



# black hat<sup>®</sup>

## USA 2019

AUGUST 3-8, 2019  
MANDALAY BAY / LAS VEGAS



# Hunting for bugs, catching dragons

Nicolas Joly - @n\_joly

MSRC Vulnerabilities and Mitigations Team



Attacking  
Outlook  
with s

Inbox - nico@nicodomain.com - Outlook

File Home Send / Receive Folder View Tell me what you want to do...

New Email New Items Delete Reply Reply All Forward Quick Steps Move Unread/ Read Follow Up Search People Address Book Filter Email Send/Receive All Folders Send/Receive

Favorites

- Inbox 1
- Sent Items
- Deleted Items 1
- Sent Items
- Deleted Items 1
- Junk E-mail
- Outbox
- RSS Feeds
- Search Folders

nico@nicodomain.com

- Inbox
- Sent Items
- Deleted Items 22

Search Current Mailbox (Ctrl+E) Current Mailbox

All Unread By Date Newest

Today

nico  
hello 03:37

Reply Reply All Forward

nico <nico@nicodomain.co> 1 03:37

hello

Connected 100%



Activate Windows  
Go to Settings to activate Windows.



# Outlook exploits?

- Uncommon, not seen in the wild for a while
  - I Love You / Love Letter, early 2000
- Badwinmail reported by Haifei Li in late 2015:
  - Showed how to load Flash in Outlook
  - Leveraged a known Flash vulnerability to prove RCE
- Ryan Hanson's amazing research submitted in late 2016:
  - Issues with the RTF format
  - COMs and Monikers
  - Some cool Outlook features
- Abusing Word features
  - Embedding an EPS font (CVE-2015-2545)?



Ryan Hanson  
@ryHanson

Follow

CVE-2017-0106 (BadWinmail v2)  
CVE-2017-0199 (Word RTF RCE)  
CVE-2017-0204 (Protected View Bypass)

Acknowledgements:

[portal.msrc.microsoft.com/en-us/security ...](https://portal.msrc.microsoft.com/en-us/security...)





# Quick summary of the attack surface

## Email parsing

MIME parsing

HTML / RTF

Pictures (GDI or Office stacks)

Fonts

OLE Objects

Calendars, iCals, vCards, contacts

Attachments

TNEF, MAPI properties

...

## Email protocols

SMTP

POP3/IMAP

Exchange Active Sync

Exchange Web Services

Autodiscover

...

## Misc

Macros

SensePost's Ruler (rules, scripts, homepage)

...

## Spoofing

Certs issues

Name spoofing

S/MIME

DRMs

...



# What this talk covers

## Email parsing

~~MIME parsing~~

~~HTML / RTF~~

~~Pictures (GDI or Office stacks)~~

~~Fonts~~

## OLE Objects

~~Calendars, iCals, vCards, contacts~~

## Attachments

**TNEF, MAPI properties**

...

## Email protocols

~~SMTP~~

~~POP3/IMAP~~

~~Exchange Active Sync~~

~~Exchange Web Services~~

~~Autodiscover~~

...

## Misc

~~Macros~~

~~SensePost's Ruler (rules, scripts, homepage)~~

...

## Spoofing

~~Certs issues~~

~~Name spoofing~~

~~S/MIME~~

~~DRMs~~

...



MSRC

# Why this talk?

- Exploits for Outlook exist but we only occasionally receive reports of dragons outstanding issues
- Why aren't researchers reporting to us?
  - Lack of public research, blog posts describing issues?
  - Lack of interest in the area?
  - Symbols unavailable for Office?

- How can we help our finders?
- Let's talk about our own research!
- Note:

- **The vulnerabilities discussed in the following slides have all been resolved**

An Interesting Outlook Bug - Haifei's random thoughts

[justhaifei1.blogspot.com/2017/03/an-interesting-outlook-bug.html](http://justhaifei1.blogspot.com/2017/03/an-interesting-outlook-bug.html)

Mar 27, 2017 - Due to the complexity of Office code and Microsoft keeps refusing to release Office symbols (I've said about this 1 million times), it's really hard ...



Haifei Li  
@HaifeiLi

Follow

This is the pain of no-Office-symbols.  
[#bluehatv17](#)







# Where to start? RichText emails?

## How email message formats affect Internet email messages in Outlook

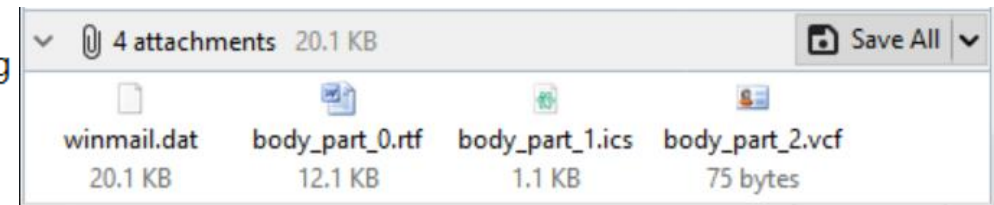
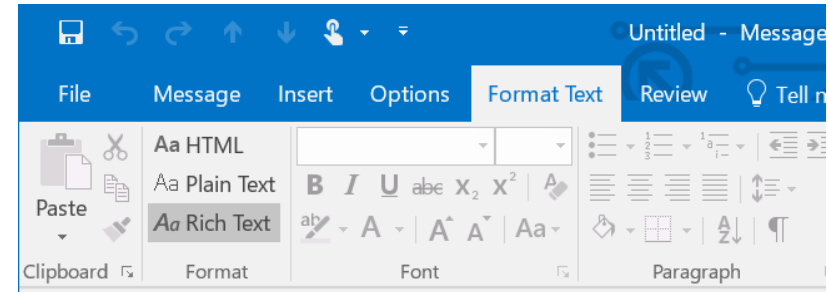
Applies to: Outlook 2019, Microsoft Office Outlook 2007, Microsoft Office Outlook 2003, [More](#)

The use of TNEF is commonly affected by settings in Outlook that are referred to as Microsoft Outlook Rich Text Format (RTF). Rich Text Format and TNEF are not exactly the same, but they are closely related.

A TNEF-encoded message contains a plain text version of the message, and a binary attachment that "packages" various other parts of the original message. The binary attachment is named Winmail.dat, and may include the following:

- The formatted text version of the message.
- OLE objects (for example, embedded pictures, Word documents).
- **Special Outlook features** (for example, custom forms, voting buttons, and meeting requests).
- Regular file attachments that were added to the original message.

Special Outlook features





What's this?

noicant - Meeting Response

File

Received: from NICOLAPTOP ([33.0.0.1]) by nicodomain.com

From

Edit As: Hex

Run Script

Run Template

To:

0

1

2

3

4

5

6

7

8

9

A

B

C

D

E

F

0123456789ABCDEF

Subj

0000h:

78

9F

3E

22

1B

0C

01

06

90

08

00

04

00

00

00

00

xÿ>".....

Date

0010h:

00

01

00

01

00

01

07

90

06

00

08

00

00

00

E4

04

.....ä.

Mess

0020h:

00

00

00

00

00

00

E8

00

01

08

80

07

00

18

00

00

.....è...€.....

MIME

0030h:

00

49

50

4D

2E

4D

69

63

72

6F

73

6F

66

74

20

4D

.IPM.Microsoft M

Cont

0040h:

61

69

6C

2E

4E

6F

74

65

00

31

08

01

03

90

06

00

ail.Note.1.....

X-Ma

0050h:

A8

13

00

00

24

00

00

00

0B

00

02

00

01

00

00

00

"...\$......

Thre

0060h:

03

00

26

00

00

00

00

00

0B

00

29

00

00

00

00

00

..&.....).....

X-MS

0070h:

1E

00

70

00

01

00

00

00

07

00

00

00

74

65

73

63

..p.....tesc

Cont

0080h:

61

6C

00

00

02

01

71

00

01

00

00

00

16

00

00

00

al....q.....

msip

0090h:

01

D3

E2

DD

51

D9

80

F3

C7

67

45

AD

44

A2

9E

E1

.ÓâÝQÙ€óÇgE-Dçžá

Retu

00A0h:

38

A3

0B

F9

AC

B3

00

00

0B

00

01

0E

00

00

00

00

8£.ù-³.....

This

00B0h:

02

01

0A

0E

01

00

00

00

18

00

00

00

00

00

00

00

.....

Locat

00C0h:

B7

70

C3

A0

BE

37

CF

45

AC

A7

DD

69

4A

04

71

8A

·pÃ ¾7İE-šÝiJ.qš

W

00D0h:

C2

80

00

00

03

00

14

0E

01

00

00

00

1E

00

28

0E

Â€.....(.

nic

00E0h:

01

00

00

00

33

00

00

00

30

30

30

30

30

30

32

61

....3...0000002a

Cont

00F0h:

01

6E

69

63

6F

32

40

6E

69

63

6F

64

6F

6D

61

69

.nico2@nicodomain.com.nico2@nicodomain.com....).

Cont

0100h:

6E

2E

63

6F

6D

01

6E

69

63

6F

32

40

6E

69

63

6F

6F

6D

00

00

1E

00

29

0E

....3...0000002a

Cont

0110h:

64

6F

6D

61

69

6E

2E

63

6F

6D

00

00

1E

00

29

0E

.nico2@nicodomain.com.nico2@nicodomain.com....).

Cont

0120h:

01

00

00

00

33

00

00

00

30

30

30

30

30

30

32

61

....3...0000002a

Cont

0130h:

01

6E

69

63

6F

32

40

6E

69

63

6F

64

6F

6D

61

69

.nico2@nicodomain.com.nico2@nicodomain.com....).

Cont

0140h:

6E

2E

63

6F

6D

01

6E

69

63

6F

32

40

6E

69

63

6F

6F

6D

00

00

02

01

09

10

domain.com.....

Cont

0150h:

64

6F

6D

61

69

6E

2E

63

6F

6D

00

00

02

01

09

10

.....}1..

Cont

0160h:

01

00

00

00

18

0E

00

00

14

0E

00

00

7D

31

00

00

LZFu.>åO.....`n

Cont

0170h:

4C

5A

46

75

07

3E

E5

4F

07

00

06

01

01

0B

60

6E

g102f5.d.rcp.Đ..

Cont

0180h:

67

31

30

32

66

35

00

64

00

72

63

70

0D

D0

0E

00

2...`c.Df3150B7.š

eJ8+

0190h:

32

05

0C

60

63

0D

44

66

33

31

35

30

42

37

00

F5

atch.nbthb.ò6

01A0h:

73

74

73

68

05

70

63

74

63

68

0E

D2

36

10

84

00



# TNEF specifications

- [IMS](#)
- Seq
- E
- D
- N

Startup **yesattend.b64**

Edit As: Hex Run Script Run Template: templateTNEF.bt

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	78	9F	3E	22	21	0F	01	06	90	08	00	04	00	00	00	00	x	Y	>	!	.	.	.	.	.	.	.	.	.	.	.	
0010h:	00	01	00	01	00	01	07	90	06	00	08	00	00	00	E4	04	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
0020h:	00	00	00	00	00	00	E8	00	01	08	80	07	00	20	00	00	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
0030h:	00	49	50	4D	2E	4D	69	63	72	6F	73	6F	66	74	20	53	.	I	P	M	.	M	i	c	r	o	s	f	t	.	S	
0040h:	63	68	65	64	75	6C	65	2E	4D	74	67	52	65	73	70	41	c	h	e	d	u	l	e	.	M	t	g	R	e	s	p	A
0050h:	00	48	0B	01	03	90	06	00	20	17	00	00	46	00	00	00	.	H	.	.	.	.	.	.	.	.	.	.	.	.	.	
0060h:	0B	00	02	00	01	00	00	00	03	00	26	00	00	00	00	00	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
0070h:	0B	00	29	00	00	00	00	00	1E	00	70	00	01	00	00	00	.	.	)	.	.	.	.	.	.	.	.	.	.	.	.	
0080h:	04	00	00	00	64	73	61	00	02	01	71	00	01	00	00	00	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
0090h:	16	00	00	00	01	D3	33	B8	25	6A	CE	94	D4	79	37	A9	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	

Inspector - templateTNEF.bt						
Name	Value	Start	Size	Color		Comment
> struct FILE file		0h	6h	Fg:	Bg:	
> struct ATTRIBUTE attr[0]		6h	Fh	Fg:	Bg:	ATTTNEFVERSION
> struct ATTRIBUTE attr[1]		15h	13h	Fg:	Bg:	ATTOEMCODEPAGE
> struct ATTRIBUTE attr[2]		28h	2Bh	Fg:	Bg:	ATTMESSAGECLASS
▼ struct ATTRIBUTE attr[3]		53h	172Bh	Fg:	Bg:	ATTMAPIPROPS
char level	1	53h	1h	Fg:	Bg:	
ushort name	36867	54h	2h	Fg:	Bg:	ATTMAPIPROPS
ushort type	6	56h	2h	Fg:	Bg:	
int length	1720h	58h	4h	Fg:	Bg:	
int nProps	70	5Ch	4h	Fg:	Bg:	
> struct TNEFProperty prop[0]		60h	8h	Fg:	Bg:	PidTagAlternateRecipientAllowed BOOL
> struct TNEFProperty prop[1]		68h	8h	Fg:	Bg:	PidTagPriority INT
> struct TNEFProperty prop[2]		70h	8h	Fg:	Bg:	PidTagReadReceiptRequested BOOL
> struct TNEFProperty prop[3]		78h	10h	Fg:	Bg:	PidTagConversationTopic String8
> struct TNEFProperty prop[4]		88h	24h	Fg:	Bg:	PidTagConversationIndex BINARY
> struct TNEFProperty prop[5]		ACH	8h	Fg:	Bg:	PidTagDeleteAfterSubmit BOOL



# TNEF or RTF - Rich Text Format?

- One special property

- Variations

- LZ
- M

```
using System;  
using System.IO;  
using Microsoft.Office.
```

References

```
static void Main(string[] args)  
{
```

```
    var objOutlook = new Application();  
    var accounts = objOutlook.Session.Accounts;
```

- Bit fl

- Use  
prog

```
MailItem mic = (MailItem)(objOutlook.CreateItem(OlItemType.olMailItem));  
mic.BodyFormat = OlBodyFormat.olFormatRichText;  
mic.RTFBody = System.IO.File.ReadAllBytes(@"file.rtf");
```

(no subject)



nico@nicodomain.com  
To nico2



winmail.dat  
24 KB

Reply Reply All Forward ...

Wed 20/09/2017 18:07

```
.....  
.{\rt  
icpgl  
ouico  
g2057  
057{\  
\fswi  
charse  
;)}..{  
or Ric  
.15063
```



# Examples of issues affecting Outlook

- CVE-2017-0106? Introduced by the **\template** keyword:
  - Remotely (and locally) loads files (http, smb)
  - Also loads embedded objects, like Flash
  - Dramatically extends the attack surface by allowing all the Word supported formats (docx, doc...)
- CVE-2018-0794
  - Cyclic reference in the template names leading to Use After Free
    - a.rtf => b.rtf => \not found\a.rtf
- Resolution?
  - \template no longer supported in Outlook



# Examples of issues affecting Outlook

- CVE-2019-0928
- RCE
- APOC
- DDoS
- SPOOFING
- CVE-2019-0928
- CRLF
- Reso

0170h:	02 01 09 10	01 00 00 00	16 0F 00 00	12 0F 00 00	.....
0180h:	DE (35) 00 00	4D 45 4C 41	00 00 00 00	7B 5C 72 74	E5)..MELA....{\rt
0190h:	66 31 5C 61	6E 73 69 5C	61 6E 73 69	63 70 67 31	fl\ansi\ansicpgl
01A0h:	32 35 32 5C	64 65 66 66	30 5C 6E 6F	75 69 63 6F	252\deff0\nouico
01B0h:	6D 70 61 74	5C 64 65 66	6C 61 6E 67	32 30 35 37	mpat\deflang2057
01C0h:	5C 64 65 66	6C 61 6E 67	66 65 32 30	35 37 7B 5C	\deflangfe2057{\
01D0h:	66 6F 6E 74	74 62 6C 7B	5C 66 30 5C	66 73 77 69	fonttbl{\f0\fswi
01E0h:	73 73 5C 66	70 72 71 32	5C 66 63 68	61 72 73 65	ss\fprq2\fcharse
01F0h:	74 30 20 43	61 6C 69 62	72 69 3B 7D	7D 0D 0A 7B	t0 Calibri;}})..{
0200h:	5C 2A 5C 67	65 6E 65 72	61 74 6F 72	20 52 69 63	\*\generator Ric
0210h:	68 65 64 32	30 20 31 30	2E 30 2E 31	35 30 36 33	hed20 10.0.15063
0220h:	7D 0D 0A 7B	5C 2A 5C 74	65 6D 70 6C	61 74 65 20	}..{\*\template
0230h:	61 6E 79 20	70 61 74 68	20 68 65 72	65 2C 20 20	any path here,
0240h:	61 6E 79 20	65 78 74 65	6E 73 69 6F	6E 20 20 20	any extension
0250h:	20 20 20 20	2E 64 6F 63	78 7D 5C 6C	74 72 70 61	.docx}\ltrpa

- \template no longer supported in Outlook





# Outlook Interop, how to build an email

- Provides an API to build your own emails
  - Example, create a MailItem, change the MessageClass to IPM.Contact and send it
  - See the contact form appear in the preview pane
- Each class has its own properties/features

Item	Default folder	Default message class
-----	-----	-----
Contact	Contacts	IPM.Contact
Task	Tasks	IPM.Task
Appointment	Calendar	IPM.Appointment
Note	Notes	IPM.StickyNote
Journal Entry	Journal	IPM.Activity
Mail	Inbox	IPM.Note



- Provides

- Example
- IPM.Contact

- See the

```
static void Main(string[] args)
```

- Each

```
{  
    var objOutlook = new Application();  
    var accounts = objOutlook.Session.Accounts;  
    MailItem mic = (MailItem)(objOutlook.CreateItem(OlItemType.olMailItem));  
    mic.MessageClass = "IPM.Contact";  
}
```

Task  
Appoin  
Note  
Journa  
Mail

The screenshot shows the Outlook contact form for a contact named 'nico@nicodomain.com'. The form is divided into several sections: 'Full Name...', 'Company', 'Job title', 'File as', 'Internet', 'Email...', 'Display as', 'Web page address', 'IM address', 'Business...', and 'Map It'. The 'Full Name...' field contains 'title testing middlename lastname suffix'. The 'Company' field contains 'company'. The 'Job title' field contains 'jobtitle'. The 'File as' field contains 'lastname, testing middlename'. The 'Internet' section shows 'Email...' with a dropdown arrow. The 'Email...' field contains 'nico@nicodomain.com'. The 'Display as' field contains 'nicodisplay'. The 'Web page address' field contains 'http://bing.com'. The 'IM address' field contains '@nico'. The 'Business...' field contains 'street add', '123 business address', and 'gfd4562'. The 'Map It' button is located at the bottom right. The form is titled 'Current Mailbox' and 'By Date'.



# Other class names and bugs related

- Some examples listed here <https://docs.microsoft.com/en-us/office/vba/outlook/concepts/forms/item-types-and-message-classes>
- Create a mail item and change its class to IPM.Remote
  - Used to trigger a null pointer in the preview pane
  - Reported by Etienne Stalmans and fixed as vNext
- IPM.Document.\*, aka “freedocs”
  - CVE-2017-0204, Office documents open without Protected Mode, Ryan Hanson
  - CVE-2017-8571, Office documents open without user interaction

```
static void Main(string[] args)
{
    ...
    MailItem mic = (MailItem)(objOutlook.CreateItem(OlItemType.olMailItem));
    mic.RTFBody = System.IO.File.ReadAllBytes(@"E:\temp\empty.rtf");
    mic.Subject = "Important Email";
    mic.Importance = OlImportance.olImportanceHigh;
    mic.Attachments.Add(@"E:\temp\hello.docx", OlAttachmentType.olOLE);
    mic.MessageClass = "IPM.Document.Outlook.File.msg.15";
    mic.Send();
}
```



Recycle Bin



Procmon.exe



procexp.exe

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-4KPHG1D\John]

Inbox - nico@nicodomain.com - Outlook

File Home Send / Receive Folder View Tell me what you want to do...

New Email New Items Delete Reply Reply All Forward Quick Steps Move Unread/ Read Search People Address Book Filter Email Send/Receive All Folders Send/Receive

Move to: To Manager Team Email Move Rules OneNote Follow Up Tags Find Send/Receive

Search Current Mailbox (Ctrl+E) Current Mailbox

All Unread By Date Newest

We didn't find anything to show here.

outlook data file

Inbox 1 Drafts Sent Items Deleted Items 1 Junk E-mail Outbox RSS Feeds Search Folders

nico@nicodomain.com

Inbox Drafts Sent Items Deleted Items 42 Junk Email

Filter applied Connected 10%

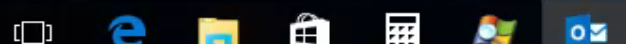
Working Set	PID	Description	C
1,728 K	612	Host Process for Windows S...	Mi
0 K	1140	Microsoft® Volume Shadow ...	Mi
840 K	1396	Spooler SubSystem App	Mi
8,792 K	756	Host Process for Windows S...	Mi
6,172 K	336	Host Process for Windows S...	Mi
15,656 K	1280	Antimalware Service Execut...	Mi
2,112 K	2336	Microsoft Network Realtime I...	Mi
12,180 K	3208	Microsoft Windows Search I...	Mi
7,372 K	4740	Microsoft Windows Search P...	Mi
6,908 K	4548	Microsoft Windows Search P...	Mi
11,576 K	5464	Microsoft Windows Search F...	Mi
1,400 K	4032	Host Process for Windows S...	Mi
5,628 K	2808	Microsoft Office Click-to-Run	Mi
144 K	5400	Host Process for Windows S...	Mi
3,132 K	564	Local Security Authority Proc...	Mi
0 K	492	Windows Logon Application	Mi
1,008 K	768	Windows Logon User Interfa...	Mi
44 K	788	Desktop Window Manager	Mi
1,200 K	1828	Client Server Runtime Process	Mi
32 K	2060	Windows Logon Application	Mi
35,024 K	2488	Desktop Window Manager	Mi
0 K	4196	Usermode Font Driver Host	Mi
27,380 K	2892	Windows Explorer	Mi
2,104 K	1492	Microsoft OneDrive	Mi
44 K	3936	Sysinternals Process Explorer	Sy
11,748 K	1204	Sysinternals Process Explorer	Sy
65,016 K	1756	Microsoft Outlook	Mi
332 K	5080	Microsoft Malware Protection...	Mi

name	Path
	C:\ProgramData\Microsoft\Windows
	C:\Users\John\AppData\Local\Micr
	C:\ProgramData\Microsoft\Windows
	C:\Windows\ServiceProfiles\LocalS
	C:\Windows\ServiceProfiles\LocalS
	C:\Windows\ServiceProfiles\LocalS
	C:\Users\John\AppData\Local\Micr
	C:\Users\John\AppData\Local\Micr
	C:\Users\John\Documents\Outlook
	C:\Users\John\AppData\Local\Micr
	C:\Windows\System32\actxprxy.dll

Activate Windows  
Go to Settings to activate Windows.



Search the web and Windows





Recycle Bin



Procmon.exe



procexp.exe

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-4KPHG1D\John]  
File Options View Process Find DLL Users Help

Inbox - nico@nicodomain.com - Outlook

File Home Send / Receive Folder View Tell me what you want to do...

New Email New Items Delete Reply Reply All Forward Quick Steps Move Unread/ Read Follow Up Search People Address Book Filter Email Send/Receive All Folders Send/Receive

Favorites

- Inbox 1
- Sent Items
- Deleted Items 1

outlook data file

- Inbox 1
- Drafts
- Sent Items
- Deleted Items 1
- Junk E-mail
- Outbox
- RSS Feeds
- Search Folders

nico@nicodomain.com

- Inbox
- Drafts
- Sent Items
- Deleted Items 43
- Junk Email

Search Current Mailbox (Ctrl+E) Current Mailbox

All Unread By Date Newest

Today

nico  
Important Email oIOLE link  
Empty doc <end> 08:42

Hello from Word!

Author: Nicolas Joly

Filter applied Connected 10%

Integrity

- System
- System
- System
- System
- System
- System
- System
- System
- Medium
- Medium

C:\WINDOWS\system32\cmd.exe

E:\workshop>sendmail2\_word.py

E:\workshop>sendmail2\_eq.py



Search the web and Windows



08:47  
17/07/2019



# TNEF / .MSG format

- Use Interop to create Outlook .msg files

```
static void Main(string[] args)
{
    var objOutlook = new Application();
    var accounts = objOutlook.Session.Accounts;
    MailItem mic = (MailItem)(objOutlook.CreateItem(OlItemType.olMailItem));
    mic.MessageClass = "IPM.Contact";

    mic.SaveAs("email.msg");
}
```





# TNEF / .MSG format

- Use Inte

email.msg

email.msg

Folder

Name	Size [B]
__attach_version1.0_#00000000	
__nameid_version1.0	
__recip_version1.0_#00000000	
__properties_version1.0	1584
__substg1.0_001A001F	46
__substg1.0_00310102	100
__substg1.0_0037001F	26
__substg1.0_003B0102	24
__substg1.0_003D001F	0
__substg1.0_003F0102	114
__substg1.0_0040001F	38
__substg1.0_00410102	114
__substg1.0_0042001F	38
__substg1.0_00430102	114
__substg1.0_0044001F	38
__substg1.0_004F0102	128
__substg1.0_0050001F	38

General

Type	Storage
Name	email.msg
File size	58,368 B
Count	65
Created	25/06/2019 22:43:18



# MAPI properties, TNEF and .MSG?

- TNEF is “a hierarchy of rich message properties”, a succession of particular attributes, called MAPI properties, forming a stream.
- Example below with a Task message:

Name	Other Names	Tag	Type	Value	Value (alternate view)
PR_ICON_INDEX	PidTagIconIndex, ptagIconIndex	0x10800003	PT_LONG	1282	0x502
PR_IMPORTANCE	PidTagImportance, ptagImportance	0x00170003	PT_LONG	1	0x1
PR_INTERNET_CPID	PidTagInternetCodepage, ptagInt...	0x3FDE0003	PT_LONG	28591	0x6FAF
PR_LAST_MODIFICATION_TIME	PidTagLastModificationTime, pta...	0x30080040	PT_SYSTIME	10:36:08.221 AM 26/03/2019	Low: 0xB8F994D0 Hig
PR_LAST_MODIFIER_NAME_W	PidTagLastModifierName, PR_LAS...	0x3FFA001F	PT_UNICODE	Nicolas.Joly@microsoft.com	cb: 52 lpb: 4E0069006
PR_MAPPING_SIGNATURE	PidTagMappingSignature, ptagM...	0x0FF80102	PT_BINARY	cb: 16 lpb: 973A0FEF6454AC44B3E...	..idT~D³lLc\...
PR_MDB_PROVIDER	PidTagStoreProvider	0x34140102	PT_BINARY	cb: 16 lpb: 5494A1C0297F101BA58...	T.;Ä)ll.¥...+*%.
PR_MESSAGE_ATTACHMENTS	PidTagMessageAttachments, pta...	0x0E12000D	PT_OBJECT	Object	
PR_MESSAGE_CLASS_W	PidTagMessageClass, PR_MESSAG...	0x001A001F	PT_UNICODE	IPM.Task	cb: 16 lpb: 490050004
PR_MESSAGE_DELIVERY_TIME	PidTagMessageDeliveryTime	0x0E060040	PT_SYSTIME	03:54:05.120 PM 22/09/2017	Low: 0x047EDC00 Hig
PR_MESSAGE_FLAGS	PidTagMessageFlags, ptagMessag...	0x0E070003	PT_LONG	17	0x11

- A MAPI property is defined by a **PID**, a **Type** and a **value**



# MAPI properties, TNEF and .MSG?

- A .MSG is an OLE Storage document, with streams matching MAPI properties, and sub-storages matching MAPI objects
  - Properties are defined in the \_\_properties\_version1.0 stream:

Small properties  
(**integers**, bools...) are  
defined in that stream

00000000	00 00 00 00	00 00 00 00	01 00 00 00	01 00 00 00
00000010	01 00 00 00	01 00 00 00	00 00 00 00	00 00 00 00
00000020	40 00 07 30	02 00 00 00	30 31 0B E2	BF E3 D4 01
00000030	40 00 07 30	02 00 00 00	30 31 0B E2	BF E3 D4 01
00000040	03 00 F7 0F	02 00 00 00	00 00 00 00	00 00 00 00
00000050	03 00 F4 0F	02 00 00 00	02 00 00 00	00 00 00 00
00000060	03 00 0D 34	02 00 00 00	79 0E 04 00	00 00 00 00
00000070	1F 00 04 0E	02 00 00 00	02 00 00 00	03 00 00 00
00000080	1F 00 03 0E	02 00 00 00	02 00 00 00	03 00 00 00
00000090	1F 00 02 0E	02 00 00 00	2A 00 00 00	03 00 00 00
000000A0	0B 00 02 00	06 00 00 00	01 00 00 00	00 00 00 00
000000B0	03 00 17 00	06 00 00 00	01 00 00 00	00 00 00 00
000000C0	1F 00 1A 00	00 00 00 00	12 00 00 00	03 00 00 00
000000D0	0B 00 20 00	06 00 00 00	00 00 00 00	00 00 00 00

@ 0 01 00 00  
@ 0 01 00 00  
÷  
ô  
4 y  
\*  
#

Arrays, **strings** or other objects are defined in their own streams. For example the message class property is defined in \_\_substg1.0\_001A001F:

00000000 | 49 00 50 00 4D 00 2E 00 54 00 61 00 73 00 6B 00 | I P M . T a s k



# OLE objects in an email, really?

- From Haifei's research, we know that we can embed objects
- How are these processed exactly? Can we load scripts?
- The OLE storages are easy to manipulate
  - What else is hiding in there?
- Test case, insert an object in an email, put some breakpoints on the usual COM interoperability functions in ole32.dll
  - ReadClassStg, OpenStorageEx, etc.
  - Pictures and links are processed differently
  - With an object link (CLSID\_StdOleLink) we can hit OleLoad()





O

- From Haif
- How are t
- The OLE s
  - What el
- Test case, usual COM
  - ReadCla
  - Pictures
  - With an

email.msg    Untitled.msg

**Untitled.msg**

- \_\_attach\_version1.0\_#00000000
  - \_\_substg1.0\_3701000D**
    - Document Summary Information
    - Summary Information
    - CompObj
    - DocumentSummaryInformation
    - MailStream
    - ObjInfo
    - Ole
    - OlePres000
    - SummaryInformation
    - Workbook
  - \_\_properties\_version1.0
  - \_\_substg1.0\_0FF90102
  - \_\_substg1.0\_3001001F
  - \_\_substg1.0\_37020102
  - \_\_substg1.0\_370A0102
  - \_\_nameid\_version1.0

**Folder**

Name	Size [B]
CompObj	107
Document Summary Information	244
DocumentSummaryInformation	12
MailStream	6
ObjInfo	58
Ole	2014
OlePres000	224
Summary Information	15508
SummaryInformation	
Workbook	

**General**

Type	Storage
Name	__substg1.0_3701000D
Size	18,173 B
Count	8
Created	25/06/2019 22:50:11

ects

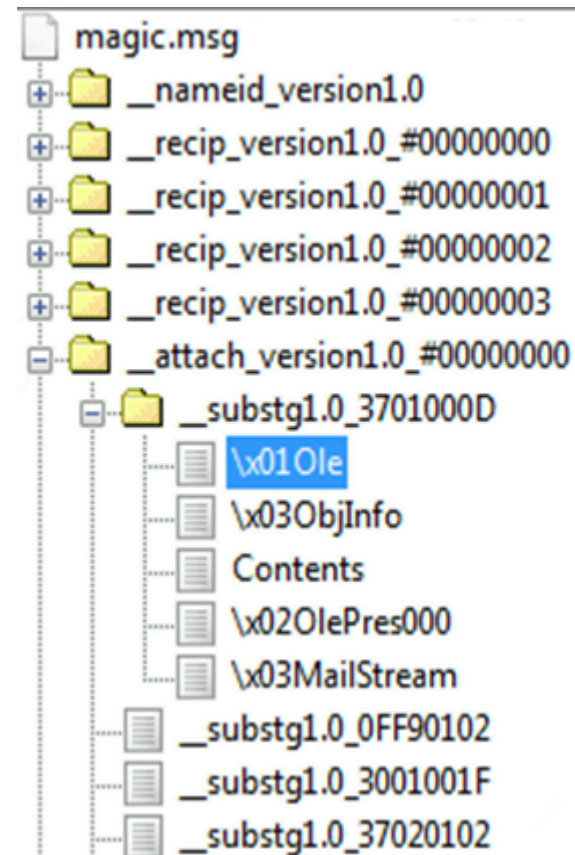
ints on the





# Invoking COM Monikers from a .MSG

- Create an RTF email and insert a link (you may want to use an older version of Outlook)
- Save it to a .MSG storage
- Locate the OLE storage specifically created
- Create a new `\x01Ole` stream underneath
- Hit `OleLoad()`
- Instantiate monikers
- Profit!







# Unmarshalling COM Monikers

```
1615 // read size LONG followed by persistent moniker
1616 STDAPI ReadMonikerStm ( LPSTREAM pstm, LPMONIKER* ppmk)
1617 {
```

This function can be used to load an object that supports the **IPersistStream** interface.

```
1626
1627     if ((error = StRead (pstm, &cb, sizeof(DWORD))) != NOERROR)
1628         return error;
1629
1630     if (cb == NULL)
1631         return NOERROR;
1632
1633     return OleLoadFromStream (pstm, IID_IMoniker, (LPLPVOID) ppmk);
1634 }
```



# Example: FileMoniker, CVE-2018-0950

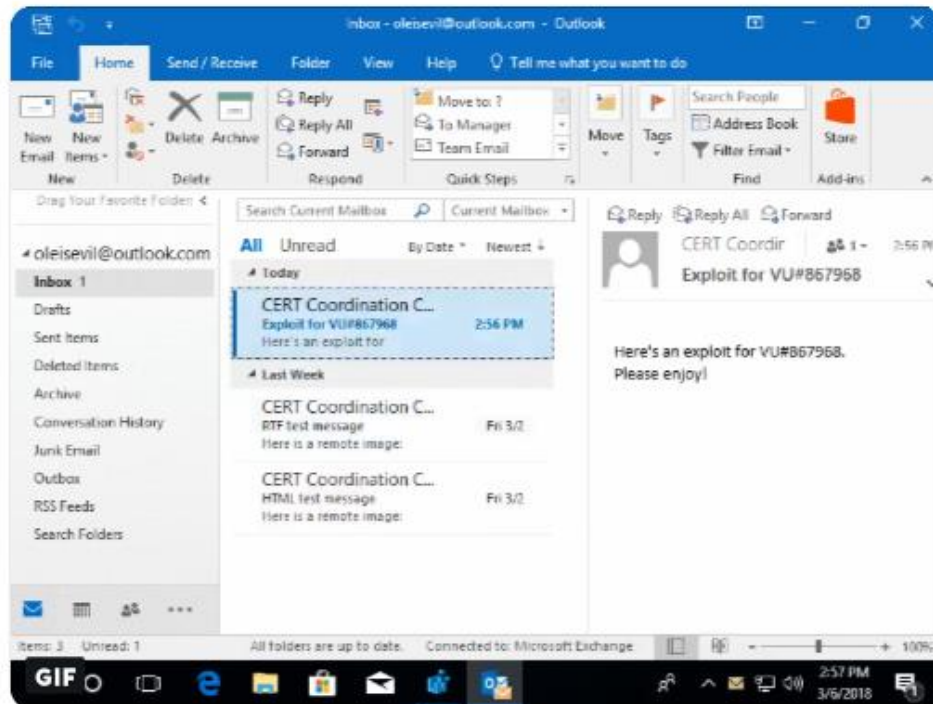


**Will Dormann**

@wdormann

Follow

Combine with an SMB vulnerability, and you've got some real fun.



10:31 am - 10 Apr 2018

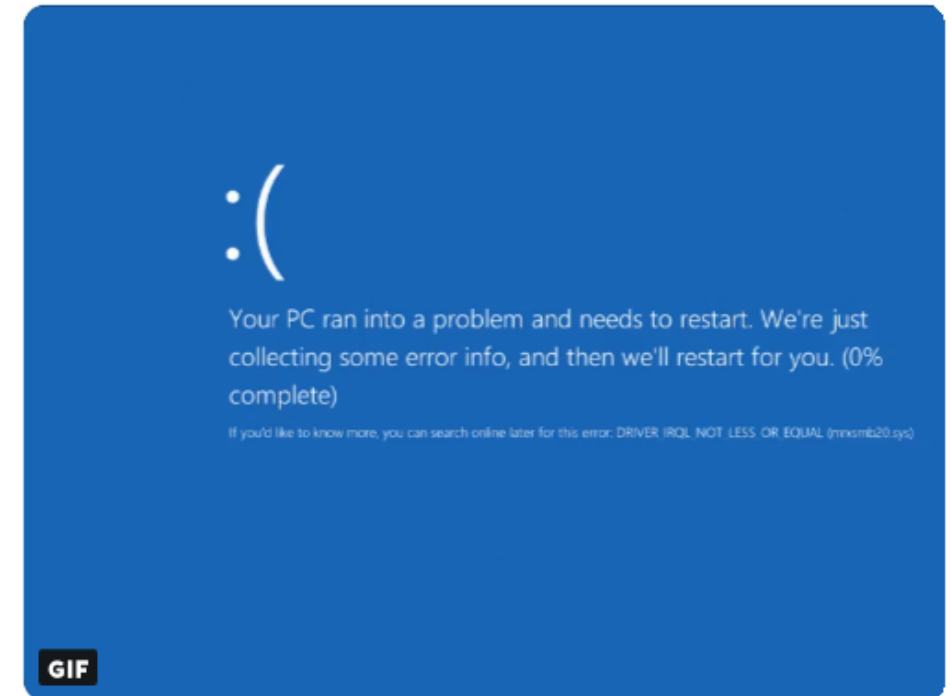


**Will Dormann**

@wdormann

Follow

Combine with an SMB vulnerability, and you've got some real fun.



10:31 am - 10 Apr 2018



# More with the FileMoniker

- Ever looked at CFileMoniker::RestoreShellLink in Ole32?

```
NT_VERIFY(S_OK == m_pShellLink->QueryInterface(IID_IPersistStream,
    (void**)&pps));

memset(&li0, 0, sizeof(li0));
NT_VERIFY(S_OK == pstm->Seek(li0, STREAM_SEEK_SET, &uli));
NT_ASSERT(uli.LowPart == 0 && uli.HighPart == 0);

if (S_OK != (hr=pps->Load(pstm)))
```

- FileMonikers support .LNK shortcuts:
  - CVE-2018-0825, integer overflow in StructuredQuery
  - Load dlls with CVE-2017-8464?

```
(e24.e34): Access violation - code c0000005 (first/second chance
eax=56eb9000 ebx=56eb6fe4 ecx=0000013a edx=0000013a esi=
eip=777531ce esp=0055cb40 ebp=0055cb68 iopl=0 nv up ei pl n
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010
ucrtbase!memcpy+0x4e:
777531ce f3a4 rep movs byte ptr es:[edi],byte ptr [esi]
0:000> kc
#
00 ucrtbase!memcpy
01 combase!CMemStm::Read
02 SHCore!Stream_Read
03 StructuredQuery!StructuredQuery1::ReadPWSTR
04 StructuredQuery!StructuredQuery1::ReadPROPVARIANT
05 StructuredQuery!StructuredQuery1::LeafCondition::Load
06 StructuredQuery!SQ_IUnknown_LoadKnownImplFromStream
07 StructuredQuery!LoadConditionFromStream
24 windows_storage!CShellLink::Load
25 ole32!CFileMoniker::RestoreShellLink
26 ole32!CFileMoniker::EnableTracking
27 ole32!CTrackingFileMoniker::EnableTracking
28 ole32!CTrackingCompositeMoniker::EnableTracking
29 ole32!CDefLink::EnableTracking
2a ole32!CDefLink::Load
2b ole32!wCreateObject
2c ole32!OleLoadWithoutBinding
2d ole32!OleLoad
```



# Another example: OBJREF

- The objref moniker allows unmarshalling arbitrary objects on the IUnknown interface:



```
STDMETHODIMP CObjrefMoniker::Load(IStream *pStream)
{
    HRESULT hr;
    ULONG    cbRead;

    mnkDebugOut((DEB_ITRACE, "CObjrefMoniker::Load(%p,%p)\n", this, pStream));

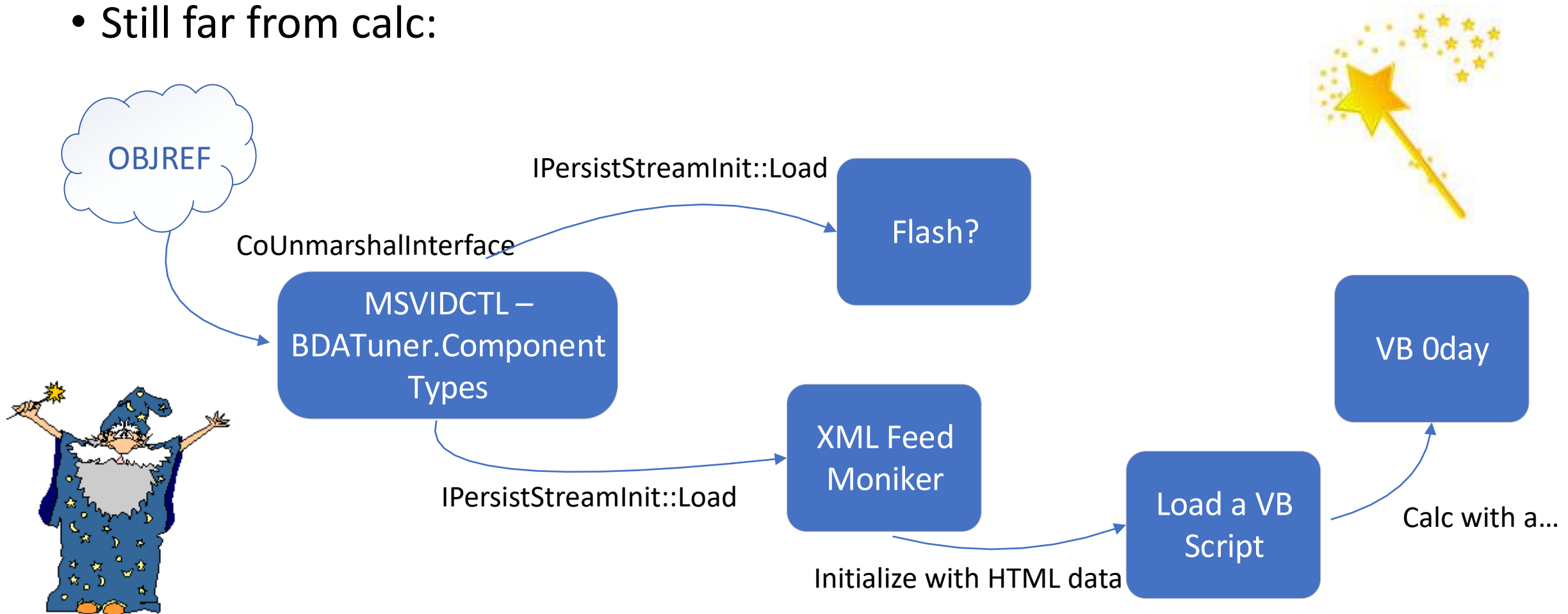
    if (!pStream)
        return E_INVALIDARG;

    // Unmarshal the object we're wrapping
    return CoUnmarshalInterface(pStream, IID_IUnknown, (LPVOID *) &m_pUnk);
}
```



# OBJREF – Building the exploit chain

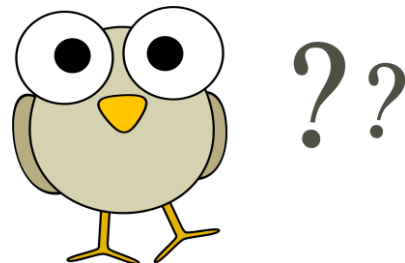
- Still far from calc:





# Multiple bugs fixed in this attack

- Restrict the objects loaded by msvidctl.dll
  - CVE-2016-0142, CVE-2016-7248, CVE-2018-0881
- Prevent the objref and XML Feed Moniker objects from loading in Office via the COM Activation filter
- Do not load OLE objects in the pane
  - CVE-2018-0950
- Fix another VBScript bug
  - And block VBScript as well in the Activation Filter (recent Office branches only)
- Restrict objects loaded by DiagnosticsHub.StandardCollector service
  - CVE-2018-0824
  - How is this related at all?







# From the preview pane to system



- This issue does not only apply to Office, COM marshalling is extensively used by the system
- The attack surface is quite large:
  - VARIANTS
  - SAFEARRAYs
- We just need to find a system COM with a method that accepts such argument



# SafeArrays are generic

- They can contain bytes, integers, strings, all sorts of objects:
- Including VT\_UNKNOWN objects
- Look at the logic in LPSAFEARRAY\_Unmarshal
  - We can quickly reach another CoUnmarshalInterface
  - And replay the attack

```
0:010> kc
07 msvidctl!CComponentTypes::Load
08 msvidctl!IMarshalByValueImpl<CComponents>::UnmarshalInterface
09 combase!CustomUnmarshalInterface
0a combase!CoUnmarshalInterface
0b combase!CoUnmarshalInterface
0c combase!WdtpInterfacePointer UserUnmarshalWorker
0d combase!WdtpInterfacePointer UserUnmarshal
0e OLEAUT32!LPSAFEARRAY_Unmarshal
0f RPCRT4!NdrpUserMarshalUnmarshall
10 RPCRT4!NdrUserMarshalUnmarshall
11 RPCRT4!NdrTypeUnmarshall
12 RPCRT4!NdrpServerUnMarshal
13 RPCRT4!NdrStubCall2
14 RPCRT4!NdrStubCall3
```



```
typedef enum tagVARENUM
{
    VT_EMPTY = 0x0000,
    VT_NULL = 0x0001,
    VT_I2 = 0x0002,
    VT_I4 = 0x0003,
    VT_R4 = 0x0004,
    VT_R8 = 0x0005,
    VT_CY = 0x0006,
    VT_DATE = 0x0007,
    VT_BSTR = 0x0008,
    VT_DISPATCH = 0x0009,
    VT_ERROR = 0x000A,
    VT_BOOL = 0x000B,
    VT_VARIANT = 0x000C,
    VT_UNKNOWN = 0x000D,
    VT_DECIMAL = 0x000E,
    VT_I1 = 0x0010,
    VT_UI1 = 0x0011,
    VT_UI2 = 0x0012,
    VT_UI4 = 0x0013,
    VT_I8 = 0x0014,
    VT_UI8 = 0x0015,
    VT_INT = 0x0016,
    VT_UINT = 0x0017,
    VT_VOID = 0x0018,
    VT_HRESULT = 0x0019,
    VT_PTR = 0x001A,
    VT_SAFEARRAY = 0x001B,
    VT_CARRAY = 0x001C,
```

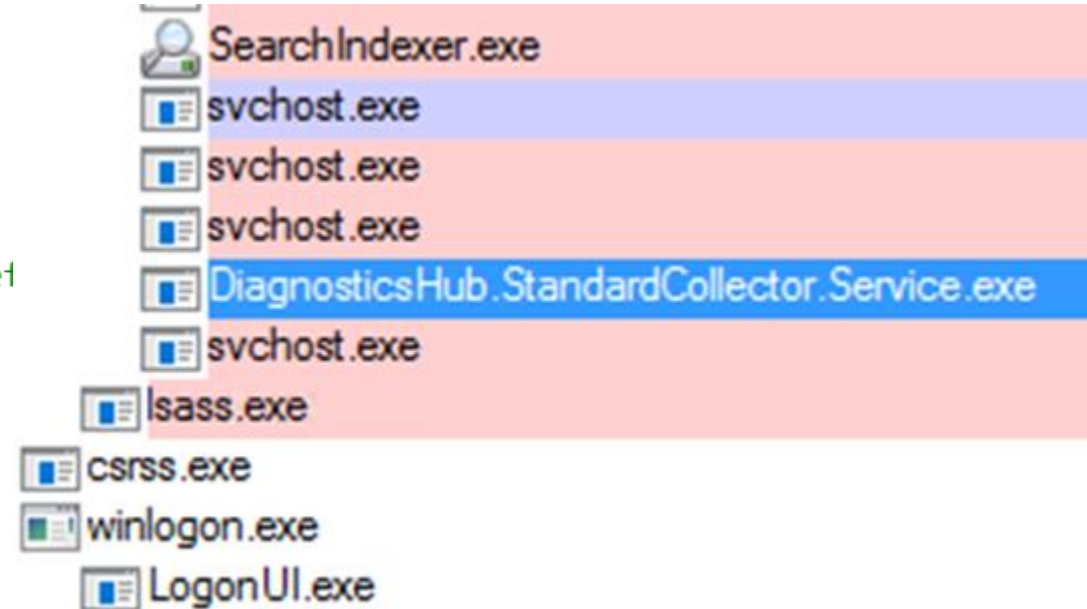


# Ex: Diagnostics Hub Standard Collector Service

```
namespace Microsoft
{
    namespace DiagnosticsHub
    {
        namespace StandardCollector
        {
            /// <summary>
            /// ETW-specific implementation of <see cref="ICollectionSession">
            /// </summary>
            class EtwCollectionSession :
            {
                public ICollectionSession,
                public ICollectionSessionEx,
                public IDebuggerCollectionSession,
                public ISupportErrorInfo,
                public CModuleRefCount
            }
        }
    }
}
```

...

```
HRESULT STDMETHODCALLTYPE GetGraphDataUpdates(
    /* [in] */ __RPC__in REFGUID agentId,
    /* [in] */ __RPC__in SAFEARRAY * counterIdAsBstrs,
    /* [retval][out] */ __RPC__out struct GraphDataUpdates *result);
```



- Just calling GetGraphDataUpdates is enough to trigger the chain





Inbox - nico@nicodomain.com - Outlook

File Home Send / Receive Folder View Tell me what you want to do...

New mail Items Delete Reply Reply All Forward Quick Steps Move Tags Find Send/Receive

Search Current Mailbox (Ctrl+E) Current Mailbox

All Unread By Date Newest

Today

nico hello 03:37

Reply Reply All Forward

nico <nico@nicodomain.com> 1 03:37

hello

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-4KPHG1D]

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PI
audiodg.exe		6,572 K	8,184 K	35
svchost.exe		6,740 K	4,244 K	3
svchost.exe		1,896 K	236 K	6
VSSVC.exe		1,328 K	4 K	11
spoolsv.exe		6,252 K	1,204 K	13
svchost.exe		6,152 K	2,008 K	7
svchost.exe	< 0.01	5,380 K	6,836 K	3
MsMpEng.exe	0.15	99,148 K	11,356 K	12
NisSrv.exe		4,568 K	28 K	23
SearchIndexer.exe		24,232 K	8,420 K	32
SearchProtocolHost.exe		11,108 K	7,168 K	24
svchost.exe		6,104 K	12 K	40
OfficeClickToRun.exe	0.02	35,044 K	2,588 K	28
svchost.exe		1,252 K	144 K	54
lsass.exe		4,360 K	2,260 K	5
winlogon.exe		1,712 K	8 K	4
LogonUI.exe		12,992 K	1,008 K	7
dwm.exe		12,612 K	52 K	7
csrss.exe	0.02	1,348 K	300 K	18
winlogon.exe		1,848 K	4 K	20
dwm.exe	0.35	35,780 K	37,004 K	24
fontdrvhost.exe		660 K	4 K	41
explorer.exe	0.09	37,692 K	33,252 K	28
OneDrive.exe	0.06	4,804 K	4,644 K	14
procexp.exe		2,540 K	4 K	39
procexp64.exe	7.94	14,196 K	9,048 K	12
OUTLOOK.EXE		153,632 K	107,780 K	51

Name	Description	Company Name
{AFBF9F1A-8EE8-4...		
~FontCache-FontFa...		
~FontCache-S-1-5...		
~FontCache-Syste...		
~nico@nicodomain...		
~Outlook.pst.tmp		
~WRF{7C906450-6...		
actxprxy.dll	ActiveX Interface Marshaling Library	Microsoft Corporation
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation
amsi.dll	Anti-Malware Scan Interface	Microsoft Corporation
AppVIsvStream64.dll	AppVIsvStream64	Microsoft Corporation

CPU Usage: 9.73% Commit Charge: 67.13% Processes: 53 Physical Usage: 8



Attacking  
Exchange  
with s



# Attacking Exchange with emails

- Where to start?
  - ShadowBrokers' EnglishmansDentist targeting Exchange 2003
  - Voicemail Transcription RCE via .NET deserialization ([CVE-2018-8302](#), not an email scenario)
- Various attack scenarios:
  - Are we already authenticated?
  - Are we playing with memory corruptions? Replaying tokens? Web issues?
- Is everything handled by managed code?
  - Looking at Exchange Onprem gives a good idea of what's running
  - exRPC32.dll, what's that?
- Some tools:
  - MFCMapi







# MFCMapi, your best friend

Inbox: FW: smime

Actions Folder Search Property Table Tools

Instance Key	Att?	From	To	Subject	Conversation ID
✉ cb: 4 lpb: 00202544	True	nico	nico2@nicodomain.com	Test shortcut xp 2	cb: 16 lpb: 3AA5399CD5...
✉ cb: 4 lpb: 002025E4	True	nico@nicodomain.com	nico2	FW: dfs	cb: 16 lpb: 1BB555563D3...
✉ cb: 4 lpb: 00202604	False	nico@nicodomain.com	'nico2'	fds	cb: 16 lpb: 79061C93664...
✉ cb: 4 lpb: 00202624	False	nico@nicodomain.com	nico2	FW:	cb: 16 lpb: B8744A1FB80...
✉ cb: 4 lpb: 00202644	True	nico@nicodomain.com	nico2	FW: smime	cb: 16 lpb: EA99B6B967C...
✉ cb: 4 lpb: 00202664	False	nico@nicodomain.com	nico2	IPM Meeting tentative	cb: 16 lpb: DA805DA718...
✉ cb: 4 lpb: 002026A4	False	nico@nicodomain.com	nico2	fds	cb: 16 lpb: 52A66B85D82...

< >

Name	Other Names	Tag	Type	Value	Value (alternate view)
0x0F030102		0x0F030102	PT_BINARY	cb: 16 lpb: B8FB7D0694E41B43869...	,ú)...ä.C...ª Á.È
UNI 0x8009001F		0x8009001F	PT_UNICODE	rpmsg.message	cb: 26 lpb: 720070006D0I
UNI 0x800D001F		0x800D001F	PT_UNICODE	nico@nicodomain.com	cb: 38 lpb: 6E006900630C
UNI 0x800E001F		0x800E001F	PT_UNICODE	00000020nico@nicodomain.com	cb: 56 lpb: 30003000300C
0x80190003		0x80190003	PT_LONG	0	0x0
0x80250003		0x80250003	PT_LONG	16384	0x4000
0x803B0102		0x803B0102	PT_BINARY	cb: 100 lpb: 50004F0050003A002F0...	P.O.P.:././3.3...0...0...1.2..
0x803F0003		0x803F0003	PT_LONG	1	0x1
UNI 0x8040001F		0x8040001F	PT_UNICODE	multipart/mixed; boundary="------"	cb: 178 lpb: 6D0075006C
0x8051000B		0x8051000B	PT_BOOLEAN	True	
0x8076000B		0x8076000B	PT_BOOLEAN	False	

Properties retrieved from: Items: 49 Properties: 94

Property Editor

Tag: 0x803F0003  
Type: PT\_LONG

Unsigned Decimal

1

Hex

0x00000001

Smart View



# exRPC and MAPI properties

- Loaded by MExchangeDelivery.exe
- Several functions parse properties found in TNEF emails:
  - A property has a pid and a type:
    - PT\_STRING8
    - PT\_INT
    - PT\_BINARY...
- Is there any bug left?

```
case PROP_ID(ptagPostReplyFolderEntries):  
    ec = EcMakeFidlFromFEL(pmsgobj,  
        &pprv[iprv],  
        &pprvRpc[iprvRpc], (PV)pprvRpc);  
    if (ec)  
    {  
        ecProblem = ecComputed;  
        goto Problem;  
    }
```

```
switch (pid)  
{  
default:  
    if (piprv)  
        piprv[iprvRpc] = iprv;  
    pprvRpc[iprvRpc++] = pprv[iprv];  
    break;  
  
case PROP_ID(ptagSubject):  
    if (PROP_TYPE(ptag) == PT_STRING8)  
    {  
        else if (PROP_TYPE(ptag) == PT_UNICODE)  
        {  
            else  
            {  
                ecProblem = ecPropType;  
                goto Problem;  
            }  
            break;  
        }  
    }
```



# EcParseEntryId

- Called for pid ptagConflictEntryId, only accepts a byte array
- No checks on the property type
- Supported variants are stored on 0x18 bytes on 64-bit
  - Scalars at offset +8
  - Pointers at +0x10
- Probably a DoS at worst

```
loc_180097D20:          ; lpEntryID
mov     rdx, [rsi+10h]
mov     ecx, [rsi+8]      ; cbEntryID
xor     edi, edi
xor     eax, eax
mov     [rsp+180h+ppguid], rdi ; ppguid
mov     [rsp+180h+ppbSvrEID], rdi ; pwSeq
mov     [rbp+80h+var_B8], rax
mov     [rbp+80h+Dst], eax
mov     [rbp+80h+var_AC], ax
mov     [rbp+80h+var_A0], rax
mov     [rbp+80h+var_98], eax
mov     [rbp+80h+var_94], ax
lea     rax, [rsp+180h+pfWacky]
lea     r9, [rsp+180h+pfMessage] ; pfMessage
lea     r8, [rsp+180h+pfLongTerm] ; pfLongTerm
mov     [rsp+180h+pcSvrEID], rdi ; peit
mov     [rsp+180h+pfLongTerm], edi
mov     [rsp+180h+pfMessage], edi
mov     [rsp+180h+peidinfo], rax ; pfWacky
mov     [rsp+180h+pfWacky], edi
mov     [rbp+80h+ppltidFolder], rdi
mov     [rbp+80h+ppltidMessage], rdi
mov     [rbp+80h+Src], rdi
mov     [rbp+80h+var_A8], rdi
call    ?EcParseEntryId@@YAJKPEAUENTRYID@@PEAH11PEAG2PEAPEAU_GUID@@@Z ;
```

```
case PROP_ID(ptagConflictEntryId):
    BOOL    fLongTerm = fFalse;
    BOOL    fMessage = fFalse;
    BOOL    fWacky = fFalse;
    LTID    *pltidFolder = NULL;
    LTID    *pltidMessage = NULL;
    GID     gidFolder = { 0 };
    GID     gidMessage = { 0 };
```

```
// Do a quick parse to verify entryId is what we expect
ec = LOGONOBJ::EcParseEntryId(
    pprv[iprv].Value.bin.cb,
    (ENTRYID *)pprv[iprv].Value.bin.lpb,
    &fLongTerm,
    &fMessage,
    &fWacky,
    NULL,
    NULL,
    NULL);
if (ec)
{
    ecProblem = ec;
    goto Problem;
}
```

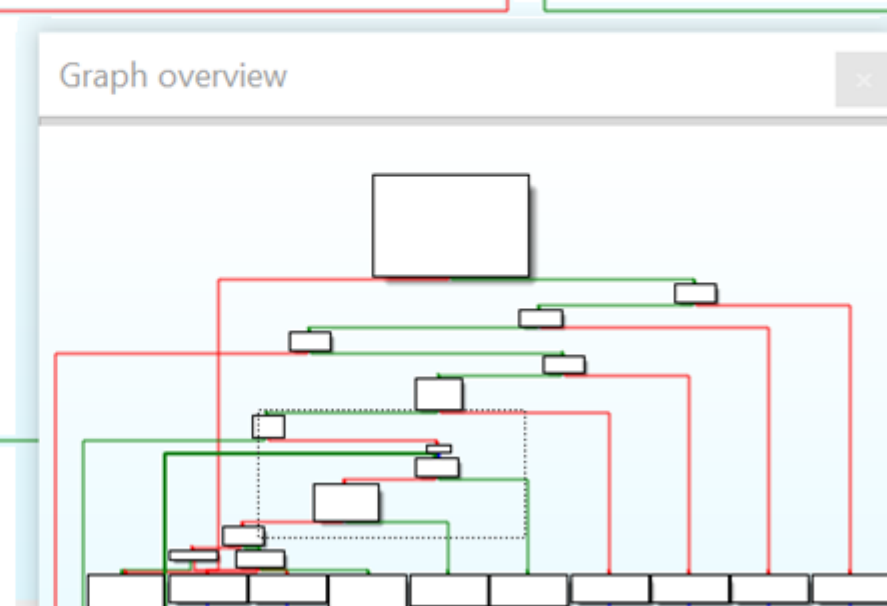


# EcMakeFidlFromFEL

- Called for pid PostReplyFolderEntries, only accepts a byte array
- A loop where data is read and partially written in the original buffer
- No bound check

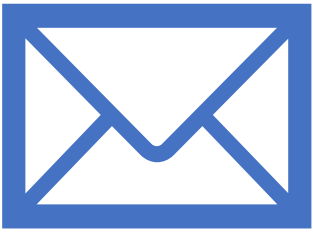
```
and [rdi+18h], ax
mov rdx, [r13+48h] ; prpc
mov rcx, [r13+10h] ; this
lea rax, [rsp+0B8h+var_80]
lea r9, [rdi+4] ; lpEntryID
mov r8d, 2Eh ; cbEntryID
mov [rsp+0B8h+peidinfo], rax ; peidinfo
call EcGetEntryIdIDs
mov ebx, eax
test eax, eax
jnz loc_180097452
```

```
loc_180097349:
cmp dword ptr [rdi], 2Eh
mov eax, 7FFFh
jnz loc_180097473
```



- We can alter one bit OOB in the last entry
  - And [rdi+18h], ax with ax = 7FFFh
  - So what do you think I did?
    - Nothing, was too hard ☹️





# Outcome of that research

- Are these issues exploitable? Very unlikely, but proves the concept
- Other issues found, essentially type confusions
  - These are likely exploitable after authentication, DoS otherwise
- Found also some issues affecting the .NET binaries
  - Null pointers leading to temporary DoS
- Uninitialized memory while parsing rules
  - PR\_EXTENDED\_RULE\_ACTIONS
  - Likely exploitable but would need an infoleak first
- Other interesting components to look at, think OWA too

**What else can YOU find?**



# References

- [https://www.fireeye.com/blog/threat-research/2015/09/attack\\_exploitingmi.html](https://www.fireeye.com/blog/threat-research/2015/09/attack_exploitingmi.html)
- <https://news.softpedia.com/news/badwinmail-microsoft-outlook-bug-can-give-attackers-control-over-pcs-497795.shtml>
- <https://insights.sei.cmu.edu/cert/2018/04/automatically-stealing-password-hashes-with-microsoft-outlook-and-ole.html>
- [https://cansecwest.com/slides/2016/CSW2016\\_Li-Xu\\_BadWinmail\\_and\\_EmailSecurityOutlook\\_final.pdf](https://cansecwest.com/slides/2016/CSW2016_Li-Xu_BadWinmail_and_EmailSecurityOutlook_final.pdf)
- [https://docs.microsoft.com/en-us/openspecs/windows\\_protocols/ms-oaut/3fe7db9f-5803-4dc4-9d14-5425d3f5461f](https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-oaut/3fe7db9f-5803-4dc4-9d14-5425d3f5461f)
- [https://docs.microsoft.com/en-us/openspecs/exchange\\_server\\_protocols/ms-oxtnef/1f0544d7-30b7-4194-b58f-adc82f3763bb](https://docs.microsoft.com/en-us/openspecs/exchange_server_protocols/ms-oxtnef/1f0544d7-30b7-4194-b58f-adc82f3763bb)
- <https://github.com/stephenegriffin/mfcmapl>
- <https://blogs.technet.microsoft.com/srd/2017/07/20/englishmansdentist-exploit-analysis/>
- <https://www.thezdi.com/blog/2018/8/14/voicemail-vandalism-getting-remote-code-execution-on-microsoft-exchange-server>
- <https://docs.microsoft.com/en-us/dotnet/api/microsoft.office.interop.outlook?view=outlook-pia>
- CVE-2017-8506, demo on slide3

# Thanks all!

@n\_joly

