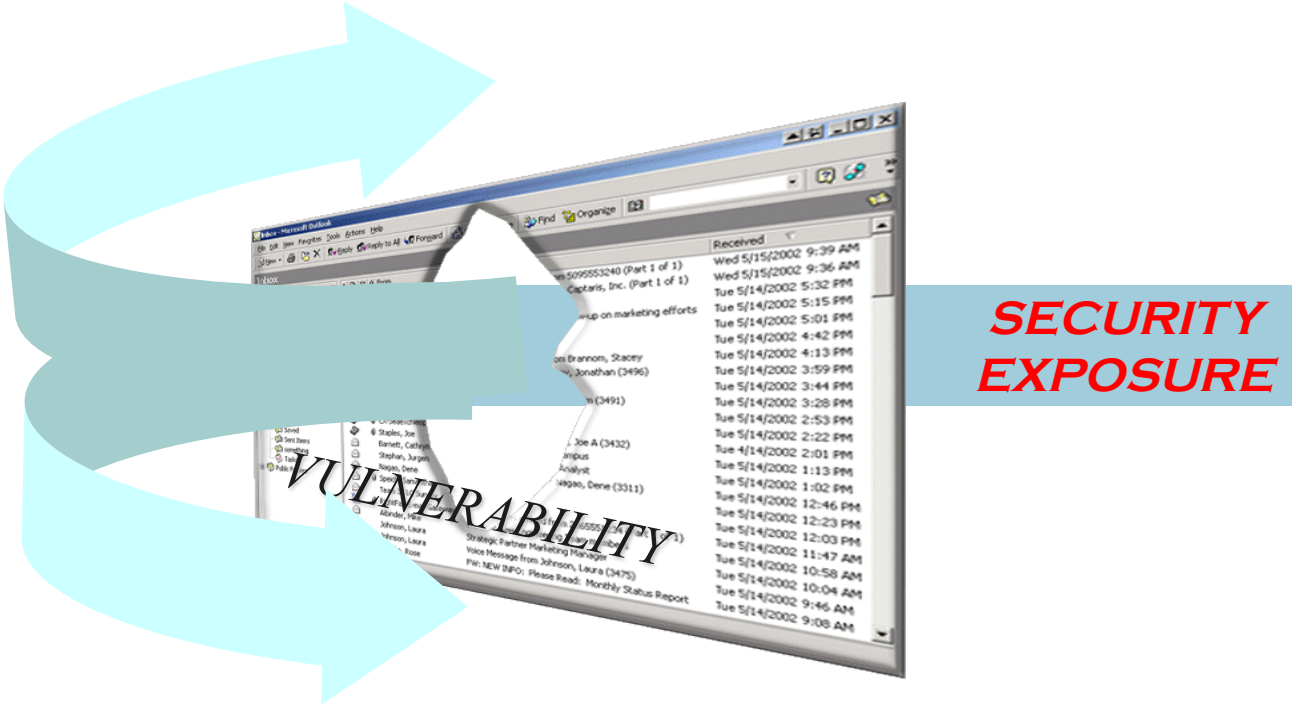
Shellcode Exploit Analysis: Tips and Tricks

Romeo Dela Cruz
Techlead - TrendlabsPH

September 26, 2014

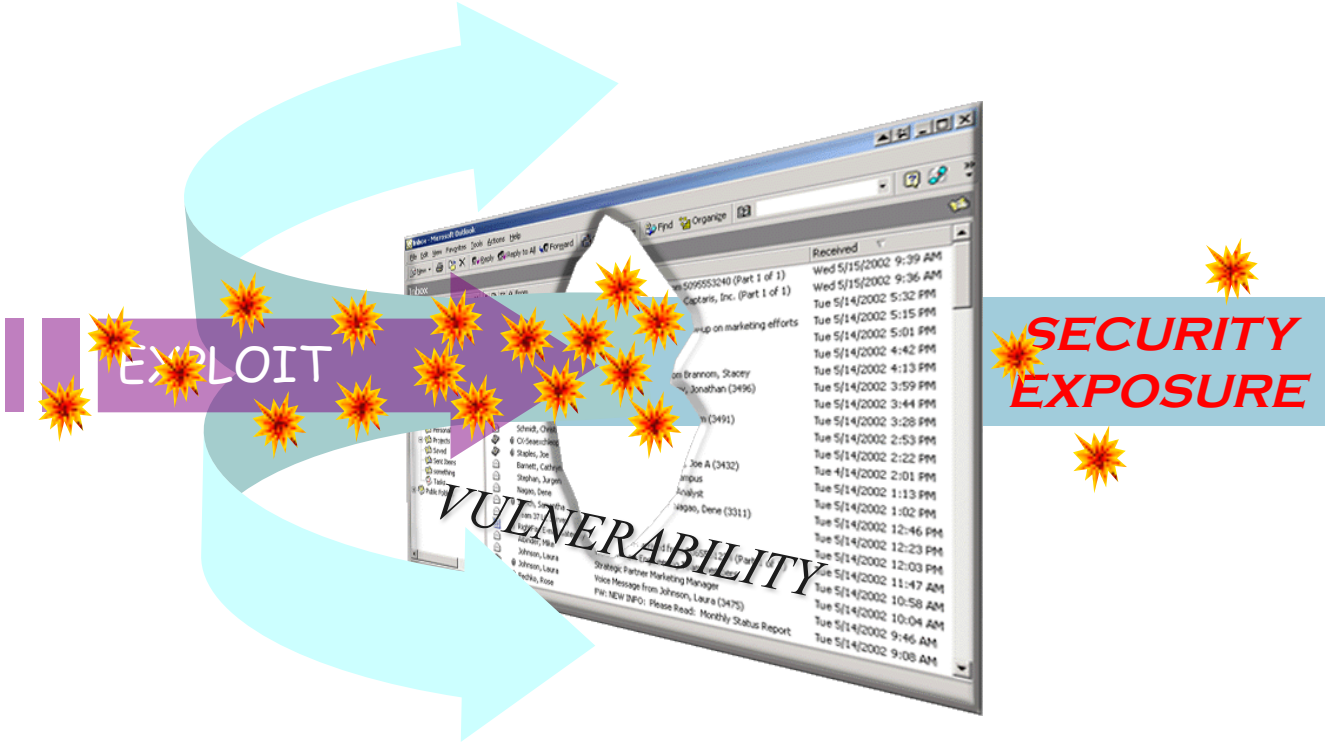
What is a Vulnerability?

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

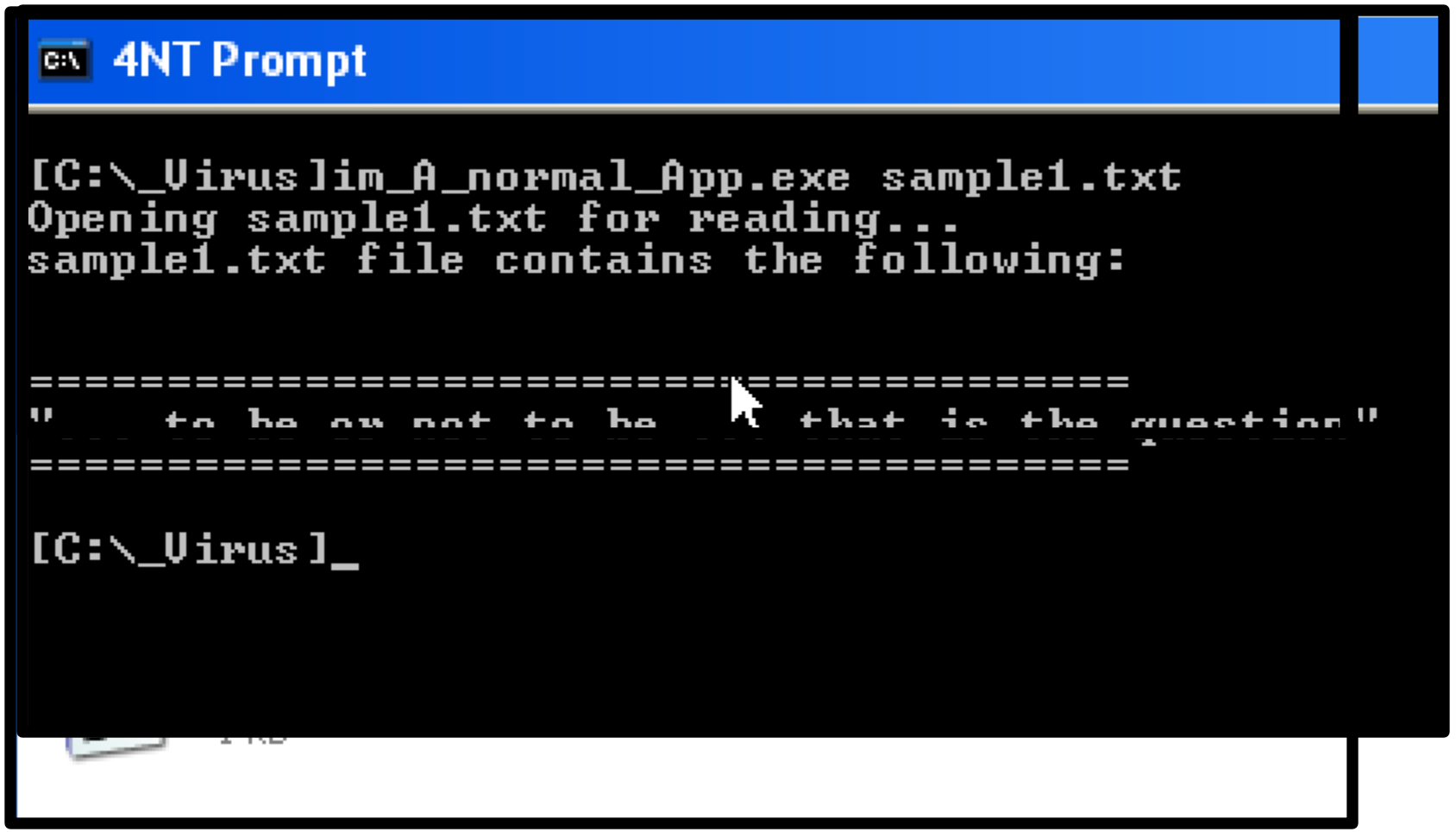


What is an Exploit?

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



Sample Program:



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:

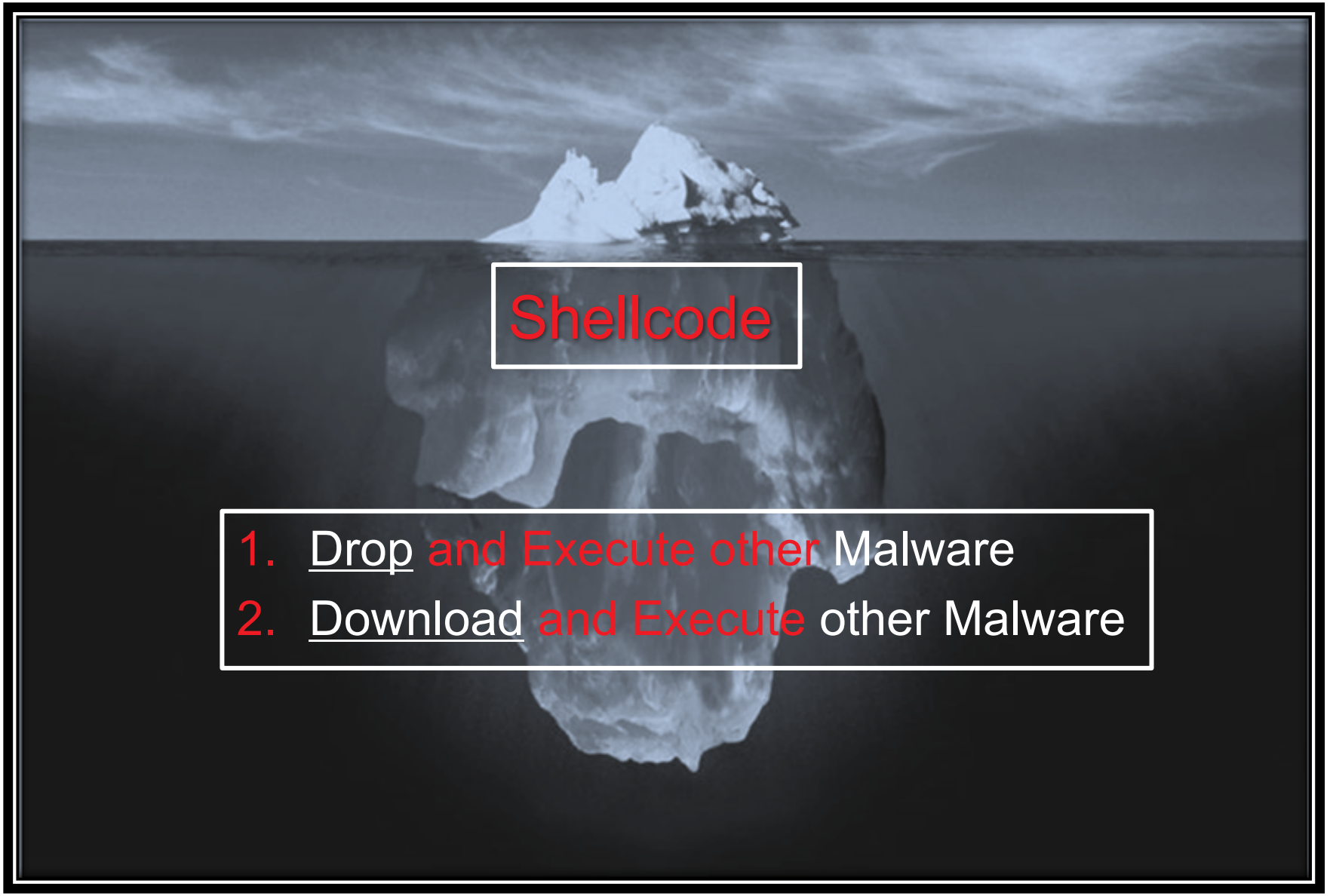
```
int __cdecl sub_401000(LPCSTR lpFileName)
{
  HANDLE v1; // edi@1
  int result; // eax@2
  DWORD v3; // eax@3
printf("%s file contains the following:\n\n", lpFileName);
printf("\n========================================\n");
v3 = GetFileSize(v1, &FileSizeHigh);
ReadFile(v1, &Buffer, v3, &NumberOfBytesRead, 0);
CloseHandle(v1);
printf("%s", &Buffer);
printf("\n========================================\n");
  }
-00001008 Buffer                db 4096 dup(?)
  v3 = GetFileSize(v1, &FileSizeHigh);
  ReadFile(v1, &Buffer, v3, &NumberOfBytesRead, 0);
  CloseHandle(v1);
  printf("%s", &Buffer);
  printf("\n========================================\n");
  result = 1;
 }
 return result;
}
```

Vulnerability ????!!!

Let's Exploit it!!!

What is a Shellcode?

- is a small piece of code used as the payload in the exploitation of a software vulnerability



Sample Shellcode:

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

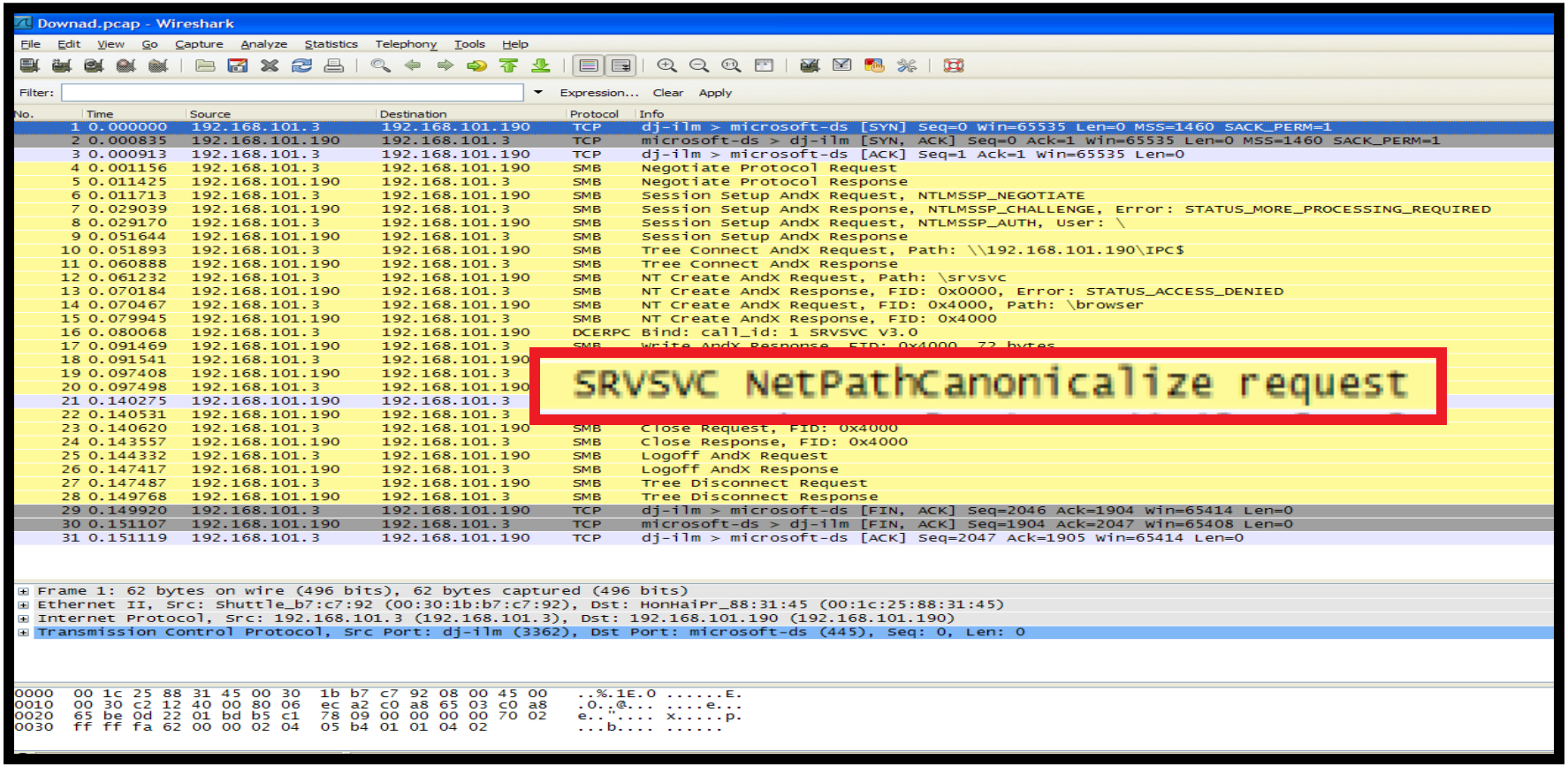
The following malware exploit this vulnerability(CVE-2008-4250) for **Network Propagation**:

WORM_DOWNAD
WORM_NEERIS

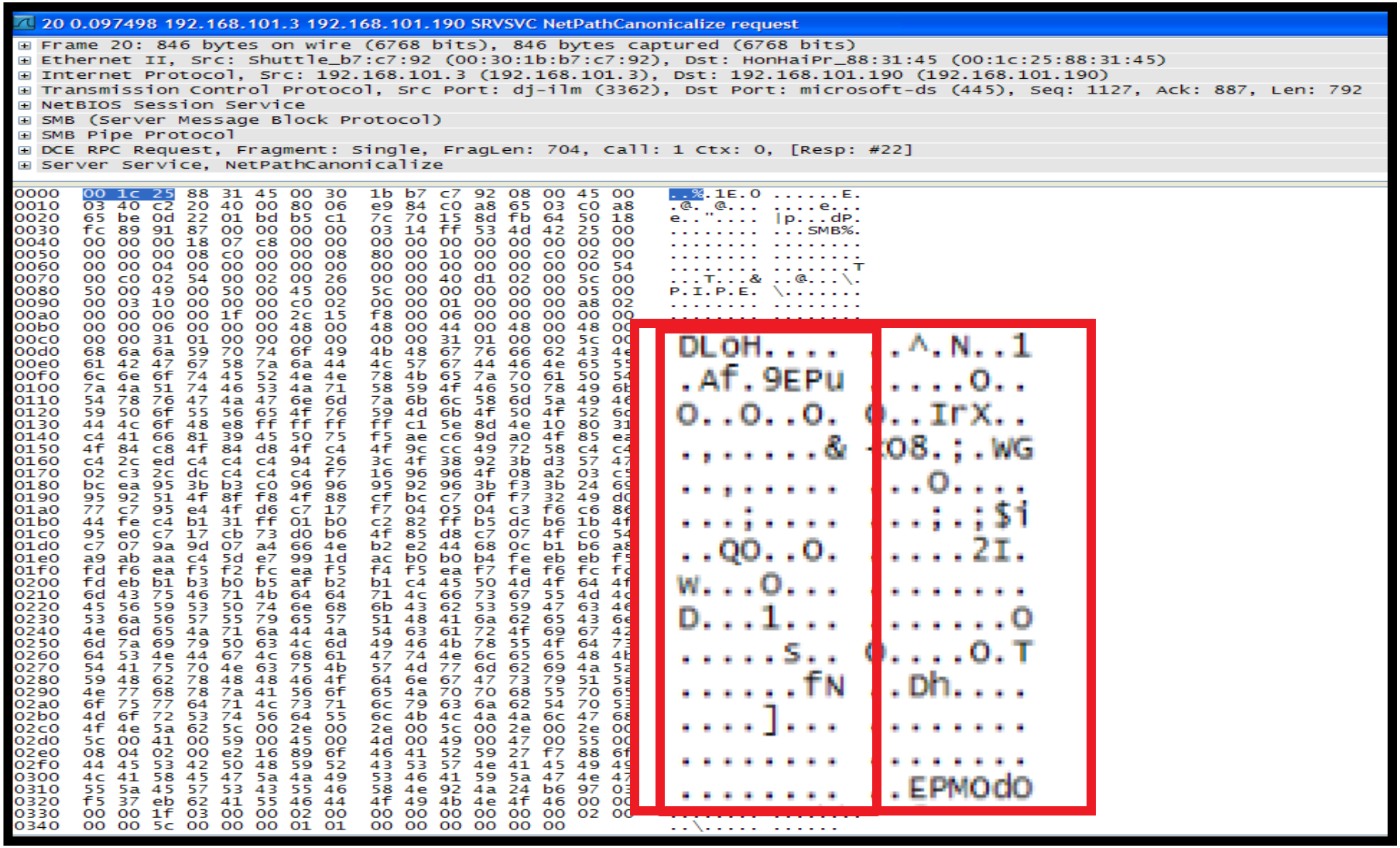
The system infected by this malware initiate an SMB(Server Message Block) session on TCP Port 445 across the Network. Then binds to the SRVSVC(Server Service) pipe using RPC (Remote Procedure Call) Protocol and proceeds to issue the NetPathCanonicalize request, which has the embedded ShellCode.

Sample Shellcode:

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

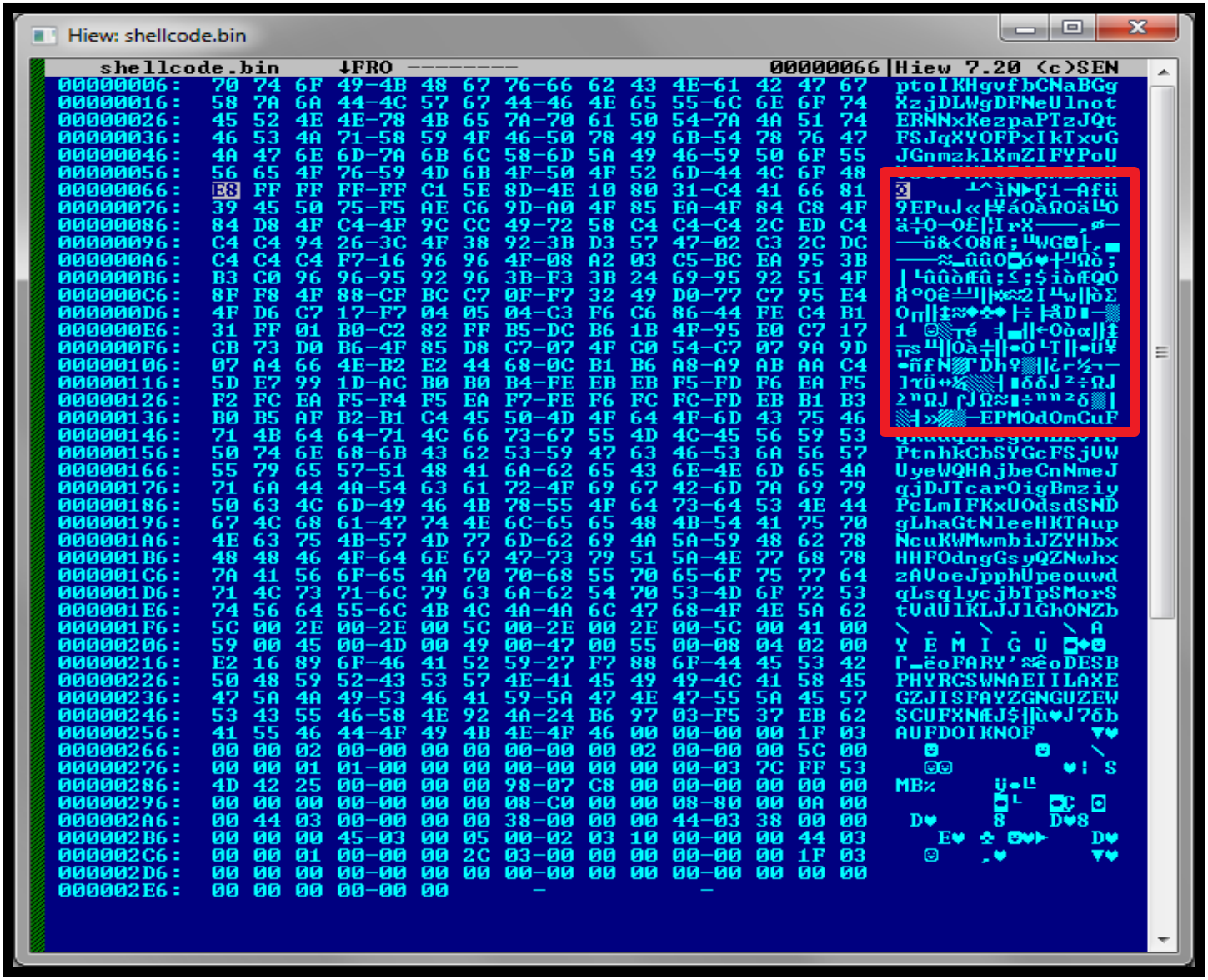


Sample Shellcode:



3/26/17 Confidential | Copyright 2013 TrendMicro Inc. 2

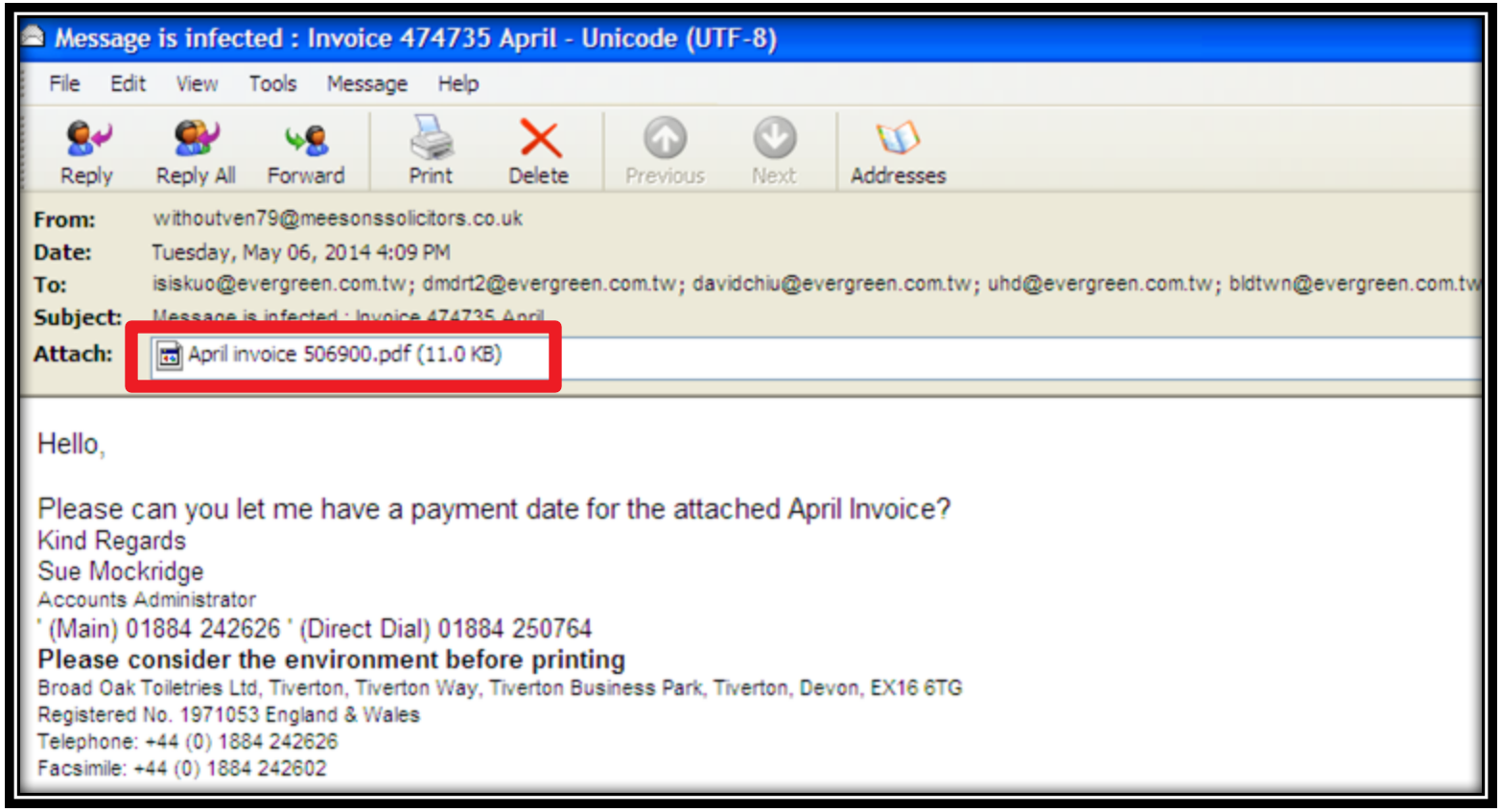
Sample Shellcode:



TREND MICRO

Exploit Malware Arrival

Spammed E-mail

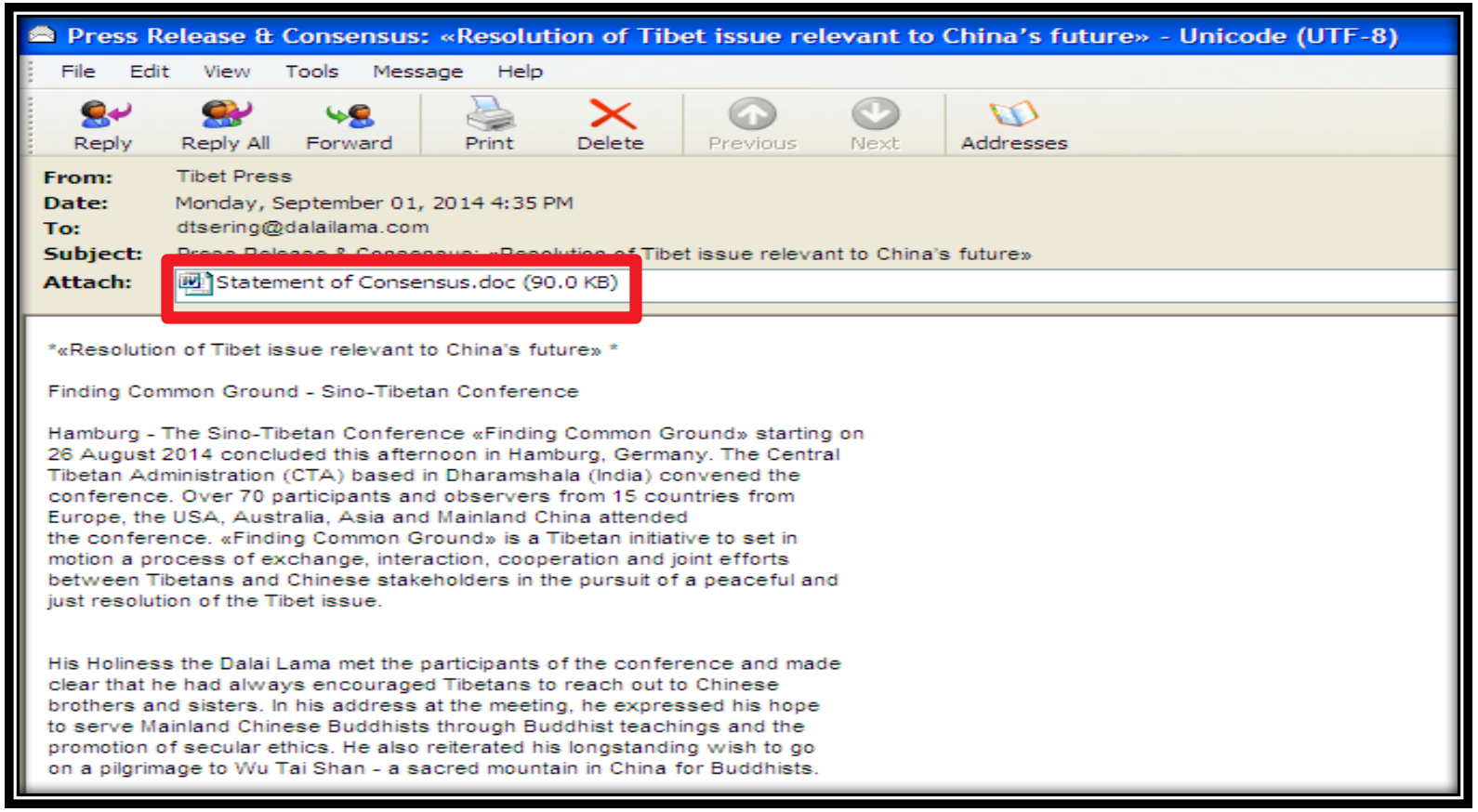


Type: Adobe PDF

Vulnerability: CVE-2013-2729

Trend Micro: TROJ_PIDIEF.YNLA

Spammed E-mail



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

TrendLabs
SECURITY INTELLIGENCE BLOG
Threat News and Information Direct from the Experts
TREND MICRO

Snapshot of Exploit Documents for April 2012

11:38 pm (UTC-7) | by Ryan Flores (Senior Threat Researcher)

Targeted attacks that are part of APT campaigns commonly use exploit documents in their social engineering ploy.

organization.

Taking data from exploit documents gathered last April, we can see that the most exploited MS Office software is MS Word.

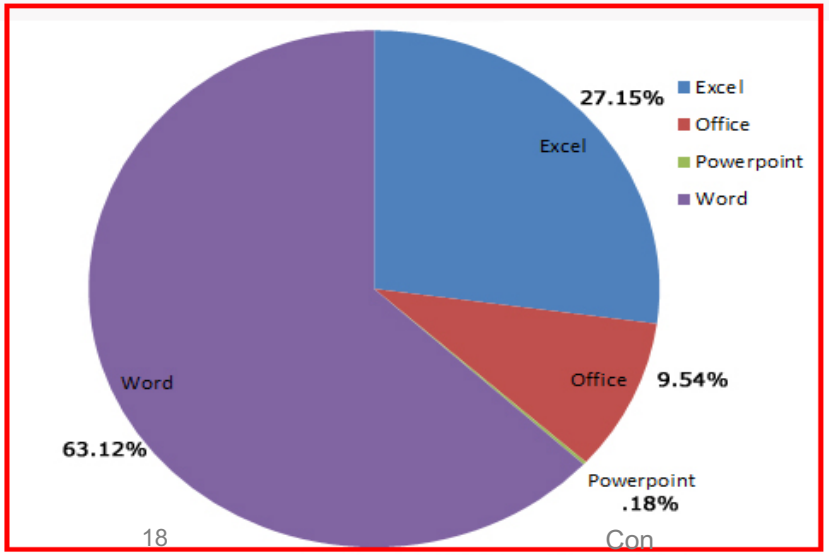
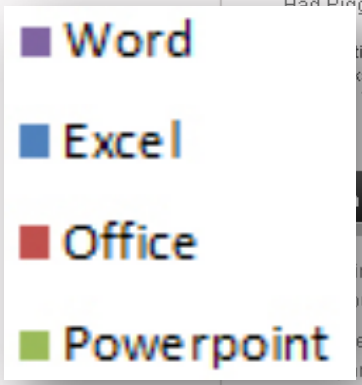


Figure 1. Most exploited MS Software for April 2012



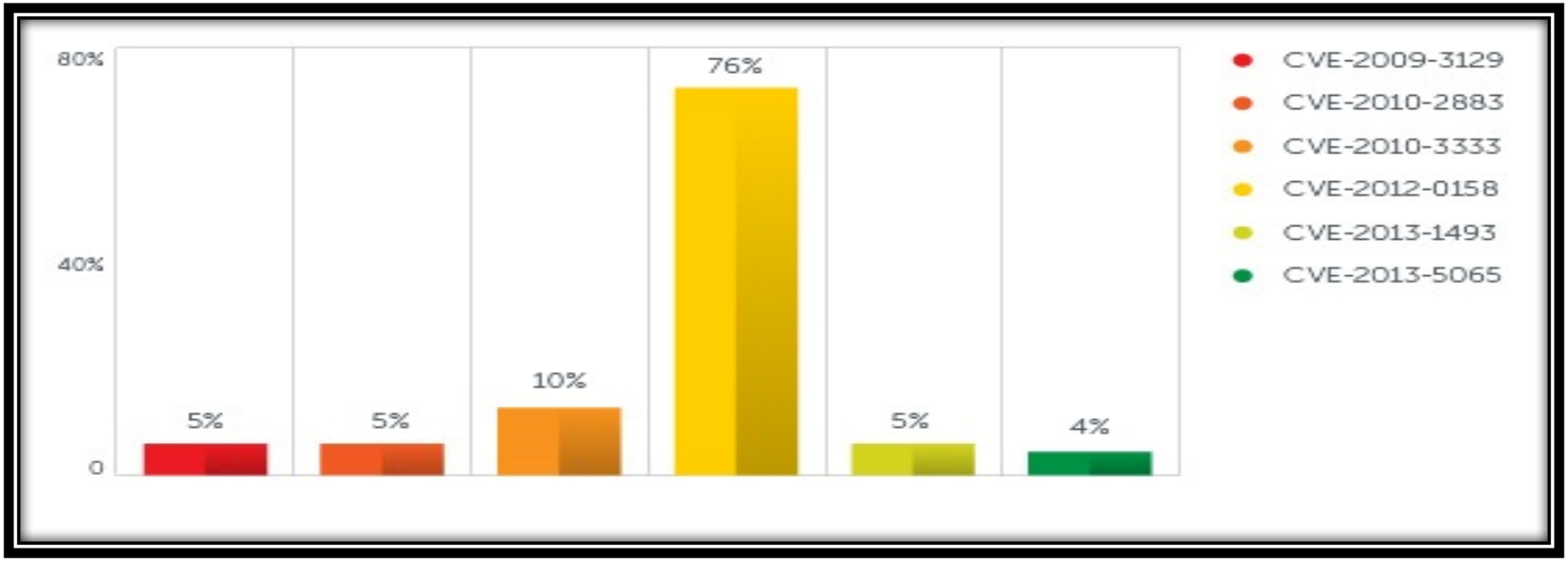
Safe NFC For Businesses
Bypassing Android Permissions: What You Need to Know
Good NFC Habits
How Mobile Ads Abuse Permissions
Malicious Developers Release Rogue Bad Piggies Versions

...tion on all mobile threats and other ...s, see Mobile Threat Information ... Trend Micro Threat Encyclopedia.

...r Posts
...ng Android Permissions: ...u Need to Know
...eme RAT Attacks on US, ...nd Other Foreign Governments

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

Exploit Kit

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

Exploit Kit Process

Blackhole
Styx
Cool Exploit Kit
Crimeboss
Red Kit
Sweet Orange

CVE-2013-0634: Vulnerability in Adobe Flash Player Could Allow Remote Code Execution

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

CVE-2013-0634: Vulnerability in Adobe Flash Player Could Allow Remote Code Execution

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

CVE-2013-0634: Vulnerability in Adobe Flash Player Could Allow Remote Code Execution

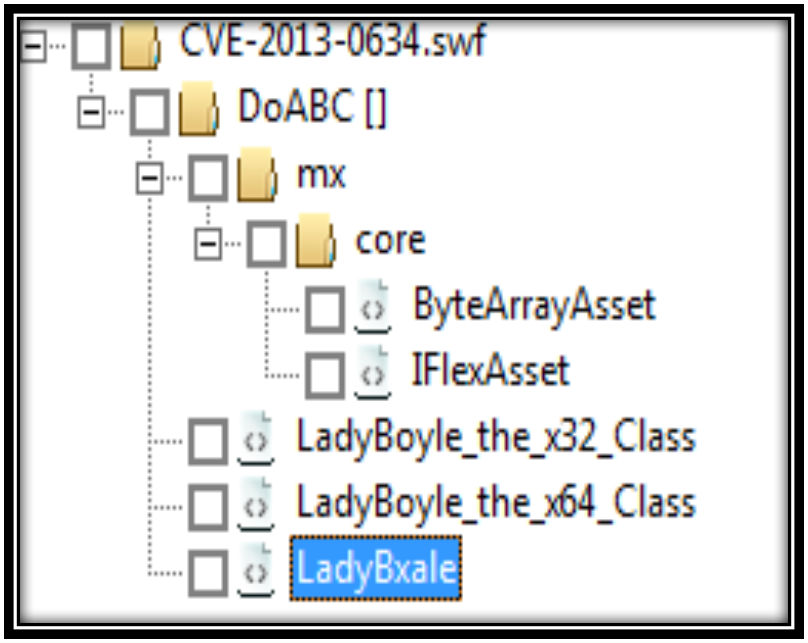
Sha1: 3cd56071b78e2f8489a4b71e0f0beec805f0bf4a
Trend Micro: SWF_EXPLOIT.JD

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

CVE-2013-0634: Vulnerability in Adobe Flash Player Could Allow Remote Code Execution

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

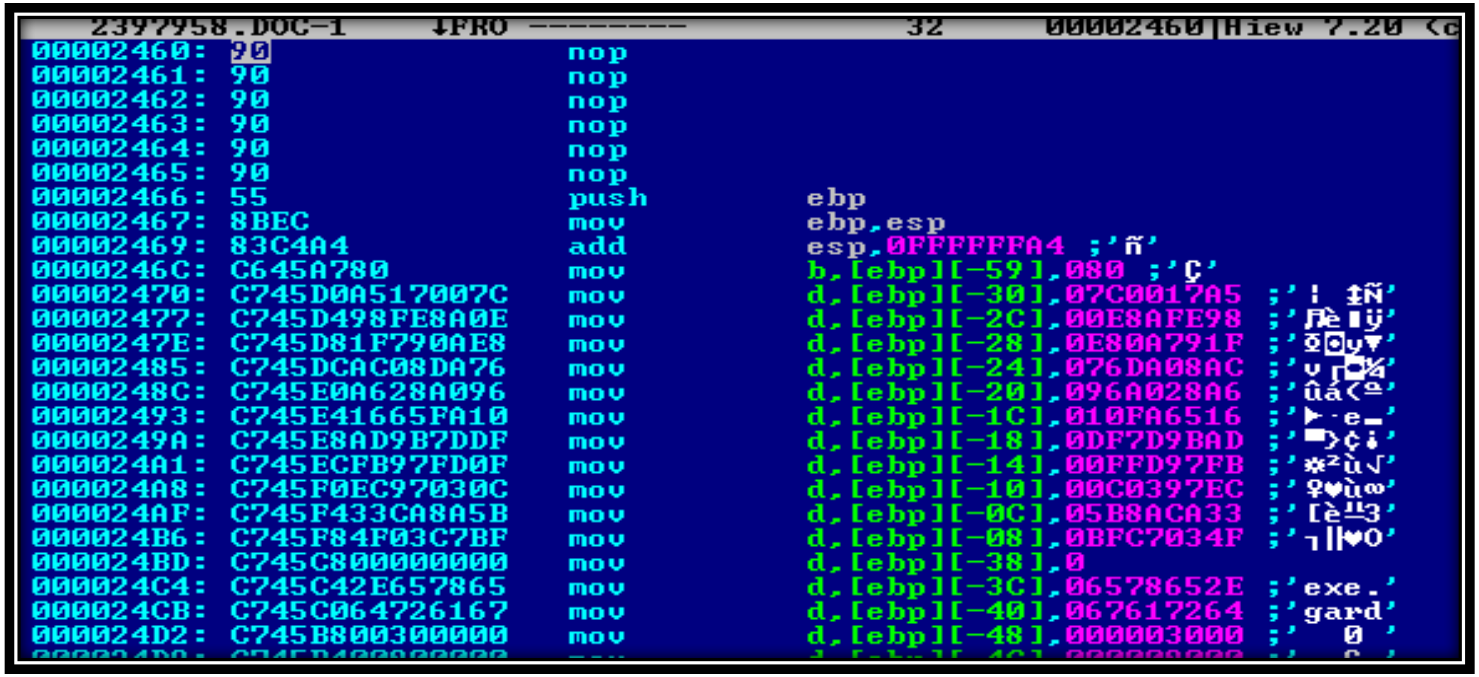
Locating Shellcode:

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)

Sample Shellcode

```
00017831: EB0D                  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                  jne     000017837   ---↑ (2)
0001783F: C3                    retn
```

```
00004E04: 90                    nop
00004E05: 90                    nop
00004E06: 90                    nop
00004E07: 90                    nop
00004E08: 90                    nop
00004E09: 90                    nop
00004E0A: 90                    nop
00004E0B: 90                    nop
00004E0C: 90                    nop
00004E0D: 90                    nop
00004E0E: 50                    push    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
00004E20: E2FA                  loop    000004E1C   ---↑ (2)
```


2397958.DOC-1 ↓FRO -------- 32 00002460 Hiew 7.20 (c
00002460: 90 nop
00002461: 90 nop
00002462: 90 nop
00002463: 90 nop
00002464: 90 nop
00002465: 90 nop
00002466: 55 push ebp
00002467: 8BEC mov ebp,esp
00002469: 83C4A4 add esp,0FFFFFFA4 ;'ñ'
0000246C: C645A780 mov b,[ebp][-59],080 ;'Ç'
00002470: C745D0A517007C mov d,[ebp][-30],07C0017A5 ;'¥ ↕Ñ'
00002477: C745D498FE8A0E mov d,[ebp][-2C],00E8AFE98 ;'Ñè■ÿ'
0000247E: C745D81F790AE8 mov d,[ebp][-28],0E80A791F ;'▼◘y▼'
00002485: C745DCAC08DA76 mov d,[ebp][-24],076DA08AC ;'v┌◘¼'
0000248C: C745E0A628A096 mov d,[ebp][-20],096A028A6 ;'ûá<º'
00002493: C745E41665FA10 mov d,[ebp][-1C],010FA6516 ;'►·e▬'
0000249A: C745E8AD9B7DDF mov d,[ebp][-18],0DF7D9BAD ;'■>¢¡'
000024A1: C745ECFB97FD0F mov d,[ebp][-14],00FFD97FB ;'☼²ù√'
000024A8: C745F0EC97030C mov d,[ebp][-10],00C0397EC ;'♀♥ù∞'
000024AF: C745F433CA8A5B mov d,[ebp][-0C],05B8ACA33 ;'[è‼3'
000024B6: C745F84F03C7BF mov d,[ebp][-08],0BFC7034F ;'┐╟♥O'
000024BD: C745C800000000 mov d,[ebp][-38],0
000024C4: C745C42E657865 mov d,[ebp][-3C],06578652E ;'exe.'
000024CB: C745C064726167 mov d,[ebp][-40],067617264 ;'gard'
000024D2: C745B8003000000 mov d,[ebp][-48],000003000 ;' 0 '


00002E01: EB1C jmps 000002E1F ---↓ (1)
00002E03: 33C0 xor eax,eax
00002E05: 5E pop esi
00002E06: 8BFE mov edi,esi
00002E08: 33C9 xor ecx,ecx
00002E0A: B17A mov cl,07A ;'z'
00002E0C: B502 mov ch,2
00002E0E: AC lodsb
00002E0F: 51 push ecx
00002E10: 90 nop
00002E11: C0C004 rol al,4
00002E14: FEC1 inc cl
00002E16: 59 pop ecx
00002E17: AA stosb
00002E18: E2F4 loop 000002E0E ---↑ (2)
00002E1A: E805000000 call 000002E24 ---↓ (3)

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