

ACKcmd 后门分析

December 14, 2001

Sinbad Technical Publications
Website: <http://sinbad.zhoubin.com>
© Copyright 2001, All Rights Reserved

1.简介

ACKcmd 是提供 Win2000 下远程命令 Shell 的一种后门，它使用 TCP 来传输，但是不同于一般正常的 TCP 连接有三次握手，ACKcmd 仅使用了 TCP ACK 数据包，所以一般情况下可以穿越防火墙及躲避 IDS 的检测。

ACKcmd 采用 client/server 结构，在目标机器上运行 AckCmdS.exe 植入后门，入侵者在客户端运行命令 AckCmdC <target ip>即可获得一个远程的 Shell。

2.分析

我们现在用 sniffit 来观察 ACKcmd 的数据是怎样传输的。入侵者在 192.168.0.29，连入目标机器 192.168.0.2:

```
E:\Tools>ackcmdc 192.168.0.2
```

AckCmd 1.1 - The Ack Command Prompt for Windows 2000

- (c) 2000, Arne Vidstrom, arne.vidstrom@ntsecurity.nu

- For instructions see <http://ntsecurity.nu/toolbox/ackcmd/>

Type "quit" and press Enter to quit

```
AckCmd> net name <----- 输入命令
```

名称

SERVER2000

ADMINISTRATOR

命令成功完成。

```
AckCmd> quit <----- 退出
```

sniffit 抓到的包如下:

TCP Packet ID (from_IP,port-to_IP,port): 192.168.0.29.80-192.168.0.2.1054
SEQ (hex): 6060606 ACK (hex): 6060606
FLAGS: -A---- Window: 4000

Packet ID (from_IP,port-to_IP,port): 192.168.0.29.80-192.168.0.2.1054
45 E 00 . 00 . 38 8 00 . 00 . 00 . 00 . 80 . 06 . B9 . 50 P C0 . A8 . 00 . 1D .
C0 . A8 . 00 . 02 . 00 . 50 P 04 . 1E . 06 . 06 . 06 . 06 . 06 . 06 . 06 .
70 p 10 . 40 @ 00 . E6 . C6 . 00 . 00 . 02 . 04 . 05 . B4 . 01 . 01 . 04 . 02 .
6E n 65 e 74 t 20 6E n 61 a 6D m 65 e

TCP Packet ID (from_IP,port-to_IP,port): 192.168.0.2.1054-192.168.0.29.80
SEQ (hex): 6060606 FLAGS: ---R--

Packet ID (from_IP,port-to_IP,port): 192.168.0.2.1054-192.168.0.29.80
45 E 00 . 00 . 28 (04 . A8 . 00 . 00 . 80 . 06 . B4 . B8 . C0 . A8 . 00 . 02 .
C0 . A8 . 00 . 1D . 04 . 1E . 00 . 50 P 06 . 06 . 06 . 06 . 06 . 06 . 06 . 06 .
50 P 04 . 00 . 00 . 11 . EB . 00 . 00 .

TCP Packet ID (from_IP,port-to_IP,port): 192.168.0.2.1054-192.168.0.29.80
SEQ (hex): 6060606 ACK (hex): 6060606
FLAGS: -A---- Window: 4000

Packet ID (from_IP,port-to_IP,port): 192.168.0.2.1054-192.168.0.29.80
45 E 00 . 00 . CD . 04 . A9 . 00 . 00 . 80 . 06 . B4 . 12 . C0 . A8 . 00 . 02 .
C0 . A8 . 00 . 1D . 04 . 1E . 00 . 50 P 06 . 06 . 06 . 06 . 06 . 06 . 06 . 06 .
70 p 10 . 40 @ 00 . 1C . C1 . 00 . 00 . 02 . 04 . 05 . B4 . 01 . 01 . 04 . 02 .
0D . 0A . C3 . FB . B3 . C6 . 20 20 20 20 20 20 20 20 20 20
20 20 20 20 0D . 0A . 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D -
- 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D -
2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D -
2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D -
2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D - 2D -
2D - 2D - 2D - 2D - 2D - 0D . 0A . 53 S 45 E 52 R 56 V 45 E 52 R 32 2 30 0 30 0
30 0 20 20 20 20 20 20 0D . 0A . 41 A 44 D 4D M 49 I 4E N 49 I
53 S
54 T 52 R 41 A 54 T 4F O 52 R 20 20 20 0D . 0A . C3 . FC . C1 . EE .
B3 .
C9 . B9 . A6 . CD . EA . B3 . C9 . A1 . A3 . 0D . 0A . 0D . 0A .

可以看出，这次操作总共传输了三个 TCP 包。客户端的端口号是 80，服务器的端口号是 1054，这种类似于 HTTP 的通信是很容易被网管忽略的。

客户端的命令 net name 以明文方式放在 TCP 的数据段，服务器立刻返回一个

TCP RST 包，然后接着返回一个 TCP ACK，其中带着命令执行后的输出结果。

如果输出结果很长，ACKcmd 只能返回部分数据，这是作者在设计时没有考虑的。你可以运行 `dir c:\winnt\system32` 看看，只能输出部分文件列表，最后附带信息 “More...” 表示并不是返回了全部数据。

3.检测

首先，它采用的端口（80 和 1054）是固定的。要监控客户端发出的数据包，tcpdump 的过滤规则为：

```
tcp[0:2] = 80 and tcp[2:2] = 1054
```

多做几次试验，可以发现它们之间通信的 TCP ACK 包中，序列号和 ACK 号都是 0x06060606（十进制 101058054），这也是一个很重要的特征。tcpdump 的过滤规则为：

```
tcp[4:4] = 0x06060606 and tcp[8:4] = 0x06060606
```

4.缺陷

正如作者所说，这是一个使用 TCP ACK 穿越防火墙的 proof-of-concept，所以并不是很完善。数据的明文方式传输，以及在 Win2000 的任务列表中能看到 AckCmdS.exe，所以此后门不难被发现。