“ ” NSA

NSA EternalRocks
“ ” “ wannacry” MS17-010 SMB
7 NSA EternalBlue EternalRomance EternalSynergy
EternalChampion Smbtouch Architouch DoublePulsar “ wannacry”
NSA “ ” NSA

EternalRocks MS17-010 SMB EternalRocks C:\Program
Files\Microsoft Updates UpdateInstaller.exe
.net TaskScheduler and 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

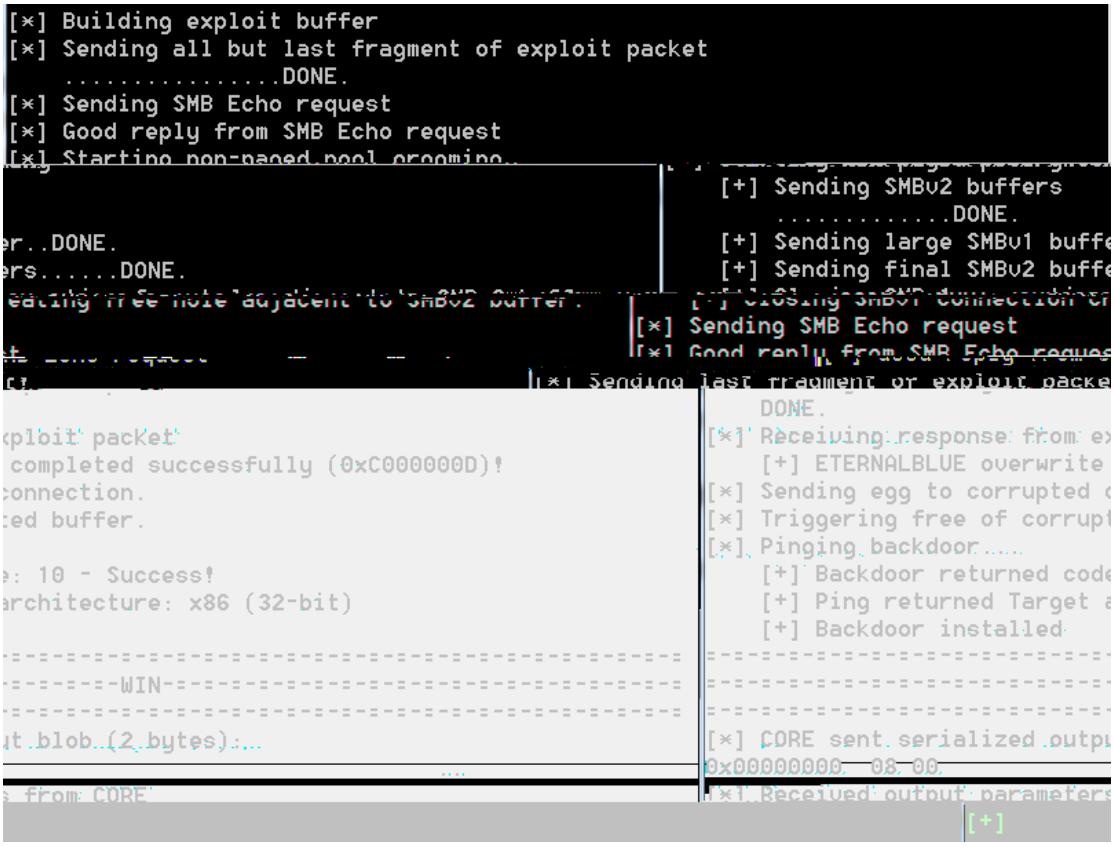
NSA “

” NSA

NSA

“ ” 7 NSA

EternalBlue	SMBv1	
EternalRomance	SMBv1	



2. (EternalRomance)

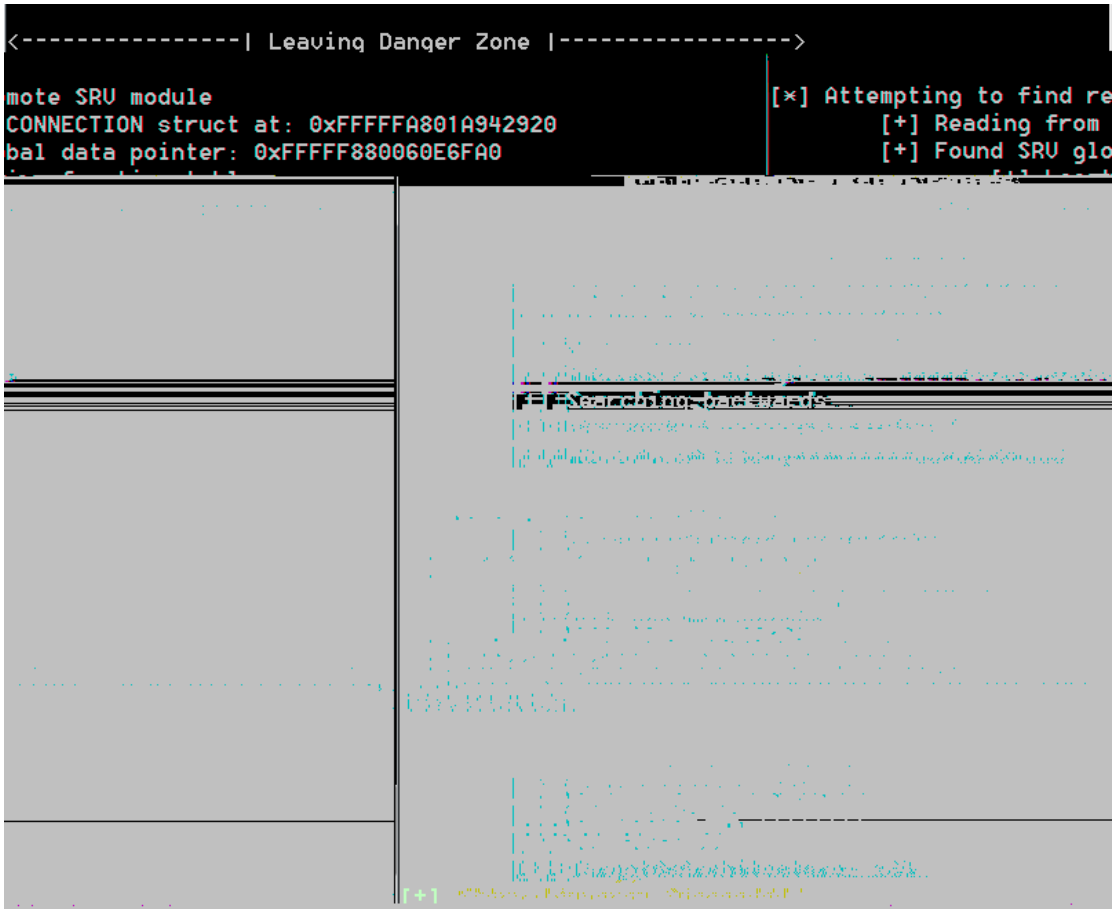
Windows XP Windows Vista Windows 7 Windows 8 Windows 10 Windows2000 Windows 2003 Windows 2008 Windows 2012

Windows XP(SP0~SP3 32 SP1~SP2 64) Windows Server 2003 SP0~SP2 32 SP1~SP2 64 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

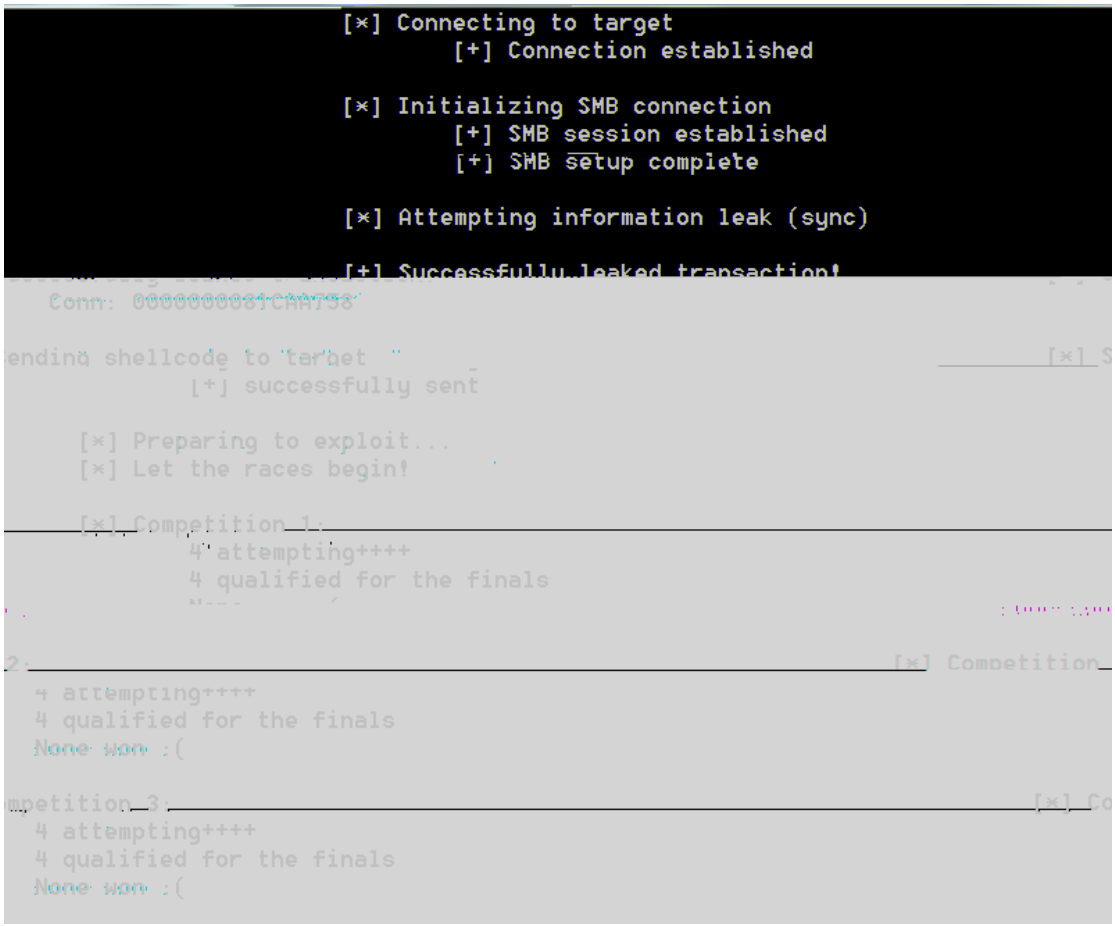


Eternalsynergy DoublePulsar DoublePulsar shellcode

4. (EternalChampion)

Windows XP(SP0~SP3 32 SP1~SP2 64) Windows Server 2003 SP0~SP2(32 SP1~SP2 64) Windows Vista( ) WindowsSERVER 2008 Windows7 WindowsSERVER 2008R2 Windows8

EternalChampion DoublePulsar shellcode



1. EternalRocks

NSA

EternalBlue	TCP_NSA_EternalBlue_( )_SMB [MS17-010] TCP_NSA_EternalBlue_( )_SMB _shellcode TCP_NSA_EternalBlue_( )_SMB (win7/2008-x64) TCP_NSA_EternalBlue_( )_SMB (win8.1/2012-x64)
EternalRomance	TCP_NSA_EternalRomance_( )_SMB [MS17-010]
EternalSynergy	TCP_NSA_SMB shellcode
EternalChampion	TCP_NSA_SMB shellcode
DoublePulsar	TCP_NSA_Windows_SMB_DoublePulsar

2. MS17-010

https://technet.microsoft.com/zh-cn/library/security/MS17-010