# Investigating targeted “payroll pirate” attacks affecting US universities | Microsoft Security Blog

By Microsoft Threat Intelligence

Published: 2025-10-09 · Archived: 2026-04-02 11:24:53 UTC

Microsoft Threat Intelligence has observed a financially motivated threat actor that we track as Storm-2657 compromising employee accounts to gain unauthorized access to employee profiles and divert salary payments to attacker-controlled accounts. These types of attacks have been dubbed “payroll pirate” by the industry. Storm-2657 is actively targeting a range of US-based organizations, particularly employees in sectors like higher education, to gain access to third-party human resources (HR) software as a service (SaaS) platforms like Workday.

In a campaign observed in the first half of 2025, we identified the actor specifically targeting Workday profiles. However, it’s important to note that any SaaS systems storing HR or payment and bank account information could be easily targeted with the same technique. These attacks don’t represent any vulnerability in the Workday platform or products, but rather financially motivated threat actors using sophisticated social engineering tactics and taking advantage of the complete lack of multifactor authentication (MFA) or lack of phishing-resistant MFA to compromise accounts. Workday has published guidance for their customers in their community, and we thank Workday for their partnership and support in helping to raise awareness on how to mitigate this threat.

Microsoft has identified and reached out to some of the affected customers to share tactics, techniques, and procedures (TTPs) and assist with mitigation efforts. In this blog, we present our analysis of Storm-2657’s recent campaign and the TTPs employed in attacks. We offer comprehensive guidance for investigation and remediation, including implementing phishing-resistant MFA to help block these attacks and protect user accounts. Additionally, we provide comprehensive detections and hunting queries to enable organizations to defend against this attack and disrupt threat actor activity.

## Analysis of the campaign

In the observed campaign, the threat actor gained initial access through phishing emails crafted to steal MFA codes using adversary-in-the-middle (AITM) phishing links. After obtaining MFA codes, the threat actor was able to gain unauthorized access to the victims’ Exchange Online and later hijacked and modified their Workday profiles.

After gaining access to compromised employee accounts, the threat actor created inbox rules to delete incoming warning notification emails from Workday, hiding the actor’s changes to the HR profiles. Storm-2657 then stealthily moved on to modify the employee’s salary payment configuration in their HR profile, thereby redirecting future salary payments to accounts under the actor’s control, causing financial harm to their victims. While the following example illustrates the attack flow as observed in Workday environments, it’s important to note that similar techniques could be leveraged against any payroll provider or SaaS platform.

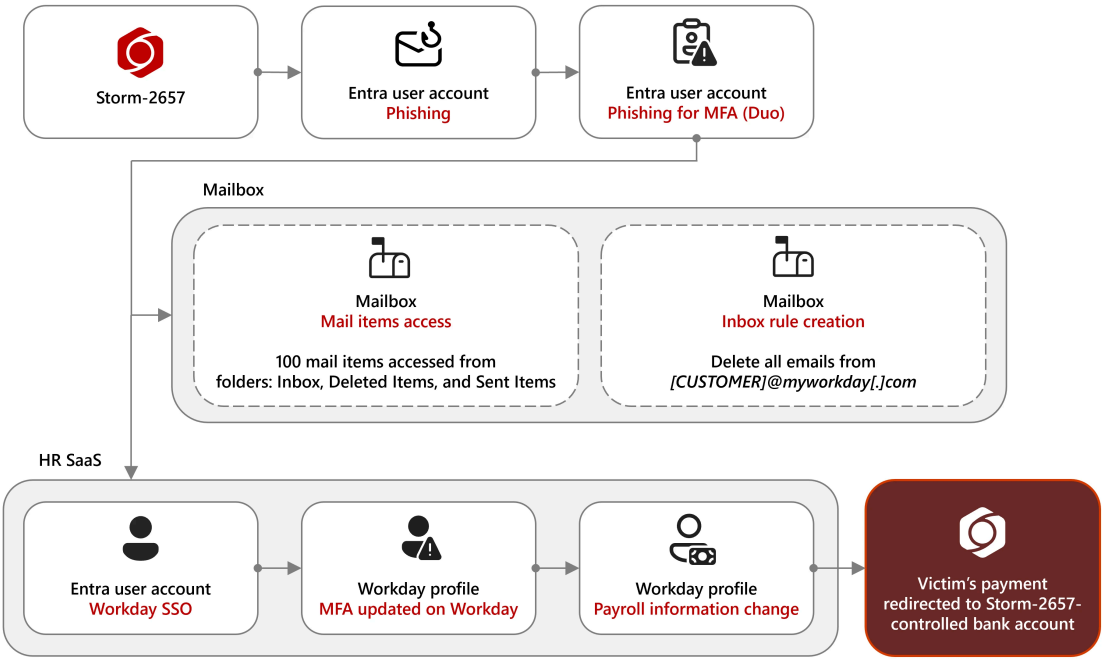


*Figure 1. Attack flow of threat actor activity in a real incident*

## Initial access

The threat actor used realistic phishing emails, targeting accounts at multiple universities, to harvest credentials. Since March 2025, we've observed 11 successfully compromised accounts at three universities that were used to send phishing emails to nearly 6,000 email accounts across 25 universities.

Some phishing emails contained Google Docs links, making detection challenging, as these are common in academic environments. In multiple instances, compromised accounts did not have MFA enabled. In other cases, users were tricked into disclosing MFA codes via AiTM phishing links distributed through email. Following the compromise of email accounts and the payroll modifications in Workday, the threat actor leveraged newly accessed accounts to distribute further phishing emails, both within the organization and externally to other universities.

The threat actor used several themes in their phishing emails. One common theme involved messages about illnesses or outbreaks on campus, suggesting that recipients might have been exposed. These emails included a link to a Google Docs page that then redirected to an attacker-controlled domain.

Some examples of the email subject lines are:

- COVID-Like Case Reported — Check Your Contact Status
- Confirmed Case of Communicable Illness
- Confirmed Illness

In one instance, a phishing email was sent to 500 individuals within a single organization, encouraging targets to check their illness exposure status. Approximately 10% of recipients reported the email as a suspected phishing attempt.

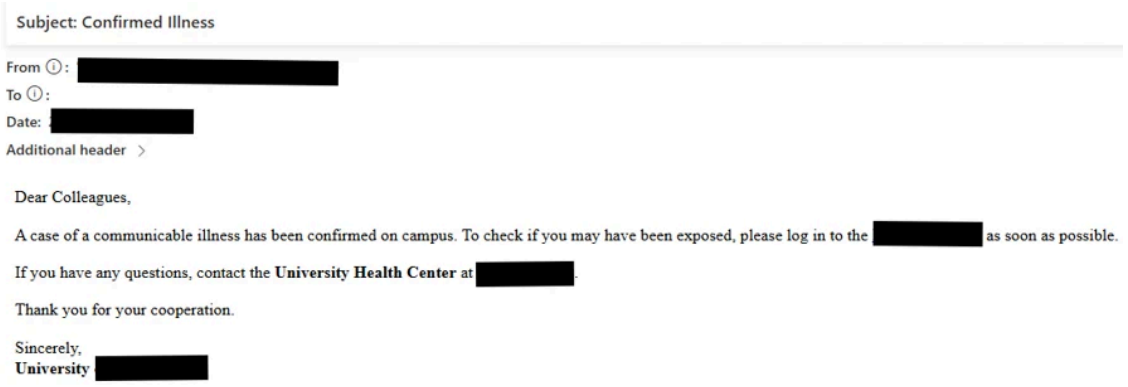


*Figure 2. Sample of a phishing email sent by the threat actor with illness exposure related theme*

The second theme involved reports of misconduct or actions by individuals within the faculty, with the goal of tricking recipients into checking the link to determine if they are mentioned in the report.

Some examples of the subject lines are:

- Faculty Compliance Notice – Classroom Misconduct Report
- Review Acknowledgment Requested – Faculty Misconduct Mention

The most recently identified theme involved phishing emails impersonating a legitimate university or an entity associated with a university. To make their messages appear convincing, Storm-2657 tailored the content based on the recipient's institution. Examples included messages that appear to be official communications from the university president, information about compensation and benefits, or documents shared by HR with recipients. Most of the time the subject line contained either the university name or the university's president name, further enhancing the email's legitimacy and appeal to the intended target.

Some examples of the subject lines are:

- Please find the document forwarded by the HR Department for your review
- [UNIVERSITY NAME] 2025 Compensation and Benefits Update
- A document authored by [UNIVERSITY PRESIDENT NAME] has been shared for your examination.

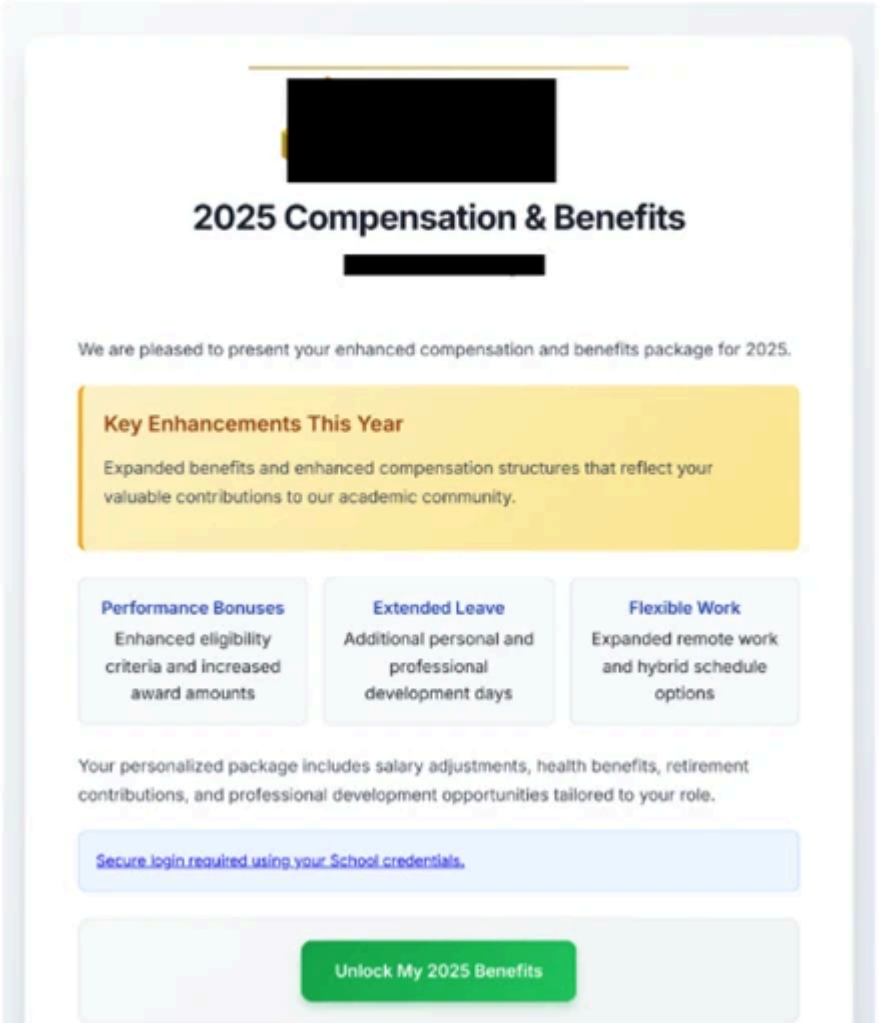


*Figure 3. Sample of a phishing email sent by the threat actor with HR related theme*

## Defense evasion

Following account compromise, the threat actor created a generic inbox rule to hide or delete any incoming warning notification emails from the organization's Workday email service. This rule ensured that the victim would not see the notification emails from Workday about the payroll changes made by the threat actor, thereby minimizing the likelihood of detection by the victim. In some cases, the threat actor might have attempted to stay under the radar and hide their traces from potential reviews by creating rule names solely using special characters or non-alphabetic symbols like "…." or "\'\'\'\'".

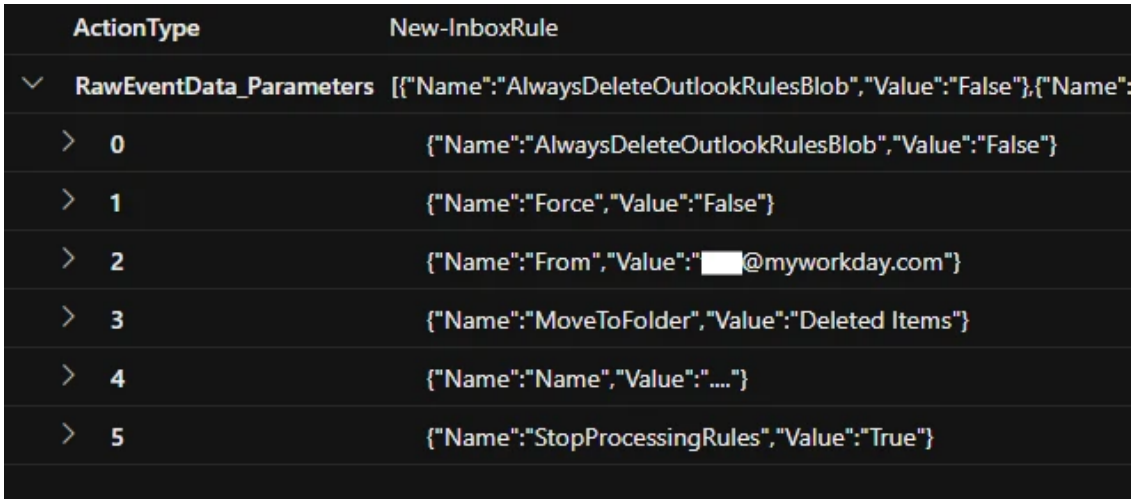


*Figure 4. An example of inbox rule creation to delete all incoming emails from Workday portal captured through Microsoft Defender for Cloud Apps*

## Persistence

In observed cases, the threat actor established persistence by enrolling their own phone numbers as MFA devices for victim accounts, either through Workday profiles or Duo MFA settings. By doing so, they bypassed the need for further MFA approval from the legitimate user, enabling continued access without detection.

## Impact

The threat actor subsequently accessed Workday through single sign-on (SSO) and changed the victim's payroll/bank account information.

With the Workday connector enabled in Microsoft Defender for Cloud Apps, analysts can efficiently investigate and identify attack traces by examining Workday logs and Defender-recorded actions. There are multiple indicators available to help pinpoint these changes. For example, one indicator from the Workday logs generated by such threat actor changes is an event called "Change My Account" or "Manage Payment Elections", depending on the type of modifications performed in the Workday application audit logs:

| Column | Value |
|---|---|
| ReportId | [redacted] |
| Timestamp | 2025-08-04T13:09:10.1720000Z |
| TenantId | |
| ActionType | Manage Payment Elections |
| Application | Workday |
| ApplicationId | [redacted] |
| AccountDisplayName | |
| AccountObjectId | |
| DeviceType | Desktop |
| OSPlatform | Windows 10 |
| IPAddress | |
| IsAnonymousProxy | false |
| CountryCode | US |
| City | Redmond |
| ISP | |
| UserAgent | [redacted] |
| IsAdminOperation | false |
| ActivityObjects | [{"Type":"Account","Role":"Actor","Name":"name","Id":"id",[redacted]"ApplicationInstance":2 |
| AdditionalFields | {"IsSatelliteProvider":false} |

*Figure 5. Example of payment modification audit log as captured through Microsoft Defender for Cloud Apps*

These payroll modifications are frequently accompanied by notification emails informing users that payroll or bank details have been changed or updated. As previously discussed, threat actors might attempt to eliminate these messages either through manual deletion or by establishing inbox rules. These deletions can be identified by monitoring Exchange Online events such as *SoftDelete*, *HardDelete*, and *MoveToDeletedItems*. The subjects of these emails typically contain the following terms:

- “Payment Elections”
- “Payment Election”
- “Direct Deposit”

Microsoft Defender for Cloud Apps correlates signals from both Microsoft Exchange Online (first-party SaaS application) and Workday (third-party SaaS application), enabling thorough detection of suspicious activities that span multiple systems, as seen in the image below. Only by correlating first party and third-party signals is it possible to detect this activity spawning across multiple systems.

| Timestamp | AuditSource | Application | ActionType | AccountObjectId | AccountDisplayName | IPAddress | ISP | CountryCode | UncommonForUser |
|---|---|---|---|---|---|---|---|---|---|
| Aug 14, 2025 6:14:... | Defender for Cloud Apps ... | Microsoft Exchange Online | New-InboxRule | [redacted] | [redacted] | [redacted] | [redacted] | CA | ["Application","ISP","Acti |
| Aug 14, 2025 7:13:... | Defender for Cloud Apps ... | Workday | Change My Account | [redacted] | [redacted] | [redacted] | [redacted] | CA | ["ActivityType","ISP","Act |

*Figure 6. Example of audit logs captured through Microsoft Defender for Cloud Apps showcasing an inbox rule creation in Microsoft Exchange Online followed by payroll account modification in Workday*

## Mitigation and protection guidance

Mitigating threats from actors like Storm-2657 begins with securing user identity by eliminating traditional credentials and adopting passwordless, phishing-resistant MFA methods such as FIDO2 security keys, Windows Hello for Business, and Microsoft Authenticator passkeys.

Microsoft recommends enforcing phishing-resistant MFA for privileged roles in Microsoft Entra ID to significantly reduce the risk of account compromise. Learn how to require phishing-resistant MFA for admin roles and plan a passwordless deployment.

Passwordless authentication improves security as well as enhances user experience and reduces IT overhead. Explore Microsoft's overview of passwordless authentication and authentication strength guidance to understand how to align your organization's policies with best practices. For broader strategies on defending against identity-based attacks, refer to Microsoft's blog on evolving identity attack techniques.

If Microsoft Defender alerts indicate suspicious activity or confirmed compromised account or a system, it's essential to act quickly and thoroughly. Below are recommended remediation steps for each affected identity:

1. **Reset credentials** – Immediately reset the account's password and revoke any active sessions or tokens. This ensures that any stolen credentials can no longer be used.
2. **Re-register or remove MFA devices** – Review users MFA devices, specifically those recently added or updated.
3. **Revert unauthorized payroll or financial changes** – If the attacker modified payroll or financial configurations, such as direct deposit details, revert them to their original state and notify the appropriate internal teams.
4. **Remove malicious inbox rules** – Attackers often create inbox rules to hide their activity or forward sensitive data. Review and delete any suspicious or unauthorized rules.
5. **Verify MFA reconfiguration** – Confirm that the user has successfully reconfigured MFA and that the new setup uses secure, phishing-resistant methods.

## Microsoft Defender XDR detections

Microsoft Defender XDR coordinates detection, prevention, investigation, and response across endpoints, identities, email, apps to provide integrated protection against attacks like the threat discussed in this blog.

Customers with provisioned access can also use Microsoft Security Copilot in Microsoft Defender to investigate and respond to incidents, hunt for threats, and protect their organization with relevant threat intelligence.

| Tactic | Observed activity | Microsoft Defender coverage |
|---|---|---|
| Initial access | Threat actor gains access to account through phishing | **Microsoft Defender for Office 365**<br>– Email messages removed after delivery<br>– Email reported by user as malware or phish |

| | | |
|---|---|---|
| | | **Microsoft Defender XDR**<br>– Compromised user account in a recognized attack pattern<br>– Anonymous IP address |
| Defense Evasion | Threat actor creates an inbox rule to delete incoming emails from Workday | **Microsoft Defender for Cloud apps**<br>– Possible BEC-related inbox rule<br>– Suspicious inbox manipulation rule<br>– Suspicious Workday inbox rule creation followed by a Workday session<br>– Malicious inbox rule manipulation possibly related to BEC payroll fraud attempt |
| Impact | Threat actor gains access to victim's Workday profile and modifies payroll elections | **Microsoft Defender for Cloud apps**<br>– Suspicious payroll configuration user activity in Workday |

## Hunting queries

### Microsoft Defender XDR

The Microsoft Defender for Cloud Apps connector for Workday includes write events such as Workday account updates, payroll configuration changes, etc. These are available in the Defender XDR *CloudAppEvents* hunting tables for further investigation. Important events related to this attack include but are not limited:

- Add iOS Device
- Add Android Device
- Change My Account
- Manage Payment Elections

Install the Microsoft Defender for Cloud Apps connector for Workday to take advantage of these logging, investigation, and detection capabilities.

**Review inbox rules created to hide or delete incoming emails from Workday**

Results of the following query may indicate an attacker is trying to delete evidence of Workday activity.

```
CloudAppEvents
| where Timestamp >= ago(1d)
| where Application == "Microsoft Exchange Online" and ActionType in ("New-InboxRule", "Set-InboxRule")
```

```
| extend Parameters = RawEventData.Parameters // extract inbox rule parameters

| where Parameters has "From" and Parameters has "@myworkday.com" // filter for inbox rule with From field and @MyWorkday.com in the parameters

| where Parameters has "DeleteMessage" or Parameters has ("MoveToFolder") // email deletion or move to folder (hiding)

| mv-apply Parameters on (where Parameters.Name == "From"

| extend RuleFrom = tostring(Parameters.Value))

| mv-apply Parameters on (where Parameters.Name == "Name"

| extend RuleName = tostring(Parameters.Value))
```

**Review updates to payment election or bank account information in Workday**

The following query surfaces changes to payment accounts in Workday.

```
CloudAppEvents

| where Timestamp >= ago(1d)

| where Application == "Workday"

| where ActionType == "Change My Account" or ActionType == "Manage Payment Elections"

| extend Descriptor = tostring(RawEventData.target.descriptor)
```

**Review device additions in Workday**

The following query looks for recent device additions in Workday. If the device is unknown, it may indicate an attacker joined their own device for persistence and MFA evasion.

```
CloudAppEvents

| where Timestamp >= ago(1d)

| where Application == "Workday"

| where ActionType has "Add iOS Device" or ActionType has "Add Android Device"

| extend Descriptor = tostring(RawEventData.target.descriptor) // will contain information of the device
```

**Hunt for bulk suspicious emails from *.edu* sender**

The following query identifies email from *.edu* senders sent to a high number of users.

```
EmailEvents
```

```
| where Timestamp >= ago(7d)

| where SenderFromDomain has "edu" or SenderMailFromDomain has "edu"

| where EmailDirection == "Inbound"

| summarize dcount(RecipientEmailAddress), dcount(InternetMessageId), make_set(InternetMessageId), dcount(Subject), dcount(NetworkMessageId), take_any(NetworkMessageId) by bin(Timestamp,1d), SenderFromAddress

| where dcount_RecipientEmailAddress > 100 // number can be adjusted, usually the sender will send emails to around 100-600 recipients per day
```

**Hunt for phishing URL from identified *.edu* phish sender**

If a suspicious *.edu* sender has been identified, use the following query to surface email events from this sender address.

```
EmailEvents

| where Timestamp >= ago(1d)

| where SenderFromAddress == "<identified .edu="" phish="" sender="">"

| where EmailDirection == "Inbound"

| project NetworkMessageId, Subject, InternetMessageId

| join EmailUrlInfo on NetworkMessageId

| where Timestamp >= ago(1d)

| project Url, NetworkMessageId, Subject, InternetMessageId

</identified>
```

**Hunt for user clicks to suspicious URL from the identified *.edu* phish sender (previous query)**

If a suspicious *.edu* sender has been identified, use the below query to surface user clicks that may indicate a malicious link was accessed.

```
EmailEvents

| where Timestamp >= ago(1d)

| where SenderFromAddress == "<identified .edu="" phish="" sender="">"

| where EmailDirection == "Inbound"

| project NetworkMessageId, Subject, InternetMessageId
```

```
| join UrlClickEvents on NetworkMessageId

| where Timestamp >= ago(1d)

| project AccountUpn, Subject, InternetMessageId, DetectionMethods, ThreatTypes, IsClickedThrough // these users very likely fall into the phishing attack

</identified>
```

### Microsoft Sentinel

Install the Workday connector for Microsoft Sentinel. Microsoft Sentinel has a range of detection and threat hunting content that customers can use to detect the post exploitation activity detailed in this blog.

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with ‘TI map’) to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

#### Malicious inbox rule

The query includes filters specific to inbox rule creation, operations for messages with ‘DeleteMessage’, and suspicious keywords.

```
let Keywords = dynamic(["helpdesk", " alert", " suspicious", "fake", "malicious", "phishing", "spam", "do not click", "do not open", "hijacked", "Fatal"]);

OfficeActivity

| where OfficeWorkload =~ "Exchange"

| where Operation =~ "New-InboxRule" and (ResultStatus =~ "True" or ResultStatus =~ "Succeeded")

| where Parameters has "Deleted Items" or Parameters has "Junk Email"  or Parameters has "DeleteMessage"

| extend Events=todynamic(Parameters)

| parse Events  with * "SubjectContainsWords" SubjectContainsWords '}'*

| parse Events  with * "BodyContainsWords" BodyContainsWords '}'*

| parse Events  with * "SubjectOrBodyContainsWords" SubjectOrBodyContainsWords '}'*

| where SubjectContainsWords has_any (Keywords)

   or BodyContainsWords has_any (Keywords)

   or SubjectOrBodyContainsWords has_any (Keywords)
```

```
| extend ClientIPAddress = case( ClientIP has ".", tostring(split(ClientIP,":")[0]), ClientIP has "[", tostring(trim_start(@'[[]',tostring(split(ClientIP,"]")[0]))), ClientIP )

| extend Keyword = iff(isnotempty(SubjectContainsWords), SubjectContainsWords, (iff(isnotempty(BodyContainsWords),BodyContainsWords,SubjectOrBodyContainsWords )))

| extend RuleDetail = case(OfficeObjectId contains '/' , tostring(split(OfficeObjectId, '/')[-1]) , tostring(split(OfficeObjectId, '\\')[-1]))

| summarize count(), StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated) by Operation, UserId, ClientIPAddress, ResultStatus, Keyword, OriginatingServer, OfficeObjectId, RuleDetail

| extend AccountName = tostring(split(UserId, "@")[0]), AccountUPNSuffix = tostring(split(UserId, "@")[1])

| extend OriginatingServerName = tostring(split(OriginatingServer, " ")[0])
```

**Risky sign-in with new MFA method**

This query identifies scenarios of risky sign-ins tied to new MFA methods being added.

```
let mfaMethodAdded=CloudAppEvents
    | where ActionType =~ "Update user."
    | where RawEventData has "StrongAuthenticationPhoneAppDetail"
    | where isnotempty(RawEventData.ObjectId) and isnotempty(RawEventData.Target[1].ID)
    | extend AccountUpn = tostring(RawEventData.ObjectId)
    | extend AccountObjectId = tostring(RawEventData.Target[1].ID)
    | project MfaAddedTimestamp=Timestamp,AccountUpn,AccountObjectId;
    let usersWithNewMFAMethod=mfaMethodAdded
    | distinct AccountObjectId;
    let hasusersWithNewMFAMethod = isnotempty(toscalar(usersWithNewMFAMethod));
    let riskySignins=AADSignInEventsBeta
    | where hasusersWithNewMFAMethod
    | where AccountObjectId in (usersWithNewMFAMethod)
    | where RiskLevelDuringSignIn in ("50","100") //Medium and High sign-in risk level.
```

```
    | where Application in ("Office 365 Exchange Online", "OfficeHome")
    | where isnotempty(SessionId)
    | project SignInTimestamp=Timestamp, Application, SessionId, AccountObjectId, IPAddress,RiskLevelDuringSignIn
    | summarize SignInTimestamp=argmin(SignInTimestamp,*) by Application,SessionId, AccountObjectId, IPAddress,RiskLevelDuringSignIn;
    mfaMethodAdded
    | join riskySignins on AccountObjectId
    | where MfaAddedTimestamp - SignInTimestamp < 6h //Time delta between risky sign-in and device registration less than 6h
    | project-away AccountObjectId1
```

## Microsoft Security Copilot

Security Copilot customers can use the standalone experience to create their own prompts or run the following prebuilt promptbooks to automate incident response or investigation tasks related to this threat:

- Incident investigation
- Microsoft User analysis
- Threat actor profile
- Threat Intelligence 360 report based on MDTI article
- Vulnerability impact assessment

Note that some promptbooks require access to plugins for Microsoft products such as Microsoft Defender XDR or Microsoft Sentinel.

## Acknowledgments

We would like to thank Workday for their collaboration and assistance in responding to this threat.

Workday customers can refer to the guidance published by Workday on their community: https://community.workday.com/alerts/customer/1229867.

## Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn, X (formerly Twitter), and Bluesky.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast.

---