Exchange Forensics for Incident Response

OWEN O'CONNOR

What we'll cover today

- Basics of Exchange
- Understanding and exploring Exchange mailboxes
- Exploring Exchange mailboxes
- Scenario walkthrough: external Exchange compromise

Basics of Microsoft Exchange

- Exchange is effectively a distributed database which stores email **as well as other content types**, accessed via a wide range of clients
- Exchange is the dominant enterprise mail system: in most industries it has effectively no competition for **internally-hosted** mail
- Exchange comes in two forms: **Exchange Server** and **Exchange Online**
- Despite the centrality of email evidence, Exchange forensics is an underdeveloped area, ripe for exploring

Disclaimers

I do not work for Microsoft or represent them in any way (nor have I ever)

I have no access to Microsoft-confidential information: this talk is based on my direct own experience and on public documentation

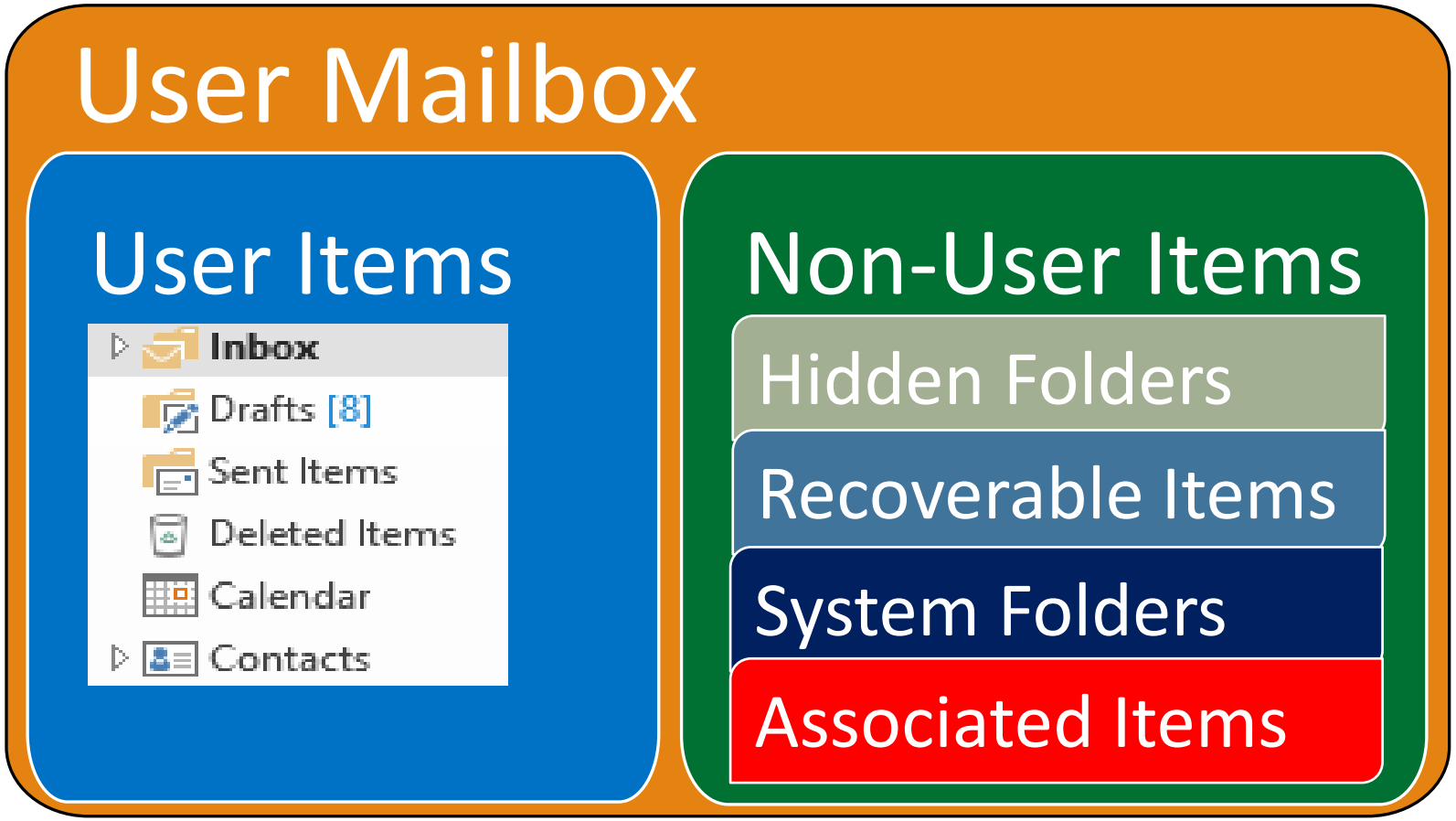
“Office 365” and other product names are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries

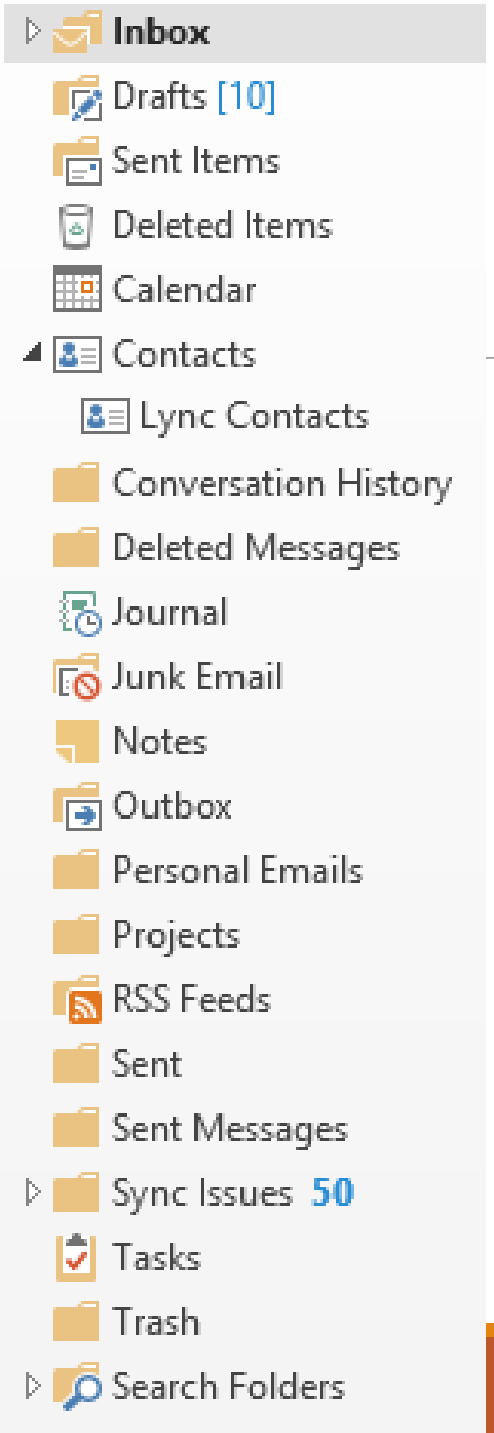
Inside an Exchange mailbox

Understanding Exchange mailboxes

Many practitioners, even very experienced ones, misunderstand the structure of an Exchange mailbox

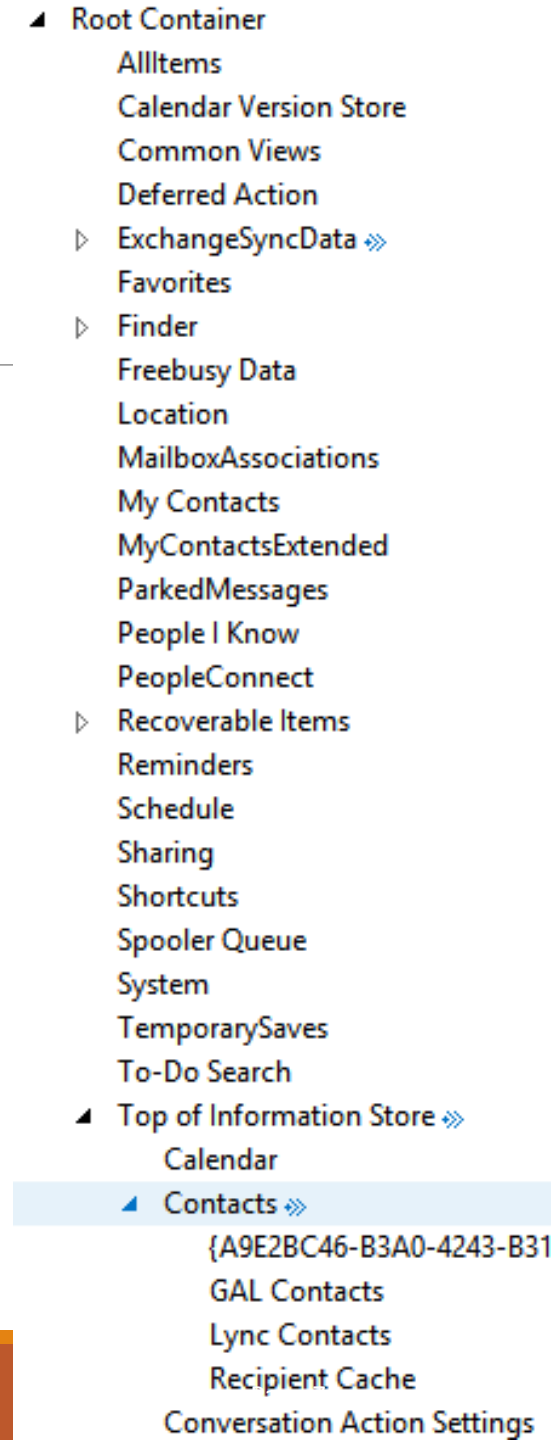
Before looking at Exchange forensics we must throw out “the Outlook view” of what’s inside a mailbox





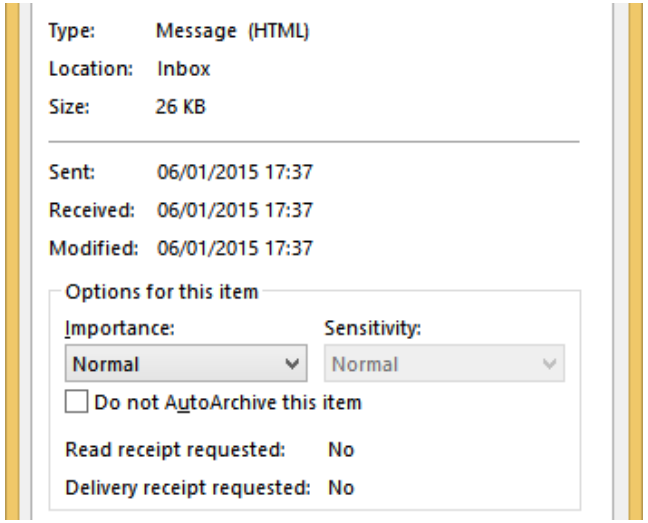
Don’t believe Outlook!

Outlook shows a hugely **simplified, misleading** view of mailbox structure



Understanding Exchange Mailboxes

Outlook also over-simplifies metadata, typically showing less than 10% of the available metadata for an email item



Finally, Outlook hides an entire class of items which often store valuable data: “Folder Associated Items” or FAIs

Tools for “whole mailbox” forensics

Using Outlook to examine mailboxes is like doing disk forensics via Windows Explorer – we need different tools to look deeper

“**MFCMAPI**” is a free tool written by Stephen Griffin from Microsoft’s Exchange team (https://mfcmapi.codeplex.com/)

MFCMAPI lets us explore the internal structure of Exchange mailboxes, including the system area and Folder Associated Items

A companion tool, “**MrMAPI**”, allows basic mailbox interaction from the command-line including exporting mailbox content

Before starting to use MFCMAPI

Before we look at MFCMAPI, 2 important warnings

1. MFCMAPI is immensely powerful and has **few "safety features"**: it is easy to accidentally delete data or render a mailbox unusable

   — Think of it like Regedit: the dangerous functions are typically pretty obvious but an accidental click could have serious consequences

2. MFCMAPI is **not designed as a forensic tool** and needs to be used with care in investigations

   — MFCMAPI is great for exploring mailboxes and researching artefacts, but standard principles apply (e.g., distinguish raw data from interpreted, validate specific findings via other tools or methods)

MFCMAPI WALKTHROUGH SLIDES UNAVAILABLE

MrMAPI: a companion tool to MFCMAPI

Once you have located an artefact via MFCMAPI, MrMAPI can often be used to export it, including across multiple mailboxes

Key Parameters

- **`-Online`** (bypass cache)
- **`-M`** (“try harder” to retrieve property values)
- **`-Profile <profile>`** (specifies a profile)
- **`-Folder #<store number>\...`** (point to other store or mailbox)

Useful Operations

- **`-Contents [-MessageClass <.>]`**
- **`-HiddenContents [-List] [-MSG]`**
- **`-ChildFolders`**
- **`-Folder`**
- **`-Size`**

Security incidents involving Exchange

Exchange as a target: “Fin4”

In late 2014 FireEye / Mandiant published details of an actor they labelled “Fin4”

- https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf

Fin4 targeted companies involved in non-public M&A discussions, including acquirers, acquirees and advisors

FireEye noted relatively sophisticated “soft” techniques (e.g., well-tailored phishing mails) but aspects of the subsequent exploitation were quite basic

“Fin4” actor: Exchange-related actions

Fin4 is notable for their actions around Exchange

- Targeted phishing mails reached users via corporate Exchange servers
- Fake login pages for the Exchange web interface ("Outlook Web App") harvested Exchange login credentials
- Mailboxes were accessed externally, exploiting the fact that Outlook Web App is often publicly exposed
- Compromised mailboxes were mined for additional targets and existing email threads were “hijacked”
- Compromised mailboxes had inbox rules created to silently delete emails which might indicate detection of Fin4 activity (e.g., IT alerts)

Intrusion scenario walkthrough

Intrusion scenario

To illustrate a few in-mailbox artefacts we'll use a scenario similar to Fin4

Ossino Inc is a growing biotech company with 500 staff in 3 offices

- Ossino uses Exchange Online for email, has a growing public profile
- Ossino expects news on a key corporate event to emerge in January 2016

Our attacker is targeting Ossino in order to:

1. Establish access to Ossino's email systems prior to the significant event
2. Obtain confidential background information about the key event
3. Monitor Ossino's email traffic to learn details as early as possible

LIMITED INTRUSION WALKTHROUGH SLIDES AVAILABLE

Responder tasking

After learning of the breach, Ossino need to investigate several questions:

1. How did the initial compromise occur?
2. Which mailboxes were targeted for access?
3. What specifically was the attacker seeking?
4. What historical information was compromised?
5. Did the attacker gain admin access and if so what else was done?
6. What needs to be done to contain and remediate the breach?

Initial responder actions

Ossino examined the key Exchange audit trails and learned that:

1. That mailbox access auditing is disabled by default and that this audit trail was disabled on all mailboxes
2. The “admin actions” log was empty and the retention period was set to 0 days, effectively disabling this audit trail
3. Message tracking logs **were** available

Which mailboxes were first compromised?

Message tracking logs show a series of suspicious inbound emails in a short period of time but platform logs are insufficient to tell which mailboxes were actually compromised

OWA artefacts can help indicate **whether OWA has been** used with a mailbox, when it was **first used** and (often) when it was **last used**

1. Root FAI “IPM.Configuration.Aggregated.OwaUserConfiguration”
2. Root FAI “IPM.Configuration.OWA.ViewStateConfiguration”
3. Root FAI “IPM.Configuration.OWA.UserOptions”

Using MrMAPI to access OWA artefacts

Listing FAIs at the mailbox root:

```
mrmapi -Online -Profile Collection1 -HiddenContents
-Folder @ -List
```

- “-Online” bypasses the cache
- “-Profile” selects a specific MAPI profile (here named “Collection1”)
- The pseudo-folder “@” selects the true mailbox root (top of mailbox)

Using MrMAPI to access OWA artefacts

Collecting any root FAIs with a specific message class:

```
mrmapi -On -Pr Collection1 -HiddenContents -Folder @
-MessageClass IPM.Configuration.OWA.UserOptions
```

- “-HiddenContents” without “–List” outputs items as XML
- “-MessageClass” filters collection by item type
- “-Output” specifies a folder to receive the XML properties in addition to a set of folder properties and an index file (both XML)
- Creation and modification timestamps reveal OWA usage patterns

Using MrMAPI to access OWA artefacts

If you configure a mailbox to access multiple mailboxes, MrMAPI can collect from specific “stores”, or be scripted to loop through a set

```
mrmapi -On -H -Folder #9\@ -Output .\Out1
```

- The “-Folder” option with the # prefix accepts either a store number or store entry ID
- Use “-Store” to have MrMAPI display the available stores for a particular profile

What was the attacker seeking?

Ossino now knows that a number of mailboxes were accessed but has no idea what the attacker was seeking

Looking more deeply at one of our earlier OWA artefacts might help

`mrmapi -On -H -F @ -Me IPM.Configuration.OWA.ViewStateConfiguration`

Property **0x7C070102** is an XML structure with a property of "**SearchHistory**" an ordered list of previous **search terms used in OWA**

Note: this artefact is not always present even when OWA searches have been run and can be difficult to reproduce, for reasons which are unclear

What historical information was compromised?

Ossino needs to know more about what data the attacker viewed

In at least Exchange Online, the "**IPM.Activity**" artefact can help

```
mrmapi -On -H -F "Recoverable Items\Purges" -Me IPM.Activity
```

- Property **0x7C080102** in each item contains XML data representing "activity" for a particular "session" – e.g., an OWA or Outlook session
- Alongside **start and stop times** are MAPI "**entry IDs**"
- MrMAPI and MFCMAPI will accept entry IDs to view / export an item

Did the attacker gain admin access?

Ossino has seen indications of attacker interest in IT staff mailboxes

Has the attacker gained Exchange admin access?

`mrmapi -On -H -F @ -Me IPM.Configuration.Suite.Storage`

Property **0x7C070102** contains XML data for the web “app bar” including a value for “**LastAccessedDateAdminPortal**”

Timestamps on and within this artefact can also highlight newly elevated accounts since elevation will add the web admin app

What else was done?

In Exchange Online it can be difficult to **retrieve the last logon time** directly (e.g., to detect hijacking of previously dormant mailboxes)

An inbox FAI **“IPM.Configuration.UserProfile”** contains XML data in property **0x7C070102** which included the value “**LastLogonTime**”

What else was done?

ActiveSync synchronisation provides a powerful way to monitor compromised mailboxes

Exchange stores ActiveSync data in system folders at **\ExchangeSyncData**

Sub-folders are names with **ActiveSync device IDs** which typically indicate the device type or app, often including a unique device ID such as an iOS device serial number

Data within this structure, including item and folder timestamps, can reveal newly-added devices or indicate the last sync time

EAS search queries are represented by search folders under “\Finder”

Closing

Summing up

1. Re-think the importance and value of Exchange data (attackers are already doing so!)
2. Don’t be misled by Outlook: the true content of an Exchange mailbox is very different
3. In Exchange investigations, in-mailbox artefacts are often more valuable than logs or other “traditional” sources of evidence
4. MFCMAPI and MrMAPI are very powerful: MFCMAPI for identifying and researching useful artefacts, MrMAPI for bulk collection
5. Learning more about Exchange will pay off for all types of forensics

Questions?

owen@owenoconnor.ie
www.exchangeforensics.org