Level3，选择 3) – Standard TCP (i386-winnt Level3 exe)

>按配置生成exe(此处不具体介绍，参照其他文章)

>DanderSpiritz控制端选择PeddleCheap-Listen-Start Listening

>在目标主机直接执行exe

>等待回连

操作同正常的反向连接木马

注：

日志文件下生成2个文件PC_Level3_exe.base和PC_Level3_exe.configured。PC_Level3_exe.base为模板文件，来自于ResourcesPcLevel3i386-winntrelease，PC_Level3_exe.configured为配置后的文件

(2) Level3，选择 6) – HTTP Proxy (x64-winnt Level3 sharedlib)

按配置生成PC_Level3_http_dll.configured(此处不具体介绍，参照其他文章)

加载方式：

1.利用DoublePulsar加载dll

(此处不具体介绍，参照其他文章)

2.手动加载dll

使用dumpbin查看dll的导出函数，如下图

ordinal为1对应的dll导出函数名为rst32

也就是说，我们可以尝试通过rundll32直接加载该dll

命令行代码如下：

```
rundll32 PC_Level3_http_dll.configured,rst32
```

木马正常回连

注：

对于http协议的木马，记得设置listen协议的时候要选择http

(3) Level4，选择 17) – Standard TCP (i386-winnt Level4 exe)

按配置生成PC_Level4_exe.configured(可使用高级模式，指定固定监听端口)

启动exe后执行netstat -ano可看到开启了固定端口

DanderSpiritz控制端选择PeddleCheap-Connect，选择ip，填入Level 4对应的端口

正向连接

(4) Level4，选择 9) – Standard TCP Generic (i386-winnt Level4 sharedlib)

按配置生成PC_Level4_dll.configured(可使用高级模式，指定固定监听端口)

查看其导出函数，如下图

也就是说，不支持直接通过rundll32加载

猜测：

Level4的木马要一直运行在后台，考虑到隐蔽性，所以不支持该功能

给出一种dll加载的测试方法：通过APC注入

如下图，成功加载，打开监听端口

参考代码：

<https://github.com/3gstudent/Inject-dll-by-APC/blob/master/test.cpp>

注：

被注入的程序需要管理员权限，否则会因为权限问题无法打开监听端口

给出另二种dll加载的测试方法：通过Application Compatibility Shims

可参考以下链接：

<https://3gstudent.github.io/3gstudent.github.io/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E4%B8%AD%E7%9A%84Application-Compatibility-Shims>

如下图，成功加载，打开监听端口

(5) Level4，选择 11) – Standard TCP AppCompat-enabled (i386-winnt Level4 sharedlib)

根据字面意思，猜测是支持Application Compatibility Shims

比较Generic和AppCompat-enabled的区别：

二者大小一样，就是AppCompat-enabled多了一个导出函数GetHookAPIs

如下图

0x03 木马功能

木马连接成功后，自动开始信息搜集，返回各种详细信息。比较人性化的设计是会自动询问用户是否提权，在检测到环境安全后会询问用户是否需要导出hash。

待信息搜集完成后，输入help可获得支持的操作

注：

help获得的内容不完整，输入aliases可获得更多操作命令介绍

help+命令可获得具体命令的操作介绍

例如，输入help eventlogedit，回显如图

1、日志操作功能

关于日志操作的命令如下：

>eventlogclear

>eventlogedit

>eventlogfilter

>eventlogquery

具体功能如下：

eventlogquery：

统计日志列表，查询所有日志信息，包含时间，数目

可查询指定类别的日志信息，包含时间，数目，命令如下：

```
eventlogquery -log Setup
```

该操作等价于

```
wevtutil.exe gli setup
```

注：wevtutil.exe操作系统默认包含

eventlogfilter：

查看指定类别的日志内容

命令如下：

```
eventlogfilter -log Setup -num 19
```

该操作等价于

```
wevtutil qe /f:text setup
```

eventlogedit：

删除单条日志

可删除单条日志内容，命令如下：

```
eventlogedit -log Setup -record 1
```

注：

record序号可通过eventlogfilter获得

该命令暂时没有公开工具支持

eventlogclear：

删除该类日志所有内容

命令如下：

```
eventlogclear -log Microsoft-Windows-Dhcpv6-Client/Admin
```

该操作等价于

```
wevtutil cl Microsoft-Windows-Dhcpv6-Client/Admin
```

0x04 木马查杀思路

DanderSpritz的木马生成方式如下：

文件夹ResourcesPcLevel3和ResourcesPcLevel4下保存模板文件，固定位置预留参数配置信息，实际生成时向模板文件写入配置信息

目前杀毒软件已经对这些模板文件成功识别并查杀，同时，这些模板文件的代码并没有开源，也会提高在恶意利用上面的门槛

建议普通用户：更新系统补丁、更新杀毒软件病毒库，就能够防范该工具的攻击。

0x05 小结

本文分享了DanderSpritz的测试心得，希望能够帮助大家在技术研究上对其有更好的认识，省略了部分具体利用细节和章节，以防该工具被滥用。

>本文为 3gstudent 原创稿件，授权嘶吼独家发布，未经许可禁止转载；如若转载，请注明原文地址：<http://www.4hou.com/technology/4538.html>

点击收藏 | 0 关注 | 1

1. 1 条回复



[野驴](#) 2017-05-04 14:20:54

分析到位，感谢分享。

0 回复Ta

[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](#)