splunk>

SPLUNK 快訊

2024 年 第 76 期

## > 狩獵 M365 入侵者

1 月 19 日，Microsoft 發佈了一份公告，披露了針對其 M365 租戶的網路安全事件，並將攻擊歸咎於 Midnight Blizzard，這是一家由國家資助的參與者，也稱為 Nobelium 和 APT29。 在此之後，1 月 24 日，Microsoft 團隊通過一篇全面的博客文章擴展了最初的公告，提供了有關攻擊的更多見解，並概述了威脅參與者利用的具體策略、技術和程式。 此外，安全研究員安迪·羅賓斯（Andy Robbins）通過博客文章和視頻提供了寶貴的見解，為尋求更好地瞭解這一事件的捍衛者提供了關鍵資源。

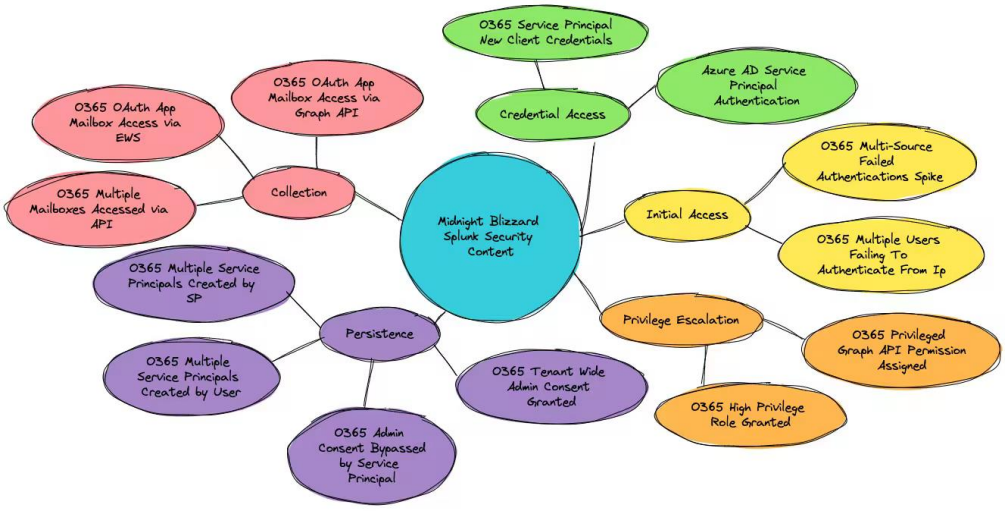
在這篇博客文章中，Splunk 威脅研究團隊 介紹了 Microsoft 博客文章所描述的攻擊鏈，旨在識別和分享網路安全防禦者的實用檢測和搜尋策略。 認識到一些攻擊細節仍然未知，我們將基於知情的假設進行分析，並概述更廣泛的檢測策略，這些策略雖然不是特定於此事件，但可以應用於類似場景。

**解碼攻擊鏈**

在本節中，我們將剖析 Midnight Blizzard 之後的攻擊鏈，逐個戰術分解它。 對於每種策略，我們從 Microsoft 博客文章中的關鍵語句開始，該語句描述了對手採取的步驟，並探索它們以尋找潛在的檢測機會。

所介紹的檢測策略主要來自 Office 365 的統一審核日誌，並在我們研究網站上的 Nobelium Group 分析中進行了詳細介紹。 還可以在 Office 365 故事中找到它們：Office 365 帳戶接管、Office 365 持久性機制 和 Office 365 收集技術。 對於喜歡使用 Entra ID 紀錄作為其主要數據源的使用者，還可以在此處找到相應的 Entra ID 檢測：Azure AD 帳戶接管 、Azure AD 持久性 和 Azure AD 持久性。

最後，我們的 attack_data 開源專案包含本文中所有模擬攻擊技術的數據集。 對於檢測工程師來說，尤其是那些無法進行自己類比的工程師來說，這是一個關鍵資源，它為開發和驗證檢測策略提供了實用數據。



splunk>

**初始訪問**

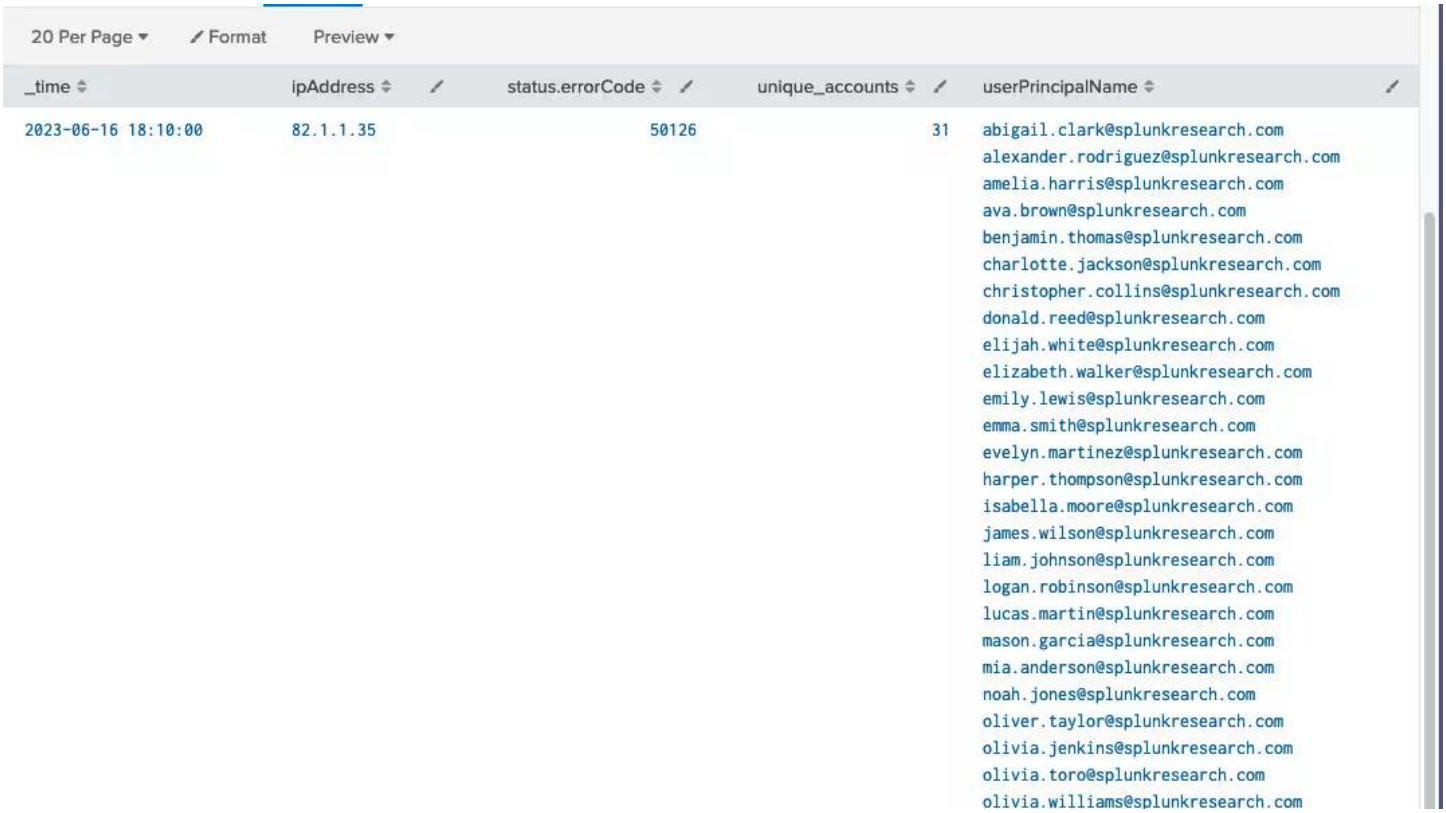
*Midnight Blizzard 利用密碼噴射攻擊成功破壞了未啟用多重身份驗證 （MFA） 的舊版非生產測試租戶帳戶*

Source

檢測工程師可以利用統一審核日誌和 Entra ID 紀錄上的錯誤代碼 50126 來識別傳統的密碼噴射攻擊，在這種攻擊中，大量使用者無法在短時間內從一個源 IP 進行身份驗證。

### O365 Multiple Users Failing To Authenticate From Ip

```
`o365_management_activity` Workload=AzureActiveDirectory Operation=UserLoginFailed ErrorNumber=50126
| bucket span=5m _time
| stats dc(user) as unique_accounts values(user) as user values(LogonError) as LogonError values(signature) as signature values(UserAgent) as UserAgent by _time, src_ip
| where unique_accounts > 10
```



20 Per Page ▾ Format Preview ▾

| _time | ipAddress | status.errorCode | unique_accounts | userPrincipalName |
|---|---|---|---|---|
| 2023-06-16 18:10:00 | 82.1.1.35 | 50126 | 31 | abigail.clark@splunkresearch.com<br>alexander.rodriguez@splunkresearch.com<br>amelia.harris@splunkresearch.com<br>ava.brown@splunkresearch.com<br>benjamin.thomas@splunkresearch.com<br>charlotte.jackson@splunkresearch.com<br>christopher.collins@splunkresearch.com<br>donald.reed@splunkresearch.com<br>elijah.white@splunkresearch.com<br>elizabeth.walker@splunkresearch.com<br>emily.lewis@splunkresearch.com<br>emma.smith@splunkresearch.com<br>evelyn.martinez@splunkresearch.com<br>harper.thompson@splunkresearch.com<br>isabella.moore@splunkresearch.com<br>james.wilson@splunkresearch.com<br>liam.johnson@splunkresearch.com<br>logan.robinson@splunkresearch.com<br>lucas.martin@splunkresearch.com<br>mason.garcia@splunkresearch.com<br>mia.anderson@splunkresearch.com<br>noah.jones@splunkresearch.com<br>oliver.taylor@splunkresearch.com<br>olivia.jenkins@splunkresearch.com<br>olivia.toro@splunkresearch.com<br>olivia.williams@splunkresearch.com |

攻擊者可能會選擇執行更隱蔽的密碼噴射活動，這些活動使用不同國家/地區的分散式 IP 位址網路來逃避安全控制。這可能會繞過前面的分析邏輯。 但是，我們可以使用不同的策略：在短時間內識別表現出特定特徵的身份驗證峰值。

20 Per Page ▾ Format Preview ▾ < Prev 1 2 Next >

| _time | category | user | src_ip | appDisplayName | OS | errorCode |
|---|---|---|---|---|---|---|
| 2023-11-06 20:53:22.553 | SignInLogs | Sophia.Miller@splunkresearch.com | 18.246.176.217 | Azure Active Directory PowerShell | Windows | 50126 |
| 2023-11-06 20:53:17.278 | SignInLogs | Logan.Robinson@splunkresearch.com | 18.246.176.33 | Azure Active Directory PowerShell | Windows | 50126 |
| 2023-11-06 20:53:11.769 | SignInLogs | Amelia.Harris@splunkresearch.com | 44.233.54.196 | Azure Active Directory PowerShell | Windows | 50126 |
| 2023-11-06 20:53:07.632 | SignInLogs | Elijah.White@splunkresearch.com | 35.90.133.30 | Azure Active Directory PowerShell | Windows | 50126 |
| 2023-11-06 20:53:02.660 | SignInLogs | Robert.Turner@splunkresearch.com | 35.92.26.38 | Azure Active Directory PowerShell | Windows | 50126 |
| 2023-11-06 20:52:57.263 | SignInLogs | Mary.Evans@splunkresearch.com | 34.223.69.241 | Azure Active Directory PowerShell | Windows | 50126 |
| 2023-11-06 20:52:46.015 | SignInLogs | Christopher.Collins@splunkresearch.com | 35.93.126.64 | Azure Active Directory PowerShell | Windows | 50126 |
| 2023-11-06 20:52:45.462 | SignInLogs | Isabella.Moore@splunkresearch.com | 34.223.70.198 | Azure Active Directory PowerShell | Windows | 50126 |
| 2023-11-06 20:52:42.775 | SignInLogs | Elizabeth.Walker@splunkresearch.com | 35.93.127.69 | Azure Active Directory PowerShell | Windows | 50126 |

在下面的分析中，我們計算了關鍵指標，例如：

1. 唯一使用者 IP 組合的數量
2. 不同用戶的計數
3. 來源 IP 和國家的多樣性
4. 失敗的登錄嘗試中涉及的唯一數量的使用者代理

通過自定義這些指標的閾值，我們可以尋找偏離正常行為的模式。

**O365 Multi-Source Failed Authentications Spike**

```
`o365_management_activity` Workload=AzureActiveDirectory Operation=UserLoginFailed ErrorNumber=50126
| bucket span=5m _time
| eval uniqueIPUserCombo = src_ip . "-" . user
| stats dc(uniqueIPUserCombo) as uniqueIpUserCombinations, dc(user) as uniqueUsers,
dc(src_ip) as uniqueIPs, values(user) as user, values(src_ip) as ips, values(user_agent) as user_agents by _time
| where uniqueIpUserCombinations > 20 AND uniqueUsers > 20 AND uniqueIPs > 20
```

splunk>

20 Per Page ▾ | Format | Preview ▾

| _time | uniqueIpUserComb | uniqueUsers | uniqueIPs | uniqueUserAgents | users | ips |
|---|---|---|---|---|---|---|
| 2023-11-06 20:50:00 | 30 | 30 | 29 | 1 | Abigail.Clark@splunkresearch.onmicrosoft.com | 18.246.176.105 |
| | | | | | Alexander.Rodriguez@splunkresearch.onmicrosoft.com | 18.246.176.2 |
| | | | | | Amelia.Harris@splunkresearch.onmicrosoft.com | 18.246.176.217 |
| | | | | | Ava.Brown@splunkresearch.onmicrosoft.com | 18.246.176.33 |
| | | | | | Benjamin.Thomas@splunkresearch.onmicrosoft.com | 18.246.176.48 |
| | | | | | Charlotte.Jackson@splunkresearch.onmicrosoft.com | 18.246.176.80 |
| | | | | | Christopher.Collins@splunkresearch.onmicrosoft.com | 18.246.176.85 |
| | | | | | Donald.Reed@splunkresearch.onmicrosoft.com | 34.223.69.193 |
| | | | | | Elijah.White@splunkresearch.onmicrosoft.com | 34.223.69.241 |
| | | | | | Elizabeth.Walker@splunkresearch.onmicrosoft.com | 34.223.70.18 |
| | | | | | Emily.Lewis@splunkresearch.onmicrosoft.com | 34.223.70.198 |
| | | | | | Emma.Smith@splunkresearch.onmicrosoft.com | 35.90.132.190 |
| | | | | | Evelyn.Martinez@splunkresearch.onmicrosoft.com | 35.90.133.240 |
| | | | | | Harper.Thompson@splunkresearch.onmicrosoft.com | 35.90.133.25 |
| | | | | | Isabella.Moore@splunkresearch.onmicrosoft.com | 35.90.133.30 |
| | | | | | James.Wilson@splunkresearch.onmicrosoft.com | 35.92.26.38 |
| | | | | | Liam.Johnson@splunkresearch.onmicrosoft.com | 35.93.124.137 |
| | | | | | Logan.Robinson@splunkresearch.onmicrosoft.com | 35.93.124.198 |
| | | | | | Lucas.Martin@splunkresearch.onmicrosoft.com | 35.93.126.64 |
| | | | | | Mary.Evans@splunkresearch.onmicrosoft.com | 35.93.127.129 |
| | | | | | Mason.Garcia@splunkresearch.onmicrosoft.com | 35.93.127.13 |
| | | | | | Mia.Anderson@splunkresearch.onmicrosoft.com | 35.93.127.47 |
| | | | | | Noah.Jones@splunkresearch.onmicrosoft.com | 35.93.127.69 |
| | | | | | Oliver.Taylor@splunkresearch.onmicrosoft.com | 44.233.54.169 |
| | | | | | Olivia.Williams@splunkresearch.onmicrosoft.com | 44.233.54.196 |
| | | | | | Paul.Morgan@splunkresearch.onmicrosoft.com | 44.233.54.28 |
| | | | | | Robert.Turner@splunkresearch.onmicrosoft.com | 44.233.54.40 |
| | | | | | Sebastian.Lee@splunkresearch.onmicrosoft.com | 44.233.55.40 |
| | | | | | Sophia.Miller@splunkresearch.onmicrosoft.com | 44.233.55.57 |
| | | | | | William.Davis@splunkresearch.onmicrosoft.com | |

**憑據訪問**

*Midnight Blizzard 利用其初始訪問許可權來識別和破壞舊版測試 OAuth 應用程式，該應用程式提升了對 Microsoft 公司環境的訪問許可權*

Source

為了破壞舊版 OAuth 應用程式並代表它執行操作，參與者必須更改其配置並向應用程式註冊物件添加新憑據。 我們可以通過篩選「更新應用程式 - 證書和機密管理事件」來監視這些操作。 通過關注此事件，我們可以監控和回應 Entra ID 許可權升級攻擊中的這種常見策略。

**O365 Service Principal New Client Credentials**

```
`o365_management_activity` Workload=AzureActiveDirectory Operation="Update
application*Certificates and secrets management "
| stats earliest(_time) as firstTime latest(_time) as lastTime by user
ModifiedProperties{}.NewValue object ObjectId
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

splunk>

100 Per Page ▾ Format Preview ▾

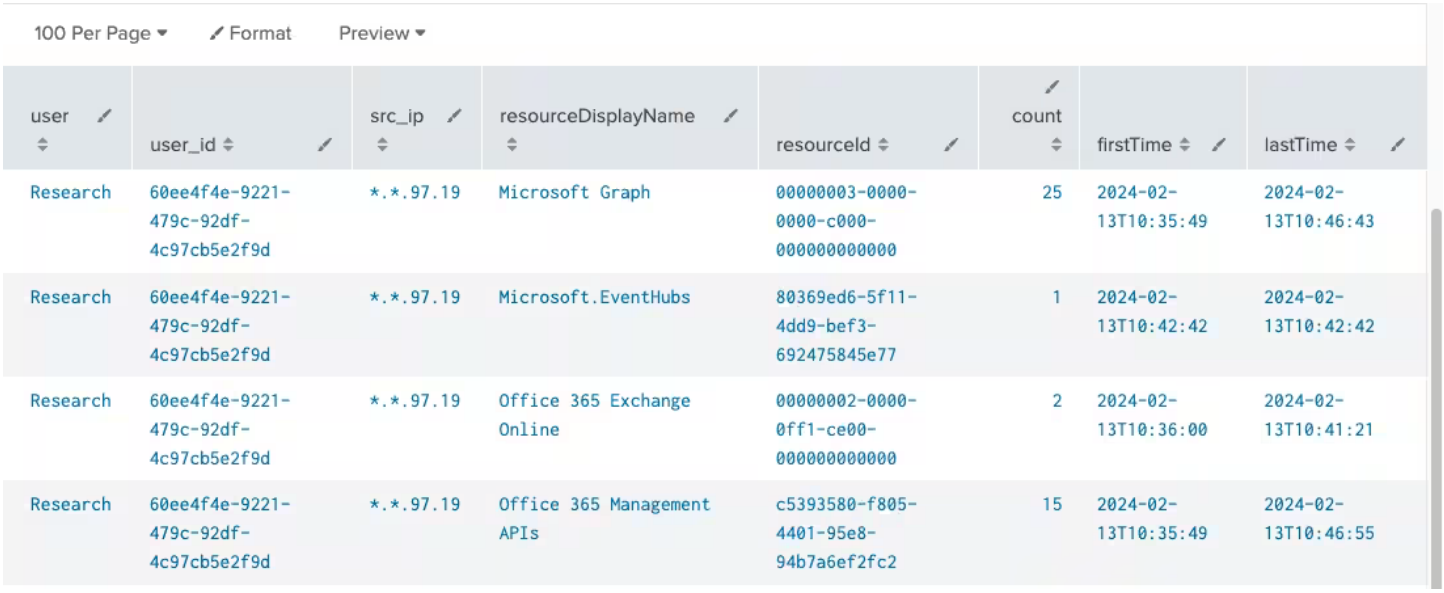
| user | ModifiedProperties{}.NewValue | object | ObjectId | firstTime |
|---|---|---|---|---|
| attacker@splunkresearch.com | KeyDescription | App1 | Application_fa9d3cd6-c0cd-4e26-a4b4-f744ccc6c851 | 2024-01-31T11:32:47 |
| attacker@splunkresearch.com | [ "[KeyIdentifier=16e732ae-7adc-4577-b790-f9bca0464d1b,KeyType=Password,KeyUsage=Verify,DisplayName=Read]" ] | App1 | Application_fa9d3cd6-c0cd-4e26-a4b4-f744ccc6c851 | 2024-01-31T11:32:47 |
| attacker@splunkresearch.com | [ "[KeyIdentifier=41572925-6554-4843-833b-86bc7c1a2f23,KeyType=Password,KeyUsage=Verify,DisplayName=read]" ] | App1 | Application_fa9d3cd6-c0cd-4e26-a4b4-f744ccc6c851 | 2024-01-31T14:23:59 |

添加憑據后，攻擊者必須以與應用程式註冊關聯的服務主體的身份進行身份驗證，才能利用其許可權。 請務必注意，默認情況下，統一審核日誌僅記錄使用者互動式身份驗證 事件，不包括服務主體身份驗證。 為了有效地監視這些活動，我們需要依賴 Entra ID 日誌和 ServicePrincipalSignInLogs 類別。

瞭解哪些服務主體正在進行身份驗證以及從組織中的哪些位置進行身份驗證有助於識別未經授權的訪問和濫用。 不幸的是，在具有眾多應用程式的大型環境中映射這些關係可能具有挑戰性。 儘管很複雜，但對於安全團隊來說，跟蹤和清點與服務主體關聯的源 IP 作為威脅搜尋練習是值得的。

**Azure AD Service Principal Authentication**

```
`azure_monitor_aad` operationName="Sign-in activity" category=ServicePrincipalSignInLogs
| rename properties.* as *
| stats count earliest(_time) as firstTime latest(_time) as lastTime by user, user_id, src_ip,
resourceDisplayName, resourceId
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```



100 Per Page ▾ Format Preview ▾

| user | user_id | src_ip | resourceDisplayName | resourceId | count | firstTime | lastTime |
|---|---|---|---|---|---|---|---|
| Research | 60ee4f4e-9221-479c-92df-4c97cb5e2f9d | *.*.97.19 | Microsoft Graph | 00000003-0000-0000-c000-000000000000 | 25 | 2024-02-13T10:35:49 | 2024-02-13T10:46:43 |
| Research | 60ee4f4e-9221-479c-92df-4c97cb5e2f9d | *.*.97.19 | Microsoft.EventHubs | 80369ed6-5f11-4dd9-bef3-692475845e77 | 1 | 2024-02-13T10:42:42 | 2024-02-13T10:42:42 |
| Research | 60ee4f4e-9221-479c-92df-4c97cb5e2f9d | *.*.97.19 | Office 365 Exchange Online | 00000002-0000-0ff1-ce00-000000000000 | 2 | 2024-02-13T10:36:00 | 2024-02-13T10:41:21 |
| Research | 60ee4f4e-9221-479c-92df-4c97cb5e2f9d | *.*.97.19 | Office 365 Management APIs | c5393580-f805-4401-95e8-94b7a6ef2fc2 | 15 | 2024-02-13T10:35:49 | 2024-02-13T10:46:55 |

**許可權提升**

*Midnight Blizzard 利用其初始訪問許可權來識別和破壞舊版測試 OAuth 應用程式，該應用程式提升了對 Microsoft 公司環境的訪問許可權*

Source

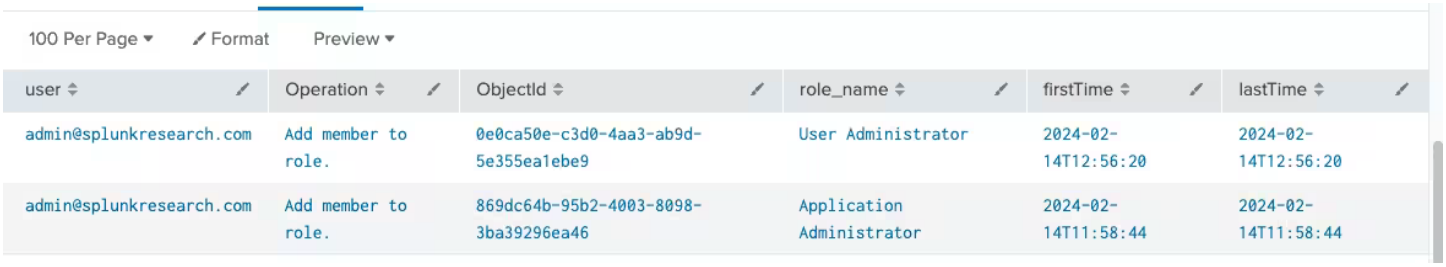
授予被破壞應用程式的高級許可權的確切性質尚不清楚，但它們很可能是在攻擊之前建立的。 在許多組織中，這是一個常見問題，在這些組織中，通常會為標識分配比必要許可權更多的許可權。 在 M365/Entra ID 生態系統中，監視 Entra ID 角色和 API 許可權（如 Graph 和 Exchange Online）至關重要。

可以通過「將成員添加到角色」和「更新應用程式」有效地監視這些事件。 防禦者可以專注於關鍵角色（如“全域管理員”或“特權角色管理員”）和敏感的 API 許可權（如“Application.ReadWrite.All”、“AppRoleAssignment.ReadWrite.All”和“RoleManagement.ReadWrite.Directory”。 這不是一個廣泛的清單，應該由捍衛者量身定製。

**O365 High Privilege Role Granted**

```
`o365_management_activity` Operation="Add member to role."
Workload=AzureActiveDirectory
| eval role_id = mvindex('ModifiedProperties{}.NewValue',2)
| eval role_name = mvindex('ModifiedProperties{}.NewValue',1)
| where role_id IN ("29232cdf-9323-42fd-ade2-1d097af3e4de",
"f28a1f50-f6e7-4571-818b-6a12f2af6b6c", "62e90394-69f5-4237-9190-012177145e10")
| stats earliest(_time) as firstTime latest(_time) as lastTime by user Operation ObjectId
```

```
role_name
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```



100 Per Page ▾ Format Preview ▾

| user | Operation | ObjectId | role_name | firstTime | lastTime |
|---|---|---|---|---|---|
| admin@splunkresearch.com | Add member to role. | 0e0ca50e-c3d0-4aa3-ab9d-5e355ea1ebe9 | User Administrator | 2024-02-14T12:56:20 | 2024-02-14T12:56:20 |
| admin@splunkresearch.com | Add member to role. | 869dc64b-95b2-4003-8098-3ba39296ea46 | Application Administrator | 2024-02-14T11:58:44 | 2024-02-14T11:58:44 |

**O365 Privileged Graph API Permission Assigned**

```
`o365_management_activity` Workload=AzureActiveDirectory Operation="Update application."
| eval newvalue = mvindex('ModifiedProperties{}.NewValue',0)
| ssrc input=newvalue
| search
"{}.RequiredAppPermissions{}.EntitlementId"="1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9" OR
"{}.RequiredAppPermissions{}.EntitlementId"="06b708a9-e830-4db3-a914-8e69da51d44f"
OR "{}.RequiredAppPermissions{}.EntitlementId"="9e3f62cf-ca93-4989-b6ce-bf83c28f9fe8"
| eval Permissions = '{}.RequiredAppPermissions{}.EntitlementId'
| stats count earliest(_time) as firstTime latest(_time) as lastTime values(Permissions)
by user, object, user_agent, Operation
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

splunk>

100 Per Page ▾ Format Preview ▾

| user | object | ObjectId | Operation | count | firstTime | lastTime | values(Permissions) |
|---|---|---|---|---|---|---|---|
| attacker@splunkresearch.com | STRT_ReadEmail | Application_75924835-d844-4947-96ba-18074e997386 | Update application. | 3 | 2024-01-30T10:24:59 | 2024-01-30T15:30:18 | 06b708a9-e830-4db3-a914-8e69da51d44f 1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9 570282fd-fa5c-430d-a7fd-fc8dc98a9dca 7427e0e9-2fba-42fe-b0c0-848c9e6a8182 810c84a8-4a9e-49e6-bf7d-12d183f40d01 9e3f62cf-ca93-4989-b6ce- |

**堅持**

| *該參與者創建了其他惡意 OAuth 應用程式* |
|---|

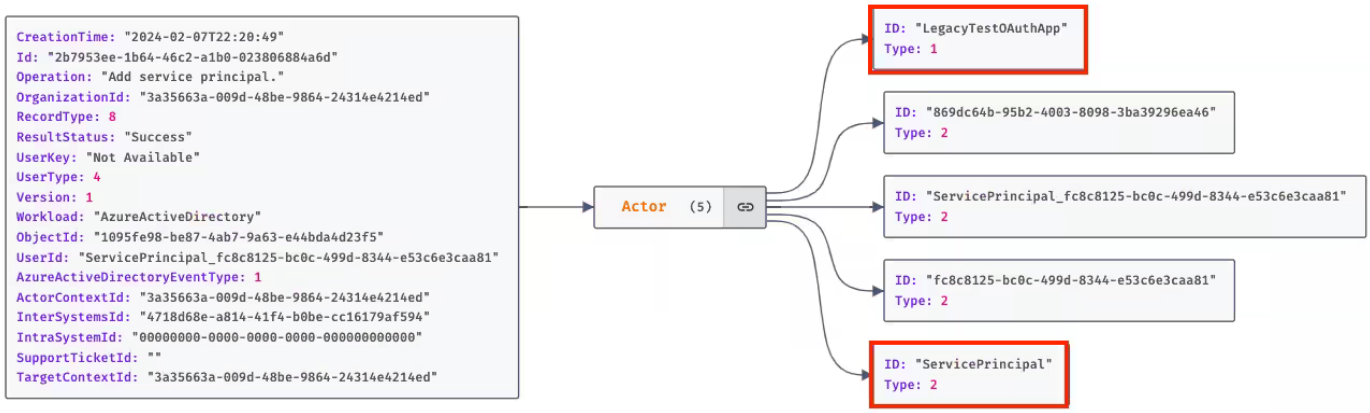
Source

在 Entra ID 環境中創建新的 OAuth 應用程式時，將觸發「添加應用程式」和「添加服務主體」事件。 由於活動環境中頻繁出現合法觸發器，因此監視應用程式創建可能具有挑戰性。

100 Per Page ▾ Format Preview ▾

| _time | Operation | UserId | object | ObjectId |
|---|---|---|---|---|
| 2024-02-07 17:31:14 | Add application. | attacker@splunkresearch.com | Malicious11 | Application_aef7a9a6-428e-4f0f-ab09-b0f10b21bda6 |
| 2024-02-07 17:31:14 | Add service principal. | attacker@splunkresearch.com | Malicious11 | e06366ca-8489-4748-b6a2-d7e4332f45c1 |
| 2024-02-07 17:31:08 | Add application. | attacker@splunkresearch.com | Malicious10 | Application_852b916a-d355-4991-82af-444a9f8e107f |
| 2024-02-07 17:31:08 | Add service principal. | attacker@splunkresearch.com | Malicious10 | 6afcdaf6-7dc9-43d2-a707-4274d499e479 |
| 2024-02-07 17:31:02 | Add application. | attacker@splunkresearch.com | Malicious9 | Application_8294d9f8-20c4-4323-ad9f-e2d075f2ea2e |
| 2024-02-07 17:31:02 | Add service principal. | attacker@splunkresearch.com | Malicious9 | c57490e5-d8bb-441d-a3b8-aa94b24d19cf |

但是，在短時間內創建多個應用程式的方案可能值得監視。 此外，我們的分析顯示，統一審核日誌中的"參與者"字段可用於確定應用程式是由使用者還是服務主體創建的。 這種額外的洞察力提供了額外的背景資訊，使我們能夠開發有針對性的檢測分析。




### O365 Multiple Service Principals Created by User

```
`o365_management_activity` Workload=AzureActiveDirectory Operation="Add service principal."
| bucket span=10m _time
| eval len=mvcount('Actor{}.ID')
| eval userType = mvindex('Actor{}.ID',len-1)
| search userType = "User"
| eval displayName = object
| stats count earliest(_time) as firstTime latest(_time) as lastTime values(displayName) as displayName dc(displayName) as unique_apps by src_user
| where unique_apps > 3
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

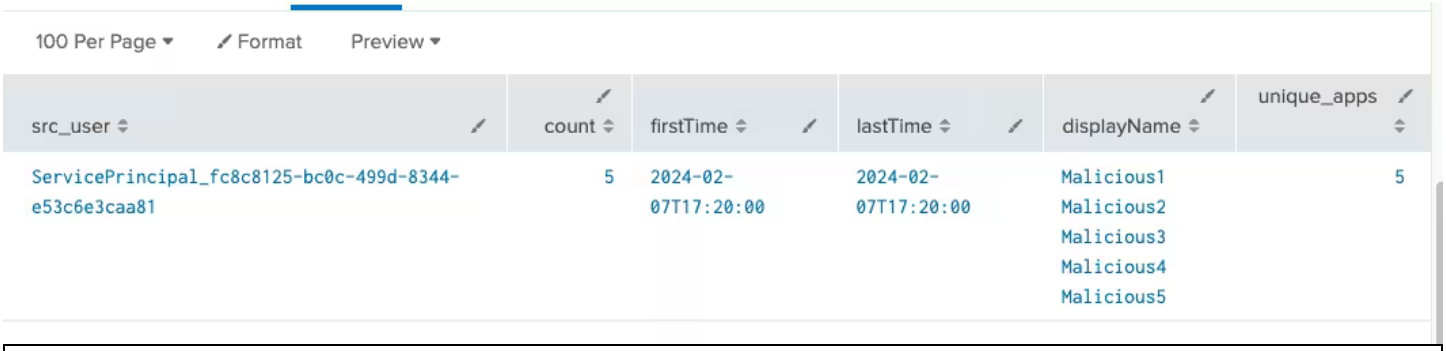
100 Per Page ▾ Format Preview ▾

| src_user | count | firstTime | lastTime | displayName | unique_apps |
|---|---|---|---|---|---|
| attacker@splunkresearch.com | 6 | 2024-02-07T17:30:00 | 2024-02-07T17:30:00 | Malicious10<br>Malicious11<br>Malicious6<br>Malicious7<br>Malicious8<br>Malicious9 | 6 |

splunk>

**O365 Multiple Service Principals Created by SP**

```
`o365_management_activity` Workload=AzureActiveDirectory Operation="Add service principal."
| bucket span=10m _time
| eval len=mvcount('Actor{}.ID')
| eval userType = mvindex('Actor{}.ID',len-1)
| search userType = "ServicePrincipal"
| eval displayName = object
| stats count earliest(_time) as firstTime latest(_time) as lastTime values(displayName) as
displayName dc(displayName) as unique_apps by src_user
| where unique_apps > 3
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```



100 Per Page ▾ Format Preview ▾

| src_user | count | firstTime | lastTime | displayName | unique_apps |
|---|---|---|---|---|---|
| ServicePrincipal_fc8c8125-bc0c-499d-8344-e53c6e3caa81 | 5 | 2024-02-07T17:20:00 | 2024-02-07T17:20:00 | Malicious1<br>Malicious2<br>Malicious3<br>Malicious4<br>Malicious5 | 5 |

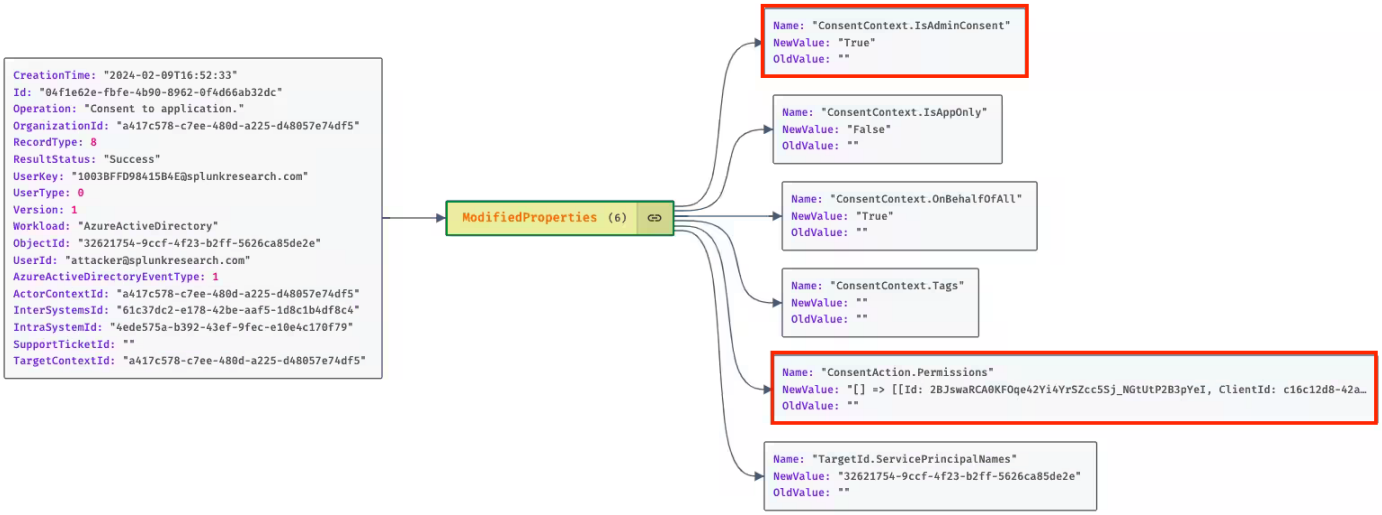
*然後，威脅參與者使用舊版測試 OAuth 應用程式向他們授予 Office 365 Exchange Online full_access_as_app 角色，該角色允許訪問郵箱*

Source

Midnight Blizzard 授予自己一個敏感的 Exchange Online API 許可權，以繼續進行電子郵件收集。 在通過 Azure 門戶進行的典型高特權 API 許可權分配過程中，會發生兩個關鍵事件：

1. 首先，將許可權分配給 OAuth 應用程式，生成“更新應用程式”事件。
2. 然後，管理員同意該許可權，觸發“同意應用程式”事件。

授予組織範圍許可權的管理員同意（稱為租戶範圍的管理員同意）特別敏感。 這些同意允許應用程式代表整個組織執行操作，因此它們對監視至關重要。 通過檢查 ModifiedProperties 字段，我們可以開發租戶範圍 管理員同意的分析。




**O365 Tenant Wide Admin Consent Granted**

```
`o365_management_activity` Operation="Consent to application."
| eval new_field=mvindex('ModifiedProperties{}.NewValue', 4)
| rex field=new_field "ConsentType: (?[^\,]+)"
| rex field=new_field "Scope: (?[^\,]+)"
| search  ConsentType = "AllPrincipals"
| stats count min(_time) as firstTime max(_time) as lastTime by Operation, user, object,
ObjectId, ConsentType, Scope
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

100 Per Page ▾ Format Preview ▾

| Operation | user | object | ObjectId | ConsentType | Scope | count | firstTime | lastTime |
|---|---|---|---|---|---|---|---|---|
| Consent to application. | attacker@splunkresearch.com | TestOAuth | 32621754-9ccf-4f23-b2ff-5626ca85de2e | AllPrincipals | User.Read | 1 | 2024-02-09T11:52:33 | 2024-02-09T11:52:33 |

但是，Microsoft 描述的攻擊鏈可能不會觸發“更新應用程式”或“同意應用程式”事件。 上述語句暗示攻擊者未使用 Azure 門戶進行標準許可權分配。 相反，他們濫用舊版應用程式的服務主體許可權，以程式設計方式更改許可權，繞過 正常的同意過程。

為了更深入地瞭解此方法，我們使用 Microsoft Graph PowerShell SDK 中的 New-MgServicePrincipalAppRoleAssignedTo commandlet 複製了這些步驟。 此類比證實了我們的理論：與通常的兩個事件不同，僅觸發“將應用角色分配添加到服務主體”事件。

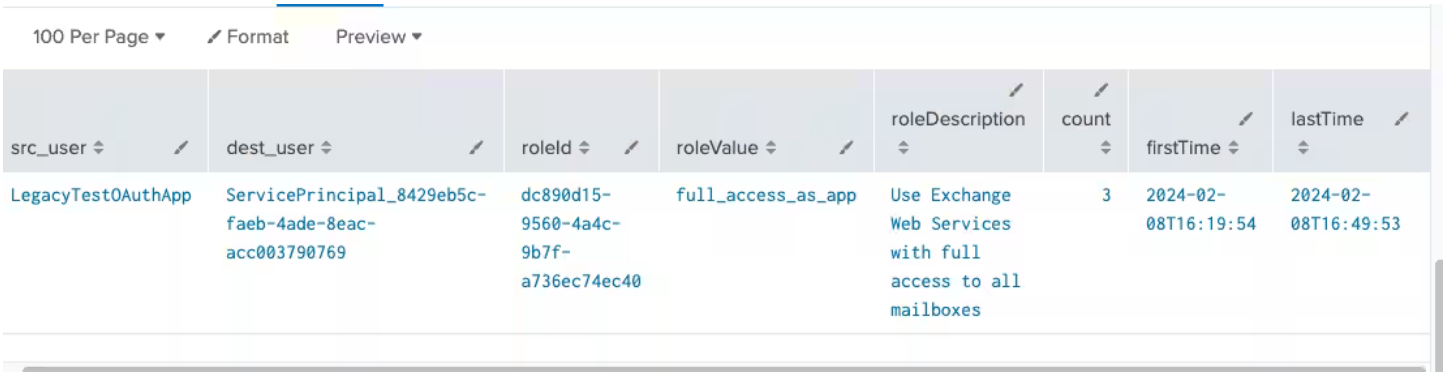
```
$servicePrincipal = Get-MgServicePrincipal -Filter "displayName eq 'MaliciousApp'"
$EolServicePrincipal = Get-MgServicePrincipal -Filter "servicePrincipalType eq 'Application'
and displayName eq 'Office 365 Exchange Online'"
$appRole = $EolServicePrincipal.AppRoles | Where-Object { $_.Value -eq
"full_access_as_app" -and $_.AllowedMemberTypes -contains "Application" }

$params = @{
principalId = $servicePrincipal.Id
resourceId = $EolServicePrincipal.Id
appRoleId = $appRole.Id
}
New-MgServicePrincipalAppRoleAssignedTo -ServicePrincipalId $servicePrincipal.Id
-BodyParameter $params
```

在日誌中查看“將應用角色分配添加到服務主體”事件時，我們注意到“參與者”欄位可用於確定是服務主體還是管理員使用者執行了該操作。 這促使我們創建了一個新的分析方法，旨在捕獲服務主體可能通過以程式設計方式將 API 許可權分配給其他服務主體來繞過管理員同意過程的情況。

**O365 Admin Consent Bypassed by Service Principal**

```
`o365_management_activity` Workload=AzureActiveDirectory Operation="Add app role
assignment to service principal."
| eval len=mvcount('Actor{}.ID')
| eval userType = mvindex('Actor{}.ID',len-1)
| eval roleId = mvindex('ModifiedProperties{}.NewValue', 0)
| eval roleValue = mvindex('ModifiedProperties{}.NewValue', 1)
| eval roleDescription = mvindex('ModifiedProperties{}.NewValue', 2)
```

```
| eval dest_user = mvindex('Target{}.ID', 0)
| search userType = "ServicePrincipal"
| eval src_user = user
| stats count earliest(_time) as firstTime latest(_time) as lastTime by src_user dest_user
roleId roleValue roleDescription
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```



100 Per Page ▾ Format Preview ▾

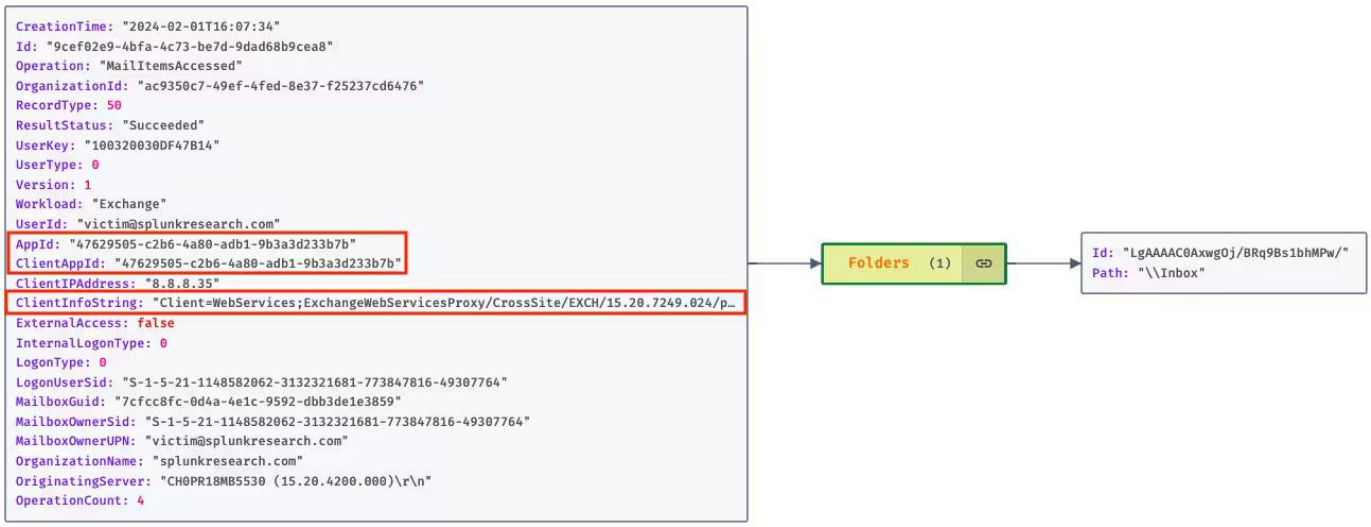
| src_user | dest_user | roleId | roleValue | roleDescription | count | firstTime | lastTime |
|---|---|---|---|---|---|---|---|
| LegacyTestOAuthApp | ServicePrincipal_8429eb5c-faeb-4ade-8eac-acc003790769 | dc890d15-9560-4a4c-9b7f-a736ec74ec40 | full_access_as_app | Use Exchange Web Services with full access to all mailboxes | 3 | 2024-02-08T16:19:54 | 2024-02-08T16:49:53 |

**收集**

*Midnight Blizzard 利用這些惡意 OAuth 應用程式向 Microsoft Exchange Online 進行身份驗證並針對 Microsoft 公司電子郵件帳戶*

Source

在獲得正確的許可權后，攻擊者開始從公司帳戶收集電子郵件詳細資訊。 防禦者可以使用統一審核日誌中的“Mailitemsaccessed”事件跟蹤此類活動。 此日誌記錄最初僅適用於 E5 許可證，現在將擴展到標準 M365 使用者。 此事件中的一個重要元素是 ClientAppId，它標識代表使用者執行訪問的 Microsoft Entra 應用的 ID。 在利用 OAuth 應用程式、Exchange Web 服務、PowerShell 和 Python 用戶端類比此技術期間，我們一致發現 ClientAppId 為 **47629505-c2b6-4a80-adb1-9b3a3d233b7b。**




但是，我們無法找到確認此 GUID 實際分配給 Exchange Web 服務的 Microsoft 文件。 為了避免錯誤分類，我們利用了 ClientInfoString 欄位，該欄位提供有關用於執行操作的電子郵件客戶端的資訊。 在我們的測試中，此欄位始終以相同的字串開頭。

100 Per Page ▾ Format Preview ▾

| _time | ClientIPAddress | ClientInfoString |
|---|---|---|
| 2024-02-01 11:07:34 | 8.8.8.35 | Client=WebServices;ExchangeWebServicesProxy/CrossSite/EXCH/15.20.7249.024/python-requests/2.25.1[AppId=47629505-c2b6-4a80-adb1-9b3a3d233b7b]; |
| 2024-01-31 11:59:31 | 8.8.8.35 | Client=WebServices;ExchangeWebServicesProxy/CrossSite/EXCH/15.20.7249.020/Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.22621.2506[AppId=47629505-c2b6-4a80-adb1-9b3a3d233b7b]; |
| 2024-01-30 20:02:17 | 8.8.8.44 | Client=WebServices;ExchangeWebServicesProxy/CrossSite/EXCH/15.20.7249.020/Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.22621.2506[AppId=47629505-c2b6-4a80-adb1-9b3a3d233b7b]; |

**O365 OAuth App Mailbox Access via EWS**

```
`o365_management_activity` Workload=Exchange Operation=MailItemsAccessed AppId=*
ClientAppId=*
| regex ClientInfoString="^Client=WebServices;ExchangeWebServices"
|  stats count earliest(_time) as firstTime latest(_time) as lastTime values(ClientIPAddress)
as src_ip by user ClientAppId OperationCount AppId ClientInfoString
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

100 Per Page ▾ Format Preview ▾

| user | ClientAppId | OperationCount | AppId | count | firstTime | lastTime | src_ip |
|---|---|---|---|---|---|---|---|
| victim@splunkresearch.com | 47629505-c2b6-4a80-adb1-9b3a3d233b7b | 4 | 47629505-c2b6-4a80-adb1-9b3a3d233b7b | 3 | 2024-01-30T20:02:17 | 2024-02-01T11:07:34 | 8.8.8.35<br>8.8.8.44 |

雖然 Midnight Blizzard 這次選擇利用 Exchange Web 服務來收集電子郵件，但防禦者應該意識到，該場景還將允許他們獲得敏感的 Microsoft Graph API 許可權並以不同的方式收集電子郵件。 知道了這一點，我們還編寫了一個不同的分析標記 Graph API 郵箱訪問。

**O365 OAuth App Mailbox Access via Graph API**

```
`o365_management_activity` Workload=Exchange Operation=MailItemsAccessed AppId=*
AppId=00000003-0000-0000-c000-000000000000
| stats count earliest(_time) as firstTime latest(_time) as lastTime values(ClientIPAddress)
by user ClientAppId OperationCount AppId
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

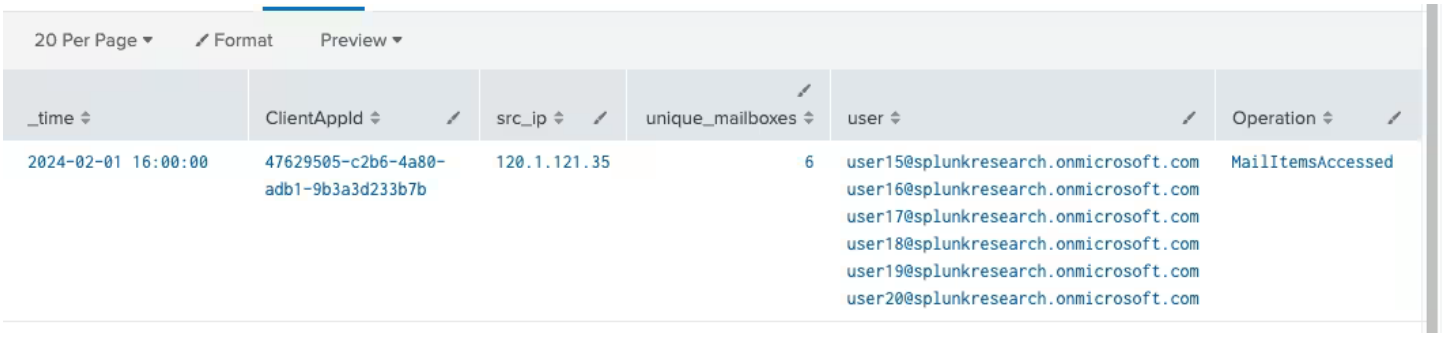
100 Per Page ▾ Format Preview ▾

| user | ClientAppId | OperationCount | AppId | count | firstTime | lastTime | values(ClientIPAddress) |
|---|---|---|---|---|---|---|---|
| victim@splunkresearch.com | 867f0d29-0eab-4017-b691-c4713cc7d7b0 | 4 | 00000003-0000-0000-c000-000000000000 | 2 | 2024-01-31T11:35:09 | 2024-01-31T13:44:21 | 8.8.8.152<br>8.8.8.25 |
| victim@splunkresearch.com | 9a9c8232-73c8-45f4-b0e9-28f525a42a8f | 4 | 00000003-0000-0000-c000-000000000000 | 2 | 2024-02-01T12:49:25 | 2024-02-09T11:26:09 | 8.8.8.40<br>8.8.8.88 |
| victim@splunkresearch.com | e9cf522e-fb53-40ab-8cdb-666962ecc953 | 1 | 00000003-0000-0000-c000-000000000000 | 3 | 2024-02-07T16:45:02 | 2024-02-07T16:48:22 | 8.8.8.152<br>8.8.8.25<br>8.8.8.88 |

值得監視的額外行為是，當 OAuth 應用程式在短時間內通過 API （如 EWS 或 Microsoft Graph）以程式設計方式存取多個郵箱時。 雖然日記和合規性應用程式可能合法地需要此類訪問許可權，但具有如此廣泛的郵箱訪問許可權的應用程式通常是例外，應由安全團隊詳細記錄和清點。

**O365 Multiple Mailboxes Accessed via API**

```
`o365_management_activity` Workload=Exchange Operation=MailItemsAccessed AppId=*
ClientAppId=*
| bucket span=10m _time
| eval matchRegex=if(match(ClientInfoString,
"^Client=WebServices;ExchangeWebServices"), 1, 0)
| search (AppId="00000003-0000-0000-c000-000000000000" OR matchRegex=1)
| stats values(ClientIPAddress) as src_ip dc(user) as unique_mailboxes values(user) as user
by _time ClientAppId ClientInfoString
| where unique_mailboxes > 5
```



20 Per Page ▾ Format Preview ▾

| _time | ClientAppId | src_ip | unique_mailboxes | user | Operation |
|---|---|---|---|---|---|
| 2024-02-01 16:00:00 | 47629505-c2b6-4a80-adb1-9b3a3d233b7b | 120.1.121.35 | 6 | user15@splunkresearch.onmicrosoft.com<br>user16@splunkresearch.onmicrosoft.com<br>user17@splunkresearch.onmicrosoft.com<br>user18@splunkresearch.onmicrosoft.com<br>user19@splunkresearch.onmicrosoft.com<br>user20@splunkresearch.onmicrosoft.com | MailItemsAccessed |

**結束語**

在不斷發展的雲計算環境中，組織越來越多地面臨新的攻擊媒介，例如我們今天探索的攻擊媒介。 雲環境中的錯誤配置可能會為攻擊者打開對租戶的廣泛控制權的大門。 對於防禦者來說，超越傳統的以端點為中心的策略並加深他們對雲中這些新興威脅的理解至關重要。

Splunk 威脅研究團隊 仍然致力於通過檢測策略、SOAR 行動手冊、博客文章和開源專案等內容為網路安全社區提供支援。 我們希望這篇博文能為防禦者提供資源，以加強他們對類似民族國家攻擊的態勢，並適應不斷變化的網路威脅環境。