black hat®
USA 2019

AUGUST 3-8, 2019

MANDALAY BAY / LAS VEGAS

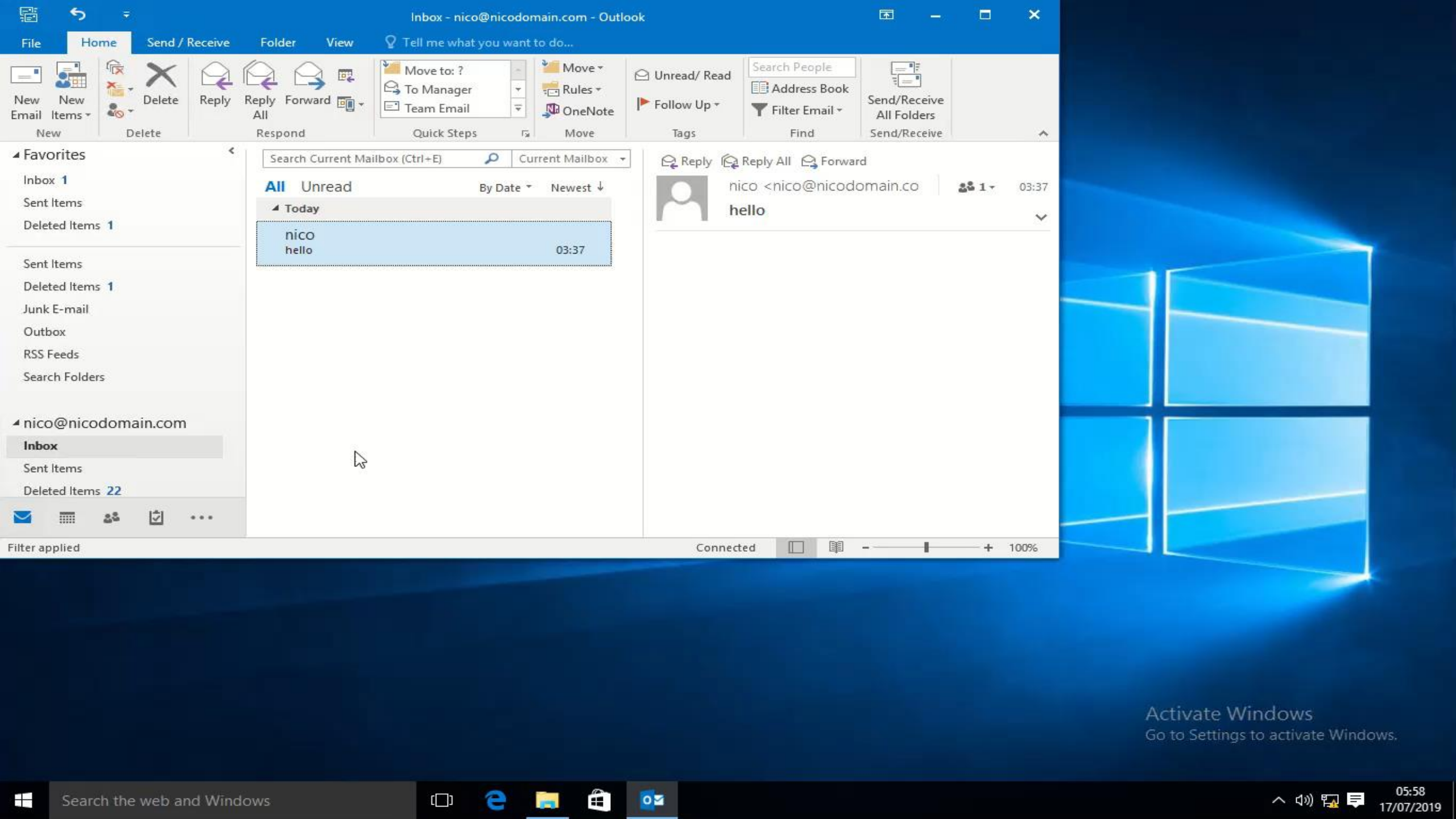
#BHUSA @BLACK HAT EVENTS

Hunting for bugs, catching dragons

Nicolas Joly - @n_joly
MSRC Vuln E rabilities and Mitigati o ns Team

Microsoft

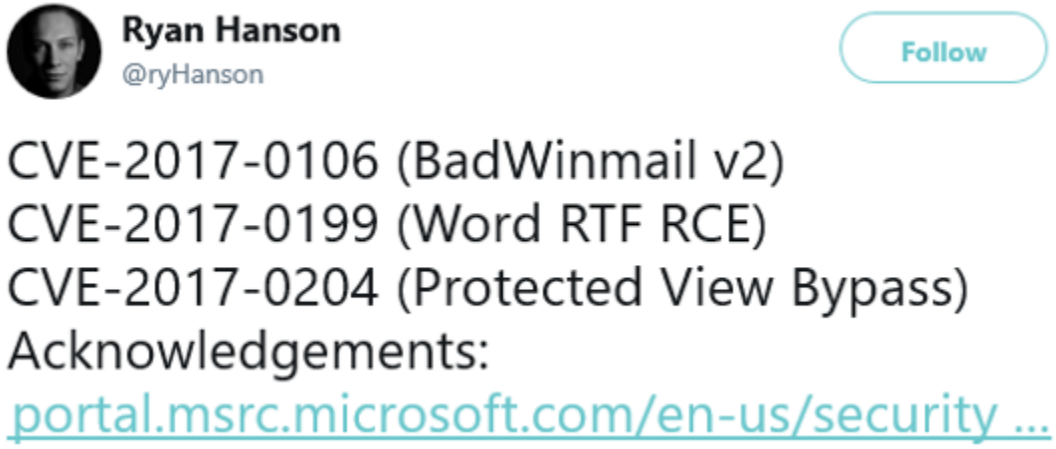
Attacking Outlook with ✉s


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
Move to: ?
To Manager
Team Email
Move
Rules
OneNote
Unread/ Read
Follow Up
Search People
Address Book
Filter Email
Send/Receive All Folders
New
Delete
Respond
Quick Steps
Move
Tags
Find
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
Filter applied
Connected
100%
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
05:58
17/07/2019

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)?

news.softpedia.com



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~~
…

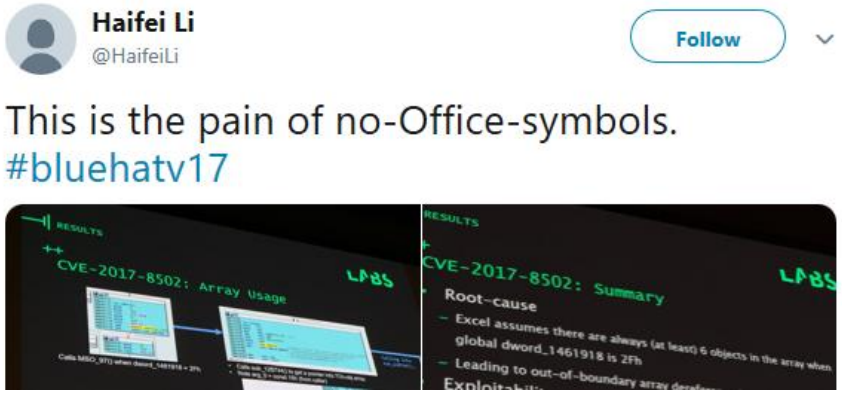
Misc
~~Macros~~
~~SensePost's Ruler (rules, scripts, homepage)~~
…

Spoofing
~~Certs issues~~
~~Name spoofing~~
~~S/MIME~~
~~DRMs~~
…

Why this talk?

An Interesting Outlook Bug - Haifei's random thoughts
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 ...

- 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**

Where to start? RichText emails?

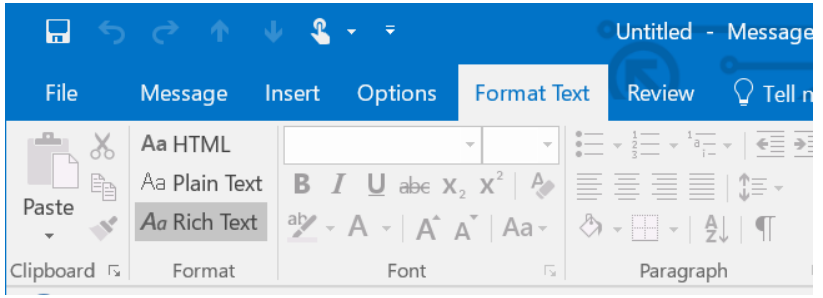
How email message formats affect Internet email messages in Outlook

Applies to: Outlook 2019, Microsoft Office Outlook 2007, Microsoft Office Outlook 2003, More

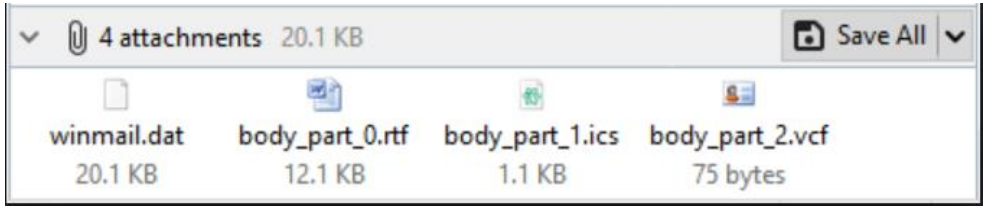
The use of TNEF is commonly affected by settings in Outlook that are referred to as Microsoft Outlook Rich Text Format (RTF). Rich Text Format and TNEF are not exactly the same, but they are closely related.

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. In binary attachment is named Winmail.dat, and may include th

- The formatted text version of the messa
- OLE objects (for example, embedded p Office 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



https://support.microsoft.com/sq-al/help/290809

noicant - Meeting Response

File | Meeting Response | Developer

Delete | Reply | Reply All | Forward | Quick Steps | Move | Rules | Actions | Assign Policy | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select

Delete | Respond | Quick Steps | Move | Tags | Editing

Fri 22/09/2017 16:41

nico@nicodomain.com

noicant

To nico@nicodomain.com

When 22 September 2017 17:00-17:30 (UTC+00:00) Dublin, Edinburgh, Lisbon, London.

Location

We couldn't find this meeting in the calendar. It may have been moved or deleted.
nico@nicodomain.com has declined this meeting.

fdsfds  **ds**

noicant - Meeting Response

```
Received: from NICOLAPTOP ([33.0.0.1]) by nicodomain.com
From: <nico2@nicodomain.com>
To: <nico@nicodomain.com>
Subject: test
Date: Thu, 3 May 2019 13:51:27 +0100
Message-ID: <000801d3e2dd$7347a000$59d6e000$@nicodomain.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_0009_01D3E2E5.D50C0800"
X-Mailer: Microsoft Outlook 16.0
Thread-Index: AdPi3VHZgPPHZ0WtRKKe4TijC/mssw==
X-MS-TNEF-Correlator: 00000000B770C3A0BE37CF45ACA7DD694A04718A24012000
Content-Language: en-gb
msip_labels: MSIP_Label_f42aa342-8706-4288-bd11-ebb85995028c_Enabled=True; MSIP
Return-Path: <nico2@nicodomain.com>

This is a multipart message in MIME format.

------=_NextPart_000_0009_01D3E2E5.D50C0800
Content-Type: text/plain;
    charset="us-ascii"
Content-Transfer-Encoding: 7bit



------=_NextPart_000_0009_01D3E2E5.D50C0800
Content-Type: application/ms-tnef;
    name="winmail.dat"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="winmail.dat"

eJ8+IhsMAQaQCAAEAAAAAAABAAEAAQeQBgAIAAAA5AQAAAAAADoAAEIgAcAGAAAAElQTS5NaWNy
```

What's this?

noicant - Meeting Response

```
Received: from NICOLAPTOP ([33.0.0.1]) by nicodomain.com
From
To:
Subj
Date
Mess
MIME
Cont
Delet
Delet
Fri 22/
nicO
noica
To
When
Locatic
W
nic
fdsf
X-Ma
Thre
X-MS
Cont
msip
Retu
This
----
Cont
Cont
Cont
----
Cont
Cont
Cont
eJ8+
```

Edit As: Hex | Run Script | Run Template

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	78	9F	3E	22	1B	0C	01	06	90	08	00	04	00	00	00	00	xŸ>".....
0010h:	00	01	00	01	00	01	07	90	06	00	08	00	00	00	E4	04	.....ä.
0020h:	00	00	00	00	00	00	E8	00	01	08	80	07	00	18	00	00	.....è...€.....
0030h:	00	49	50	4D	2E	4D	69	63	72	6F	73	6F	66	74	20	4D	.IPM.Microsoft M
0040h:	61	69	6C	2E	4E	6F	74	65	00	31	08	01	03	90	06	00	ail.Note.1.....
0050h:	A8	13	00	00	24	00	00	00	0B	00	02	00	01	00	00	00	¨...$.....
0060h:	03	00	26	00	00	00	00	00	0B	00	29	00	00	00	00	00	..&.....).....
0070h:	1E	00	70	00	01	00	00	00	07	00	00	00	74	65	73	63	..p.....tesc
0080h:	61	6C	00	00	02	01	71	00	01	00	00	00	16	00	00	00	al....q.....
0090h:	01	D3	E2	DD	51	D9	80	F3	C7	67	45	AD	44	A2	9E	E1	.ÓâÝQÙ€óÇgE-D¢žá
00A0h:	38	A3	0B	F9	AC	B3	00	00	0B	00	01	0E	00	00	00	00	8£.ù¬³.....
00B0h:	02	01	0A	0E	01	00	00	00	18	00	00	00	00	00	00	00	.....
00C0h:	B7	70	C3	A0	BE	37	CF	45	AC	A7	DD	69	4A	04	71	8A	·pÃ ¾7ÏE¬§ÝiJ.qŠ
00D0h:	C2	80	00	00	03	00	14	0E	01	00	00	00	1E	00	28	0E	Â€.....(.
00E0h:	01	00	00	00	33	00	00	00	30	30	30	30	30	30	32	61	....3...0000002a
00F0h:	01	6E	69	63	6F	32	40	6E	69	63	6F	64	6F	6D	61	69	.nico2@nicodomai
0100h:	6E	2E	63	6F	6D	01	6E	69	63	6F	32	40	6E	69	63	6F	n.com.nico2@nico
0110h:	64	6F	6D	61	69	6E	2E	63	6F	6D	00	00	1E	00	29	0E	domain.com....).
0120h:	01	00	00	00	33	00	00	00	30	30	30	30	30	30	32	61	....3...0000002a
0130h:	01	6E	69	63	6F	32	40	6E	69	63	6F	64	6F	6D	61	69	.nico2@nicodomai
0140h:	6E	2E	63	6F	6D	01	6E	69	63	6F	32	40	6E	69	63	6F	n.com.nico2@nico
0150h:	64	6F	6D	61	69	6E	2E	63	6F	6D	00	00	02	01	09	10	domain.com.....
0160h:	01	00	00	00	18	0E	00	00	14	0E	00	00	7D	31	00	00	..........}1..
0170h:	4C	5A	46	75	07	3E	E5	4F	07	00	06	01	01	0B	60	6E	LZFu.>åO.....`n
0180h:	67	31	30	32	66	35	00	64	00	72	63	70	0D	D0	0E	00	g102f5.d.rcp.Ð..
0190h:	32	05	0C	60	63	0D	44	66	33	31	35	30	42	37	00	F5	2..`c.Df3150B7.õ

TNEF specifications

- [MS-OXTNEF]
- Sequence of objects, containers and properties
  - Easy to parse
  - Developed an 010 template
  - Might release in the future

TNEF specifications

- [MS-
- Sequ
  - E
  - D
  - M

Startup | yesattend.b64

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

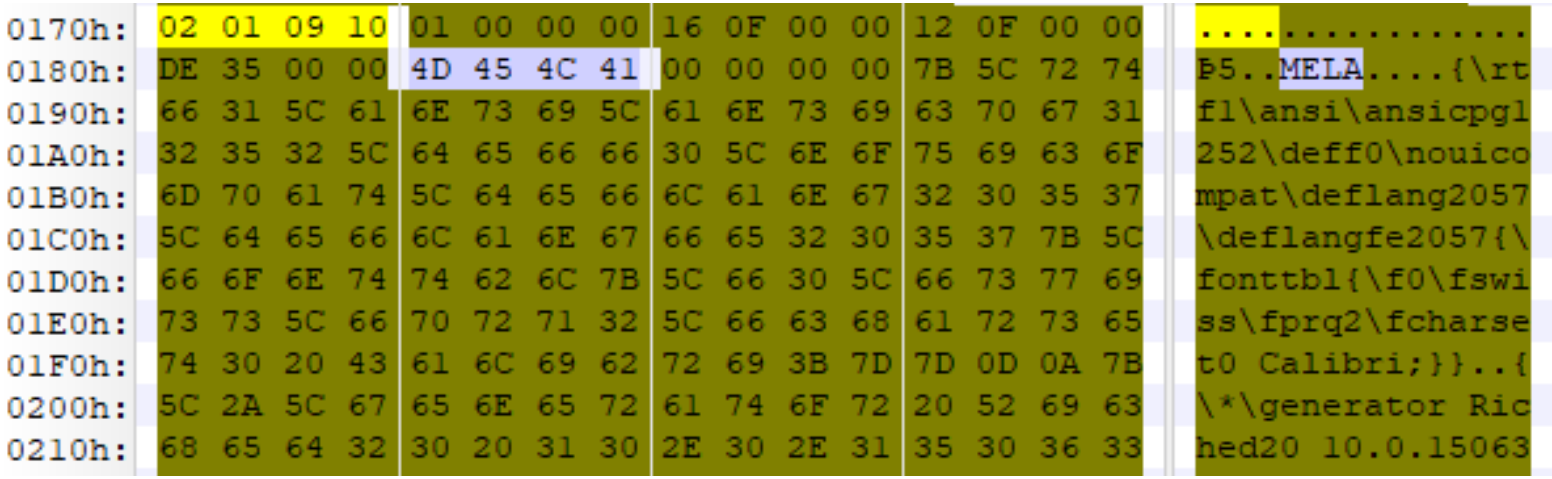
```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 78 9F 3E 22 21 0F 01 06 90 08 00 04 00 00 00 00  xŸ>"!.....·.....
0010h: 00 01 00 01 00 01 07 90 06 00 08 00 00 00 E4 04  ..... ..... ....ä.
0020h: 00 00 00 00 00 00 E8 00 01 08 80 07 00 20 00 00  ......è..·€.. ..
0030h: 00 49 50 4D 2E 4D 69 63 72 6F 73 6F 66 74 20 53  .IPM.Microsoft S
0040h: 63 68 65 64 75 6C 65 2E 4D 74 67 52 65 73 70 41  chedule.MtgRespA
0050h: 00 48 0B 01 03 90 06 00 20 17 00 00 46 00 00 00  .H..... ...F...
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  ..)..... ..p.....
0080h: 04 00 00 00 64 73 61 00 02 01 71 00 01 00 00 00  ....dsa. ..q.....
0090h: 16 00 00 00 01 D3 33 B8 25 6A CE 94 D4 79 37 A9  .....Ó3¸%jÎ”Ôy7©
```

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 PR_RTF_COMPRESSED = 0x10090102
- Various encodings
  - LZFu? Compressed RTF, default
  - MELA? Plain RTF, easy to change



- Bit flipping this field will generally result in a broken email
- Use instead the Outlook Interop Library and send TNEF emails programmatically

TNEF or RTF - Rich Text Format?

- One special property PR_RTF_COMPRESSED – 0x10090102
- Varic
  - LZ
  - M
- Bit fl
- Use
  prog

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

0 references
static void Main(string[] args)
{
    var objOutlook = new Application();
    var accounts = objOutlook.Session.Accounts;

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

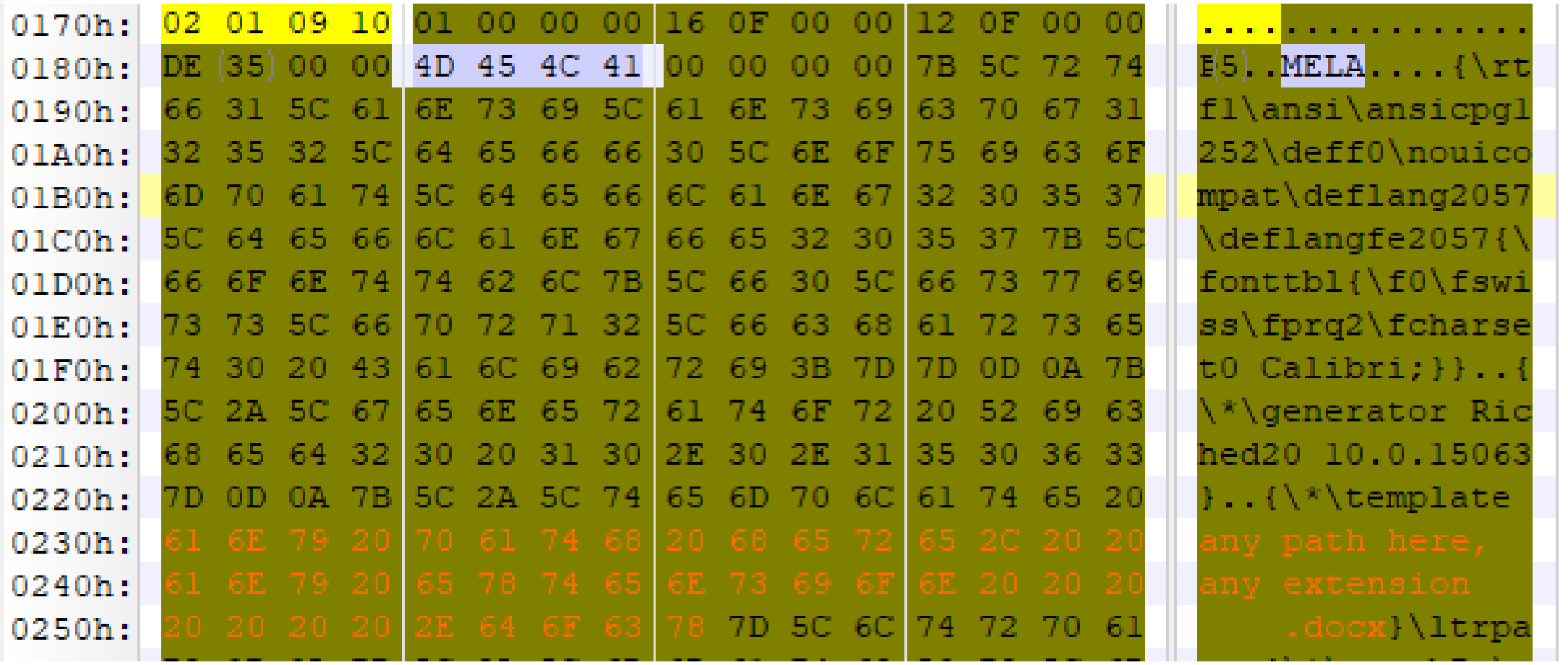
```
.....
..{\rt
sicpgl
nouico
ng2057
2057{\
0\fswi
charse
;}}..{
or Ric
.15063
```

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-
  - R
  - A
  - D
    su
- CVE-
  - C
- Reso
  - \template no longer supported in Outlook

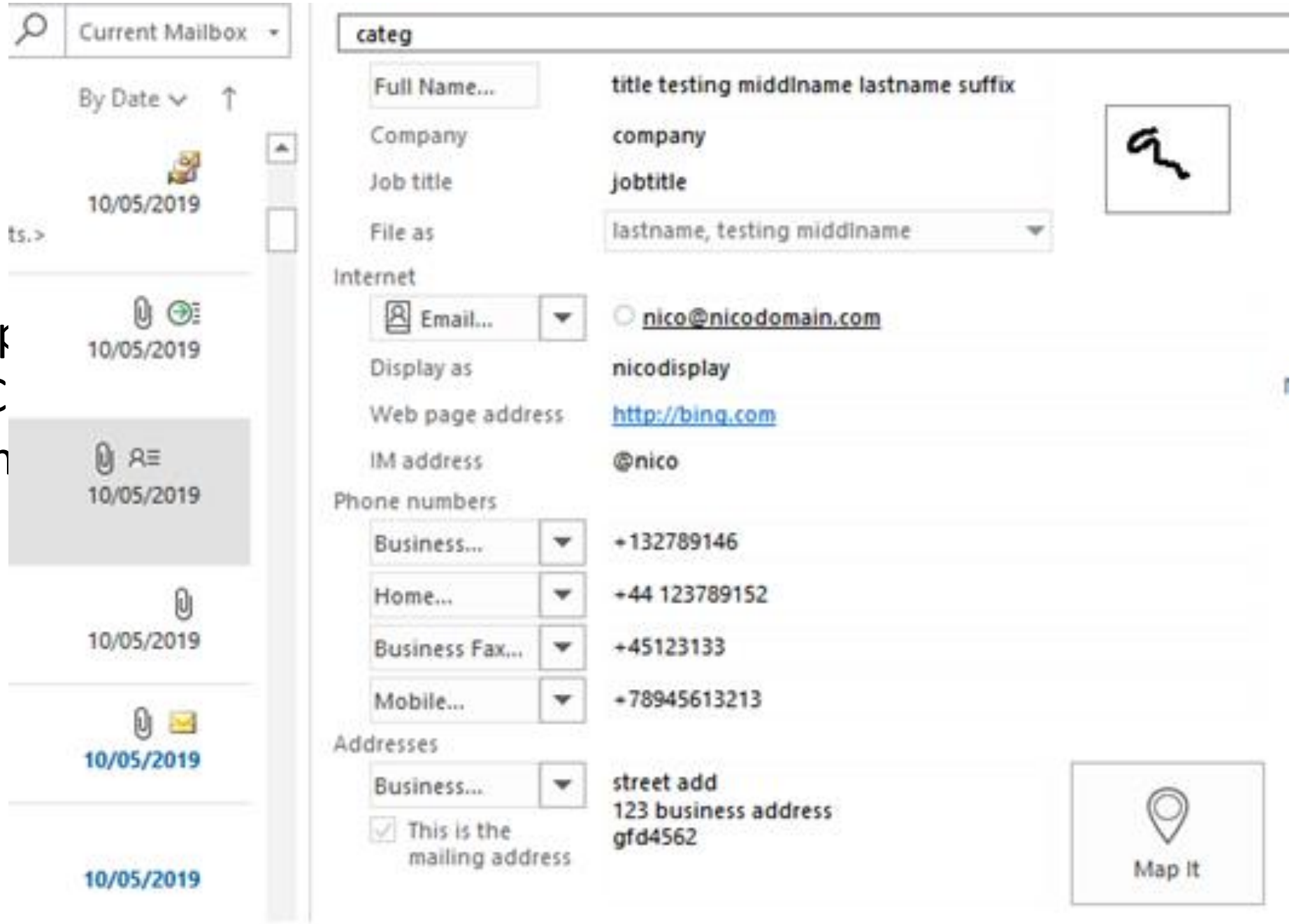


Outlook Interop, how to build an email

- 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

```
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";
```

- Provides
  - Examp
    IPM.C
  - See th



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

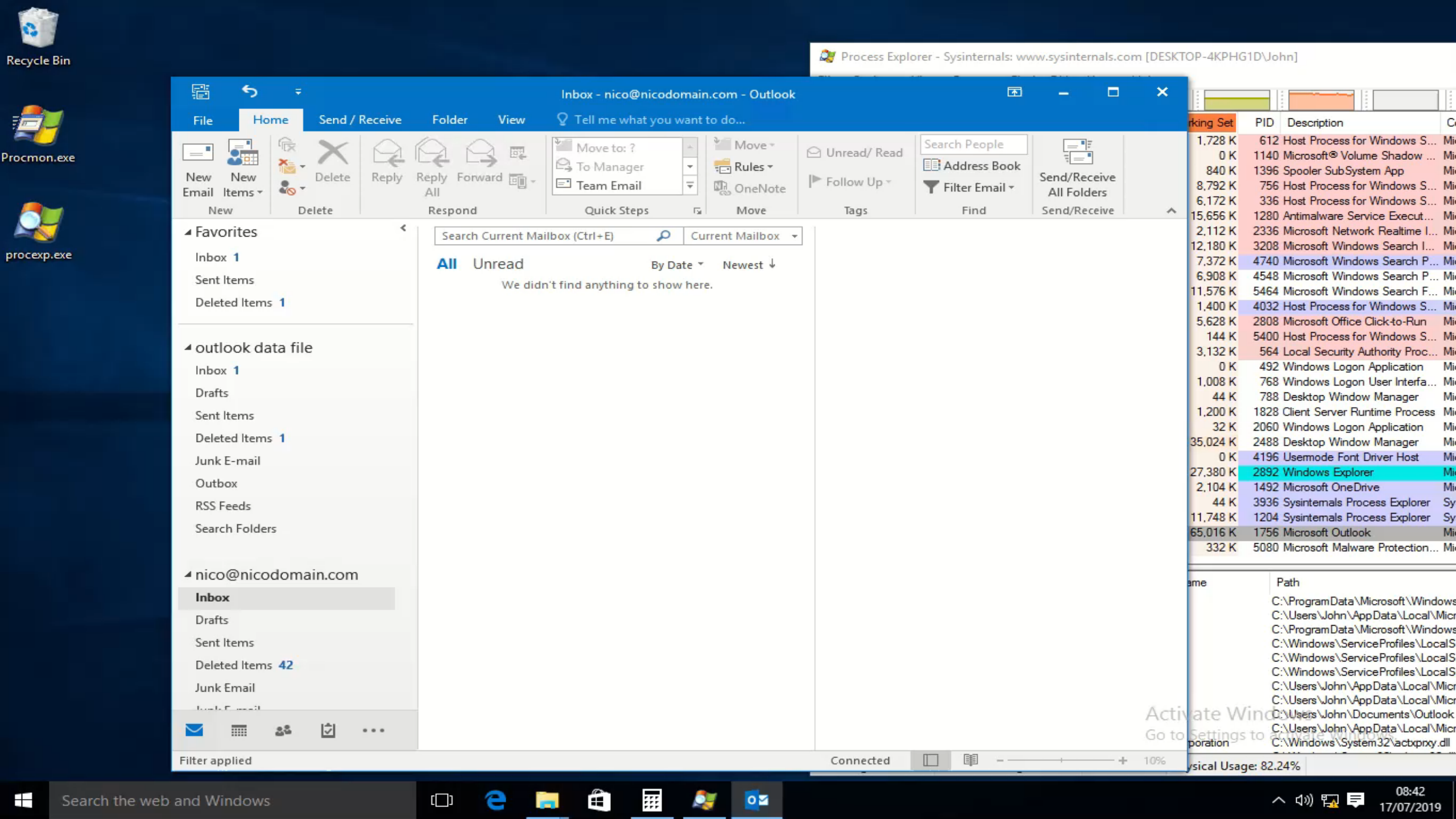
- Each class has its own properties/features

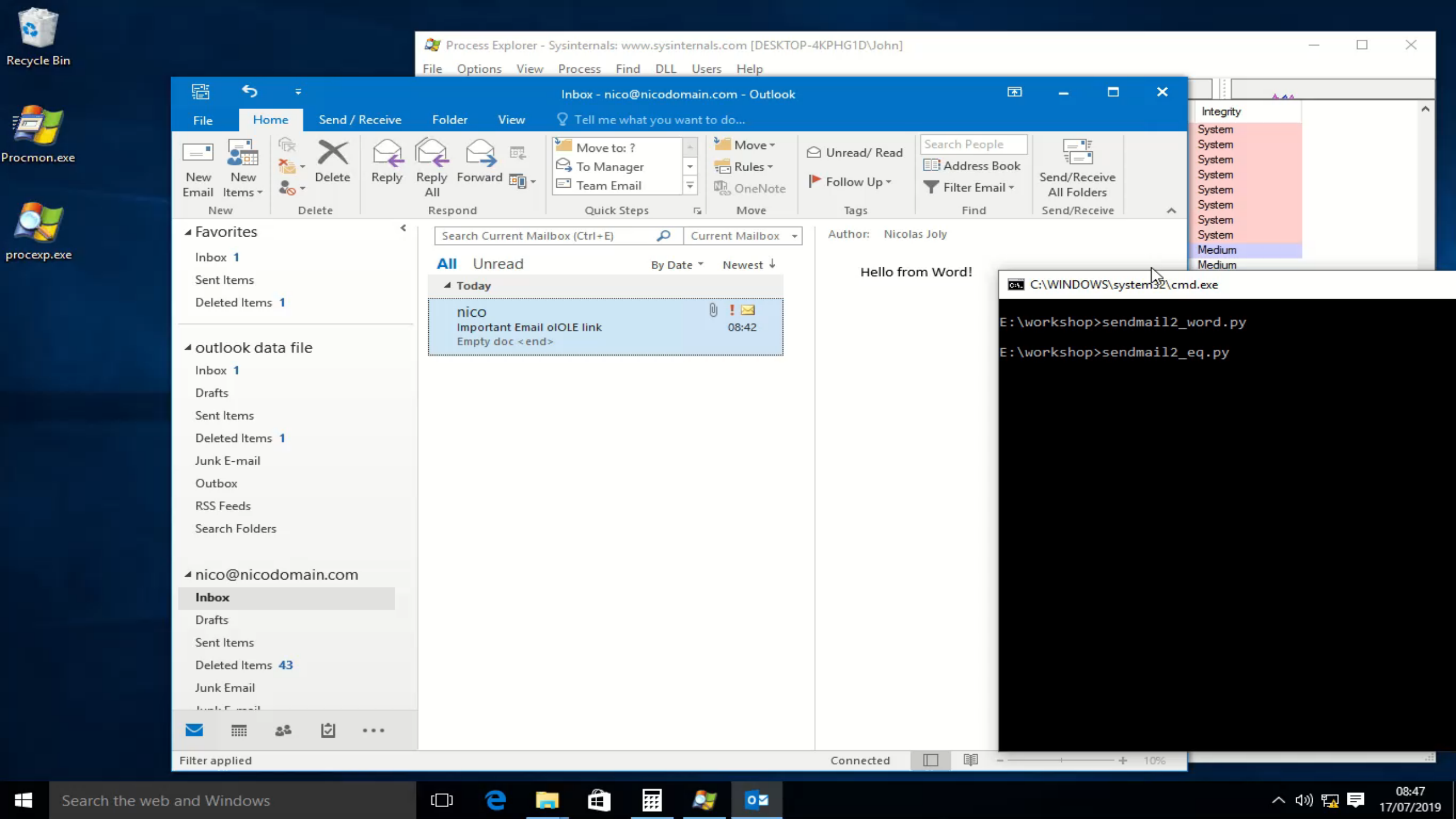
Item	Default folder	Default message class
Contact	Contacts	IPM.Contact
Task	Tasks	IPM.Task
Appointment	Calendar	IPM.Appointment
Note	Notes	IPM.StickyNote
Journal Entry	Journal	IPM.Activity
Mail	Inbox	IPM.Note

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
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
Move to: ?
To Manager
Team Email
Move
Rules
OneNote
Unread/ Read
Follow Up
Search People
Address Book
Filter Email
Send/Receive All Folders
New
Delete
Respond
Quick Steps
Move
Tags
Find
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 42
Junk Email
Search Current Mailbox (Ctrl+E)
Current Mailbox
All
Unread
By Date
Newest
We didn't find anything to show here.
Filter applied
Connected
10%
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-4KPHG1D\John]
Working Set
PID
Description
1,728 K 612 Host Process for Windows S...
0 K 1140 Microsoft® Volume Shadow ...
840 K 1396 Spooler SubSystem App
8,792 K 756 Host Process for Windows S...
6,172 K 336 Host Process for Windows S...
15,656 K 1280 Antimalware Service Execut...
2,112 K 2336 Microsoft Network Realtime I...
12,180 K 3208 Microsoft Windows Search I...
7,372 K 4740 Microsoft Windows Search P...
6,908 K 4548 Microsoft Windows Search P...
11,576 K 5464 Microsoft Windows Search F...
1,400 K 4032 Host Process for Windows S...
5,628 K 2808 Microsoft Office Click-to-Run
144 K 5400 Host Process for Windows S...
3,132 K 564 Local Security Authority Proc...
0 K 492 Windows Logon Application
1,008 K 768 Windows Logon User Interfa...
44 K 788 Desktop Window Manager
1,200 K 1828 Client Server Runtime Process
32 K 2060 Windows Logon Application
35,024 K 2488 Desktop Window Manager
0 K 4196 Usermode Font Driver Host
27,380 K 2892 Windows Explorer
2,104 K 1492 Microsoft OneDrive
44 K 3936 Sysinternals Process Explorer
11,748 K 1204 Sysinternals Process Explorer
65,016 K 1756 Microsoft Outlook
332 K 5080 Microsoft Malware Protection...
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
Physical Usage: 82.24%
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
08:42
17/07/2019


Recycle Bin
Procmon.exe
procexp.exe
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-4KPHG1D\John]
File Options View Process Find DLL Users Help
Integrity
System
System
System
System
System
System
System
System
Medium
Medium
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
Move to: ?
To Manager
Team Email
Move
Rules
OneNote
Unread/ Read
Follow Up
Search People
Address Book
Filter Email
Send/Receive All Folders
New
Delete
Respond
Quick Steps
Move
Tags
Find
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
Author: Nicolas Joly
Hello from Word!
Filter applied
Connected
10%
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

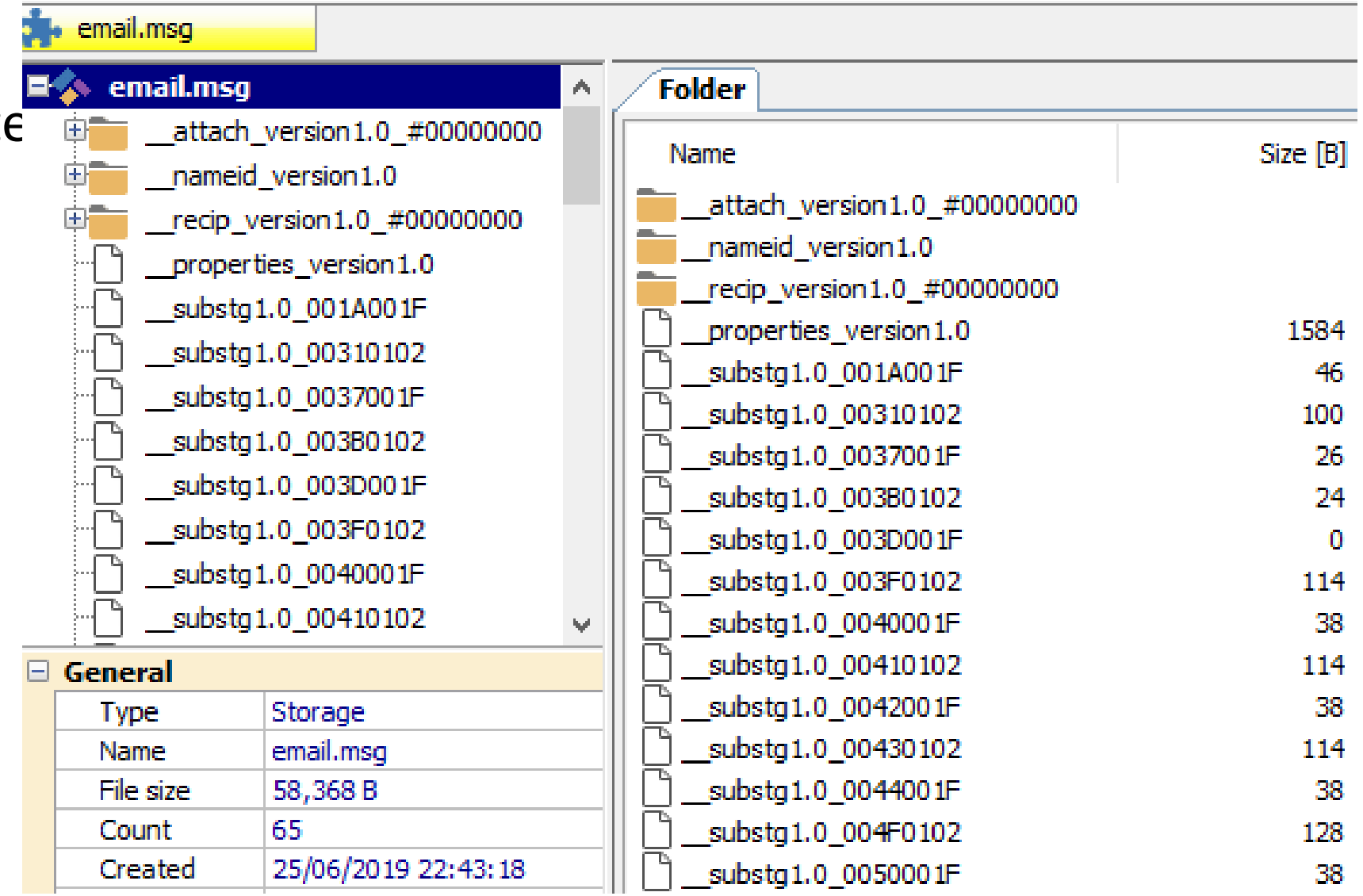
TNEF / .MSG format

- 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



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:

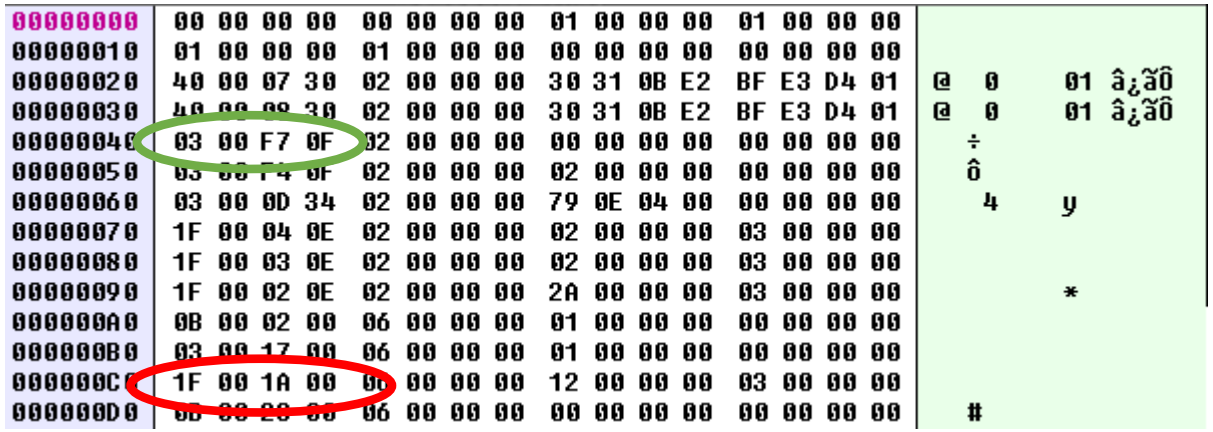
Name	Other Names	Tag	Type	Value	Value (alternate view)
PR_ICON_INDEX	PidTagIconIndex, ptagIconIndex	0x10800003	PT_LONG	1282	0x502
PR_IMPORTANCE	PidTagImportance, ptagImportance	0x00170003	PT_LONG	1	0x1
PR_INTERNET_CPID	PidTagInternetCodepage, ptagInt...	0x3FDE0003	PT_LONG	28591	0x6FAF
PR_LAST_MODIFICATION_TIME	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...	.:.ïdT¬ D³íLc\...
PR_MDB_PROVIDER	PidTagStoreProvider	0x34140102	PT_BINARY	cb: 16 lpb: 5494A1C0297F101BA58...	T.¡À)▯..¥...+*%.
PR_MESSAGE_ATTACHMENTS	PidTagMessageAttachments, pta...	0x0E13000D	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

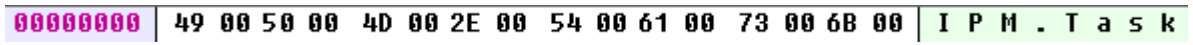
MAPI properties, TNEF and .MSG?

- 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



Arrays, strings or other objects are defined in their own streams. For example the message class property is defined in __substg1.0_001A001F:

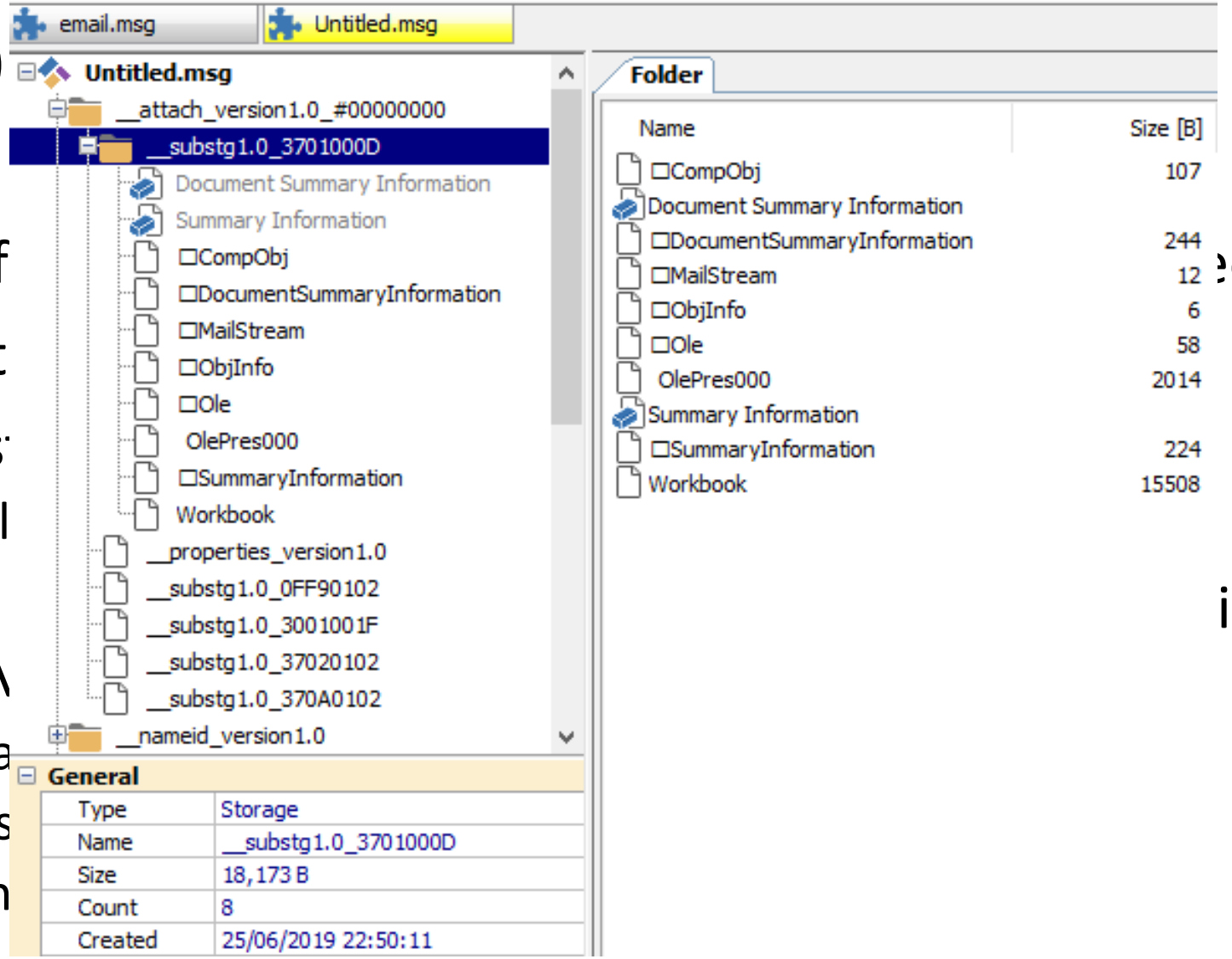


OLE objects in an email, really?

- 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()

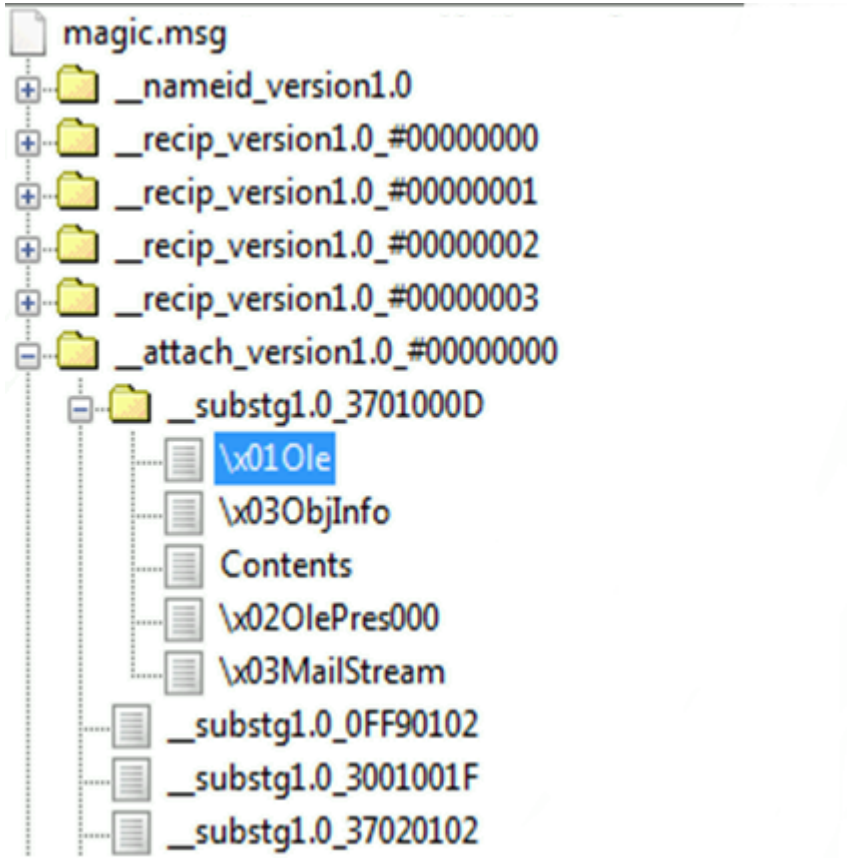
O

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



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.

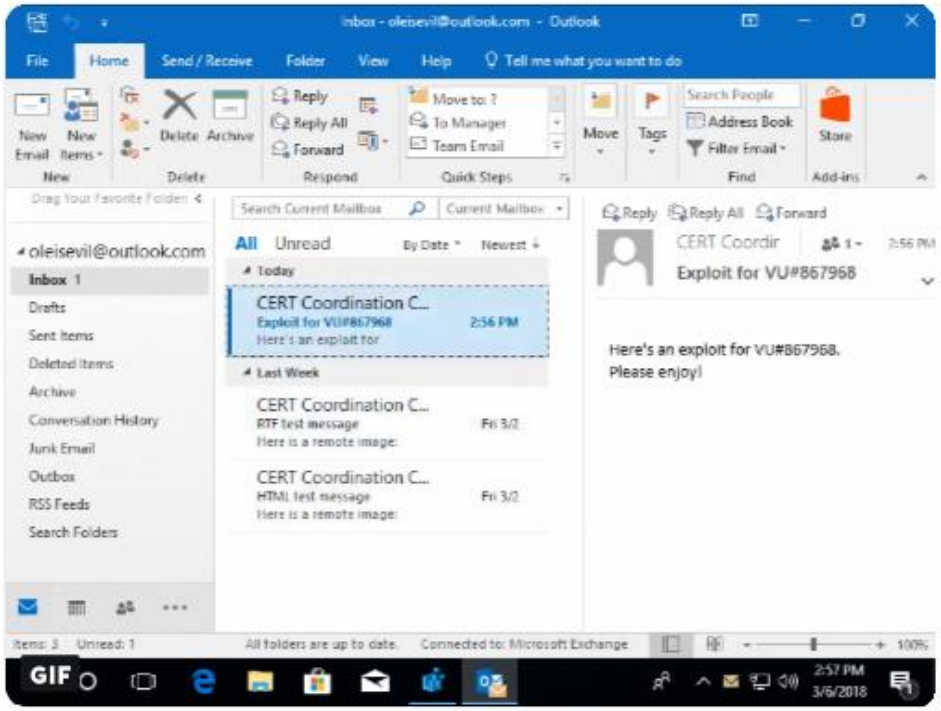
```
1627       if ((error =  StRead (pstm, &cb, sizeof(DWORD))) != NOERROR)
1628           return error;
1629
1630       if (cb == NULL)
1631           return NOERROR;
1632
1633       return OleLoadFromStream (pstm, IID_IMoniker, (LPLPVOID) ppmk);
1634   }
```

Example: FileMoniker, CVE-2018-0950

Will Dormann
@wdormann

Follow

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

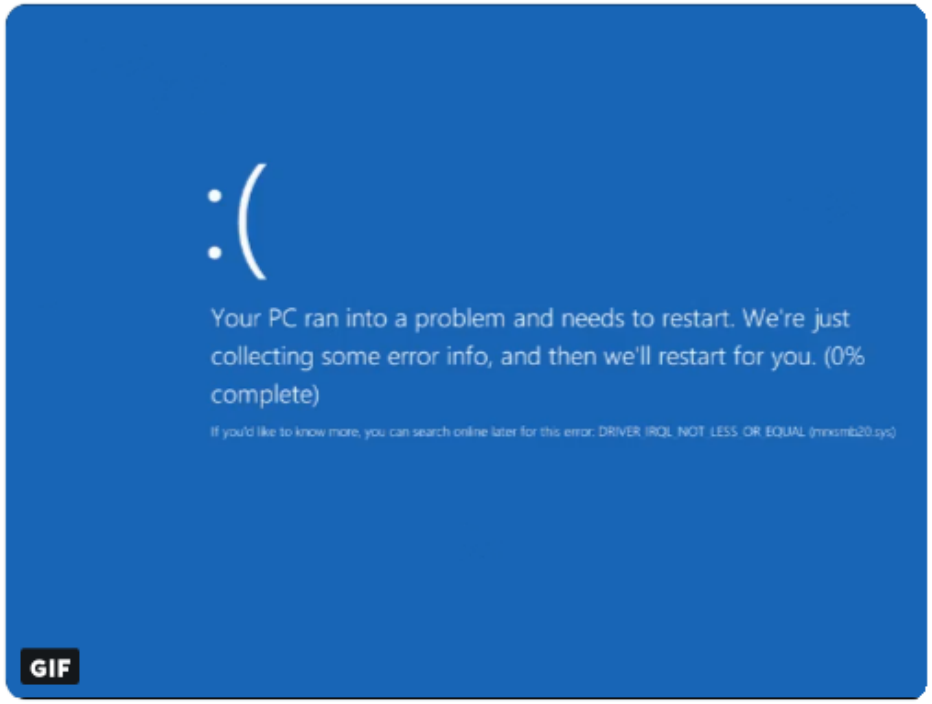


10:31 am - 10 Apr 2018

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!IStream_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:

OBJREF

IPersistStreamInit::Load

Flash?

CoUnmarshalInterface

MSVIDCTL – BDATuner.Component Types

VB 0day

XML Feed Moniker

IPersistStreamInit::Load

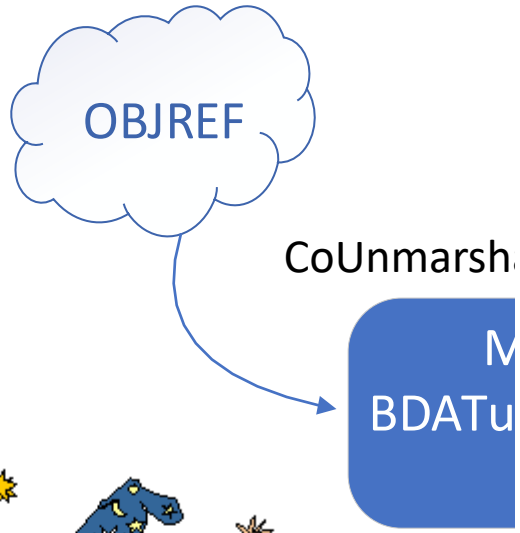
Load a VB Script

Initialize with HTML data

Calc with a...

OBJREF – Building the exploit chain

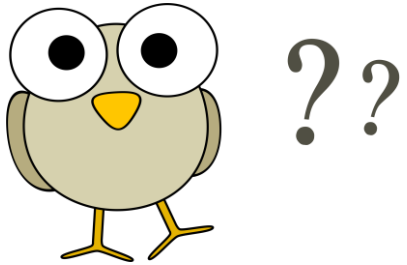
- Still far from calc:



```
388 STDMETHODIMP CComponentTypes::Load(LPSTREAM pStm) {
389     try {
390         LONG c;
391         DWORD cbSize = 0;
392         HRESULT hr = pStm->Read(&c, sizeof(c), &cbSize);
399
400         for (long count = 0; count < c; ++count) {
401             GUID2 g;
402             hr = pStm->Read(&g, sizeof(g), &cbSize);
403             if (FAILED(hr)) {
404                 return hr;
405             }
406             PQPersistStream ps;
407             hr = CoCreateInstance(g, NULL, CLSCTX_INPROC, IID_IPersistStreamInit, rei
408             if (FAILED(hr)) {
409                 return hr;
410             }
411             hr = ps->Load(pStm);
```

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

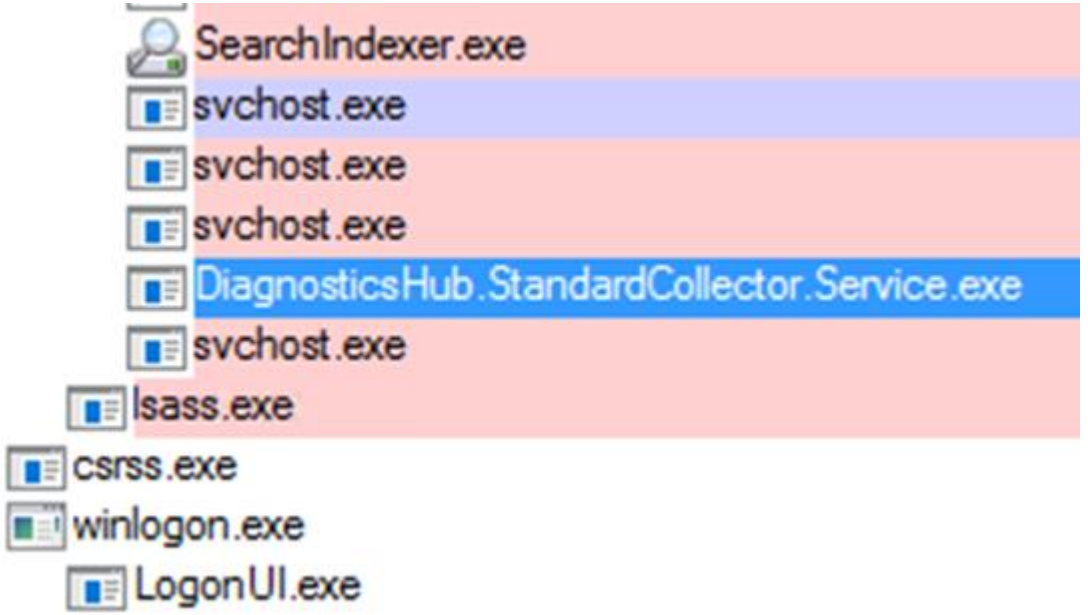
- They can contain bytes, integers, strings, all sorts of objects:
- Including VT_UNKNOWN objects
- Look at the logic in LPSAFEARRAY_Unmarshal
  - We can quickly reach another CoUnmarshalInterface
  - And replay the attack

```
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
```

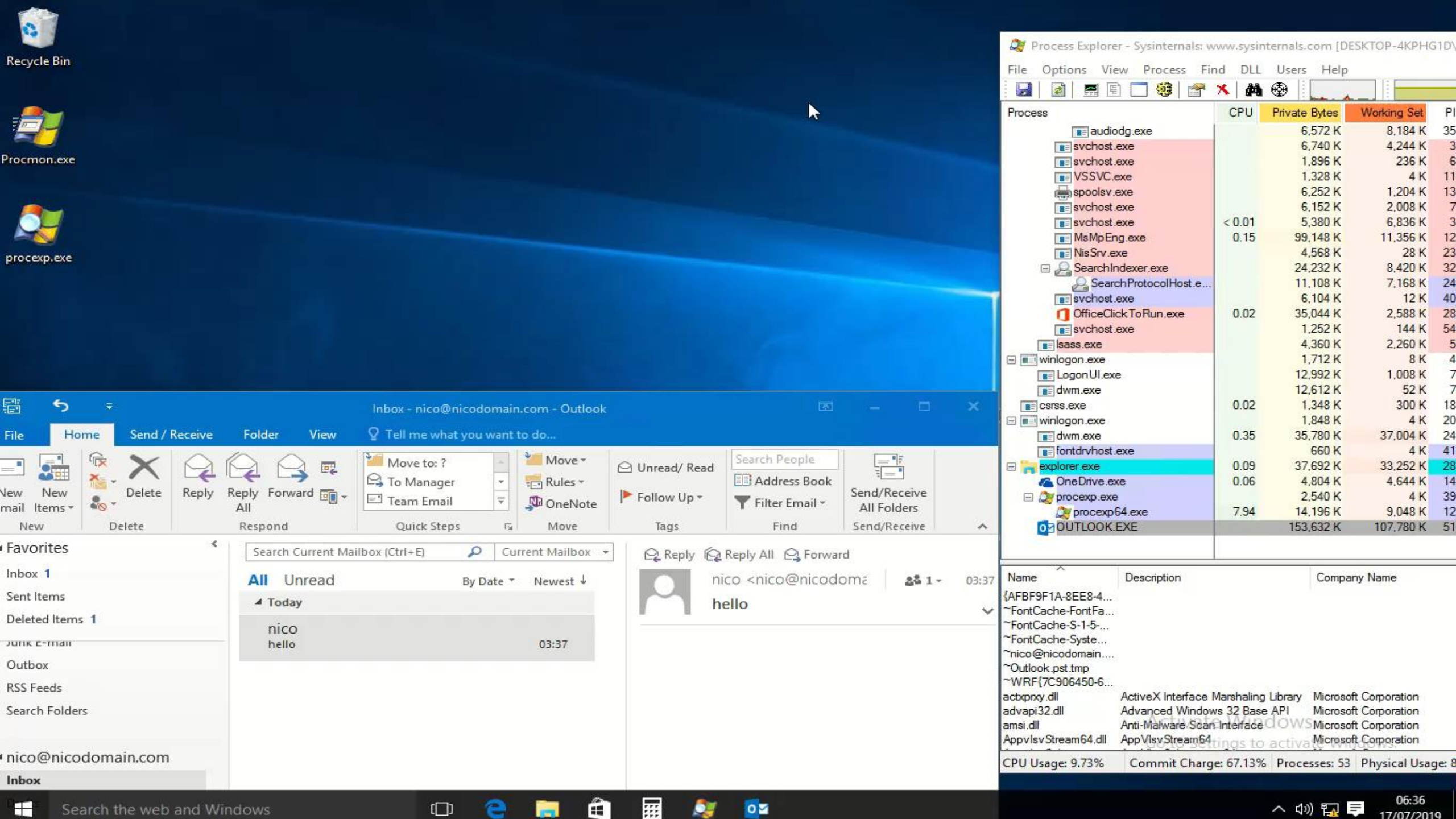
```
typedef  enum tagVARENUM
{
  VT_EMPTY = 0x0000,
  VT_NULL = 0x0001,
  VT_I2 = 0x0002,
  VT_I4 = 0x0003,
  VT_R4 = 0x0004,
  VT_R8 = 0x0005,
  VT_CY = 0x0006,
  VT_DATE = 0x0007,
  VT_BSTR = 0x0008,
  VT_DISPATCH = 0x0009,
  VT_ERROR = 0x000A,
  VT_BOOL = 0x000B,
  VT_VARIANT = 0x000C,
  VT_UNKNOWN = 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
            /// </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

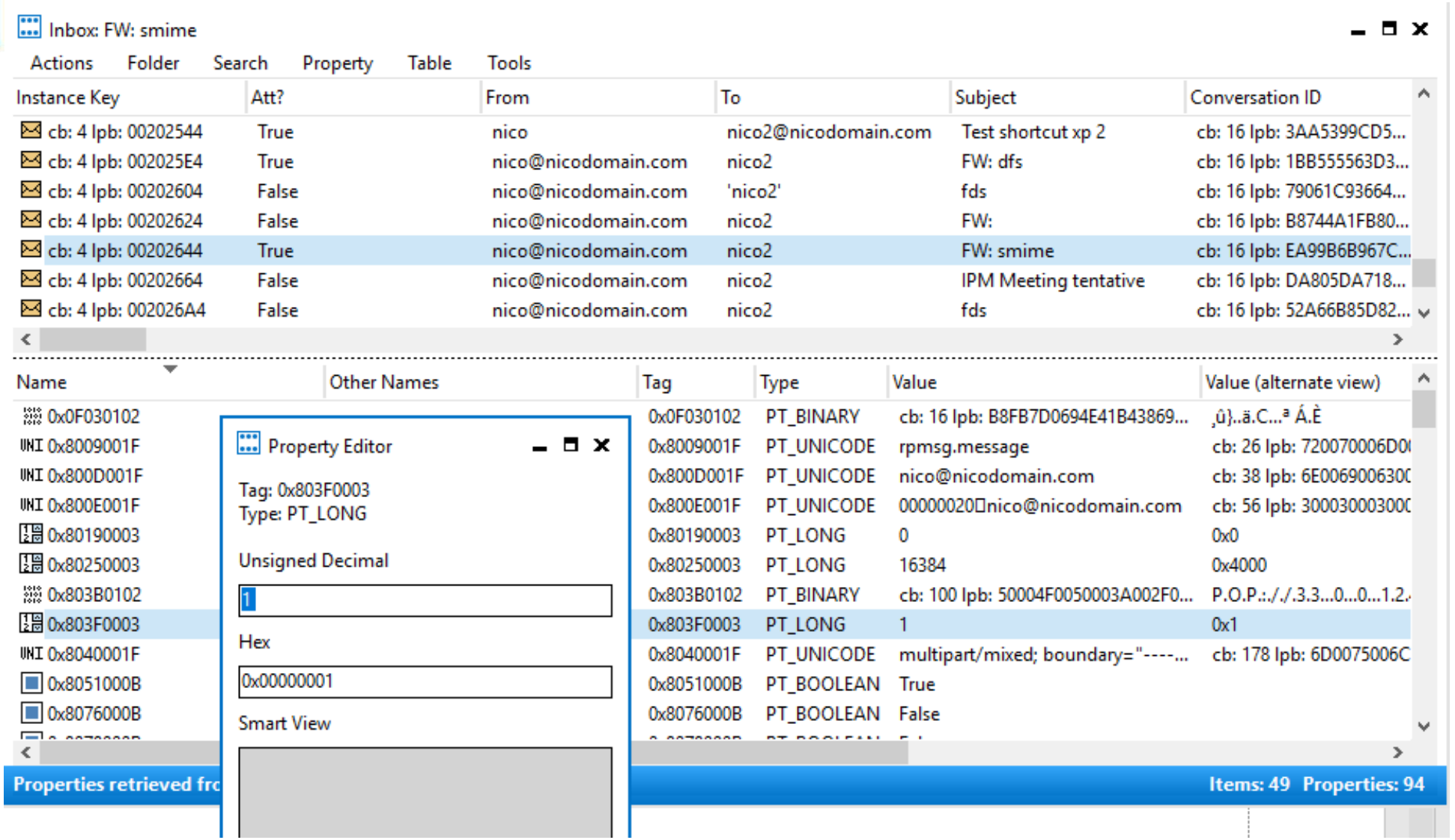

Recycle Bin
Procmon.exe
procexp.exe
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-4KPHG1D\
File Options View Process Find DLL Users Help
Process CPU Private Bytes Working Set
audiodg.exe 6,572 K 8,184 K
svchost.exe 6,740 K 4,244 K
svchost.exe 1,896 K 236 K
VSSVC.exe 1,328 K 4 K
spoolsv.exe 6,252 K 1,204 K
svchost.exe 6,152 K 2,008 K
svchost.exe < 0.01 5,380 K 6,836 K
MsMpEng.exe 0.15 99,148 K 11,356 K
NisSrv.exe 4,568 K 28 K
SearchIndexer.exe 24,232 K 8,420 K
SearchProtocolHost.e... 11,108 K 7,168 K
svchost.exe 6,104 K 12 K
OfficeClickToRun.exe 0.02 35,044 K 2,588 K
svchost.exe 1,252 K 144 K
lsass.exe 4,360 K 2,260 K
winlogon.exe 1,712 K 8 K
LogonUI.exe 12,992 K 1,008 K
dwm.exe 12,612 K 52 K
csrss.exe 0.02 1,348 K 300 K
winlogon.exe 1,848 K 4 K
dwm.exe 0.35 35,780 K 37,004 K
fontdrvhost.exe 660 K 4 K
explorer.exe 0.09 37,692 K 33,252 K
OneDrive.exe 0.06 4,804 K 4,644 K
procexp.exe 2,540 K 4 K
procexp64.exe 7.94 14,196 K 9,048 K
OUTLOOK.EXE 153,632 K 107,780 K
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
Inbox - nico@nicodomain.com - Outlook
File Home Send / Receive Folder View Tell me what you want to do...
New mail New Items Delete Reply Reply All Forward
New Delete Respond
Move to: ? To Manager Team Email
Quick Steps
Move Rules OneNote
Move
Unread/ Read Follow Up
Tags
Search People Address Book Filter Email
Find
Send/Receive All Folders
Send/Receive
Favorites
Inbox 1
Sent Items
Deleted Items 1
Outbox
RSS Feeds
Search Folders
nico@nicodomain.com
Inbox
Search Current Mailbox (Ctrl+E) Current Mailbox
All Unread By Date Newest
Today
nico
hello
03:37
Reply Reply All Forward
nico <nico@nicodoma
1
03:37
hello
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
06:36
17/07/2019

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



exRPC and MAPI properties

- Loaded by MSExchangeDelivery.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

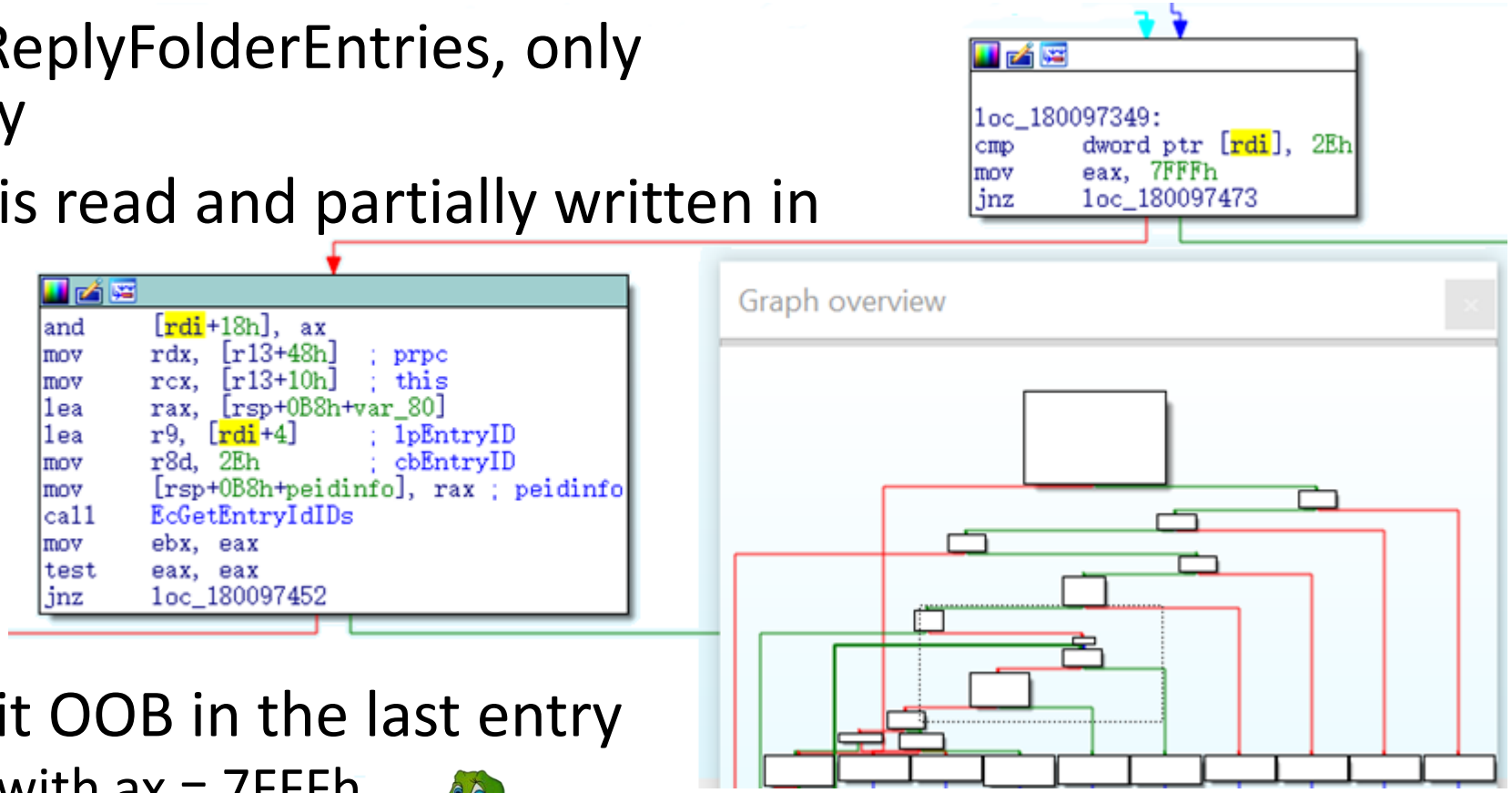
- Called for pid ptagConflictEntryId, only accepts a byte array
- No checks on the property type
- Supported variants are stored on 0x18 bytes on 64-bit
  - Scalars at offset +8
  - Pointers at +0x10
- Probably a DoS at worst

```
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 ;
```

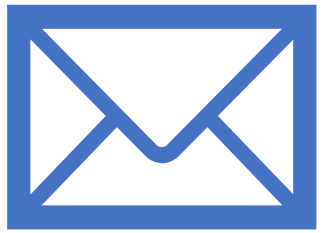
```
case PROP_ID(ptagConflictEntryId):
    BOOL    fLongTerm = fFalse;
    BOOL    fMessage = fFalse;
    BOOL    fWacky = fFalse;
    LTID    *pltidFolder = NULL;
    LTID    *pltidMessage = NULL;
    GID     gidFolder = { 0 };
    GID     gidMessage = { 0 };

    // 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



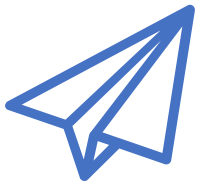
- We can alter one bit OOB in the last entry
  - And [rdi+18h], ax with ax = 7FFFh
  - So what do you think I did?
    - Nothing, was too hard ☹



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://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://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://github.com/stephenegriffin/mfcmapi
- 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
- interoplib
- CVE-2017-8506, demo on slide3

Thanks all!

@n_joly