Dragon Advance Tech

Microsoft 365 Forensics Playbook

Best Practices for Acquisition of Email boxes and Unified Audit Logs For Microsoft 365 (Exchange Online)

Version 1.1

Release date: June 2022

Frankie Li, Ken Ma and Eric Leung
ir@dragonadvancetech.com

Table of Contents

Introduction

Organizations are migrating their data and workloads to the cloud at rapid rates. According to IDC[1], "the total worldwide spending on cloud services, will surpass $1.3 trillion by 2025 while sustaining a compound annual growth rate of 16.9%". In another article, Gartner[2] "says the ongoing pandemic and the surge in digital services are making cloud the centerpiece of new digital experience ... [the projected] global cloud revenue for 2022 will show an increase of $66 billion to total $474 billion". In an Ermetic study funded by IDC[3], "98% of the organization experienced at least one cloud data breach in the past 18 months, compared to 79% in 2020". The survey further indicates "63% of all organizations had sensitive data exposed in the cloud and this number ballooned to 85% for companies with large cloud footprints. To guarding the gate, 85% of organizations, security budgets are on the rise".

Researchers have pointed out significant gaps and challenges in applying traditional digital forensics to the cloud paradigm. They defined evaluation criteria based on a survey methodology to allow users to evaluate future cloud forensic approaches. In this paper, we propose to collect "CSP-enabled logs" and/or "CSP-stored content" as "forensically sound" evidence from SaaS applications.

By adopting the similar principles described in the document called: "Best Practices for Acquiring Online Content" and "Best Practices for Digital Evidence Acquisition from Cloud Service Providers" from SWGDE[4]. We prepare this playbook to provide detailed procedures in acquiring the "best available" forensics evidence from Microsoft Exchange Online (or M365, Office 365).

The collected evidence, including the mailbox in "PST"[5] format and the "Unified Audit Logs" can help to rebuild the timeline or facilitate the reconstruction of criminal events, such as insider fraud (email box, takeover identity), phishing attacks (email body, takeover identity), spoofing attacks (email header), or business email compromise (email header & email body, compromised identity) cases.

[1] https://www.idc.com/getdoc.jsp?containerId=prUS48208321
[2] https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences
[3] https://l.ermetic.com/wp-idc-survey-results-2021
[4] https://www.swgde.org/documents/published
[5] https://www.systoolsgroup.com/forensics/outlook-pst/

Overview Approach

We believe that the mailboxes if PST format should contain the "best available information" for the fraud investigations, and the Unified Audited Logs should contain the "most relevance evidence" that can help the responders to investigate phishing, spoofing, and BEC attacks.

Microsoft 365 will keep the whole mailbox, including the deleted emails, in the cloud storage for a period of 30 days[6], even though the Microsoft 365 license has been removed from the suspects' accounts. In this case, the victim organization keeps the email accounts with active licenses even though the suspects left the organization. Microsoft Exchange

Online provides a feature called eDiscovery can allow properly authorized users to create a search[7] query[8] by making the mailbox into a state of "litigation hold[9]" to "export[10]" the whole mailbox, together with deleted or even purged emails. After the query is executed, eDiscovery features will allow eDiscovery users to "export[11]" or download the mailbox in "PST" format by using the Edge browser plugin[12], eDiscovery Export Tool.

As part of the SaaS service of Microsoft 365, Microsoft Exchange Online customers can use Microsoft PowerShell to download the Unified Audit Logs. The eDiscovery query also allows users to create a query to extract relevant emails from multiple mailboxes by using subject and email body contents by using regular expressions. If the customer subscribed the suitable licenses, such as Microsoft 365 E5 license, investigators can access the in-depth threat-related data from the tenant to implement proactive defense policies for threat hunting.

In this forensic playbook, we only take the standard approach to extract the mailbox, in PST format and download the Unified Audit Logs (UAL) to perform an investigation. Using the downloaded UAL, we uploaded it to our Splunk instance and created a BEC Dashboard (Appendix 3) for our investigations.

[6] https://docs.microsoft.com/en- us/microsoft-365/compliance/inactive-mailboxes-in-office-365
[7] https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content-in-core-ediscovery
[8] https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery
[9] https://docs.microsoft.com/en-us/microsoft-365/compliance/change-the-hold-duration-for-an-inactive-mailbox
[10] https://docs.microsoft.com/en-us/microsoft-365/compliance/export-content-in-core-ediscovery
[11] https://docs.microsoft.com/en-us/microsoft-365/compliance/export-a-content-search-report
[12] https://docs.microsoft.com/en-us/powershell/module/exchange/search-unifiedauditlog?view=exchange-ps

eDiscovery and Content Search

Electronic discovery, or eDiscovery, identifies and delivers electronic information that can be used as evidence in legal cases. eDiscovery tools could be used in Microsoft 365 to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams.

Mailboxes and sites could be searched in the same eDiscovery search, and the search results could be exported. Core eDiscovery cases could be used to identify, hold, and export content found in mailboxes and sites. If your organization has an Office 365 E5 or Microsoft 365 E5 subscription (or related E5 add-on subscriptions), you can further manage custodians and analyze content by using the feature-rich Advanced eDiscovery solution in Microsoft 365.[13]

This section will go through the steps of a best practice for conducting an eDiscovery investigation with a deep explanation.

eDiscovery Roles

There are two primary Roles in Microsoft 365 are “eDiscovery Manager” and “eDiscovery Administrator”, you have to assign the eDiscovery “Role” to a user, in order to have appropriate permission to use the eDiscovery tools.

- **eDiscovery Manager:**
  - Create and manage a case they created.
  - Add members to the case they created.
  - Perform content search, preview, and export search results, associated with a case.
- **eDiscovery Administrator:**
  - Perform the same content search and case management as eDiscovery Manager.
  - Access all cases data in the organization.
  - Manage any eDiscovery case.

Role assignment

Create an independent account for the eDiscovery Administrator in your organization

1. Login to Microsoft 365 compliance center (https://compliance.microsoft.com) with Global Administrator privilege.
2. Create a specific user account designated for eDiscovery management.
3. Configure the MFA for this specific user account.
4. Assign the “eDiscovery Administrator” role to this account.
   a. In the Microsoft 365 compliance center, select “Permissions” from the left pane.
   b. On the “Permissions & Roles” page, click the “Roles” link, under “Compliance center”.
   c. On the “Compliance center roles” page, search “eDiscovery Manager”.
   d. Click on the “eDiscovery Manager”, a flyout page will show on the right-hand side.
   e. Click the “Edit” link, adjacent to the “eDiscovery Administrator”.

[13] https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

f. On the new flyout page “Editing Choose eDiscovery Administrator”, click on the “Choose eDiscovery Administrator”.
g. Click the “Add” and select the newly created account, which is reserved for the eDiscovery Management.
h. Click “Done” and “Save” to confirm the role assignment.

P.S. This account is only used for the eDiscovery management, and shall not use this account to perform other unauthorized tasks.

5. (Optional) Create alert rules to monitor login and activities for this account.

Assign eDiscovery Manager to an account for case investigation

6. Create a user account designated for case investigation, if needed.
7. Verify the MFA is enabled for the user account.
8. Assign the “eDiscovery Manager” role to this account.
    a. In the Microsoft 365 compliance center, select “Permissions” from the left pane.
    b. On the “Permissions & Roles” page, click the “Roles” link, under “Compliance center”.
    c. On the “Compliance center roles” page, search “eDiscovery Manager”.
    d. Click on the “eDiscovery Manager”, a flyout page will show on the right-hand side.
    e. Click the “Edit” link, adjacent to the “eDiscovery Manager”.
    f. On the new flyout page “Editing Choose eDiscovery Manager”, click on the “Choose eDiscovery Manager”.
    g. Click the “Add” and select the account, which is assigned for the eDiscovery Case Investigation.
    h. Click “Done” and “Save” to confirm the role assignment.

Create an eDiscovery case

1. Login to Microsoft 365 compliance center (https://compliance.microsoft.com) with eDiscovery Manager privilege.
2. In the left navigation pane, click eDiscovery > Core under the “Solutions” section.
3. Click the “+ Create a case” and fill in the Case name and Description from the right flyout page, then click “Save”.

Reserving content in legal hold

Preserve content relevant to the investigation by placing a legal hold on the content locations in a case. This secures electronically stored information from inadvertent (or intentional) deletion during your investigation.

4. Click into the case that was just created.
5. Click the “+ Create” button under the Hold tab.
6. Type in a Name of the hold, which must be unique in your organization and click Next.
7. On the “Choose locations” page, toggle the “Exchange mailboxes” and click “Choose users, groups, or teams” to specify the mailboxes to place on hold.
8. Create a query-based hold using keywords or conditions.
9. Review and Submit the hold.

10. Check and ensure the status is turned from processing to On(Success).

Carrying out eDicovery content search

We can create multiple different searches under a case. In each content search, the search statistics can help us to refine a search query. Also, allow us to preview the search result quickly.

1. Click into the case that you want to perform a content search.
2. Under the Searches tab, click the "+ New Search"
3. Enter Name and Description
4. On the "Choose locations" page, toggle the "Exchange mailboxes" and click "Choose users, groups, or teams" to specify the scope.
5. Untick the Add AppContent for On-Premises Users
6. On the "Define your search conditions" page, type a keyword query and add conditions to the search query if necessary. If you leave the keyword box empty, all content located in the specified content locations is included in the search results.
7. Review the setting and Click Submit

Export of Mailbox in PST

This section will go through the steps of best practices for exporting mailbox in PST, following the forensics principle.

1. Selecting the search that needs to be exported, go into eDiscovery > Core > Searches > the search needs to be exported.
2. Configure export options, Click Actions > Export results
   - Export results are exporting the search result
   - Export reports are exporting the search statistics
3. Choose All items, including ones that have unrecognized format, are encrypted, or weren't indexed for other reasons
4. It is recommended to use this option for easy management, Choose *One PST file containing all messages in a single folder*
5. It is recommended to export everything to serve forensics purposes, Untick *Enable de-duplication for Exchange content*
6. Click *Export* A
7. Click *Okay and X* to close
8. Click *Exports*
9. Click the export just created
10. Make sure using a Windows system and Microsoft Edge is used to perform the following procedures
11. Documentation of the Windows system is also needed. E.g., OS, Windows defender config, network config, etc.
12. Wait the *Status* turns from *Scheduling…* to *the export has completed.*
13. If the size is over 10 Gb, the Microsoft downloader will split the PST file into multiple files. Check out the size of the export file.
14. To avoid this, the upper limit needs to be configured using the config attached. Please adjust the limit based on the size of the file that needs to be exported.
15. https://github.com/EricLeungDATC/MicrosoftForensicsAssets

For the example code, it sets to 20Gb.
Please save the code into .reg and run it.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\Client\eDiscovery\ExportTool]
"PstSizeLimitInBytes"="21474836480"
```

16. Click *Copy to clipboard* under *Export key*
17. Click *Download results*
18. Click *Open*, then click *Install,* a .NET application to download the file by Microsoft downloader
19. Paste the Export key that is copied before and choose the download location.
20. Click *Start*
21. Check if all the status have ticks, to confirm the export is successful
22. The MD5 of the PST files export by different time is different.
    However, by matching the docID in the manifest.xml of each email in 2 PST files, the integrity of the 2 PST files can be proven
23. Verify the integrity by the code in appendix 1

Unified Audit Logs

This section serves as a guide on using PowerShell to download the Office 365 unified audit log.

TOOLS AND RESOURCES:

- PowerShell
- Exchange-Online add-on for PowerShell

STEP BY STEP PROCEDURES:

PowerShell script for downloading UAL [Appendix 2]

1. Configure the **output folder name**, **days to check**.
2. Now the code is ready to run and download numerous of .csv unified audit log.
3. Open PowerShell with admin right
   PS C:\> cd path\to\the\code
   PS path\to\the\code > & '.\code.ps1'
   a. If Security warning regarding running code from the internet appeared, reply with R, which is "Run once".
   b. If Error regarding "The term 'Connect-ExchangeOnline' is not recognized' appeared,
      i. Install PowerShellGet 2.0 with following command,
         PS C:\> Install-Module PowerShellGet -Force
      ii. Reply Y to install and import the NuGet provider
      iii. Close and open PowerShell with admin right
      iv. Install Exchange Online PowerShell V2 Module
         PS C:\> Install-Module -Name ExchangeOnlineManagement
      v. Reply Y to install the module
4. Log in to your Microsoft account
5. The log will be downloaded as a CSV file named by the date and time with corresponding hashes in "hash.txt" in the 'Output' folder, in this case, it is 'UnifiedAuditLog-[CompanyName]-[date]'.
6. Please be noted the md5 hashes will be created for later integrity proving purposes.

Reference:

Modify from:
https://github.com/cyberisltd/Office-365-Tools/blob/master/unifiedlogsearch.ps1
https://docs.microsoft.com/en-us/powershell/exchange/exchange-online/exchange-online-powershell-v2/exchange-online-powershell-v2
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/search-unifiedauditlog
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance
Update from:
https://www.easy365manager.com/office-365-forensics-using-powershell-and-search-unifiedauditlog/
https://github.com/counteractive/Get-UnifiedAuditLog
https://github.com/counteractive/Get-UnifiedAuditLog/blob/master/Get-UnifiedAuditLog.psm1

Appendix

1. PST Download Verification Scripts

```
import sys
from xml.dom import minidom

if len(sys.argv)!=3:
    print("usage: python compare2.py file1.xml file2.xml")
else:
    file1 = minidom.parse(sys.argv[1])
    print("loaded " + sys.argv[1])
    file2 = minidom.parse(sys.argv[2])
    print("loaded " + sys.argv[2])

    document1 = file1.getElementsByTagName('Document')
    print("got docsId in file1")
    document2 = file2.getElementsByTagName('Document')
    print("got docsId in file2")

    print("length of doc1: " + str(len(document1)))
    print("length of doc2: " + str(len(document2)))
    same = 0

    if len(document1) == len(document2):
        for elem1 in document1:
            #print(elem1.attributes['DocID'].value)
            found = False
            for elem2 in document2:
                if elem1.attributes['DocID'].value == elem2.attributes['DocID'].value:
                    #print(elem1.attributes['DocID'].value + " is equal " +
elem2.attributes['DocID'].value +"\n")
                    same += 1
                    if same % 500 == 0:
                        print("Match amount: " + str(same))
                    found = True
                    break
            if found == False:
                print("they are not the same as cannot find a file1 docID in file2")
                break
    else:
        print("they are not the same as the number of the docID are different")

    if same == len(document1):
        print("these docs are the same")
    else:
        print("they are not the same")
```

2. UAL download PowerShell script

```
### Microsoft 365 Audit Logs Downloader
    # =============== CHANGE THESE =============== #
    $days = 1 # days to check
    $hoursPerBatch = 12  # Download 12 hours at a time, until the start date/time is reached
    $currentDate = Get-Date
    $OutputFolder = "UnifiedAuditLog_"+$tenant+"_"+$currentDate.ToString('yyyyMMdd')
    # ============================================ #

    # Microsoft 365 Login with MFA Enabled
    $Session = Connect-ExchangeOnline -UserPrincipalName $upn -ShowProgress $false

    # Set Current Date 12:00:00 am as $EndDate and set $StartDate - days to check
    $ErrorActionPreference = "Stop"
    $EndDate = $currentDate.Date.ToUniversalTime()
    $InitialDate = $EndDate.Date.AddDays(-$days)

    If(!(Test-Path $OutputFolder)) {
          New-Item -ItemType Directory -Force -Path $OutputFolder
    }

    "Window is from: $InitialDate -> $EndDate"
    do {
        # Download 12 hours at a time, until the start date/time is reached
        $StartDate = $EndDate.AddHours(-$hoursPerBatch)
        "Running search for $StartDate -> $EndDate"
        do {
            $time = $EndDate
            # Search the defined date(s), SessionId + SessionCommand in combination with the loop
will return and append 5000 object per iteration until all objects are returned (maximum limit is
50k objects)
            do {
                try {
                    $auditOutput = Search-UnifiedAuditLog -StartDate $StartDate -EndDate $EndDate
-SessionId "$StartDate -> $EndDate" -SessionCommand ReturnLargeSet -ResultSize 5000
                    $errorvar = $false
                }
                catch {
                    $errorvar = $true
                    "An error occured. Trying again."
                }
            } while ($errorvar)
            if ($auditOutput) {
                "Results received (" + ($(Get-Date) - $time) + "), writing to file..."
                $filename = "$StartDate - $EndDate.csv".Replace(":",".").Replace("/","-")
                #$auditOutput | Select-Object -Property AuditData | ConvertTo-Csv -
NoTypeInformation | Select-Object -Skip 1 | % {$_ -replace '""','"'} | % {$_ -replace '^"','' -
replace '"$',''} | Add-Content -Path "$OutputFolder\$filename" -Encoding UTF8
                $auditOutput | Select-Object -ExpandProperty AuditData | Select-Object -Skip 1 |
Add-Content -Path "$OutputFolder\$filename" -Encoding UTF8
                #Write-Output $auditOutput
                Get-FileHash -Path "$OutputFolder\$filename" | Format-List >>
"$OutputFolder\FileHash.txt"
            }
        } while ($AuditOutput)
        $endDate = $EndDate.AddHours(-$hoursPerBatch)
    } while ($InitialDate -lt $StartDate)
```

3. BEC Dashboard – Screenshots