

The slide features a light blue background with abstract black and red geometric shapes at the top. In the top left corner is the FireEye logo. The main title 'Reversing the Gophe Spambot' is in large red font, with a subtitle 'Confronting COM Code and Surmounting STL Snags' in smaller gray font below it. In the bottom right corner is the FLARE logo, which consists of the word 'FLARE' in black with a blue lightning bolt symbol integrated into the letter 'A'. On the left side, there is a small white circle containing a stylized lowercase 'q'.

FireEye

Reversing the Gophe Spambot

Confronting COM Code and Surmounting STL Snags

Michael Bailey (@mykill)
BSides 2020
8 Feb 2020

FLARE

1

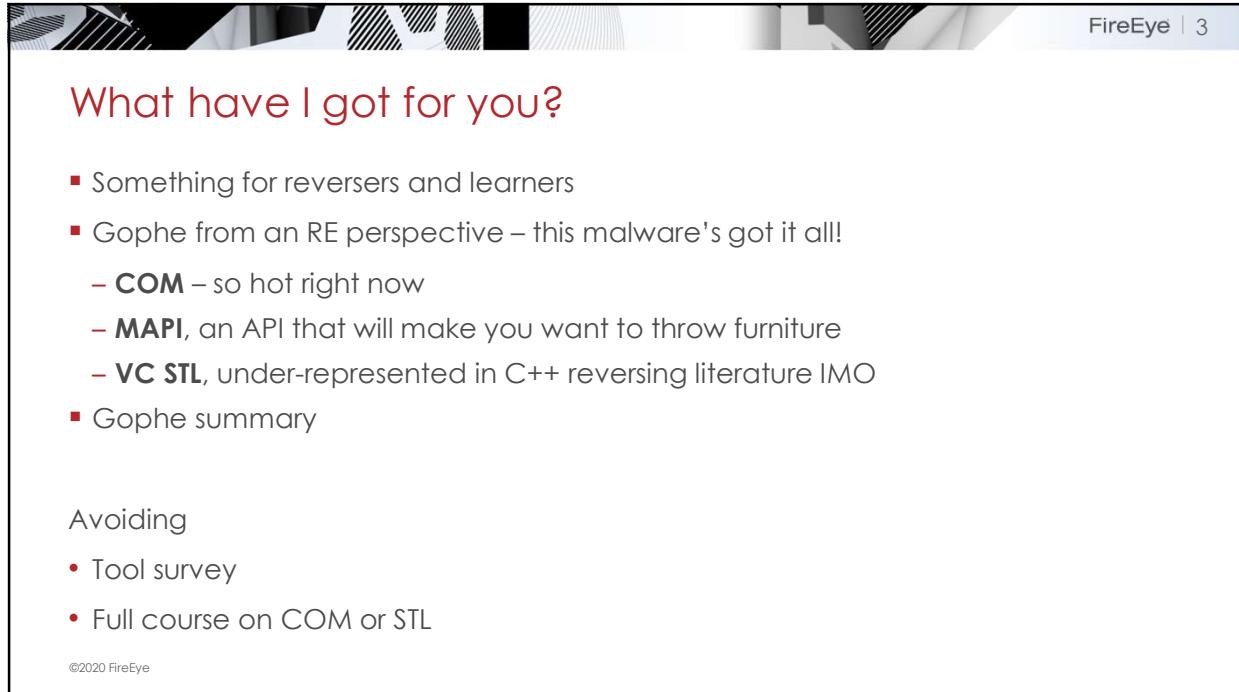
The slide has a decorative header bar with abstract black and white geometric shapes. The FireEye logo is in the top right corner. The title 'Michael Bailey (@mykill)' is in large red font. Below the title is a bulleted bio:

- Husband, Daddy, Bon Vivant
- Remote from Huntsville, AL
 - FLARE Reverse Engineer
 - Manager
 - Offensive Task Force
- Previously
 - Mandiant Red Team
 - Linux/Windows kernel @ Pikewerks
 - Bought by Raytheon
 - Windows server admin
- For fun
 - Babies, Foreign language, spinning DNB

On the right side, there are two photographs: one of Michael Bailey speaking on stage, and another of him and his family (wife and two young children) sitting together.

©2020 FireEye

2

A decorative header graphic featuring abstract black and white geometric shapes, including triangles and lines, set against a light gray background.

FireEye | 3

What have I got for you?

- Something for reversers and learners
- Gophe from an RE perspective – this malware's got it all!
 - **COM** – so hot right now
 - **MAPI**, an API that will make you want to throw furniture
 - **VC STL**, under-represented in C++ reversing literature IMO
- Gophe summary

Avoiding

- Tool survey
- Full course on COM or STL

©2020 FireEye

3

A decorative header graphic featuring abstract red and black geometric shapes, including triangles and lines, set against a dark red background.

FireEye | 4

Gophe

Aka MailClient, spambot extraordinaire

4

FireEye | 5

Harper's Index of Gophe

(MD5: D9630C174B8FF5C0AA26168DF523E63E)

Statistic	Figure
Size in bytes	2,783,232
Seconds to parse and auto-analyze in IDA 7.1	92
Size of WinMain in bytes	11,139
Number of monitors that would be needed to stack vertically to display all of WinMain at once	~90
WinMain function ranked by size	#2
Embedded PE-COFF binaries	3
Number of bytes in all .text sections combined	1,910,507
Number of functions in all binaries combined	9,792

©2020 FireEye

5

FireEye | 6

Graph View of WinMain, Maximized

The graph shows a highly complex and dense call graph for the WinMain function. The nodes are represented by small rectangles of various colors, and the edges represent function calls between them. A prominent vertical cluster of nodes is visible on the left side of the graph. An orange arrow with the text "One Screen" points to this cluster, indicating that the entire graph is too large to fit onto a single screen.

©2020 FireEye

6

17

Component Object Model

^ old font because 1993 technology

7

FireEye | 8

COM

Facts	Primer
<ul style="list-style-type: none"> ▪ Out of 250,000 PE-COFF samples from a private corpus of mostly malware, 22% call <code>CoCreateInstance</code> ▪ COM can abet persistence (<code>IShellLink</code> or <code>ITaskService</code>), FireWall modification (<code>HNetCfg.FwMgr</code>) and more ▪ Indirect calls hide code semantics 	<ul style="list-style-type: none"> ▪ A CoClass (COM class) can be identified by: <ul style="list-style-type: none"> – ProgID (e.g. <code>WScript.Shell</code>) – CLSID (a GUID) ▪ A CoClass implements one or more interfaces ▪ Interfaces define a virtual function table, identified uniquely by an: <ul style="list-style-type: none"> – IID – Interface ID (also a GUID) ▪ CoCreateInstance takes a CLSID and an IID and returns an interface pointer (called <code>ppv</code>)

`loc_4138F8:`
 `mov ecx, [eax]`
 `lea edx, [ebp+var_30]`
 `push edx`
 `push eax`
 `call dword ptr [ecx+34h]`
 `mov eax, [ebp+var_30]`
 `test eax, eax`
 `jz loc_4139C9`

©2020 FireEye

8

FireEye | 9

Pointer to Pointer to Vtable (ppv) and Indirect Calls

```

p → lpVtbl →
    +-----+
    | QueryInterface |
    +-----+
    | AddRef       |
    +-----+
    | Release      |
    +-----+
    | ...          |
    +-----+
  
```

`mov eax, [ebp+ppv]`
`push edi`
`push offset unk_685050`
`push eax`
`mov ecx, [eax]`
`call dword ptr [ecx]`
`mov esi, eax`

`loc_415961:`
`mov eax, [ebp+ppv]`
`push eax`
`mov ecx, [eax]`
`call dword ptr [ecx+8]`
`test esi, esi`
`jns short loc_415974`

©2020 FireEye

9

FireEye | 10

IDA Pro Structures

Type name	Declaration	Type library
ITaskScheduler	struct ITaskScheduler {	MS SDK (Windows XP)
ITaskSchedulerVtbl	struct ITaskSchedulerVtbl *lpVtbl;	MS SDK (Windows XP)
ITaskService	};	MS SDK (Windows XP)
ITaskServiceVtbl	struct ITaskServiceVtbl {	MS SDK (Windows XP)
ITaskSettings	struct ITaskSettingsVtbl *lpVtbl;	MS SDK (Windows XP)
ITaskSettings2	};	MS SDK (Windows XP)
ITaskSettings2Vtbl	struct ITaskSettings2Vtbl {	MS SDK (Windows XP)
ITaskSettings3	struct ITaskSettings3Vtbl *lpVtbl;	MS SDK (Windows XP)
ITaskSettings3Vtbl	};	MS SDK (Windows XP)
ITaskSettings4Vtbl	struct ITaskSettings4Vtbl {	MS SDK (Windows XP)
ITaskSettingsVtbl	struct ITaskSettingsVtbl *lpVtbl;	MS SDK (Windows XP)
ITaskTrigger	};	MS SDK (Windows XP)
ITaskTriggerVtbl	struct ITaskTriggerVtbl {	MS SDK (Windows XP)
ITaskVariables	struct ITaskVariablesVtbl *lpVtbl;	MS SDK (Windows XP)
ITaskVariablesVtbl	};	MS SDK (Windows XP)
ITaskbarList	struct ITaskbarList {	MS SDK (Windows XP)
ITaskbarList2	struct ITaskbarList2Vtbl *lpVtbl;	MS SDK (Windows XP)
ITaskbarList2Vtbl	};	MS SDK (Windows XP)
ITaskbarList3	struct ITaskbarList3 {	MS SDK (Windows XP)
ITaskbarList3Vtbl	struct ITaskbarList3Vtbl *lpVtbl;	MS SDK (Windows XP)
ITaskbarList4	};	MS SDK (Windows XP)
ITaskbarList5Vtbl	struct ITaskbarList5Vtbl {	MS SDK (Windows XP)
ITemplatePrinter	struct ITemplatePrinterVtbl *lpVtbl;	MS SDK (Windows XP)
ITemplatePrinter2	};	MS SDK (Windows XP)
ITemplatePrinter2Vtbl	struct ITemplatePrinter2Vtbl {	MS SDK (Windows XP)
ITemplatePrinter3	struct ITemplatePrinter3Vtbl *lpVtbl;	MS SDK (Windows XP)
ITemplatePrinter3Vtbl	};	MS SDK (Windows XP)

©2020 FireEye

10

FireEye | 11

COM is a Game of Types

```

    mov    eax, [ebp+ppv]
    push   edi
    push   offset unk_685050
    push   eax
    mov    ecx, [eax]
    calll dword ptr [ecx]
    mov    esi, eax

    loc_415961:
    mov    eax, [ebp+ppv]
    push   eax
    mov    ecx, [eax]
    calll dword ptr [ecx+8]
    test  esi, esi
    jns   short loc_415974
  
```

```

    mov    eax, [ebp+ppv]
    push   edi ; ppvObject
    push   offset stru_685050 ; riid
    push   eax ; This
    mov    ecx, [eax]
    calll [ecx+IUnknownVtbl.QueryInterface]
    mov    esi, eax

    loc_415961:
    mov    eax, [ebp+ppv]
    push   eax ; This
    mov    ecx, [eax]
    calll [ecx+IUnknownVtbl.Release]
    test  esi, esi
    jns   short loc_415974
  
```

©2020 FireEye

11

FireEye | 12

CoCreateInstance Xref 1/2 – Vanilla

```

Pseudocode-A
1 bool __thiscall sub_404540(void *this)
2 {
3     void *v1; // esi
4     LPVOID ppv; // [esp+4h] [ebp-4h]
5
6     v1 = this;
7     ppv = 0;
8     return CoInitialize(0) < 0
9     || CoCreateInstance(&rclsid, 0, 1u, &riid, &ppv)
10    || (*int(_stdcall **)(LPVOID)(*_DWORD *)ppv + 0xC))(ppv) < 0
11    || (*int(_stdcall **)(LPVOID, void **)(*_DWORD *)ppv + 0x14))(ppv, v1) >= 0;
12 }
  
```

```

IDA View-A
.rdata:00491650 ; IID riid           dd 56FDF342h ; Data1
.rdata:00491650 .rdata:00491650          dw 0FD6Dh ; DATA XREF: sub_404540
.rdata:00491650 .rdata:00491650          dw 110h ; Data2
.rdata:00491650 .rdata:00491650          db 95h, 8Ah, 0, 60h, 97h, 0C9h, 0A0h, 90h; Data3
.rdata:00491660 ; IID rclsid          dd 56FDF344h ; Data1
.rdata:00491660 .rdata:00491660          dw 0FD6Dh ; DATA XREF: sub_404540
.rdata:00491660 .rdata:00491660          dw 110h ; Data2
.rdata:00491660 .rdata:00491660          db 95h, 8Ah, 0, 60h, 97h, 0C9h, 0A0h, 90h; Data3
.rdata:00491670 unk_491670          db 0Ch ; DATA XREF: sub_442190+8C7f0
.rdata:00491670 .rdata:00491670          ; sub_442190+8C7f0
  
```

©2020 FireEye

12

FireEye | 13

SDK Headers

Before I knew about a much slicker trick

```
C:\Program Files (x86)\Windows Kits\10\Include\10.0.17763.0\um>findstr /I 56fdf344-fd6d-11d0-958a-006097c9a090
C:\Program Files (x86)\Windows Kits\10\Include\10.0.17763.0\um>gvim ShObjIdl_core.h
C:\Program Files (x86)\Windows Kits\10\Include\10.0.17763.0\um>gvim ShObjIdl_core.h
```

©2020 FireEye

13

FireEye | 14

Searching COM Registrations

- Registry = **Authoritative, offline** CLSID/ProgID lookup
- Under HKCR*
 - HKCR\ ← All registered **ProgIDs**
 - HKCR\CLSID\ ← All registered **CLSIDs**
- To find a DLL given a ProgID:
 - HKCR\<YourProgID>\CLSID (Default) → GUID
 - HKCR\CLSID\{that-GUID}\
 - InprocServer32 or LocalServer32 (Default) → DLL/EXE

*HKCR is really a virtual hive composed from superimposing HKCU\Classes over HKLM\Classes

©2020 FireEye

14

FireEye | 15

This One Weird Trick

 **ostracon**
@Ostracon

Replies to @mykill

And if you set the type of the IID value to CLSID, Ida will fill in the interface/class name if it knows it, can save some redirects through the registry/comview :)

```
.rdata:200E0320 ; CLSID CLSID_IShellLinkA
.rdata:200E0320 CLSID_IShellLinkA dd 214Eh ; Data1
.rdata:200E0320 ; DATA XREF: sub_200E8FDB+2B:0
.rdata:200E0320 du 0 ; Data2
.rdata:200E0320 du 0 ; Data3
.rdata:200E0320 db 0C0h, 6 dup(0), A6h ; Data4
```

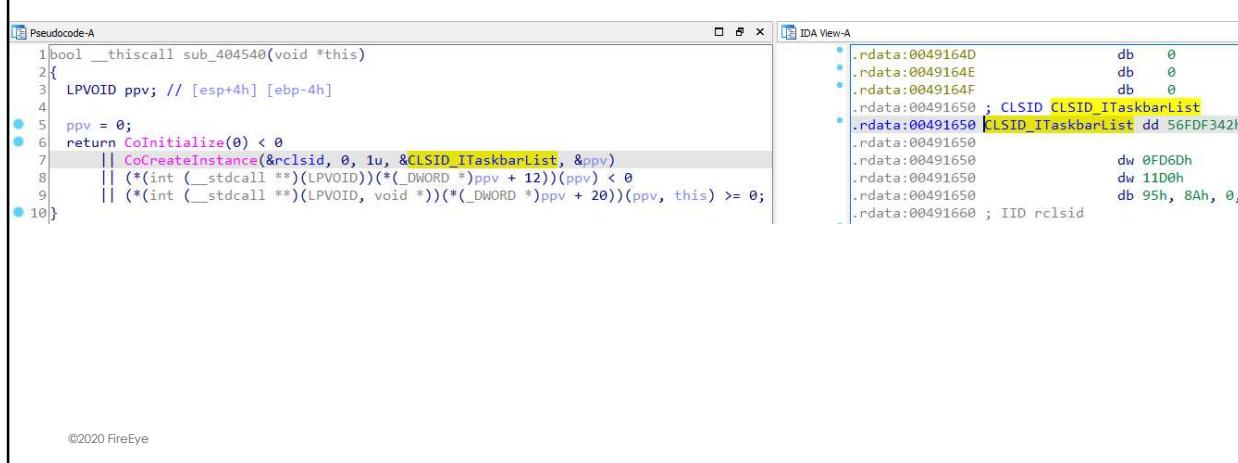
6:15 PM · Sep 11, 2018 · Twitter Web Client

©2020 FireEye

15

FireEye | 16

Can't Argue with Success



Pseudocode-A

```
1 bool __thiscall sub_404540(void *this)
2 {
3     LPVOID ppv; // [esp+4h] [ebp-4h]
4
5     ppv = 0;
6     return CoInitialize(0) < 0
7     || CoCreateInstance(&rclsid, 0, 1u, &CLSID_ITaskbarList, &ppv)
8     || (*(_stdcall **)(LPVOID)((*_DWORD *)ppv + 12))(ppv) < 0
9     || (*(_stdcall **)(LPVOID, void *))(*(_DWORD *)ppv + 20))(ppv, this) >= 0;
10 }
```

IDA View-A

.rdata:0049164D	db 0
.rdata:0049164E	db 0
.rdata:0049164F	db 0
.rdata:00491650 ; CLSID CLSID_ITaskbarList	
*.rdata:00491650 CLSID_ITaskbarList dd 56FDF342h	
.rdata:00491650	dw 0FD6Dh
.rdata:00491650	dw 11D0h
.rdata:00491650	db 95h, 8Ah, 0,
.rdata:00491660 ; IID rclsid	

©2020 FireEye

16

Finally: Interface Pointer Illumination

```

bool __thiscall sub_404540(void *this)
{
    LPVOID ppv; // [esp+4h] [ebp-4h]

    ppv = 0;
    return CoInitialize(0) < 0
        || CoCreateInstance(&clsid, 0, 1u, &iid, &ppv)
        || (*(int (__stdcall **)(LPVOID))(*(_DWORD *)pv))
        || (*(int (__stdcall **)(LPVOID, void *))(*(_D
}

```

The screenshot shows a debugger interface with assembly code. A context menu is open over a variable declaration, specifically the line `|| CoCreateInstance(&clsid, 0, 1u, &iid, &ppv)`. The menu item `Set Ivar type...` is highlighted with a blue selection bar.

©2020 FireEye

17

Finally: Interface Pointer Illumination

```

bool __thiscall taskbar_deletetab(HWND hwnd)
{
    HWND v1; // esi
    ITaskbarList *ppv; // [esp+4h] [ebp-4h]

    v1 = hwnd;
    ppv = 0;
    return CoInitialize(0) < 0
        || CoCreateInstance(&clsid_00491660_TaskbarList, 0, 1u, &iid_00491650_ITaskbarList, (LPVOID *)&ppv)
        || ppv->lpVtbl->HrInit(ppv) < 0
        || ppv->lpVtbl->DeleteTab(ppv, v1) >= 0;
}

```

A type declaration dialog box is displayed, prompting the user to "Please enter a string" and "Please enter the type declaration". The input field contains `ITaskbarList *ppv`.

©2020 FireEye

18

FireEye | 19

CoCreateInstance Xref 2/2 – Peculiar

- IID → CLSID trick is not even applicable!

Pseudocode-A

```

1 HRESULT __thiscall sub_415910(_DWORD *this, int a2, int a3, int a4)
2{
3     _DWORD *v4; // edi
4     HRESULT v5; // esi
5     LPVOID ppv; // [esp+8h] [ebp-4h]
6
7     v4 = this;
8     if ( *this )
9         (*(void (__stdcall **)(DWORD))(*(_DWORD *)*this + 8))(*this);
10    v5 = CoCreateInstance(&stru_685070, 0, 0x17u, &IID_IUnknown, &ppv);
11    if ( v5 < 0 )
12        goto LABEL_11;
13    v5 = OleRun((LPUNKNOWN)ppv);
14    if ( v5 >= 0 )
15        v5 = (**(int (__stdcall ***)(LPVOID, void *, _DWORD **))ppv)(ppv, &unk_685050, v4);
16    (*(void (__stdcall ***)(LPVOID))(*(_DWORD *)ppv + 8))(ppv);
17    if ( v5 < 0 )
18        LABEL_11:
19        *v4 = 0;
20    return v5;
21}

```

©2020 FireEye

IDA View-A

.rdata:0068505B	db 0
.rdata:0068505C	db 0
.rdata:0068505D	db 0
.rdata:0068505E	db 0
.rdata:0068505F	db 46h ; F
.rdata:00685060 ; IID_IUnknown	dd 0
.rdata:00685060 IID_IUnknown	dd 0
.rdata:00685060	dw 0
.rdata:00685060	dw 0
.rdata:00685060	db 0C0h, 6 dup(0), 46h
.rdata:00685070 ; CLSID stru_685070	dd 6F03Ah
.rdata:00685070 stru_685070	dd 6F03Ah
.rdata:00685070	dw 0
.rdata:00685070	dw 0
.rdata:00685070	db 0C0h, 6 dup(0), 46h
.rdata:00685080 aBadCast	db 'bad cast',0
.rdata:00685080	align 4
.rdata:00685089	db ': ',0
.rdata:0068508C asc_68508C	

19

FireEye | 20

GUID Easy Mode

.rdata:00685070 stru_685070	dd 6F03Ah	; Data1
.rdata:00685070	dw 0	; DATA XREF: s
.rdata:00685070	dw 0	; Data2
.rdata:00685070	dw 0	; Data3
.rdata:00685070	db 0C0h, 6 dup(0), 46h	; Data4
.rdata:006850 Output window		
.rdata:006850		
.rdata:006850 Python>uuid.UUID(bytes_le=idc.GetManyBytes(idc.here(), 16))		s
.rdata:006850 0006f03a-0000-0000-000000000046		s
.rdata:006850 Python		
.rdata:00685090 aIostream	db 'iostream',0	; DATA XREF: s

©2020 FireEye

20

FireEye | 21

CLSID Lookup

- Under HKCR\CLSID

©2020 FireEye

21

FireEye | 22

Hunting TypeLibs

- `oleview.exe` : File->View TypeLib:
 - The COM EXE or DLL itself
 - *.tlb, *.olb, even *.dll
- Found via MSDN: `msoutl.olb`
- Had to hand-create vtbl
- **BUT REMEMBER!**
- Dispinterfaces inherit from `IDispatch`
- Meaning?

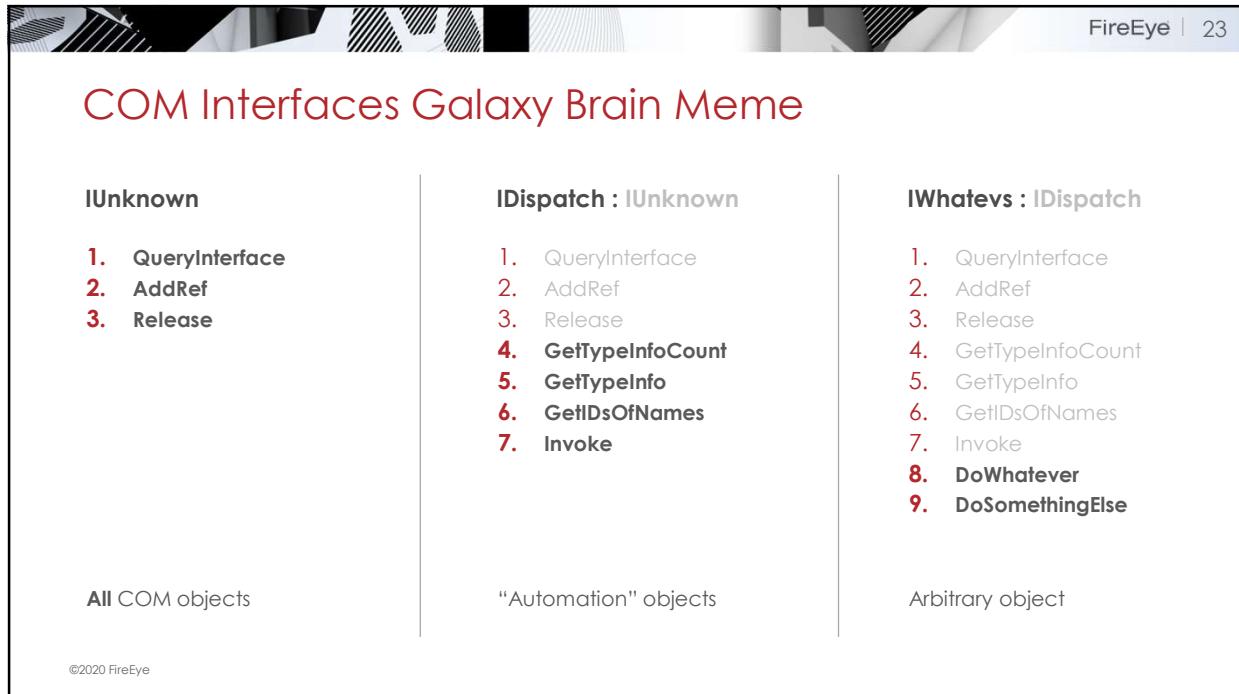
```

ITypeLib Viewer
File View
File [ ] ? 
[ 
    uuid(00063001-0000-0000-C000-000000000046),
    helpcontext(0x000002c0),
    dual
]
dispinterface _Application {
    properties:
        methods:
            [id(0x0000f000), propget, helpcontext(0x000002c1)]
                _Application Application();
            [id(0x0000f00a), propget, helpcontext(0x000002c2)]
                _ObjectClass Class();
            [id(0x0000f00b), propget, helpcontext(0x000002c3)]
                _NameSpace* Session();
            [id(0x0000f001), propget, helpcontext(0x000002c4)]
                IDispatch* Parent();
            [id(0x00000114), propget, hidden, helpcontext(0x000002c5)]
                _Assistant* Assistant();
            [id(0x00003001), propget, helpcontext(0x000002c6)]
                BSTR Name();
            [id(0x00000116), propget, helpcontext(0x000002c7)]
                BSTR Version();
            [id(0x00000111), helpcontext(0x000002c8)]
                _Explorer* ActiveExplorer();
            [id(0x00000112), helpcontext(0x000002c9)]
                _Inspector* ActiveInspector();
            [id(0x0000010a), helpcontext(0x000002ca)]
        ]
}
Ready

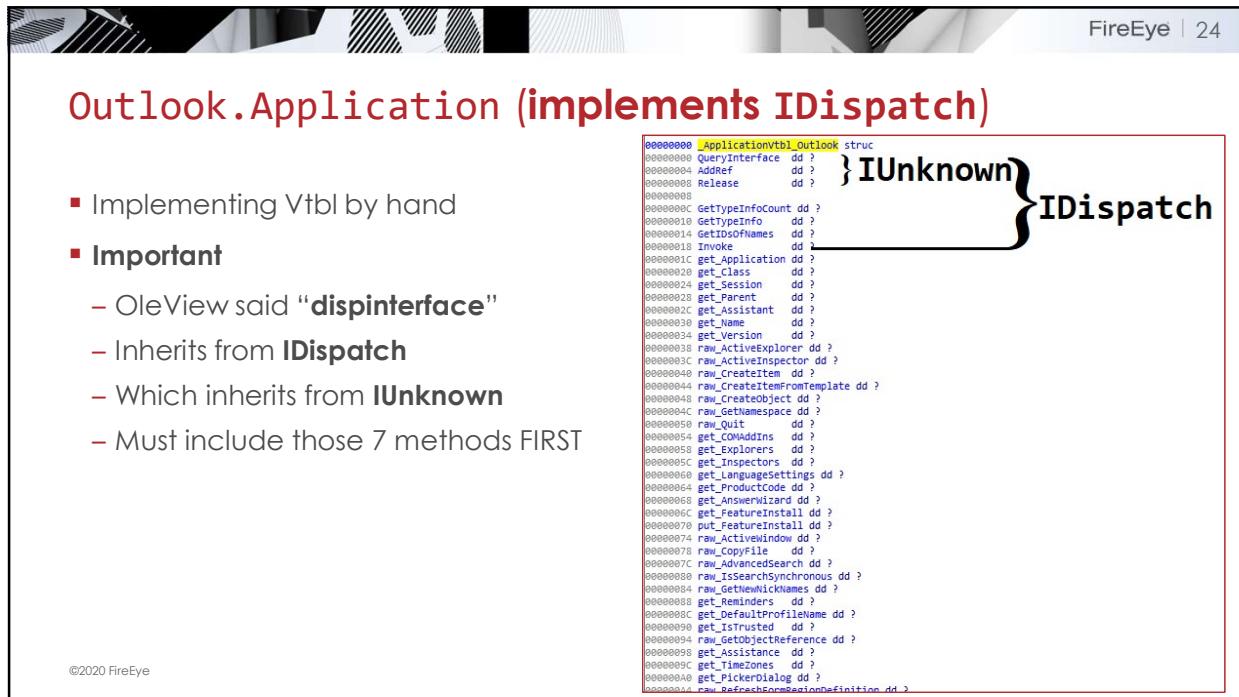
```

©2020 FireEye

22



23



24

So, What was it Doing?

```

int __thiscall get_Outlook_Application(_Application_Outlook **ppvObject, int a2, int a3, int a4)
{
    void **ppvObject_alias; // edi
    int v5; // esi
    _Application_Outlook *ppv; // [esp+8h] [ebp-4h]

    ppvObject_alias = (void **)ppvObject;
    if ( *ppvObject )
        ((void (__stdcall *)(_Application_Outlook *))(*ppvObject)->lpVtbl->Release)(*ppvObject);
    v5 = CoCreateInstance(&CLSID_Outlook_dot_Application, 0, 0x17u, &iid_00685060_IUnknown, (LPVOID *)&ppv);
    if ( v5 < 0 )
        goto LABEL_11;
    v5 = OleRun((LPUNKNOWN)ppv);
    if ( v5 >= 0 )
        v5 = ((HRESULT __stdcall *)(IUnknown *, const IID *const , void **))ppv->lpVtbl->QueryInterface)(
            (IUnknown *)ppv,
            &IID_Application,
            ppvObject_alias);
    ((void (__stdcall *)(IUnknown *))ppv->lpVtbl->Release)((IUnknown *)ppv);
    if ( v5 < 0 )
        LABEL_11:
        *ppvObject_alias = 0;
    return v5;
}
©2020 FireEye

```

25

And thennnnn?

- Getting MS Outlook version

```

CoInitializeEx(0, 2u);
ppv_Outlook_Application = 0;
v19 = 0;
if ( get_Outlook_Application((void **)&ppv_Outlook_Application, v12, v3, v4) < 0 )
    goto LABEL_26;
outlook_version = 0;
if ( !ppv_Outlook_Application )
    w_guard_check_bail(0x80004003);
((void (__stdcall *)(struct _Application_Outlook *, int *))ppv_Outlook_Application->lpVtbl->get_Version)(
    ppv_Outlook_Application,
    &outlook_version);

```

26

FireEye | 27

And thennnnn?

- Quitting Outlook

```
if ( !ppv_Outlook_Application )
    w_guard_check_bail(0x80004003);
((void (__stdcall *)(struct _Application_Outlook *))ppv_Outlook_Application->Vtbl->raw_Quit)(ppv_Outlook_Application);
v40 = 7;
v39 = 0;
```

©2020 FireEye

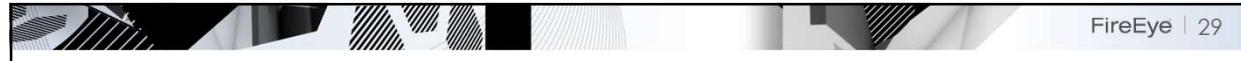
27

FireEye | 28

MAPI

Messaging API
aka
COM jungle of perpetual MSDN searches

28



Three Facts about Messaging API (MAPI)
(#3 may surprise you)

1. MAPI is based on COM

©2020 FireEye

29



Three Facts about Messaging API (MAPI)
(#3 may surprise you)

1. MAPI is based on COM
2. MAPI clients must match the processor architecture of the installed MAPI app

©2020 FireEye

30

FireEye | 31

Three Facts about Messaging API (MAPI)

(#3 may surprise you)

1. MAPI is based on COM
2. MAPI clients must match the processor architecture of the installed MAPI app
3. MAPI is supported by Thunderbird

©2020 FireEye

31

FireEye | 32

Meet MAPI

```

loc_41301F:
lea    eax, [ebp+MapiInit]
mov    [ebp+MapiInit], 0
push   eax           ; lpMapiInit
mov    [ebp+var_9C], 0
call   ds:MAPIInitialize
lea    eax, [ebp+pSession]
mov    [ebp+pSession], 0
push   eax           ; lppSession
push   62h ; 'b'      ; ulFlags
push   0              ; lpszPassword
push   0              ; lpszProfileName
push   0              ; ulUIParam
call   ds:MAPILogonEx
mov    eax, [ebp+pSession]
test   eax, eax
jnz    short loc_413079

loc_414D1B:
push   0
mov    [ebp+var_24], 3
lea    edx, [ebp+var_24]
mov    [ebp+var_20], 3001001Fh
mov    [ebp+var_1C], 0FFF0102h
mov    [ebp+var_18], 3400000Bh
mov    eax, [ecx]
push   edx
push   ecx
call   dword ptr [eax+1Ch]
test   eax, eax
mov    eax, [ebp+var_4C]
jnz    loc_414F19

```

©2020 FireEye

32

Handling MAPI

- Cascading type deps force top-down analysis
- Very documentation-driven
- Hex-Rays helps manage type propagation
 - Otherwise, more work applying XxxVtbl type to calls – see illustration →

©2020 FireEye

```

push    eax
lea     eax, [ebp+var_C]
mov    large fs:0, eax
mov    [ebp+var_10], esp
mov    esi, [ebp+arg_0]
mov    ebx, [ebp+lpMapiSession.lpVtbl]
mov    [ebp+var_50], esi
mov    [ebp+var_64], 0
mov    [ebp+var_5C], 0
mov    [ebp+var_58], 0
mov    [ebp+var_54], 0
; try {
mov    [ebp+var_4], 0
test   ebx, ebx
jnz    short loc_414CE7

```

loc_414CE7:

```

mov    eax, [ebx]
lea     ecx, [ebp+var_4C]
push   ecx
push   0
push   ebx
mov    [ebp+var_4C], 0
call   dword ptr [eax+10h]
test   eax, eax
jnz    short loc_414CCE

```

33

Algorithm for MAPI

- For each MAPI function call, may need to:
 - Check MSDN* for output value's COM type
 - Add that struct type to structures tab
 - Apply struct type to relevant variables
 - Check MSDN* to apply symbolic names for constants/enums
- Lather, rinse, repeat

©2020 FireEye

34

FireEye | 35

Lather, Rinse, Repeat

Graph overview

©2020 FireEye

35

FireEye | 36

Example

```

if ( !lpMapiSession
    || (v4 = *lpMapiSession, v20 = 0, (*(int (__stdcall **)(int *, _DWORD, int *))(v4 + 0x10))(lpMapiSession, 0, &v20) )
{
    *a1 = 0;
    a1[1] = 0;
    a1[2] = 0;
}
else
{
    v5 = v20;
    if ( v20 )
    {
        v27 = 3;
        v28 = 0x3001001F;
        v29 = 0xFFFF0102;
        v30 = 0x3400000B;
        v6 = (*(int (__stdcall **)(int, int *, _DWORD))(*(_DWORD *)v20 + 0x1C))(v20, &v27, 0) == 0;
    }
}

```

Please enter a string

Please enter the type declaration IMAPISESSION*lpMapiSession

OK Cancel

©2020 FireEye

36

FireEye | 37

Example

```

if ( !lpMapiSession
    || (v4 = lpMapiSession->lpVtbl, v20 = 0, v4->GetMsgStoresTable(lpMapiSession, 0, (LPMAPITABLE *)&v20) )
{
    *a1 = 0;
    a1[1] = 0;
    a1[2] = 0;
}
else
{
    v5 = v20;
    if ( v20 )
    {
        v27 = 3;
        v28 = 0x3001001F;
        v29 = 0xFFFF0102;
        v30 = 0x34000008;
        v6 = (*int (__stdcall **)(int, int *, ULONG))(*(_DWORD *)v20 + 0x1C))(v20, &v27, 0) == 0;
    }
}

```

©2020 FireEye

37

FireEye | 38

Beware When Using IMAPI_{XX} Interface Names...

- From MAPIDefs.h
- If you try IMAPITABLE*...
 - Hex-Rays says **Bad Declaration**
 - You **throw furniture**
 - All because capital letters

DECLARE_MAPI_INTERFACE_PTR(IMsgStore,	LPMDB);
DECLARE_MAPI_INTERFACE_PTR(IMAPIFolder,	LPMAPIFOLDER);
DECLARE_MAPI_INTERFACE_PTR(IMessage,	LPMESSAGE);
DECLARE_MAPI_INTERFACE_PTR(IAttach,	LPATTACH);
DECLARE_MAPI_INTERFACE_PTR(IAddrBook,	LPADDRBOOK);
DECLARE_MAPI_INTERFACE_PTR(IABContainer,	LPABCONT);
DECLARE_MAPI_INTERFACE_PTR(IMailUser,	LPMAILUSER);
DECLARE_MAPI_INTERFACE_PTR(IDistList,	LPDISTLIST);
DECLARE_MAPI_INTERFACE_PTR(IMAPIStatus,	LPMAPISTATUS);
DECLARE_MAPI_INTERFACE_PTR(IMAPITable,	LPMAPITABLE);
DECLARE_MAPI_INTERFACE_PTR(IProfSect,	LPPROFSECT);
DECLARE_MAPI_INTERFACE_PTR(IMAPIProp,	LPMAPIPROP);
DECLARE_MAPI_INTERFACE_PTR(IMAPIContainer,	LPMAPICONAINER);
DECLARE_MAPI_INTERFACE_PTR(IMAPIAdviseSink,	LPMAPIADVISESINK);
DECLARE_MAPI_INTERFACE_PTR(IMAPIProgress,	LPMAPIPROGRESS);
DECLARE_MAPI_INTERFACE_PTR(IProviderAdmin,	LPPROVIDERADMIN);

©2020 FireEye

38

Meanwhile, at MSDN... Same Pitfall

IMAPI Session::GetMsgStoresTable

03/08/2015 • 2 minutes to read •

Applies to: Outlook 2013 | Outlook 2016

Provides access to the message store table that contains information about all the message stores in the session profile.

```
C++  
HRESULT GetMsgStoresTable(  
    ULONG ulFlags,  
    LPMAPITABLE FAR * lppTable  
>;
```

Copy

©2020 FireEye

39

Not Helpful

lppTable

[out] A pointer to a pointer to the message store table.

©2020 FireEye

40

FireEye | 41

Gophe MAPI Usage

- Hundreds of calls
- Three of the four binaries use it
- Often in conjunction with STL
 - Strings
 - Vectors
 - Maps
 - Sets
 - Vectors of Maps (yes, really)

©2020 FireEye

41

FireEye | 42

STL

Reversing Standard Template Library Code

42

FireEye | 43

Template Caveats

- Very slippery
 - Inheritance
 - Allocators
 - Template type (e.g. <class _Ty> varies generated code/structs)
 - Mem layout fluctuation due to
 - Debug on/off
 - Security features
 - VC version
 - Inlining
 - Optimization
- Difficult to say anything absolute
 - Extra >> 2 (division by sizeof(x)=4)
 - Random constants like 0x3fffffff
 - Missing/added struct members
 - Etc.

©2020 FireEye

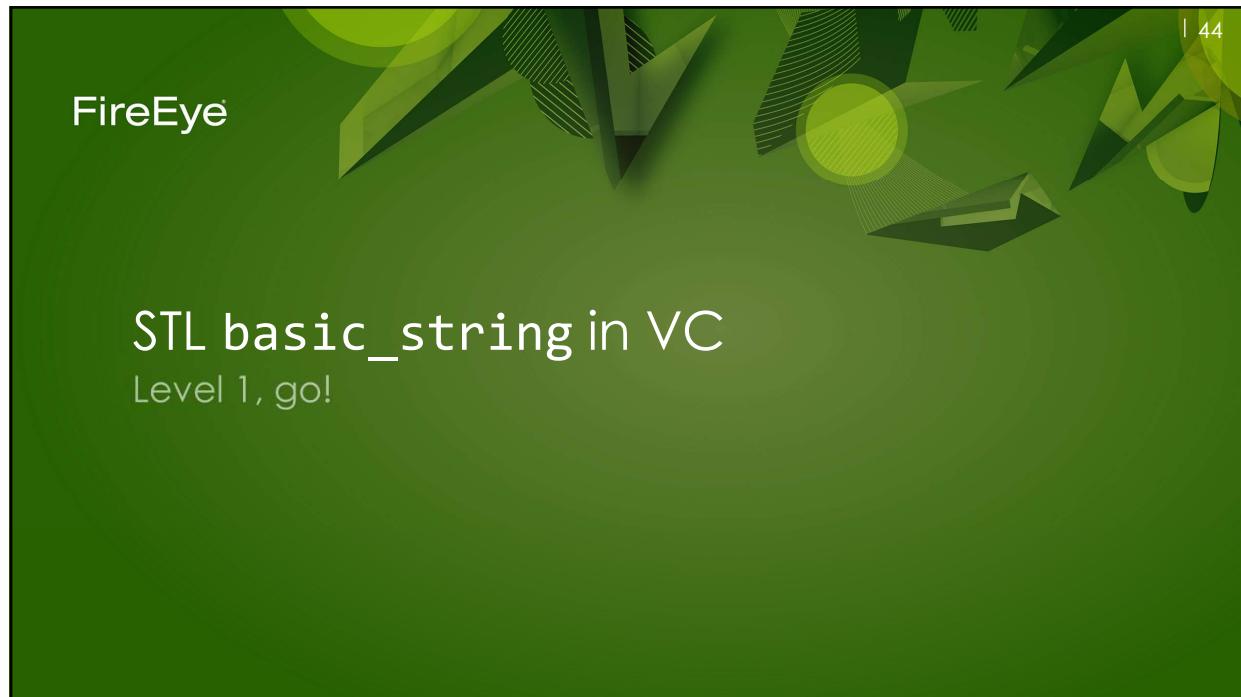


43

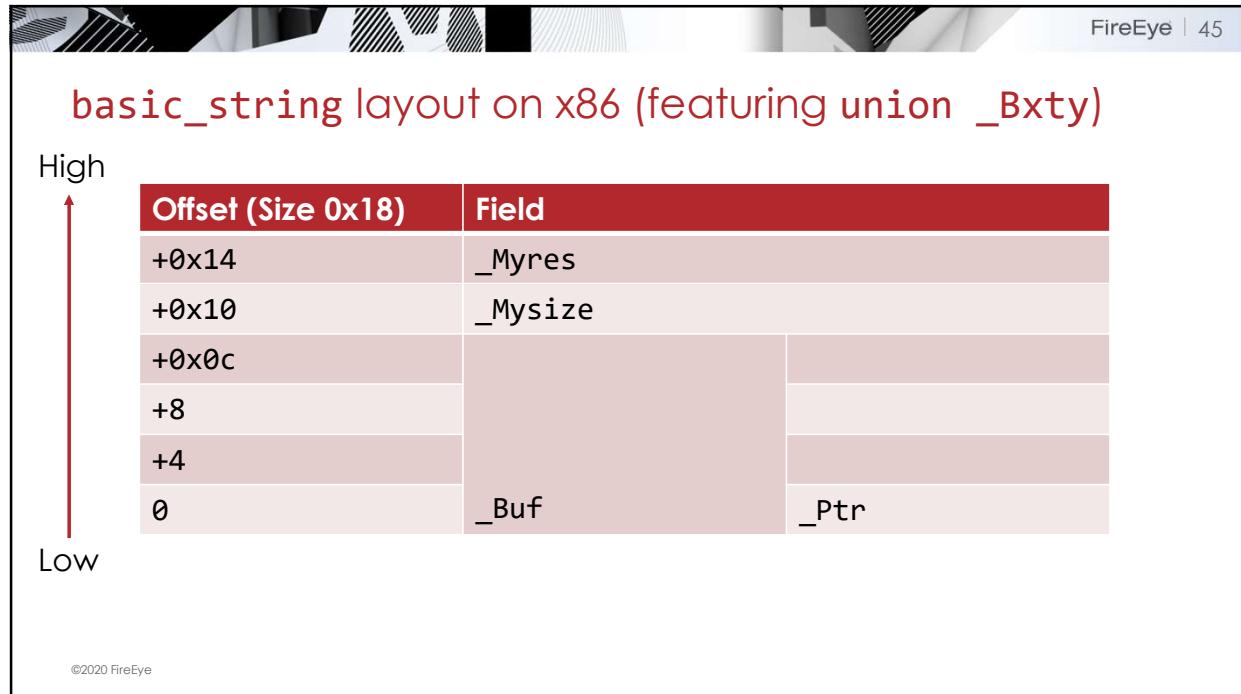
FireEye | 44

STL basic_string in VC

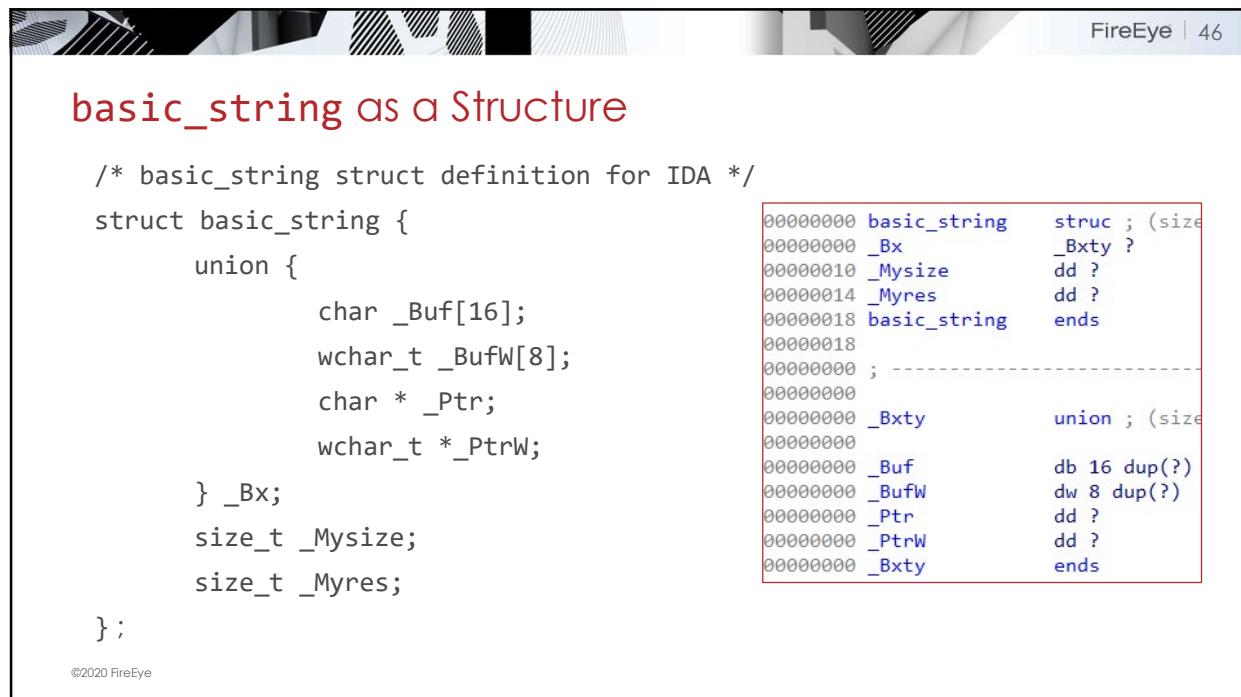
Level 1, go!



44



45



46

FireEye | 47

basic_string recognition

- Evaluates size versus embedded buffer
 - Accounts for terminating null
 - Returns pointer if greater
 - Size used indicates ASCII vs Wide
- ASCII vs. Wide strings:
 - 0x10: ASCII
 - 8: Unicode →

```

0041F77A
0041F77A loc_41F77A:
0041F77A xor    ecx, ecx
0041F77C mov    [eax], cx
0041F77F cmp    [ebx+xstring._Myres], B
0041F783 mov    [ebx+xstring._Mysize], ecx
0041F786 jb    short loc_41F78C

0041F788
0041F788 mov    eax, [ebx+xstring._Bx._Ptr]
0041F78A jmp    short loc_41F78E

0041F78C
0041F78C loc_41F78C:
0041F78C mov    eax, ebx

0041F78E
0041F78E loc_41F78E:
0041F78E push   [ebp+var_1CD0]
0041F794 xor    ecx, ecx
0041F798 xor    eax, eax
  
```

©2020 FireEye

47

FireEye | 48

STL vector in VC

Simple as 1 2 3

48

vector recognition – Before/After

49

vector recognition – Adjacent Member Initialization

```
v31 = 8v13;
v19 = a1;
v18 = a0;
v16 = 0;
v17 = 0;
v18 = 0;
v32 = 0;
if ( v22 ) { v4 = *a2, v20 = 0, ((int (_stdcall **)(int *, _DWORD, int ))(v4 + 0x10))(a2,
{ *a1 = 0;
a1[1] = 0;
a1[2] = 0;
}
else
{
v5 = v20;
if ( v20 )
{
    v27 = 3;
    v28 = 0x3001001F;
    v29 = 0xFFFF0102;
    v30 = 0x34000008;
    v6 = ((int (_stdcall **)(int, int *, _DWORD))(((_DWORD *)v20 + 0x1C))(v20, 0x27, 0) ==
    v7 = v20;
    if ( v6 )
    {
        v15 = 0;
        (*void (_stdcall **)(int, _DWORD, unsigned int ))(((_DWORD *)v20 + 0x24))(v20, 0, &v15)
        if ( v15 )
        {
            LOBYTE(v32) = 1;
            if ( v15 > 0x7FFFFFFF )
                sub_4E418("vector<T> too long");
            sub_4FB87(&v16, v15);
            v32 = 0;
            lpRows = 0;
            while ( !((int (_stdcall **)(int, signed int, _DWORD, LPSRowSet ))(((_DWORD *)v20
                v20,
                1,
                0,
                0,
```

50

vector recognition – Indirect Member Initialization

```
u31 = 0x13;
u19 = al;
u14 = 0;
u16 = 0;
u17 = 0;
u18 = 0;
u32 = 0;
if ( t@2 || (u4 = *a2, u20 = 0, (*(_stdcall **)(int *, _DWORD, int *))(u4 + 0x10))(a2,
{
    *a1 = 0;
    a1[1] = 0;
    a1[2] = 0;
}
else
{
    u5 = u20;
    if ( u20 )
    {
        u27 = 3;
        u28 = 0x3001001F;
        u29 = 0xFFB102;
        u30 = 0x3A000008;
        u6 = (*(_stdcall **)(int, int *, _DWORD))(*(_DWORD *)u20 + 0x1C)(u20, u27, 0) ==
        u7 = 02;
        if ( u6 )
        {
            u15 = 0;
            (*void (_stdcall **)(int, _DWORD, unsigned int ))(*(_DWORD *)u20 + 0x24))(u20, 0, u6);
            if ( u15 )
            {
                LOBYTE(u32) = 1;
                if ( u15 > 0xFFFFFFF )
                    sub_44E14("vector<T> too long");
                sub_415B70(u616, u15);
                u32 = 0;
                lpRows = 0;
                while ( (*(_stdcall **)(int, signed int, _DWORD, LPSRowSet ))(*(_DWORD *)u20
                    u20,
                    1,
                    0,
                    0,
```

51

vector – Three Members



```
/* vector struct definition for IDA */
struct vector {
    void *_Myfirst;           // pointer to beginning of array
    void *_Mylast;            // pointer to current end of sequence
    void *_Myend;              // pointer to end of array
};
```

```
00000000 vector      struc ; (sizeof=0xC, mappedto_1807)
00000000 _Myfirst   dd ?
00000004 _Mylast    dd ?
00000008 _Myend     dd ?
0000000C vector      ends
```

52

FireEye | 53

Hints of Vector Usage

- Adjacent variables subtracted from each other
 - Size: `_Mylast - _Myfirst`
 - Unused Capacity: `_MyEnd - _Mylast`
- Comparison of pointer difference with potential `sizeof(value_type)`

```
v5 = v90;
v6 = v91 - (_DWORD)v90;
if ( (unsigned int)(v91 - (_DWORD)v90) >= 0x20 )
{
    lpMem = 0;
    v114 = 0;
```

©2020 FireEye

53

FireEye | 54

More Hints of Vector Usage

- Address of variable passed to function containing:
 - "vector<T> too long" 😊
 - Subtraction among `*var`, `var[1]`, and/or `var[2]`
 - Division or Shift operations to scale pointer differences by value type size
 - Large constants that divide (almost) evenly into `0xffffffff`

```
v2 = this;
v3 = this[1];
v4 = a2;
if ( a2 >= v3 || (v5 = *this, *this > a2) )
{
    v15 = this[2];
    if ( v3 == v15 && (unsigned int)((int)(v15 - v3) >> 5) < 1 )
    {
        v16 = (int)(v3 - *this) >> 5;
        if ( (unsigned int)(0x7FFFFFFF - v16)
            sub_44E418("vector<T> too long");
        v17 = v16 + 1;
        v18 = (int)(v15 - *this) >> 5;
```

Output window

Python>0xffffffff/0xffffffff
0x20
0x20

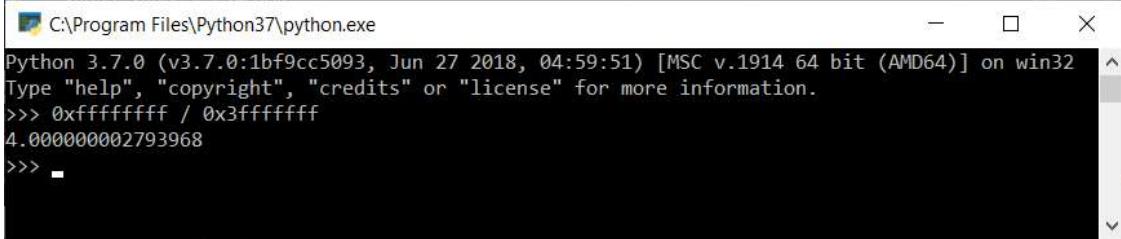
©2020 FireEye

54

FireEye | 55

Inferring vector Value Type Size – `max_size()` method

- `allocator<blah>::max_size() { return 0x3FFFFFFF; }`
- This is $0xffffffff / \text{sizeof}(_Ty)$
- In this case, 4



```
C:\Program Files\Python37\python.exe
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:59:51) [MSC v.1914 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> 0xffffffff / 0x3fffffff
4.00000002793968
>>> -
```

©2020 FireEye

55

FireEye | 56

Inferring vector Value Type Size

- Problem: how big is struct?

```
if ( v18 )
{
    struct_instack_unknown_size = v18;
    v22 = 0;
    v9 = lpRows->aRow[0].lpProps;
    if ( LOWORD(v9[2].ulPropTag) == 11 )
        v22 = v9[2].Value.i != 0;
    v10 = lpRows->aRow[0].lpProps;
    if ( LOWORD(v10->ulPropTag) == 31 )
        sub_40D9F0(v10->Value.lpszA);
    vect_func(&vec_unknown_elmt_size, (unsigned int)&struct_instack_unknown_size);
}
FreeProws(lpRows);
LOBYTE(v31) = 0;
lpRows = 0;
if ( v25 >= 8 )
    sub_40F3C0(lpMem, v25 + 1);
```

©2020 FireEye

56

FireEye | 57

Inferring vector Value Type Size

- Solution: 32 bytes

```

void __thiscall vect_func(vector *this, unsigned int struct_instack_unknown_size)
{
    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL- "+" TO EXPAND]

    v2 = this;
    _Mylast = this->_Mylast;
    struct_alias = struct_instack_unknown_size;
    if ( struct_instack_unknown_size >= _Mylast || (v5 = this->_Myfirst, this->_Myfirst > struct_instack_unknown_size) )
    {
        _Myend = this->_Myend;
        if ( _Mylast == _Myend && (unsigned int)((int)(-_Myend - _Mylast) >> 5) < 1 )
        {
            elements = (int)(-_Mylast - this->_Myfirst) >> 5;
            if ( (unsigned int)(0x7FFFFFFF - elements) < 1 )
                sub_44E418("vector<T> too long");
        }
    }
}

```

©2020 FireEye

57

FireEye | 58

Inferring vector Value Type Size

- Use inferred value type size info in the calling function to

The screenshot shows a debugger interface with two windows. On the left, a memory dump window displays assembly code and memory addresses. A specific memory location at address 0x00000044 is highlighted in yellow. On the right, a 'Structures' window shows a list of fields for a structure named 'st_20h'. The structure definition is as follows:

```

struc ; (sizeof=0x20, r^
field_0 dd ?
field_4 dd ?
field_8 dd ?
field_C dd ?
field_10 dd ?
field_14 dd ?
field_18 dd ?
field_1C dd ?
st_20h ends

```

Below the structures list, there is a text input field containing the value '3. st_20h:000C'.

©2020 FireEye

58

Inferring vector Value Type Size

- Xrefs crawling out of the woodwork:

```

if ( v16 )
{
    struct_instack_unknown_size.field_0 = (int)v16;
    LOBYTE(struct_instack_unknown_size.field_4) = 0;
    v9 = lpRows->aRow[0].lpProps;
    if ( LOWORD(v9[2].ulPropTag) == 11 )
        LOBYTE(struct_instack_unknown_size.field_4) = v9[2].Value.i != 0;
    v10 = lpRows->aRow[0].lpProps;
    if ( LOWORD(v10->ulPropTag) == 31 )
        sub_40D9F0(v10->Value.lpszA);
    vect_func(&vec_unknown_elmt_size, (unsigned int)&struct_instack_unknown_size);
}
FreeProws(lpRows);
LOBYTE(v25) = 0;
lpRows = 0;
if ( struct_instack_unknown_size.field_1C >= 8u )
    sub_40F3C0((LPVOID)struct_instack_unknown_size.field_8, struct_instack_unknown_size.field_1C + 1);

```

©2020 FireEye

59

Inferring vector Value Type Size (another example)

```

unsigned int __thiscall vect18h_func0(vector *this, int a2)
{
    vector *v2; // ebx
    int myend; // ecx
    int mylast; // esi
    unsigned int result; // eax
    int v6; // edi
    unsigned int v7; // edx
    unsigned int v8; // ecx
    unsigned int v9; // edi
    unsigned int v10; // esi

    v2 = this;
    myend = this->_Myend;
    mylast = v2->_Mylast;
    result = (myend - mylast) / 0x18;
}

```

©2020 FireEye

60

FireEye | 61

Inferring vector Value Type Size (another example)

```

1 unsigned int __thiscall vect44h_func(vector *this, int a2)
2{
3    vector *this_alias; // ebx
4    int myend; // ecx
5    int mylast; // esi
6    unsigned int _Unused_capacity; // eax
7    int oldsize; // edi
8    unsigned int v7; // edx
9    unsigned int v8; // ecx
10   unsigned int v9; // edi
11   unsigned int v10; // esi
12
13   this_alias = this;
14   myend = this->_Myend;
15   mylast = this_alias->_Mylast;
16   _Unused_capacity = (myend - mylast) / 0x44;
17   if ( _Unused_capacity < 1 )
18   {
19       oldsize = (mylast - this_alias->_Myfirst) / 0x44;
20       if ( (unsigned int)(0x3C3C3C3 - oldsize) < 1 )
21           XLength((int)"vector<T> too long");

```



©2020 FireEye

61

FireEye | 62

Inferring vector Value Type Size from size() Method

```

int __thiscall vector_size_array44h(vector *this)
{
    return (this->_Mylast - this->_Myfirst) / 0x44;
}

```

©2020 FireEye

62

FireEye | 63

Inferring vector Value Type Size From `size()` method

```
int __thiscall std::vector<std::basic_string<char, std::char_traits<char>>
{
    return (this->Mylast - this->Myfirst) / (signed int)sizeof(string);
}
```

©2020 FireEye

63

FireEye | 64

STL map and set in VC

Extra credit

64

FireEye | 65

Node Construction



```

DWORD *sub_407880()
{
    _DWORD *result; // eax

    result = operator new(0x34u);
    if ( result )
        *result = result;
    if ( result != (_DWORD *)-4 )
        result[1] = result;
    if ( result != (_DWORD *)-8 )
        result[2] = result;
    *((_WORD *)result + 6) = 257;
    return result;
}

```

```

Node34h *new_Node_size34h()
{
    _Node34h *result; // eax

    result = (_Node34h *)operator new(0x34u);
    if ( result )
        result->_NodeHdr._Left = (int)result;
    if ( result != (_Node34h *)0xFFFFFFFFFC )
        result->_NodeHdr._Parent = (int)result;
    if ( result != (_Node34h *)0xFFFFFFFFF8 )
        result->_NodeHdr._Right = (int)result;
    *((_WORD *)&result->_NodeHdr._Color) = 0x101;
    return result;
}

```

©2020 FireEye

65

FireEye | 66

Composing struct `_Node`

- Node standard fields

00000000 <code>_Node</code>	struc ; (sizeof=0x10,
00000000 <code>_Left</code>	dd ?
00000004 <code>_Right</code>	dd ?
00000008 <code>_Parent</code>	dd ?
0000000C <code>_Color</code>	db ?
0000000D <code>_Isnil</code>	db ?
0000000E <code>padding</code>	dw ?
00000010 <code>_Node</code>	ends

- Pair is just two adjacent objects
- Ex: `pair<basic_string, int>`

00000000 <code>pair_xstring_int</code> struc ; (sizeof=0x1C,	
00000000 <code>xstr</code>	xstring ?
00000018 <code>n</code>	dd ?
0000001C <code>pair_xstring_int</code>	ends

Left
Right
Parent
Color
Isnil

Pair
- Key type
- Value type

©2020 FireEye

66

FireEye | 67

Node Structure for STL map and set

```
/* node struct definition for IDA */
struct _Node {
    void *_Left;
    void *_Parent;
    void *_Right;
    char _Color;
    char _Isnil;
    short padding;
};
```

©2020 FireEye

67

FireEye | 68

Defining Structs for STL map

Here's what this looks like in IDA

- Define **value types** (e.g. string)
- Define **node struct** separately
- Define **key/value pair type(s)**
- Define **composite node type(s)**
 - Disambiguate at least by size

00000000 basic_string struc ; (sizeof=0x18, 00000000 00000000 _Bx basic_string::\$DC411C0 00000010 _ysize dd ? 00000014 _Myres dd ? 00000018 basic_string ends 00000018 00000000 ; ----- 00000000 00000000 _Node struc ; (sizeof=0x10, 00000000 00000000 _Left dd ? 00000004 _Parent dd ? 00000008 _Right dd ? 0000000C _Color db ? 0000000D _Isnil db ? 0000000E padding dw ? 00000010 _Node ends 00000010 00000000 ; ----- 00000000 00000000 pair_xstr_n struc ; (sizeof=0x1C, 00000000 00000000 str basic_string ? 00000018 n dd ? 0000001C pair_xstr_n ends 0000001C 00000000 ; ----- 00000000 00000000 _Node_size2Ch struc ; (sizeof=0x2C, 00000000 node _Node ? 00000010 pair_wstr_n pair_xstr_n ? 0000002C _Node_size2Ch ends
--

©2020 FireEye

68

1 69

Tips for Analyzing Large STL Samples

69

FireEye | 70

Hit F5

- Decomp is best for C++
- Use it if ya got it
- Also, try pressing Enter...

```

768 // /////////////////////////////////
769 // Self-delete 1/4 in WinMain (many more elsewhere)
770 // /////////////////////////////////
771 selfdel(0);
772 _loaddll(0);
773 proceed;
774 // /////////////////////////////////
775 // Proceed (no self-del yet)
776 // /////////////////////////////////
777 std::vector<char, std::allocator<char>>::_Tidy(&vectorx);
778 if ( v398 >= 8 )
779     std::Wrap_alloc<std::allocator<wchar_t>>::deallocate(pwszObjectName[0], v398 + 1);
780 v398 = 7;
781 v397 = 0;
782 LOWORD(pwszObjectName[0]) = 0;
783 connection_cleanup(HttpServerConnectionCtx2);
784
785 // /////////////////////////////////
786 // Parse HTTP response
787 // Parse collect_params:
788 // - type
789 // - from_ab
790 // - from_in_box
791 // - from_out_box
792 // - from_other
793 // - from_other
794 vector_from_response._Myfirst = 0;
795 vector_from_response._Mylast = 0;
796 vector_from_response._Myend = 0;
797 LOBYTE(phase) = 0x13;
798 if ( parse_http_response(&vector_from_response, &outbuf_http_response_html) != 1
799     || parse_collect_params_X_from_ab_X_in_box_X_other_X_out_box(&vector_from_response, &flags_010101h) != 1 )
800 {
801     flags_010101h = 0x1010101;
802 }
803 outlook_version._Myres = 7;
804 outlook_version._Mysize = 0;
805 LOWORD(outlook_version._Bx_Ptr) = 0;
806

```

©2020 FireEye

70



FireEye | 71

Hex-Rays Hot Tip

- `__thiscall` and `__fastcall` blind spots:
 - Hex-Rays doesn't always notice implicit `this` argument (or GPR usage)
 - Deceptive when using xrefs
 - Quick fix:
 - Go to disassembly
 - Compare xrefs + identify function call sites
 - Return to decompilation
 - Enter and exit missing functions
 - Other times, have to confirm and force calling convention for various functions

©2020 FireEye

71



FireEye | 72

STL Nomenclature Suggestions

- Large samples → same containers, multiple value types
- Name structs, variables, methods after `sizeof(value_type)`/key/value
- `vector`: `vect24h_emails`, `vect20h_message_stores`
- `map`: `_Node34h_email_srcType` // Node, size 34h: unique email → src type

©2020 FireEye

72



FireEye | 73

Gophe Summary

73



FireEye | 74

Gophe Summary (MD5: D9630C174B8FF5C0AA26168DF523E63E)

Overall <ul style="list-style-type: none">▪ Beacon (collect_params phase)▪ Scraps emails (MAPI):<ul style="list-style-type: none">- Contacts list- Received folder- Sent Items- Folder Hierarchy▪ Beacon (data phase)▪ Parses config further▪ Sends spam emails (MAPI)▪ Beacon (work_report phase)	Binaries <ul style="list-style-type: none">▪ MailClient5.exe – main sample<ul style="list-style-type: none">- 64-bit MAPI email scraper- 64-bit MAPI SPAM email sender- nppt_copy.dll (Mozilla NPAPI plug-in)
	Host Behaviors <ul style="list-style-type: none">▪ Obtains and uses user's email signature▪ PR_DELETE_AFTER_SUBMIT deletes spam from sent items▪ Can disable email alerts, hide (taskbar)▪ ThunderBird XUL/XPCOM and NPAPI plug-ins

©2020 FireEye

74

FireEye | 75

Gophe C2 (MD5: D9630C174B8FF5C0AA26168DF523E63E)

Host/Protocol	Phases
<ul style="list-style-type: none"> ▪ HTTPS, 195.2.252[.]67:2050: <ul style="list-style-type: none"> - GET /<RandomA> - POST /<RandomA>.com=<RandomB> - User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko 	<ul style="list-style-type: none"> ▪ collect_parms (solicits config) ▪ data (emails, semicolon delimited) ▪ work_report (survey/report) <ul style="list-style-type: none"> - Client-ConnectionId - Created - Total - Thunderbird-version - Thunderbird-plugins-installed: true false

©2020 FireEye

75

FireEye | 76

Questions?

Twitter: @mykill

FLARE-VM Windows security distribution		The FLARE On Challenge
FakeNet-NG Internet Simulation for malware		Reverse Engineering CTF 6 years running 2019: 5,790 registered, 308 finished
FLOSS – Obfuscated string decoder		
github.com/fireeye/		www.flare-on.com

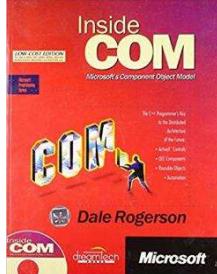
©2020 FireEye

76

FireEye | 77

References

- Dyre Malware Campaigners Innovate with Distribution Techniques:
<https://www.proofpoint.com/us/threat-insight/post/dyre-malware-campaigners-innovate-distribution-techniques>
- Layout of a COM Object:
<https://devblogs.microsoft.com/oldnewthing/20040205-00/?p=40733>



Rogerson, D., **Inside COM**, MS Press, 1997
©2020 FireEye



Box, D., **Essential COM**, Addison-Wesley, 1998

77

FireEye | 78

Extra

78

FireEye | 79

STL Structure Round-Up

Strings	Vectors	Maps/Sets
<pre>struct basic_string { union { char _Buf[16]; wchar_t _BufW[8]; char * _Ptr; wchar_t * _PtrW; } _Bx; size_t _Mysize; size_t _Myres; };</pre>	<pre>struct vector { void *_Myfirst; void *_Mylast; void *_Myend; };</pre>	<pre>// Struct header only struct _Node { void *_Left; void *_Parent; void *_Right; char _Color; char _Isnil; short padding; }; // Your Mileage May Vary!</pre>

©2020 FireEye

79

FireEye | 80

Other References

- **Registering Assemblies with COM:**
<https://docs.microsoft.com/en-us/dotnet/framework/interop/registering-assemblies-with-com>
- **Programming Outlook.Application:**
<https://docs.microsoft.com/en-us/office/troubleshoot/office-developer/automate-outlook-2010-using-c-with-mfc>
- **Building MAPI applications on 32-bit and 64-bit platforms:**
<https://docs.microsoft.com/en-us/office/client-developer/outlook/mapi/building-mapi-applications-on-32-bit-and-64-bit-platforms>
- **MAPI and Thunderbird:**
http://kb.mozilla.org/MAPI_Support

©2020 FireEye

80

FireEye | 81

Composing struct _Tree

- For completeness, here's _Tree:

```
00000000 _Tree      struc ; (sizeof=0x8,
00000000 _Myhead    dd ?
00000004 _Mysize    dd ?
00000008 _Tree      ends
```

©2020 FireEye

81

FireEye | 82

vector struct (YMMV)

VS17 release

- Aux and allocator present

```
00000000 vector      struc ; (sizeof=0x18, mappedto_59)
00000000                      ; XREF: _main/r
00000000 _Myownedaux   dd ?
00000004 _Aux2unknown  dd ?
00000008 _Alval        dd ?
0000000C _Myfirst      dd ?
00000010 _Mylast       dd ?
00000014 _Myend        dd ?
00000018 vector        ends
```

Unknown 2017 binary with STL+Boost

- Naked
 - No iterator debug
 - No _SECURE_SCL
 - No allocator fields

```
00000000 vector      struc ; (sizeof=0xC, mappedto_1807)
00000000 _Myfirst     dd ?
00000004 _Mylast      dd ?
00000008 _Myend       dd ?
0000000C vector        ends
```

©2020 FireEye

82

```
Windows PowerShell
PS>new-object -ComObject WScript.Shell | Get-Member

TypeName: System.__ComObject#{41904400-be18-11d3-a28b-00104bd35090}

Name           MemberType      Definition
----           -----          -----
AppActivate    Method         bool AppActivate (Variant, Variant)
CreateShortcut Method         IDispatch CreateShortcut (string)
Exec           Method         IWshExec Exec (string)
ExpandEnvironmentStrings Method string ExpandEnvironmentStrings (string)
LogEvent       Method         bool LogEvent (Variant, string, string)
Popup          Method         int Popup (string, Variant, Variant, Variant)
RegDelete      Method         void RegDelete (string)
RegRead        Method         Variant RegRead (string)
RegWrite       Method         void RegWrite (string, Variant, Variant)
Run            Method         int Run (string, Variant, Variant)
SendKeys       Method         void Sendkeys (string, Variant)
Environment    ParameterizedProperty IWshEnvironment Environment (Variant) {get}
CurrentDirectory Property      string CurrentDirectory () {get} {set}
SpecialFolders Property      IWshCollection SpecialFolders () {get}

PS>new-object -ComObject PNGFilter.CoPNGFilter | Get-Member

TypeName: System.__ComObject

Name           MemberType      Definition
----           -----          -----
CreateObjRef   Method         System.Runtime.Remoting.ObjRef CreateObjRef(type requestedType)
Equals         Method         bool Equals(System.Object obj)
GetHashCode    Method         int GetHashCode()
GetLifetimeService Method      System.Object GetLifetimeService()
GetType        Method         type GetType()
InitializeLifetimeService Method System.Object InitializeLifetimeService()
ToString       Method         string ToString()
```

90

FireEye | 91

QueryInterface Case Study

ShellLink implements both IShellLink and IPersistFile COM interfaces

```
IShellLink *pShellLink = NULL;
IPersistFile *pPersistFile = NULL;

CoCreateInstance(CLSID_ShellLink, NULL,
                 CLSCTX_INPROC_SERVER, IID_IShellLink,
                 reinterpret_cast<void**>(&pShellLink));

pShellLink->SetPath(sTarget);

pShellLink->QueryInterface(IID_IPersistFile,
                           reinterpret_cast<void**>(&pPersistFile));

pPersistFile->Save(lnkfilename, TRUE);

pPersistFile->Release();
pShellLink->Release();
```

©2020 FireEye

91

vector recognition – Not All Initializations Adjacent

The screenshot shows a debugger interface with assembly code and memory dump panes. The assembly pane displays instructions from 0041BD41 to 0041BD62. The memory dump pane shows memory at address 0041BD41 containing the values 00, 00, 00, 00, 00, 00, 00, 00.

```

if ( vect_iterator_pMessageStore1->ptr_IMsgStore )
{
    contacts_iter = 0;
    zero = 0;
    vect_contact_emails._Myfirst = 0;
    vect_contact_emails._Mylast = 0;
    contacts_end = 0;
    vect_contact_emails._Myend = 0;
    LOBYTE(phase) = 2;

    if ( (_BYTE)flags == 1 )

```

107

vector Recognition – Size of Value Type

- Where can you infer `sizeof(_Ty)` from below, and why?

The screenshot shows a debugger interface with assembly code and memory dump panes. The assembly pane displays instructions from 131 to 138. The memory dump pane shows memory at address 131 containing the value 00.

```

131  size_unscaled = vect_MessageStores._Mylast - vect_MessageStores._Myfirst;
132  if ( (unsigned int)(vect_MessageStores._Mylast - vect_MessageStores._Myfirst) >= 0x20 )
133  {
134      map_or_set_2ch_root? = 0;
135      v104 = 0;
136      node = new_2ch_treenode_for_map_or_set_();
137      map_or_set_2ch_root? = node;
138      v_size = size_unscaled >> 5;

```

- Recall:
 - pointer `_Myfirst`; // pointer to beginning of array
 - pointer `_Mylast`; // pointer to current end of sequence
 - pointer `_Myend`; // pointer to end of array
- Also: `size_type size() { return _Mylast - _Myfirst; }`

108