

" " NSA

NSA EternalRocks
" " " wannacry MS17010 SMB
7 NSA EternalBlue EternalRomanceEternalsynergy
EternalChampion Smbtouch Architouch DoublePulsar " wannacry
NSA " " NSA

EternalRocks MS17010 SMB EternalRocks C:\Program
File\Microsoft Updates Update\Installer.exe
.net TaskScheduleand SharpZLib
svchost.exe

(1)<</MCID 82>> BDC BT9-101>] TJ ET EMC /P <</MCID 8 [() TJ24600>11<3E7C>11<0A3E0292>>

(4)

445

(5) Tor

UpdateInstaller.exe

" " " " wannacry "

NSA

" NSA

NSA

" " 7 NSA

EternalBlue	SMBv1	
EternalRomance	SMBv1	

```

[*] 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.
eading in memory adjacent to 'SMBU2 buffer'.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet
DONE.
[*] Receiving response from exploit
[+] ETERNALBLUE overwrite
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted connection.
[*] Pinging backdoor.....
[+] Backdoor returned code
[+] Ping returned Target address
[+] Backdoor installed
-----
-----WIN-----
-----
at.blob_(2_bytes)....
[+] CORE sent serialized output
0x00000000 08 00
s from CORE
[+] Received output parameters
[+]

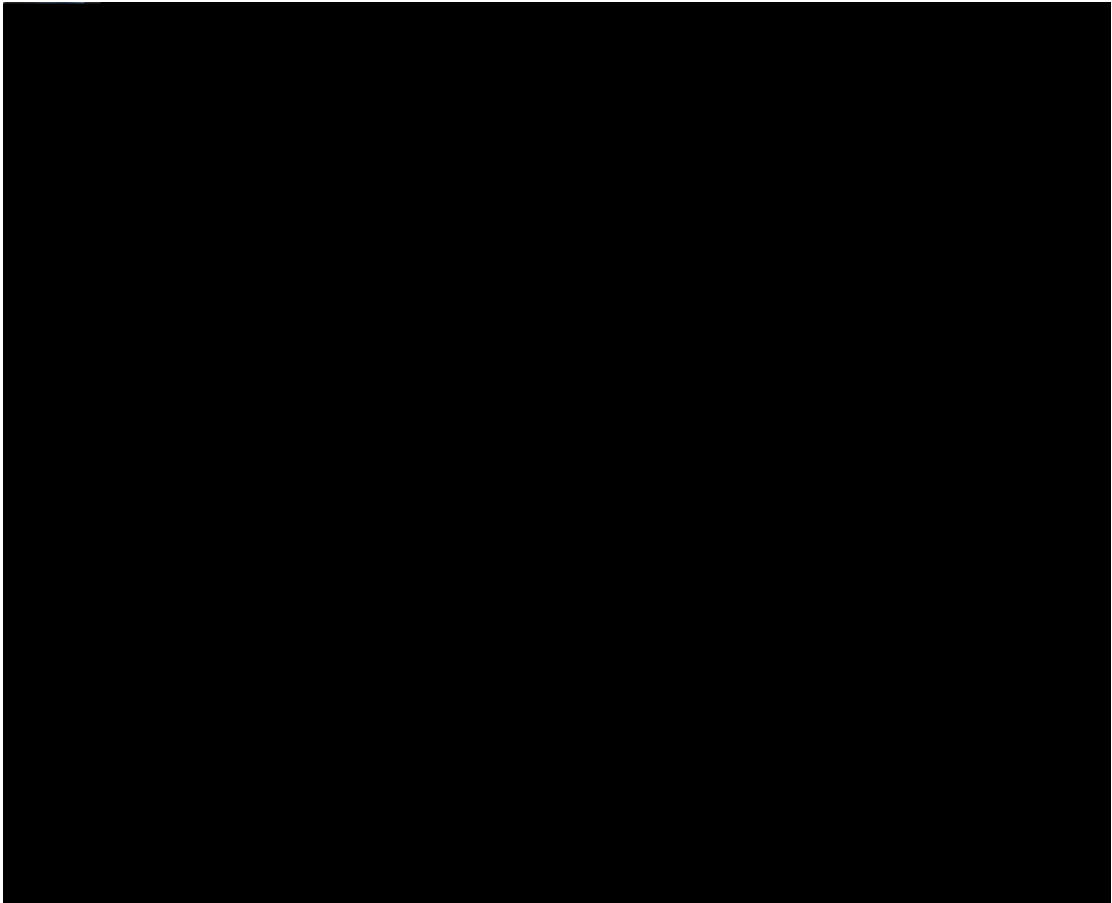
```

2. (EternalRomance)

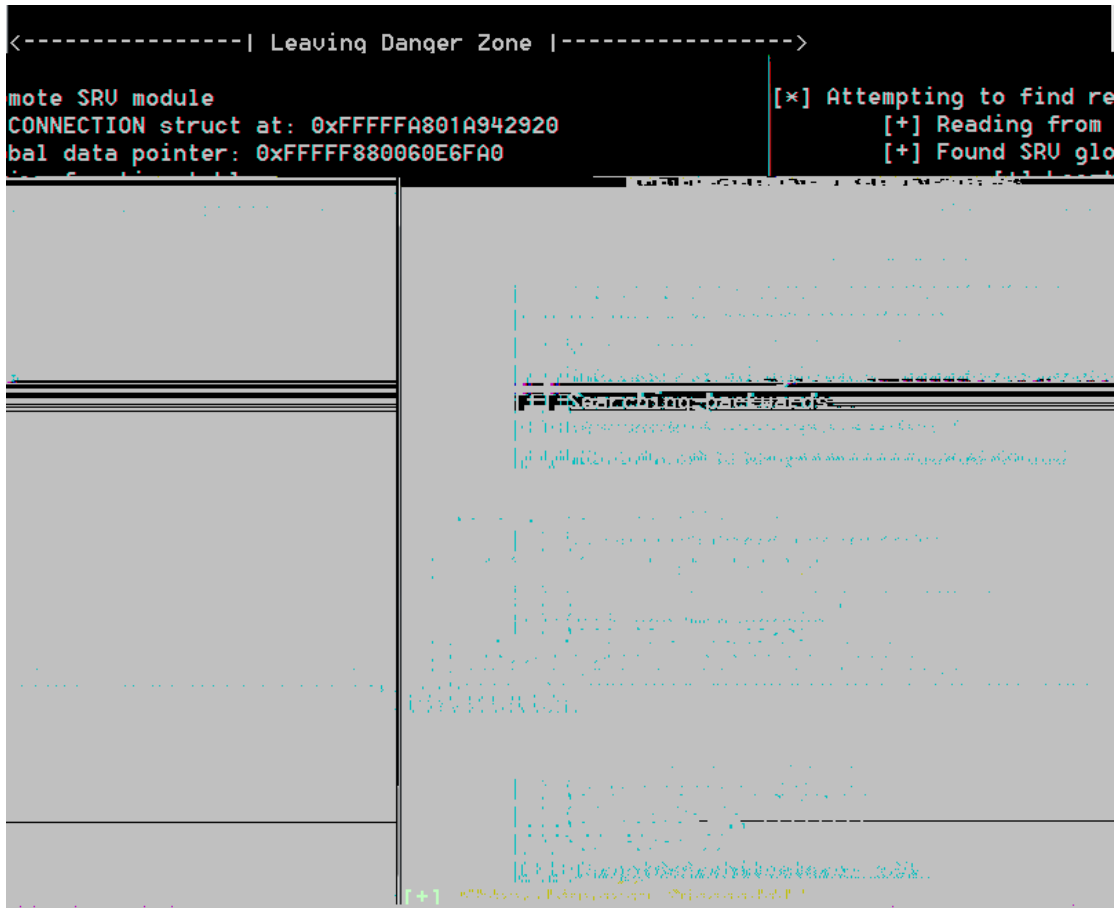
Windows XP Windows Vista Windows7 Windows 8 Windows 10
Windows2000 Windows 2003 Windows 2008 Windows 2012
Windows X(SP0~SP3 32 SP1~SP 64) Windows Server 2003
SP0~SP2 SP1~SP4 Windows Vista) WindowsSERVER 2008
Windows7 WindowsSERVER2008R2

Windows

XP



	EternalRomance	DoublePulsar
DoublePulsar		shellcode
3.	(EternalSynergy)	
	Windows 8	Windows 2012
	Windows 8 64	Windows 2012 64
		Windows 8 Windows2012
	64	



Eternalsynergy
DoublePulsar
DoublePulsar
shellcode

4. (EternalChampion)
- Windows XP (SP0~SP3 32 SP1~SP 64) Windows Server 2003
 - SP0~SP2 SP1~SP4 Windows Vista) WindowsSERVER 2008
 - Windows7 WindowsSERVER 2008R2 Windows8

EternalChampion
DoublePulsar
shellcode

```

[*] Connecting to target
    [+] Connection established

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

[*] Attempting information leak (sync)

[+] Successfully leaked transaction!

Conn: 000000004c2a7f3a

ending shellcode to target " " [x] S
    [+] successfully sent

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

[*] Competition 1:
    4 attempting++++
    4 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 :(

```

1.

EternalRocks

NSA

EternalBlue	TCP_NSA_EternalBlue_()_SMB [MS17010] TCP_NSA_EternalBlue_()_SMB _shellcode TCP_NSA_EternalBlue_()_SMB (win7/2008x64) TCP_NSA_EternalBlue_()_SMB (win8.1/2012x64)
EternalRomance	TCP_NSA_EternalRomance_()_SMB [MS17010]
EternalSjergy	TCP_NSA_SMB shellcode
EternalChampion	TCP_NSA_SMB shellcode
DoublePulsar	TCP_NSA_Windows_SMB_DoublePulsar

2.

MS17010

<https://technet.microsoft.com/zhcn/library/security/MS17010>