UNDERSTANDING THE MICROSOFT OFFICE 2016 PROTECTED-VIEW SANDBOX

Yong Chuan Koh

14th April 2017

MWR LABS

LABS

++

#whoami

Yong Chuan, Koh (@yongchuank)

- Security Researcher @ MWR Labs (SG) since 2014
- Interests:
  - Vulnerability Research
  - Reverse Engineering
  - Malware Analysis

MWR Labs

LABS

++

OUTLINE

- Introduction
- Sandbox Internals
- IPC Mechanism
- IPC Quirk
- Conclusion and Future Work

LABS

++

MS OFFICE 2016 PROTECTED-VIEW SANDBOX

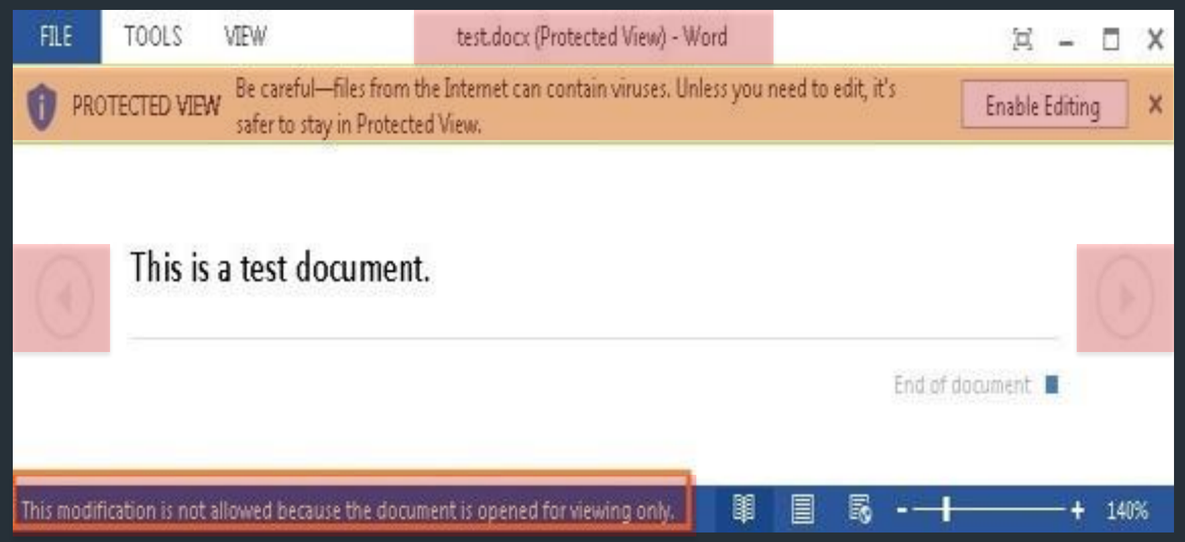
INTRODUCTION

LABS

++ SANDBOX

- Sandboxing 101
  - Wikipedia: *"…a sandbox is a security mechanism for separating running programs…A sandbox typically provides a tightly controlled set of resources for guest programs to run in, …A sandbox is implemented by executing the software in a restricted operating system environment, thus controlling the resources (…) that a process may use…"*
  - Request broker to work around certain restrictions

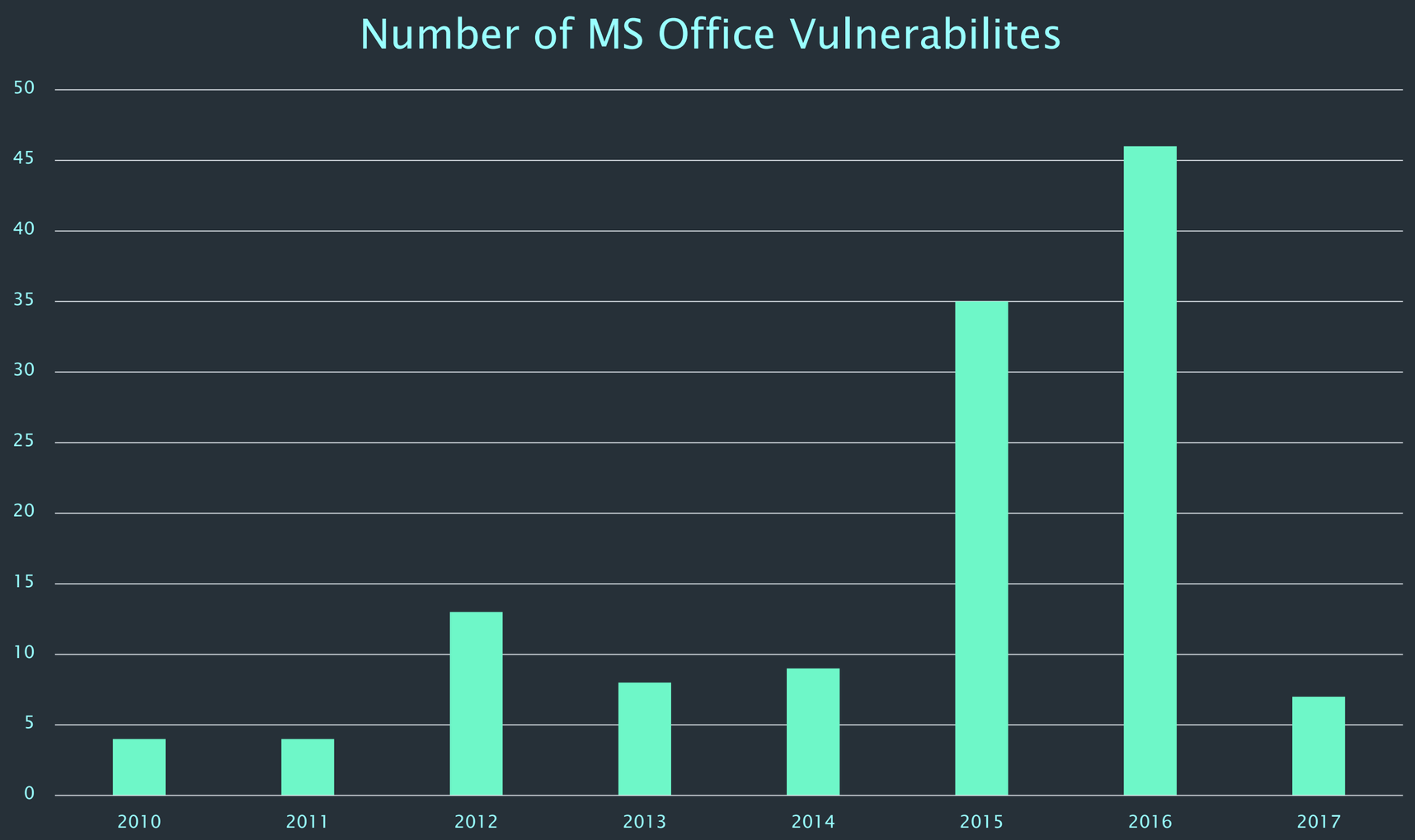
- Protected-View Sandbox
  - Introduced since MS Office 2010
  - Untrusted files are sandboxed
  - Read-only mode



LABS

++

MS OFFICE VULNERABILITIES



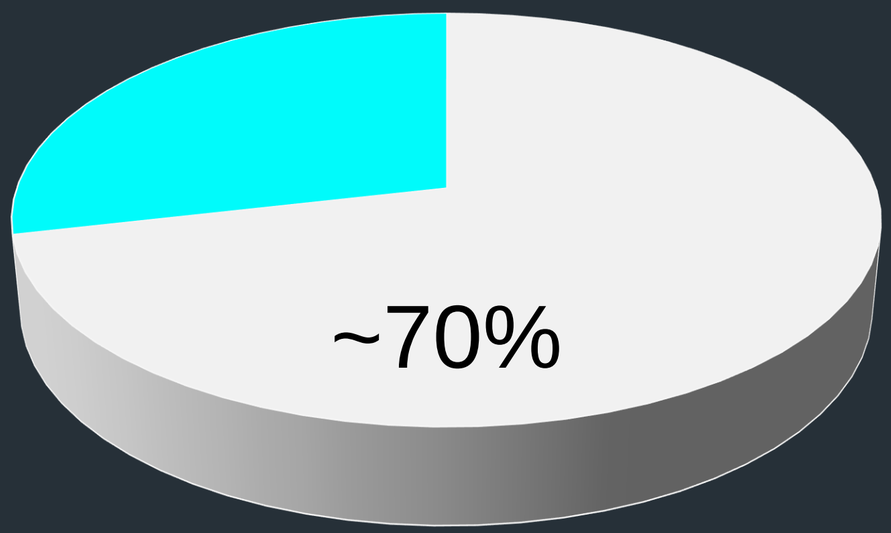
http://www.cvedetails.com/google-search-results.php?q=microsoft+office

LABS

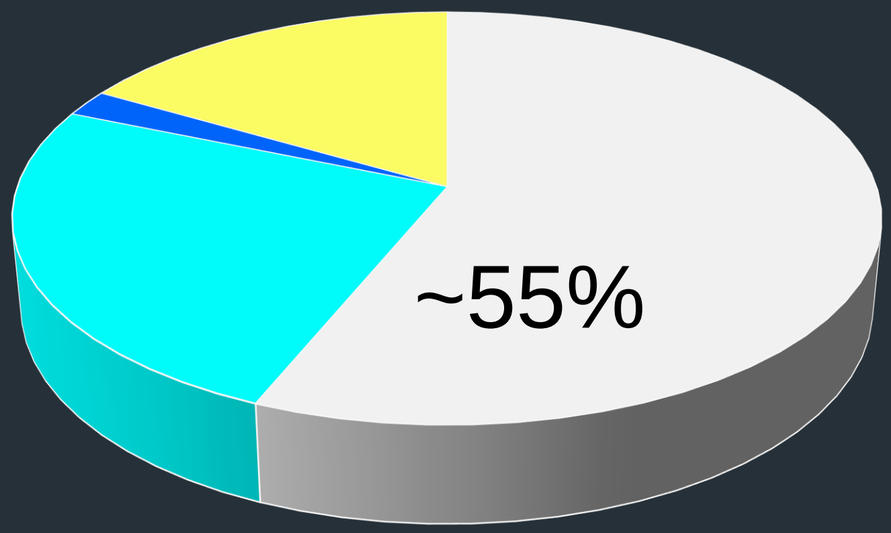
++

MS OFFICE VULNERABILITIES

2015



2016



- Relatively modest numbers (wrt IE, Edge, Win32k)
- Protected-View would have reduce impact >50% of these
- MS Investment Decision: Vulnerability Numbers < Application Impact

LABS

++

MOTIVATION

- Pwn2Own 2017
  - New “Enterprise Applications” Category
  - Learn from other researchers
  - Renewed personal interest

LABS

++

GOALS

- Updates to Protected-View 2013
  - “Understanding the Microsoft Office 2013 Protected-View Sandbox”
- Protected-View sandbox remains unbroken (?)
- Have fun…

- MS Word 2016 MSO (16.0.4266.1001)

LABS

++

MS OFFICE 2016 PROTECTED-VIEW SANDBOX

SANDBOX INTERNALS

- INITIALIZATION
- ARCHITECTURE

LABS

++ INITIALIZATION

- Starts in MSO.sub_002CAE9E()
  - arg_0: fullpath to sandbox executable
  - arg_4: sandbox executable switch (“/Embedding”)
  - arg_8: affects 3 StartUpOptions Object fields
- StartUpOptions (loc_var) Object
  - Size 0x30
  - Majority of fields seemingly take default values

LABS

++

INITIALIZATION

StartUpOptions

Offset	Type	Field	Comment	
00	DWORD	dwSandboxID	rand_s() & 0x3FFF: 16k possible values	Capabilities
04	VOID	pSandboxCapabilitySID	Array of Capability-SIDs to be added to sandbox	
08	DWORD	dwSandboxCapalibitySID	Describes 1 or more Capability-SIDs to be added to sandbox: - 0x01: add SID_InternetClient - 0x02: add SID_InternetClientServer - 0x04: add SID_PrivateNetworkClientServer - 0x08: add SID_EenterpriseAuthentication - 0x10: add SID_MSOffice (default)	
0C	DWORD	dwUnknown_0C	Constant 0x15 or otherwise	
10	DWORD	dwActiveProcessLimit	- JOBOBJECT_BASIC_LIMIT_INFORMATION.ActiveProcessLimit - Constant 1 (default)	Job Restrictions
14	HANDLE	hCompletionPort	JOBOBJECT_ASSOCIATE_COMPLETION_PORT.CompletionPort	
18	PVOID	pCompletionKey	JOBOBJECT_ASSOCIATE_COMPLETION_PORT.CompletionKey	
1C	SIZE_T	dwJobMemoryLimit	JOBOBJECT_EXTENDED_LIMIT_INFORMATION.JobMemoryLimit	

LABS

++

INITIALIZATION

StartUpOptions				
Offset	**Type**	**Field**	**Comment**	
20	LARGE_INTEGER	dwTimeLimitLowPart	JOBOBJECT_EXTENDED_LIMIT_INFORMATION. JOBOBJECT_BASIC_LIMIT_INFORMATION.PerJobUserTimeLimit	
28	BOOL	AlternateWinSta	- TRUE if ((arg_8 >> 1) & 1) == 1 - if FALSE && fAlternateWinsta: • add SID S-1-15-3-2367048223-3513148975, or - if TRUE && fLogonUser: • add SID S-1-15-3-2367048223-3513148975	Separate Desktop
29	BOOL	fAlternateWinsta	- TRUE if (arg_8 & 3) != 3 - if TRUE: • JOBOBJECT_BASIC_UI_RESTRICTIONS.UIRestrictionsClass = 0xFF - if FALSE && bUnk_2A: • JOBOBJECT_BASIC_UI_RESTRICTIONS.UIRestrictionsClass = 0 - if FALSE && !bUnk_2A: • JOBOBJECT_BASIC_UI_RESTRICTIONS.UIRestrictionsClass = 0xE8	
2A	BOOL	bUnknown_2A	Constant 1 (default)	

LABS

++ INITIALIZATION

StartUpOptions			
Offset	**Type**	**Field**	**Comment**
2B	BOOL	fLogonUser	– if TRUE && !bChkUseAC: • LogonUser (LOGON32_LOGON_NEW_CREDENTIALS) – if TRUE && bChkUseAC && !AlternateWinSta: • LogonUser (LOGON32_LOGON_NEW_CREDENTIALS)
2C	BYTE	bUnknown_2C	Unknown (copied to [esi+8Ch])
2D	BOOL	bChkUseAC	– If TRUE && HKLM\Software\Microsoft\Office\16.0\Common\Security:UseAppContainer == 1 && GetProcAddress("DeriveAppContainerSidFromAppContainerName“) != NULL: • [esi+80h] = 1
2E	BYTE	bUnknown_2E	Unknown (Copied to [esi+81h])
2F	BYTE	bUnknown_2F	Unknown

AC or Low-IL or None

LABS

++ INITIALIZATION

Create Sandbox ID

- ID: rand_s() & 3FFFh
- SandboxName: OICE_16_974FA576_32C1D314_<ID>

StartUpOptions		
Offset	**Type**	**Field**
00	DWORD	dwSandboxID

LABS

++ INITIALIZATION

Create Sandbox ID

- ID: rand_s() & 3FFFh
- SandboxName: OICE_16_974FA576_32C1D314_<ID>

Set Job Restrictions

- JOBOBJECT_BASIC_LIMIT_INFORMATION
- JOBOBJECT_ASSOCIATE_COMPLETION_PORT
- JOBOBJECT_EXTENDED_LIMIT_INFORMATION

StartUpOptions		
Offset	**Type**	**Field**
10	DWORD	dwActiveProcessLimit
14	HANDLE	hCompletionPort
18	PVOID	pCompletionKey
1C	SIZE_T	dwJobMemoryLimit
20	LARGE_INTEGER	dwTimeLimitLowPart

LABS

++ INITIALIZATION

Create Sandbox ID

- ID: rand_s() & 3FFFh
- SandboxName: OICE_16_974FA576_32C1D314_<ID>

StartUpOptions		
Offset	**Type**	**Field**
04	VOID	pSandboxCapabilitySID
08	DWORD	dwSandboxCapalibitySID

Set Job Restrictions

- JOBOBJECT_BASIC_LIMIT_INFORMATION
- JOBOBJECT_ASSOCIATE_COMPLETION_PORT
- JOBOBJECT_EXTENDED_LIMIT_INFORMATION

Add AC+Capability SIDs

- CreateAppContainerProfile(), DeriveAppContainerSidFromAppContainerName()
- **SID_MSOffice (default: SID S-1-15-3-2929230137-1657469040)**
- SID_InternetClient
- SID_InternetClientServer
- SID_PrivateNetworkClientServer
- SID_EenterpriseAuthentication

LABS

++ INITIALIZATION

Create AC Dir + Desktop

- GetAppContainerFolderPath() + “\\Temp”
- CreateWindowStationW(), GetProcessWindowStation(), SetProcessWindowStation(), CreateDesktopW()

StartUpOptions		
Offset	**Type**	**Field**
28	BOOL	AlternateWinSta
29	BOOL	fAlternateWinsta
2B	BOOL	fLogonUser

LABS

++ INITIALIZATION

Create AC Dir + Desktop

- GetAppContainerFolderPath() + “\\Temp”
- CreateWindowStationW(), GetProcessWindowStation(), SetProcessWindowStation(), CreateDesktopW()

Create+Connect IPC Pipe

- **lpPipeName: “\\.\pipe\OfficeUser_” + SandboxName**
- OpenMode: FILE_FLAG_OVERLAPPED|FILE_FLAG_FIRST_PIPE_INSTANCE|PIPE_ACCESS_DUPLEX
- PipeMode: PIPE_TYPE_MESSAGE|PIPE_READMODE_MESSAGE|PIPE_REJECT_REMOTE_CLIENTS
- MaxInstances: 1
- **OutBufferSize: 0x00002000**
- **InBufferSize: 0x00002000**
- DefaultTimeout: 50 milliseconds

LABS

++ INITIALIZATION

Start Sandbox Process

- Start child-process as:
  - AppContainer, or
  - Low-IL, or
  - Non-sandboxed
- HKLM\Software\Microsoft\Office\16.0\Common\Security:UseAppContainer

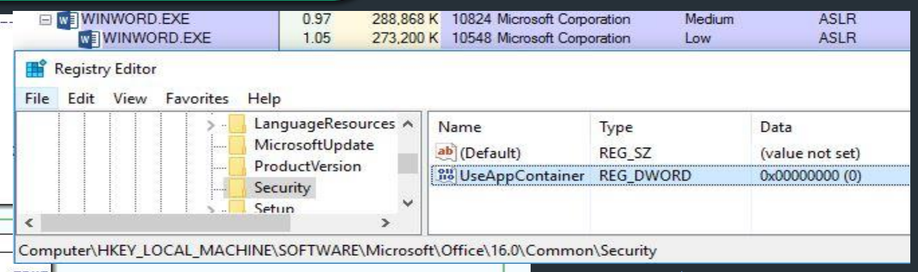
StartUpOptions		
Offset	**Type**	**Field**
2D	BYTE	bChkUseAC
2E	BYTE	bUnknown_2E

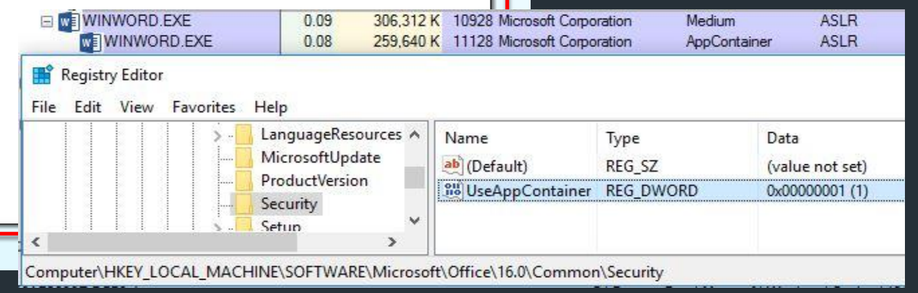
```
002CD523 mov     dl, [ebx+80h]   ; ----- ie: [esi+80h] previously ----------------------
002CD529 lea     eax, [ebp+Dst]
002CD52F add     esp, 0Ch
002CD532 mov     [ebp+STARTUP_INFO], 48h
002CD53C cmp     dword ptr [ebx+58h], 0
002CD540 mov     ecx, 414h
002CD545 mov     [ebp+var_A98], esi
002CD54B cmovz   eax, [ebp+var_AD4]
002CD552 test    dl, dl
002CD554 mov     [ebp+var_AD4], eax
002CD55A mov     eax, 80414h
002CD55F cmovnz  ecx, eax
002CD562 jz      short loc_2CD59B
```

```
002CD564 cmp     byte ptr [ebx+81h], 0 ; [esi+81h] = BYTE [StartUpOptions+2Eh], which is not set anywhere
002CD56B jz      short loc_2CD59B ; no jmp if HKLM\Software\Microsoft\Office\16.0\Common\Security:UseAppContainer = TRUE && [esi+81h] == TRUE
```

```
002CD56D lea     edi, [ebx+5Ch]
002CD570 push    edi             ; lpProcessInformation
002CD571 lea     eax, [ebp+STARTUP_INFO]
002CD577 push    eax             ; lpStartupInfo
002CD578 lea     eax, [ebp+CurrentDirectory]
002CD57E push    eax             ; lpCurrentDirectory
002CD57F push    [ebp+lpEnvironment] ; lpEnvironment
002CD585 lea     eax, [ebp+CommandLine]
002CD58B push    ecx             ; dwCreationFlags
002CD58C xor     ecx, ecx
002CD58E push    ecx             ; bInheritHandles
002CD58F push    ecx             ; lpThreadAttributes
002CD590 push    ecx             ; lpProcessAttributes
002CD591 push    eax             ; lpCommandLine
002CD592 push    ecx             ; lpApplicationName
002CD593 call    ds:CreateProcessW
002CD599 jmp     short loc_2CD5D4
```

```
002CD59B
002CD59B loc_2CD59B:             ; case 1: HKLM\Software\Microsoft\Office\16.0\Common\Security:UseAppContainer is missing
002CD59B test    dl, dl          ; case 2: HKLM\Software\Microsoft\Office\16.0\Common\Security:UseAppContainer = FALSE
002CD59B                         ; case 3: HKLM\Software\Microsoft\Office\16.0\Common\Security:UseAppContainer = TRUE && [esi+81h] == FALSE
002CD59D lea     eax, [ebx+88h]
002CD5A3 lea     edx, [ebp+STARTUP_INFO]
002CD5A9 cmovnz  eax, edi
002CD5AC lea     edi, [ebx+5Ch]
002CD5AF push    edi             ; lpProcessInformation
002CD5B0 push    edx             ; lpStartupInfo
002CD5B1 lea     edx, [ebp+CurrentDirectory]
002CD5B7 push    edx             ; lpCurrentDirectory
002CD5B8 push    [ebp+lpEnvironment] ; lpEnvironment
002CD5BE xor     edx, edx
002CD5C0 push    ecx             ; dwCreationFlags
002CD5C1 push    edx             ; bInheritHandles
002CD5C2 push    edx             ; lpThreadAttributes
002CD5C3 push    edx             ; lpProcessAttributes
002CD5C4 lea     ecx, [ebp+CommandLine]
002CD5CA push    ecx             ; lpCommandLine
002CD5CB push    edx             ; lpApplicationName
002CD5CC push    dword ptr [eax] ; hToken
002CD5CE call    CreateProcessAsUserW
```





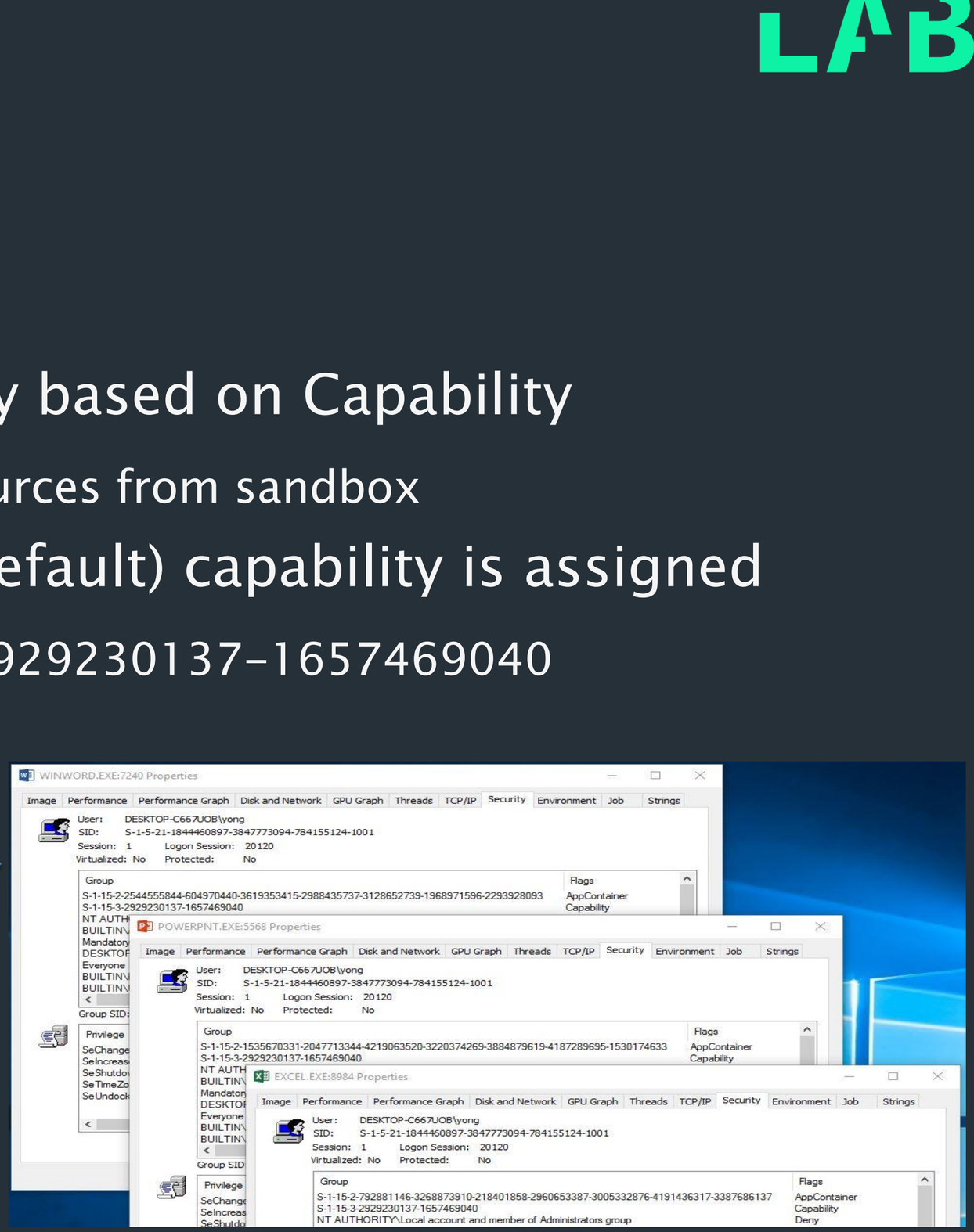
LABS

++

ARCHITECTURE

- AppContainer boundary based on Capability
  - Defines accessible OS resources from sandbox
- Protected-View: one (default) capability is assigned
  - SID_MSOffice: S-1-15-3-2929230137-1657469040
  - Undocumented

WINWORD.EXE	1.33	312,200 K	6184	Microsoft Corporation	Medium
WINWORD.EXE		251,620 K	7240	Microsoft Corporation	AppContainer
EXCEL.EXE		425,796 K	7424	Microsoft Corporation	Medium
EXCEL.EXE		605,672 K	8984	Microsoft Corporation	AppContainer
POWERPNT.EXE	0.05	260,484 K	6508	Microsoft Corporation	Medium
POWERPNT.EXE		312,400 K	5568	Microsoft Corporation	AppContainer



++

ARCHITECTURE

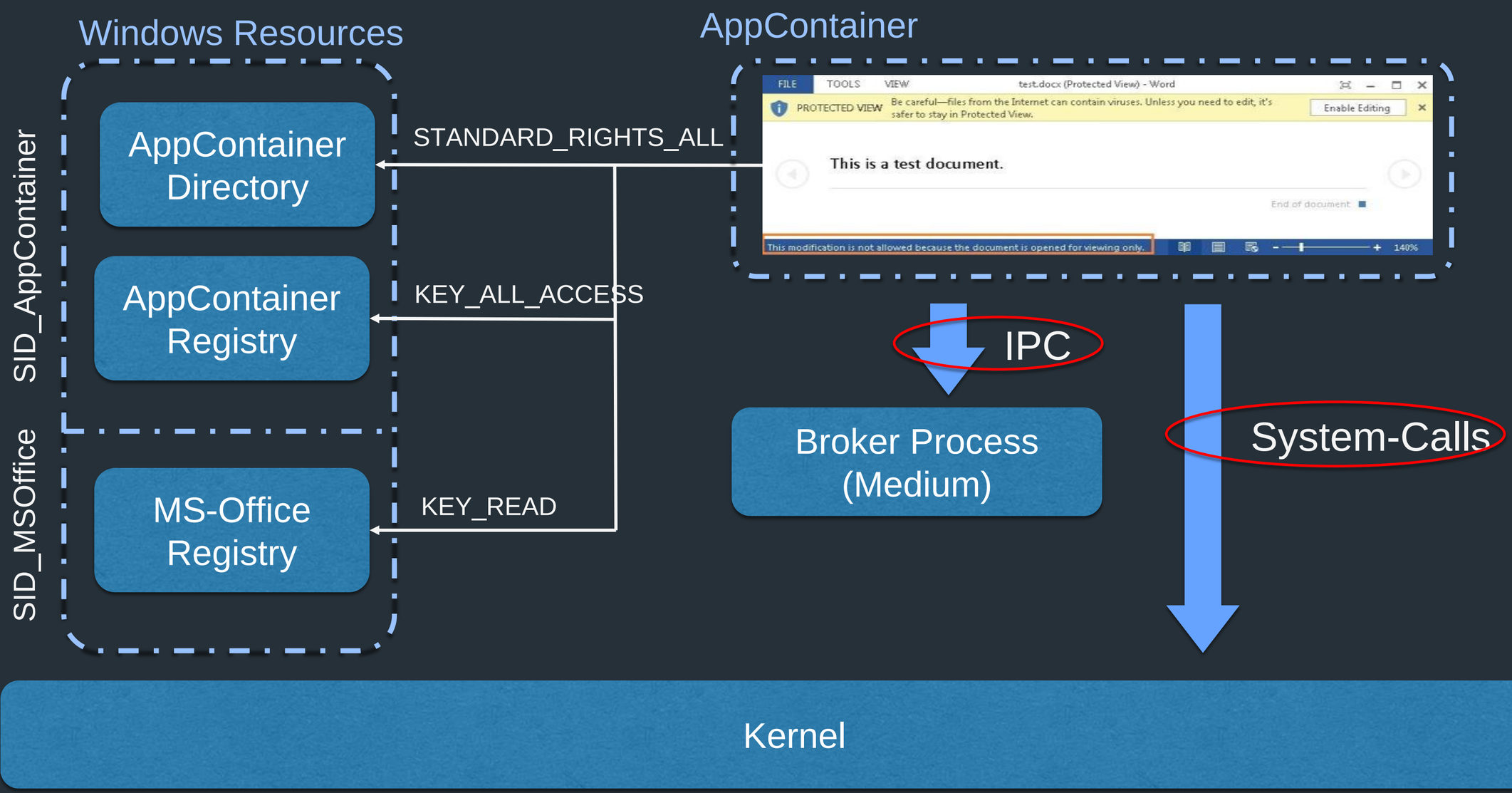
- SID_MSOffice (S-1-15-3-2929230137-1657469040)
  - File Locations
    - None
  - Networking
    - connect() fails with Permission Denied (WSAEACCES)
    - No overlap with SID_Internet*
  - Registries
    - KEY_READ: HKCU\Software\Microsoft\Office*
    - KEY_READ: HKEY_USERS\<*WinUser-SID*>\Software\Microsoft\Office*
    - FunFact: HKCU\Software\Microsoft\Office\16.0\Word\Security\Trusted Locations

SANDBOX INTERNALS

LABS

++

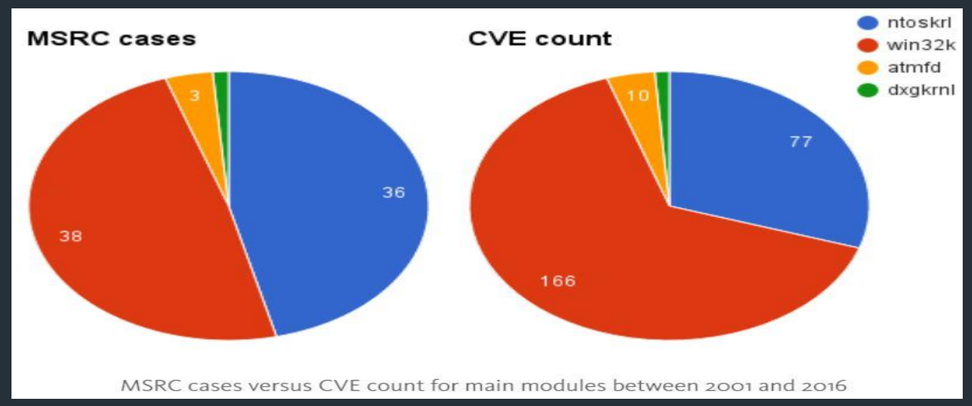
ARCHITECTURE



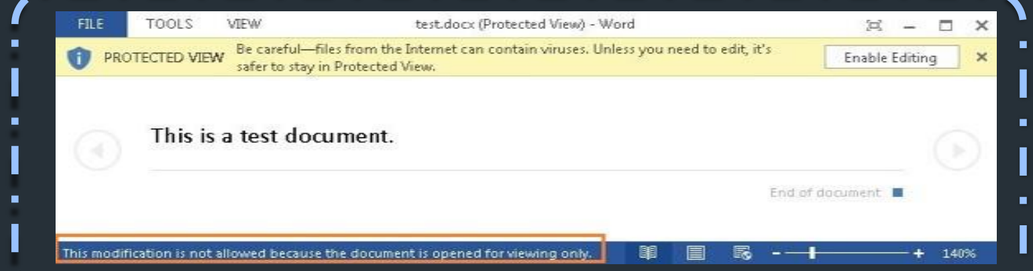
SANDBOX INTERNALS

++

ARCHITECTURE



AppContainer



IPC

Broker Process (Medium)

System-Calls

Kernel

```
0: kd> !process 0 0 winword.exe
PROCESS 981be380  SessionId: 1  Cid: 1128    Peb: 01176000  ParentCid: 0cec
    DirBase: 7fff0680  ObjectTable: d481c3c0  HandleCount: <Data Not Accessible>
    Image: WINWORD.EXE

PROCESS d232e8c0  SessionId: 1  Cid: 1b98    Peb: 00fea000  ParentCid: 1128
    DirBase: 7fff0840  ObjectTable: d4993480  HandleCount: <Data Not Accessible>
    Image: WINWORD.EXE

0: kd> dt _EPROCESS EnableFilteredWin32kAPIs 981be380
nt!_EPROCESS
   +0x2e8 EnableFilteredWin32kAPIs : 0y0
0: kd> dt _EPROCESS EnableFilteredWin32kAPIs d232e8c0
nt!_EPROCESS
   +0x2e8 EnableFilteredWin32kAPIs : 0y0
```

"How bad design decisions created the least secure driver on Windows"

LABS

++

MS OFFICE 2016 PROTECTED-VIEW SANDBOX

INTER-PROCESS COMMUNICATION MECHANISM

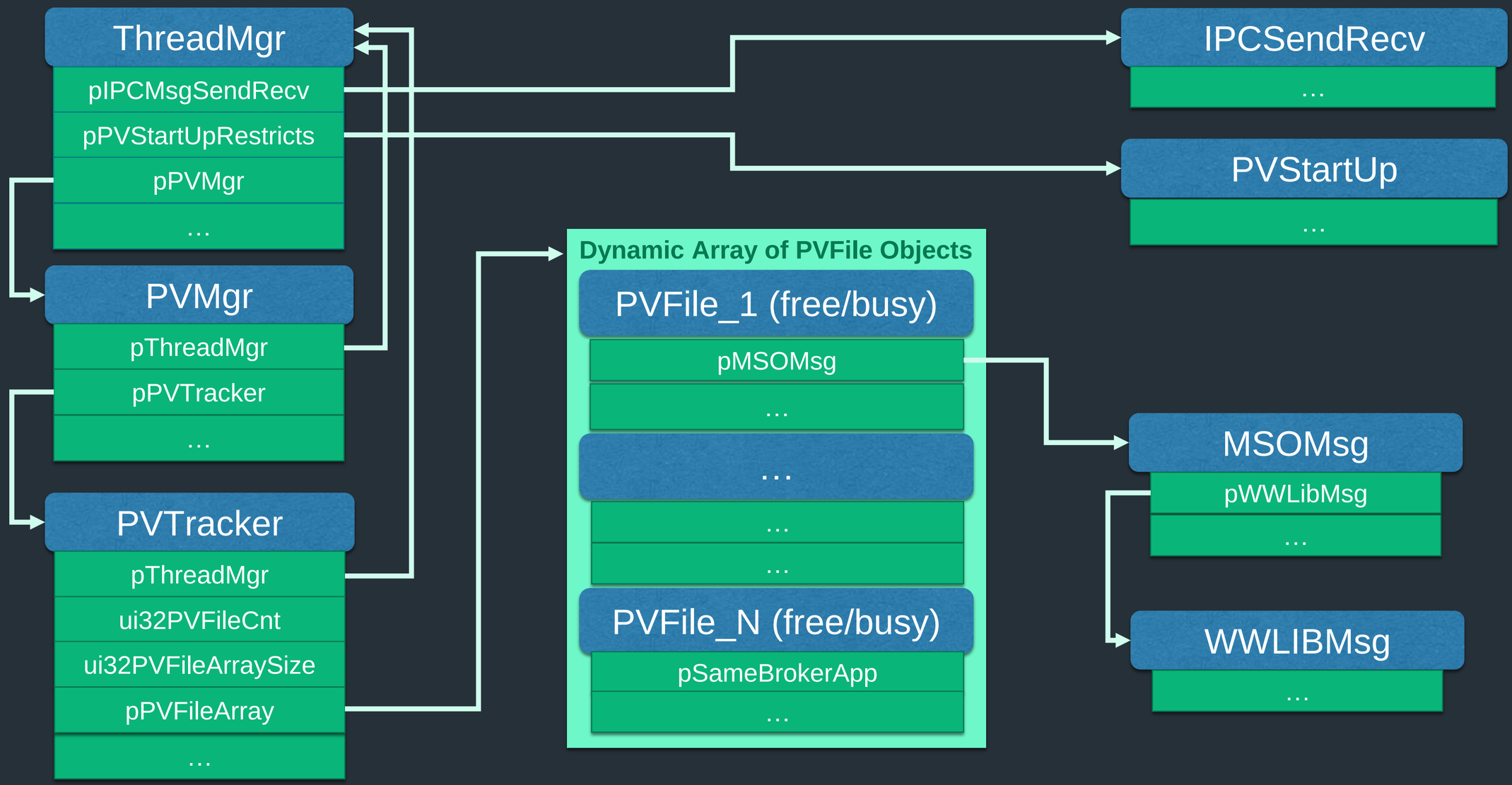
- INTERNAL OBJECTS
- MESSAGE FORMAT
- MESSAGE QUIRK: FILE I/O

IPC MECHANISM

LABS

++

INTERNAL OBJECTS



LABS

++ INTERNAL OBJECTS

ThreadMgr			
Offset	**Type**	**Field**	**Comment**
08	PVOID	pIPCMsgSendRecv	Pointer to object that sends/receives IPC messages
0C	PVOID	pPVStartUpRestricts	Pointer to object that describes sandbox startup restrictions
10	PVOID	pPVMgr	Pointer to PVMgr object

PVMgr			
Offset	**Type**	**Field**	**Comment**
04	UINT32	ui32Num	Number of PV files + 2
08	PVOID	pThreadMgr_1	Pointer to ThreadMgr object
0C	PVOID	pPVTracker_1	Pointer to PVTracker object

PVTracker			
Offset	**Type**	**Field**	**Comment**
0C	PVOID	pThreadMgr	Pointer to ThreadMgr object
14	UINT32	ui32PVFileCnt	Number of Protected-View files (ie: number of busy slots in PVFileArray)
18	UINT32	ui32PVFileArraySize	Total size of PVFileArray
20	PVOID	pPVFileArray	Pointer to array of PVFile objects

LABS

++ INTERNAL OBJECTS

PVFile			
Offset	**Type**	**Field**	**Comment**
04	UINT32	ui32ViewID	Unique ID to identify respective PV file
08	HWND	hOPHWnd	hWnd for “OPH Previewer Window” class
0C	LPWSTR	pwszFileName	Pointer to full-path to original file
10	LPWSTR	pwszTmpFileName	Pointer to full-path to tmp file in AC directory
14	PVOID	pMSOMsg	Pointer to MSOMsg object
18	UINT32	bSessAllowHyperlinks	TRUE/FALSE (used in 0x091000 message)

LABS

++ INTERNAL OBJECTS

MSOMsg			
Offset	**Type**	**Field**	**Comment**
0C	PVOID	pWWLIBMsg	Pointer to WWLIBMsg object
84	HWND	hOPHParentWnd	Used in 0x061000 and 0x101000 message
90	PVOID	pDRMStream	Used in 0x081000 message
B0	PVOID	pTaskList	Used in 0x0B1000 message

WWLIBMsg (WINWORD)			
Offset	**Type**	**Field**	**Comment**
20	UCHAR[0x2C]	ucIPC091100Contents	Array storing IPC 0x091100 message bytes
4C	UINT32	ui32IPC071100MsgID	MsgID of 0x071100 message
50	UINT32	ui32IPC081100MsgID	MsgID of 0x081100 message
54	UINT32	ui32IPC091100MsgID	MsgID of 0x091100 message
58	UINT32	ui32IPC031100MsgID	MsgID of 0x031100 message
5C	UINT32	ui32IPC041100MsgID	MsgID of 0x041100 message
60	UINT32	ui32IPC0E1100MsgID	MsgID of 0x0E1100 message
64	UCHAR[0x24]	ucIPC041100Contents	Array storing IPC 0x041100 message bytes
8C	UCHAR[0x1D4]	ucIPC031100Contents	Array storing IPC 0x031100 message bytes

LABS

++ MESSAGE FORMAT

- Two types of IPC messages
  - Protected-View Base
    - Always present
    - MSO.DLL
  - Protected-View Specific
    - Depends whether WINWORD, EXCEL or POWERPNT is used
    - WWLIB.DLL, PPCORE.DLL, EXCEL.EXE
  - Differ by 4-bytes in Message Header

IPC MECHANISM

LABS

++

MESSAGE FORMAT

Message Header

Message Body (Optional)

PVBase Header Format		
UINT32	ui32VirtualKey	Only used for 0x071000 message
UINT32	ui32MsgTag	Type of IPC message
UINT32	ui32MsgID	Matches IPC request to response; can be random
UINT32	ui32MsgSize	Total size of IPC message (max 0x2000; as per pipe creation)

PVSpecific Header Format		
UINT32	ui32VirtualKey	Only used for 0x071000 message
UINT32	ui32MsgTag	Type of IPC message
UINT32	ui32MsgID	Matches IPC request to response; can be random
UINT32	ui32MsgSize	Total size of IPC message (max 0x2000; as per pipe creation)
UINT32	**ui32ViewID**	**PV file ID (correspond to pViewFile->ui32ViewID)**

Body Format
…

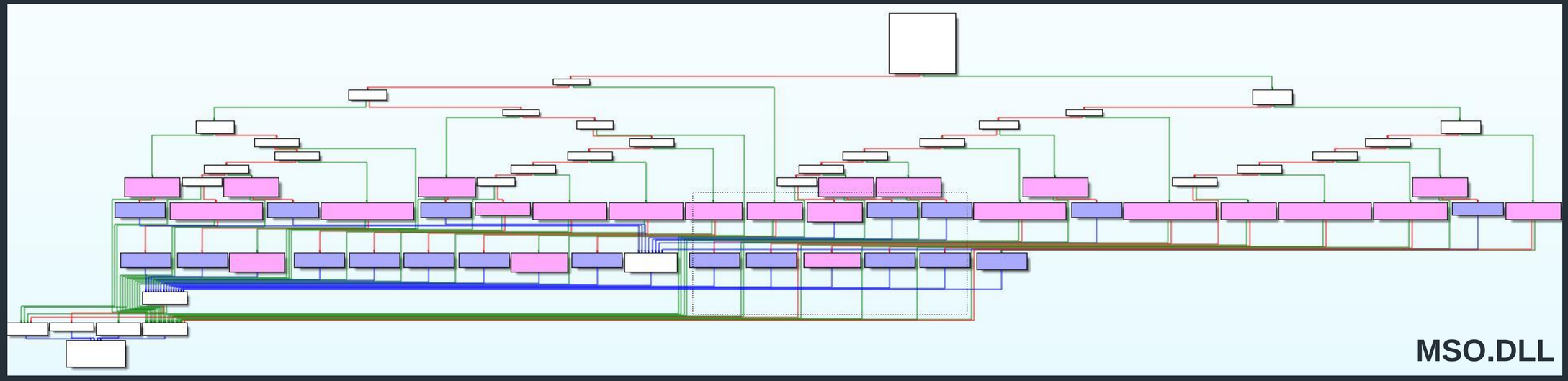
IPC MECHANISM

LABS

++

MESSAGE FORMAT

PVBase Header Format		
UINT32	ui32VirtualKey	Only used for 0x071000 message
UINT32	**ui32MsgTag**	**Type of IPC message**
…		

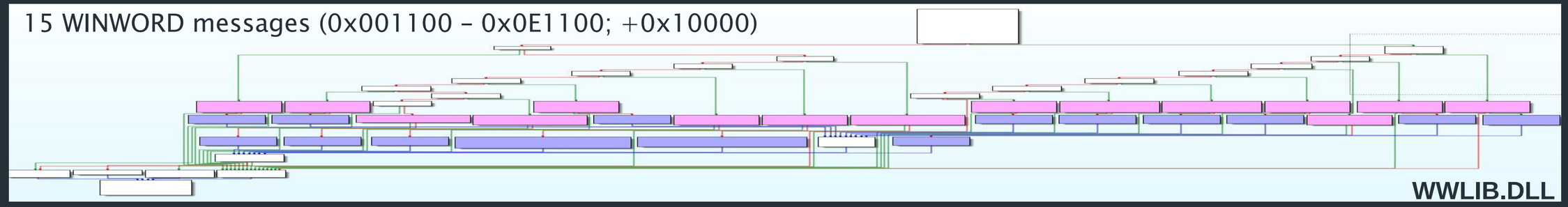


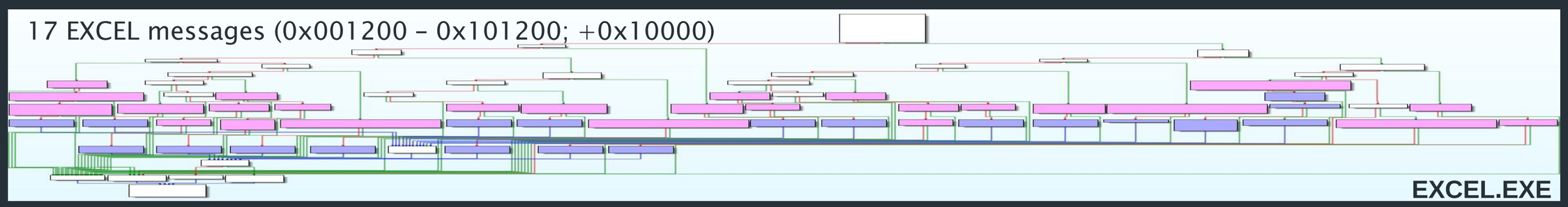
- 23 MSO messages (0x001000 – 0x161000; +0x10000)

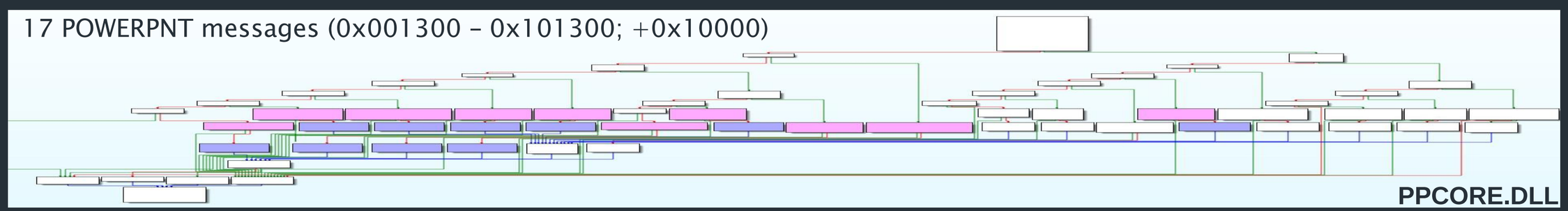
LABS

++ MESSAGE FORMAT

PVSpecifc Header Format		
UINT32	ui32VirtualKey	Only used for 0x071000 message
UINT32	**ui32MsgTag**	**Type of IPC message**
…		







LABS

++ MESSAGE FORMAT

- Sanity-check
  - Exact/Minimum message size
  - WSTRING field represented as
    - | PVOID pwzString || UINT16 wzStringLen || WCHAR wzString[N] |
  - wzStringLen <= MsgSize
  - etc
- Service message

LABS

++

MESSAGE QUIRK: FILE I/O

- *“Naming Files, Paths, and Namespaces”*

> **Note** File I/O functions in the Windows API convert "/" to "\" as part of converting the name to an NT-style name, except when using the "\\?\" prefix as detailed in the following sections.

- Some IPC messages contains *wzFileName*
  - 0x051000: wzTempFileName
  - 0x0C1000: wzAdditionalWerFileName
- *wzFileName* file meant to reside in AppContainer directory
  - Broker ensures absence of ‘\’ before appending AppContainer path
- Directory-traversal out of AppContainer boundary with ‘/’

LABS

++ MESSAGE QUIRK: FILE I/O

- Message 0x051000
  - *wzTempFileName*: Temporary, .tmp, file that Winword creates
  - Sandbox informs Broker about .tmp filename for current PV file
  - Only first 0x051000 is serviced, otherwise ignored

Message Body for 0x051000			
Offset	**Type**	**Field**	**Comment**
10	UINT32	ui32ViewID	-
14	PWSTR	pTempFileName	Pointer to wzTempFileName, or NULL
18	UINT16	ui16TempFileNameSize	Wide-length of pTempFileName
1A	WCHAR[]	wzTempFileName	File name of .tmp file

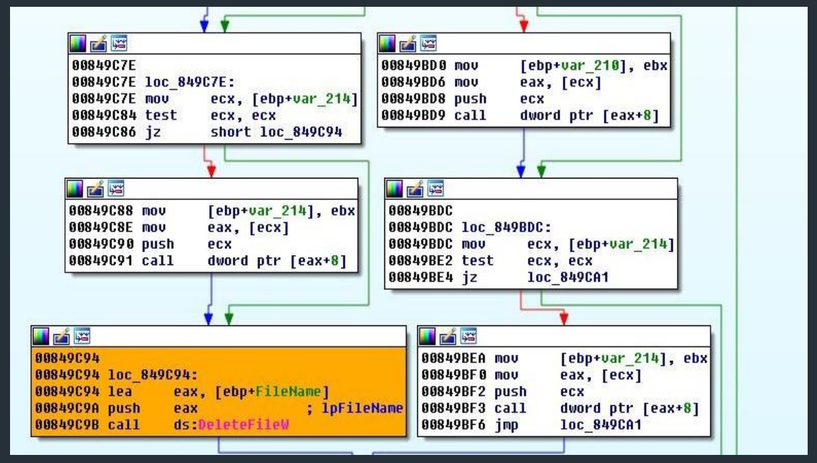
IPC MECHANISM

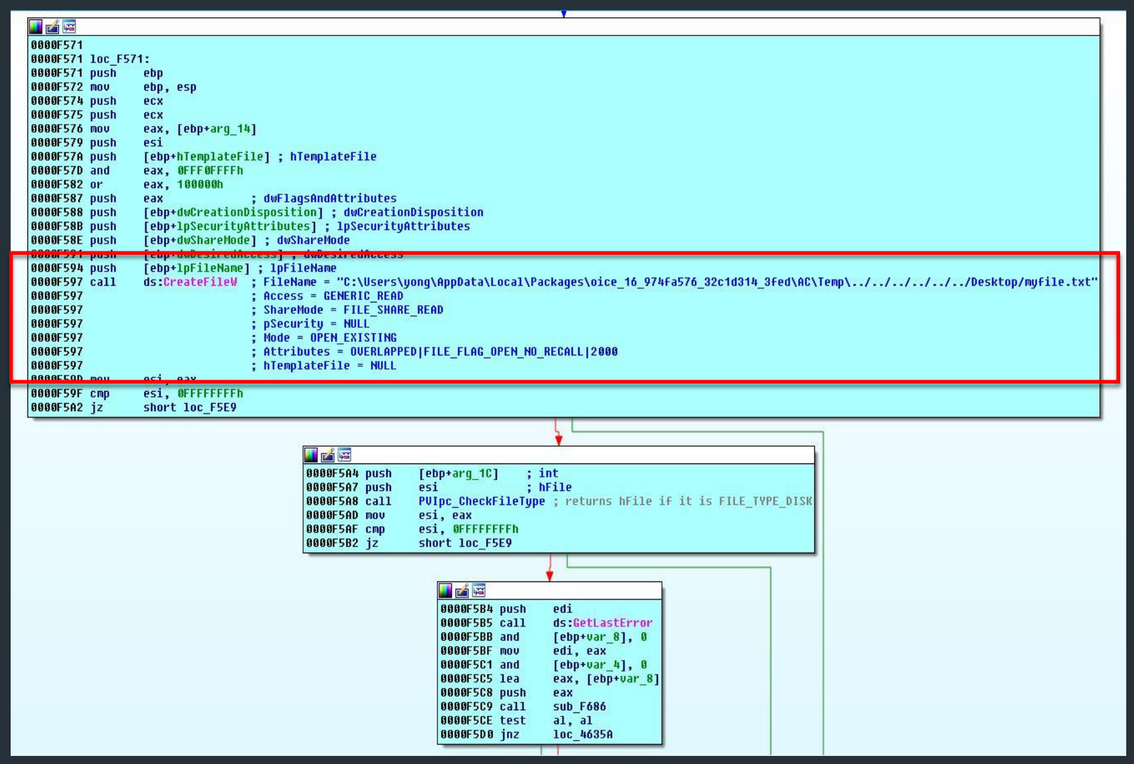
LABS

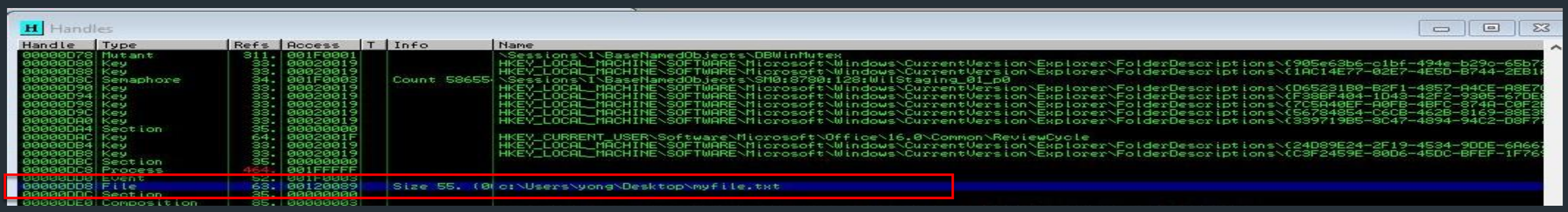
++

MESSAGE QUIRK: FILE I/O

IPC 0x051000 Message		
WCHAR[]	wzTempFileName	“../../../../../../Desktop/myfile.txt”
…		







LABS

++

MESSAGE QUIRK: FILE I/O

- Message 0x0C1000
  - *wzWerFileName*: Upload to WER server, and delete on host
  - Sandbox requests Broker to start Windows Error Reporting on behalf
- Typical: ApplicationA -> DWWIN.EXE (on ApplicationA)
- WINWORD: Sandbox -> Broker -> DWWIN.EXE (on Sandbox)
- JOBOBJECT_BASIC_LIMIT_INFOMATION.ActiveProcessLimit = 1

Message Body for 0x0C1000

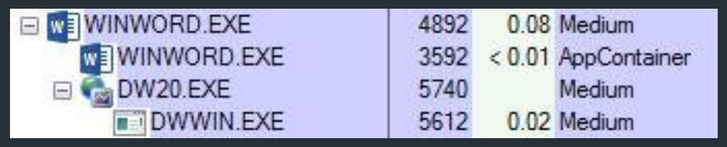
Offset	Type	Field	Comment
10	HANDLE	hSandboxSharedMem	-
14	HANDLE	hEventBrokerIsDone	Broker sets this event after DW20.EXE finishes and before terminates sandbox
18	PWSTR	pWerFileName	Pointer to wzWerFileName, or NULL
1C	UINT16	ui16WerFileNameSize	Wide-length of pWerFileName
1E	WCHAR[]	wzWerFileName	Additional WER file to submit, and created by PV

IPC MECHANISM

LABS

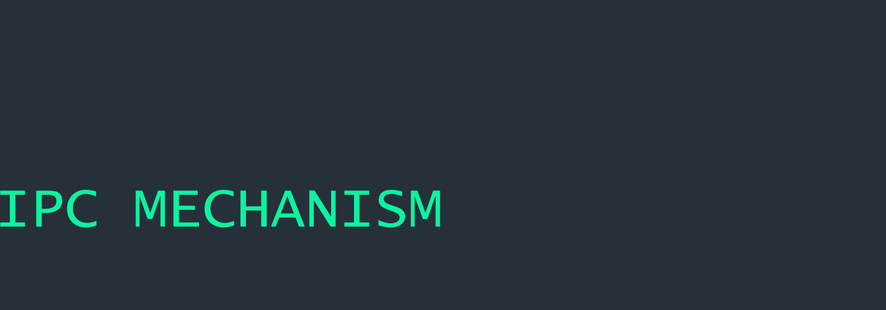
++

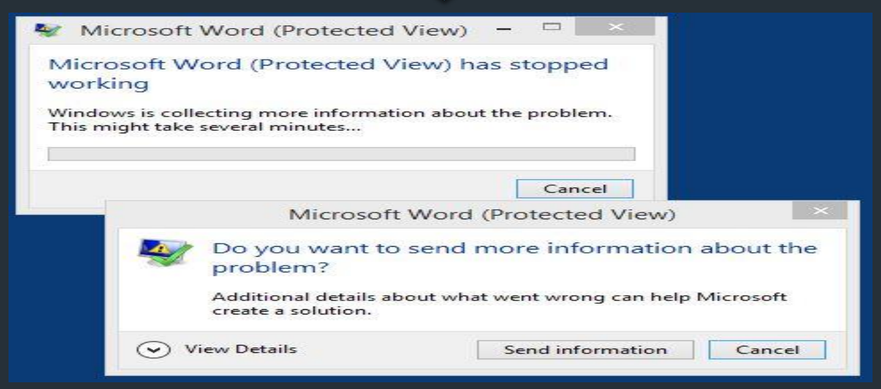
MESSAGE QUIRK: FILE I/O



IPC 0x0C1000 Message		
WCHAR[]	wzWerFileName	“../../../../../../Desktop/thisismyfile.txt”
…		

DWWIN.EXE



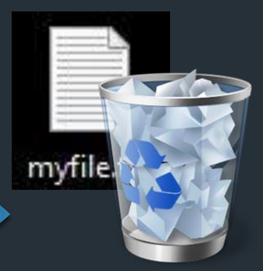


crash_metadata.xml

“Send me more info”

additional_wer_files.cab

Default: “watson.microsoft.com”
GPO : “Configure Corporate Windows Error Reporting”



LABS

++

MS OFFICE 2016 PROTECTED-VIEW SANDBOX

- CONCLUSION AND FUTURE WORK

LABS

++

CONCLUSION

- Simple Protected-View Architecture
  - SID_MSOffice capability access MF Office reg-keys (KEY_READ)

- Most effective not in containing RCE, but in disabling most functions to prevent the initial RCE

- More viable to escape Protected-View via Kernel Syscalls
  - Win32k.sys is not filtered

- Small Set of IPC messages
  - MSO (23) + WWLIB (15) / EXCEL (17) / PPCORE (17)

- Simple IPC Message Format
  - Easy to check for conformity

LABS

++

FUTURE WORK

- Check for new Protected-View features
  - 0x0F1100 (WWLIB.DLL) is removed from MS Office 2013
  - 0x161000 (MSO.DLL) is added to MS Office 2016
  - New IPC messages

MWR Labs

LABS

++

Thank You!

- Questions?