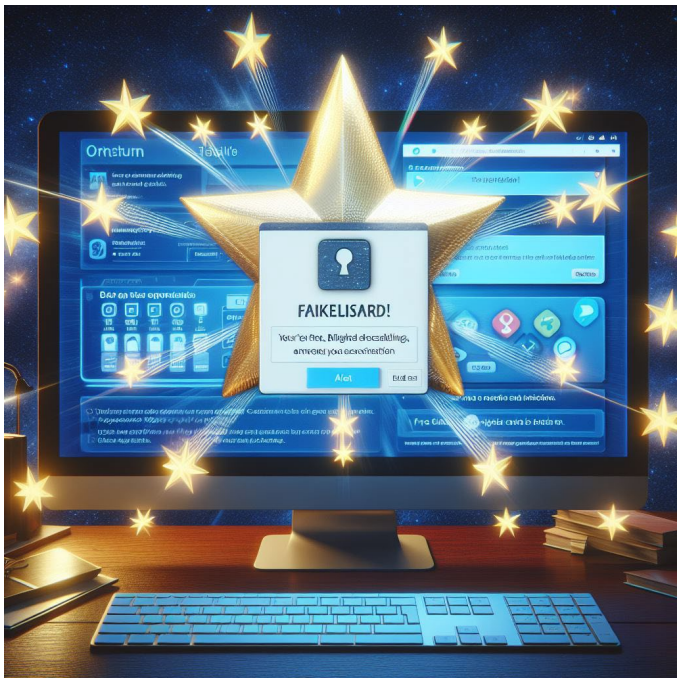

I. Introduction

Star Blizzard, also known as the Callisto Group, SEABORGIUM, BlueCharlie, TA446, COLDRIVER, and TAG-53 is known for targeting governmental organizations, defense industry, academia, think tanks, NGOs, politicians, and others in the U.S., UK, other NATO countries, and countries neighboring Russia.

Star Blizzard's spear-phishing campaigns typically involve sending spoofed emails that appear to be from legitimate individuals or organizations. These emails are designed to trick victims into providing their email account credentials, which the group then uses to gain unauthorized, persistent access to the victims' email accounts. Once they gain access, Star Blizzard is known to set up mail forwarding rules, granting them ongoing visibility of a victim's correspondence and contact lists, and using this information for follow-on targeting and phishing activities.

II. Common Targets of Spear-Phishing Attacks

Spear-phishing campaigns typically target specific individuals or organizations with the goal of stealing sensitive information such as login credentials or infecting systems with malware. The targets are often carefully researched to increase the likelihood of a successful attack. Here are some common targets:

- **High-ranking officials within organizations**: These individuals often have access to sensitive information, making them attractive targets for spear-phishing campaigns
- **Individuals involved in confidential operations**: People who handle sensitive data or operations within a company are often targeted due to the valuable information they can provide
- **Specific employees within a company**: Spear-phishing campaigns may target specific employees within a company, especially those who have access to valuable data or systems
- **Specific organizations**: Organizations themselves can be targets of spear-phishing campaigns, especially those in sectors like government, defense, academia, and non-governmental organizations (NGOs)
- **Social media users**: Spear-phishers often use social media and other publicly available sources to gather information about potential targets

Recent years have seen a variety of spear phishing attacks, some of which include:

- **Fake Websites**: Attackers create counterfeit websites that mimic legitimate ones to deceive individuals into entering their personal information
- **CEO Fraud**: This involves impersonating a high-level executive and sending emails to employees, often in the finance department, to authorize wire transfers to fraudulent accounts
- **Malware**: Emails with malicious attachments or links that install malware on the victim's device when opened
- **Smishing and Vishing**: These are forms of spear phishing via SMS (smishing) or voice calls (vishing), where attackers pose as legitimate entities to extract personal details or financial information

Spear phishing campaigns use various tactics to increase their success rate:

- **Target Selection**: Attackers choose individuals or organizations with potential access to valuable data or financial gain
- **Reconnaissance**: Extensive research is conducted on the target to gather personal information, job roles, and interests
- **Personalization**: Emails are crafted using the target's specific information to appear credible and relevant
- **Urgency and Pressure**: Messages often convey a sense of urgency or pressure to prompt immediate action from the target
- **Shared Interests**: Attackers may exploit known interests of the target to create a convincing pretext for the email
- **Authority**: Impersonating someone in a position of authority or a known contact to elicit trust and compliance

III. Targets of Star Blizzard Campaigns

Star Blizzard has targeted a variety of sectors and individuals since 2019, including:

- **Academia**: Educational institutions and individuals associated with research or possessing valuable intellectual property
- **Defense**: Entities within the defense sector, including contractors and suppliers to the military and defense industry
- **Governmental Organizations**: Various government agencies and departments that have access to sensitive national security information
- **Non-Governmental Organizations (NGOs)**: These organizations may be targeted for their involvement in sensitive political, social, or humanitarian activities
- **Think Tanks**: Organizations that perform research and advocacy on topics such as social policy, political strategy, economy, military, technology, and culture
- **High-Profile Individuals**: Politicians and other individuals who may have access to confidential information or influence over important decisions

Specific Targets of Star Blizzard's Spear-Phishing Campaigns:

- **Personal Email Addresses**: They have predominantly sent spear-phishing emails to targets' personal email addresses, which may have less stringent security controls than corporate or business email addresses
- **Corporate or Business Email Addresses**: They have also used targets' corporate or business email addresses, indicating a comprehensive approach to targeting both personal and professional aspects of their victims' lives
- **Mailing List Data and Contacts**: By gaining access to a victim's email account, they have accessed mailing list data and a victim's contacts list, which they then use for follow-on targeting and further phishing activities
- **Compromised Email Accounts**: These are used for additional phishing activity, indicating a cycle of compromise and exploitation that can self-perpetuate and expand the scope of their campaigns

A. Common Themes or Subjects in Star Blizzard's Spear-Phishing Emails

Star Blizzard's spear-phishing emails often revolve around topics of interest to the target, which they identify through extensive research using open-source resources, including social media and professional networking platforms. They may impersonate known contacts of their targets or respected experts in the field, and create email accounts and fake social media or networking profiles to engage their targets.

B. Common Attachments or Links Included in Star Blizzard's Spear-Phishing Emails

Star Blizzard's spear-phishing emails often contain malicious links or attachments. These are designed to trick the victim into providing their email account credentials, which the group then uses to gain unauthorized, persistent access to the victims' email accounts. They also create malicious domains that resemble legitimate organizations.

C. Common Indicators of Compromise (IOCs) Associated with Star Blizzard's Spear-Phishing Campaigns

Common IOCs associated with Star Blizzard's spear-phishing campaigns include:

- Unauthorized access to personal and corporate email accounts
- Setting up of mail-forwarding rules, which gives them ongoing visibility of a victim's correspondence and contact lists
- Access to mailing list data and a victim's contacts list, which they then use for follow-on targeting
- Use of compromised email accounts for further phishing activity
- Use of the open-source framework Evilginx in their spear-phishing campaigns, which allows them to harvest credentials and session cookies to bypass the use of two-factor authentication

D. Common File Types Included in Star Blizzard's Spear-Phishing Emails

Star Blizzard often includes malicious attachments in their spear-phishing emails and use file types such as PDFs, Word documents (.doc, .docx), Excel spreadsheets (.xls, .xlsx), or other types of files that can contain embedded scripts or macros

E. Common Domains or URLs Used in Star Blizzard's Spear-Phishing Campaigns

Star Blizzard has been known to use URLs that mimic legitimate file-sharing services. Some of the URLs look like this:

- https://drive.google.com/file/d/XXXXXXXXXXXXX X/view?usp=sharing
- https://onedrive.live.com/?authkey=%XXXXXXXXX XXXXXXXXXXXXXXXXX%XXXX&cid=8XXXX XXXXX9B7
- https://www.dropbox.com/s/XXXXXXXXXXXXX/St ar_Blizzard_Report.pdf?dl=0

These URLs may look legitimate, but they are actually designed to trick victims into entering their credentials or downloading malicious files

IV. Techniques of Star Blizzard Campaigns

A. Specific Techniques Used by Star Blizzard in Their Spear-Phishing Campaigns

Star Blizzard uses a variety of techniques in their spear-phishing campaigns:

- **Targeted Emails**: They predominantly send spear-phishing emails to targets' personal email addresses, although they have also used targets' corporate or business email addresses

- **Impersonation**: They create email accounts impersonating known contacts of their targets. They also create fake social media or networking profiles that impersonate respected experts
- **Malicious Domains**: They create malicious domains resembling legitimate organizations
- **Evilginx**: Star Blizzard actors use the open-source framework Evilginx in their spear-phishing campaigns, which allows them to harvest credentials and session cookies to bypass the use of two-factor authentication
- **Mail Forwarding**: After compromising the target's credentials, Star Blizzard sets up mail forwarding rules to establish ongoing visibility of a victim's correspondence and contact lists

B. *Common Social Engineering Techniques Used by Star Blizzard*

Star Blizzard's social engineering techniques include:

- **Research and Preparation**: They conduct extensive research using social media and professional networking platforms to identify topics of interest to engage their target
- **Impersonation**: They create email accounts and fake social media or networking profiles impersonating known contacts or respected experts
- **Building Rapport**: By leveraging the information gathered, they build a rapport with the target to make their spear-phishing attempts more convincing
- **Email Delivery**: The emails are crafted to appear legitimate and relevant to the target's interests or responsibilities, often containing malicious links or attachments
- **PDF Lures**: The PDF file sent by Star Blizzard is typically unreadable, with a prominent button purporting to enable reading the content. Pressing the button causes the default browser to open a link embedded in the PDF, leading to a credential-stealing

V. New Tactics, Techniques, and Procedures (TTPs) and Evasion Techniques of Star Blizzard

Star Blizzard has notably enhanced its ability to evade detection since 2022, focusing on improving its detection evasion capabilities. It was identified five new Star Blizzard evasive techniques:

- Use of Email Marketing Platforms: Star Blizzard has begun to utilize email marketing services like Mailerlite and HubSpot for directing phishing campaigns
- Password-Protected PDF Lure Documents: To aid in sneaking past email filters, Star Blizzard has started using password-protected PDF lure documents
- Use of Compromised Victim Email Accounts: They often use compromised victim email accounts to conduct spear-phishing activity against contacts of the original victim
- Malicious Links in Email Attachments: They use malicious links embedded in email attachments to direct victims to their credential-stealing sites
- Use of Compromised Credentials: Star Blizzard has been observed using compromised credentials, captured from fake log-in pages, to log in to valid victim user accounts

A. *Server-side scripts*

Star Blizzard has started using server-side scripts to prevent automated scanning of their actor-controlled servers. This tactic is an interesting approach that enhances their evasion capabilities.

Server-side scripts are scripts that run on the server, as opposed to client-side scripts that run in the user's browser. By using server-side scripts, Star Blizzard can control what information is sent to the client and what is kept on the server, making it harder for automated scanning tools to detect malicious activity.

The use of server-side scripts is part of a shift in tactics by Star Blizzard, demonstrating their adaptability and sophistication in evasion techniques. This tactic, along with others such as the use of email marketing platforms, password-protected PDF lure documents, and the use of compromised victim email accounts, has allowed Star Blizzard to continue its spear-phishing campaigns with increased stealth.

Here are some examples of functions that these server-side scripts might perform:

- **Collect and Send User Data**: In April 2023, Star Blizzard was observed moving away from using hCaptcha servers as the sole initial redirection. Instead, they started executing JavaScript code titled 'Collect and Send User Data' before redirecting the user
- **Refining the JavaScript Code**: In May 2023, the threat actor refined the JavaScript code, resulting in an updated version titled 'Docs', which is still in use today
- **Assessing the User's Environment**: The server-side JavaScript code is used to assess the user's environment. This information can be used to tailor the attack to the specific user, increasing the chances of success

The functions pluginsEmpty(), isAutomationTool(), and sendToBackend(data) are examples of the methods used in these scripts.

- **pluginsEmpty**(): This function checks if the plugins property of the navigator object is empty. Automated scanning tools often do not emulate plugins, so this function can help Star Blizzard identify and ignore such tools.
- **isAutomationTool**(): This function checks for signs that the client is an automated tool rather than a human user. This could involve checking for specific user agent

strings, the presence of certain JavaScript properties, or the speed of interactions.

- **sendToBackend**(data): This function sends collected data back to the server. The data could include the results of the previous checks or other information about the client's environment. This information can be used to tailor the attack to the specific user, increasing the chances of success.

B. Email marketing platform services

Star Blizzard has begun to utilize email marketing services like Mailerlite and HubSpot for directing its phishing campaigns. These platforms allow the threat actor to create an email campaign, which provides them with a dedicated subdomain on the service that is then used to create URLs. These URLs act as the entry point to a redirection chain ending at actor-controlled servers.

The use of these services offers several advantages to the threat actor. Firstly, emails sent through these platforms may be less likely to be flagged as spam or malicious by email filters, as they come from reputable services. Secondly, these platforms often provide tracking capabilities, allowing the threat actor to monitor the success of their campaigns.

Most Star Blizzard HubSpot email campaigns have targeted multiple academic institutions, think tanks, and other research organizations using a common theme, aimed at obtaining their credentials for a US grants management portal.

C. DNS provider

Star Blizzard has been using a Domain Name Service (DNS) provider to resolve actor-controlled domain infrastructure. This tactic allows the threat actor to manage and control the domains used in their attacks.

The use of a DNS provider offers several advantages to the threat actor. Firstly, it allows them to set up new domains quickly and easily for their attacks. Secondly, it can make it harder for defenders to block or take down the domains, as they are managed by a third-party service.

D. Randomizing DGA for actor registered domains

Star Blizzard has been using Domain Generation Algorithms (DGAs) to randomize the domain names for their infrastructure. DGAs are algorithms that generate a large number of domain names, which can be used as rendezvous points for command-and-control (C&C) servers or for other malicious purposes.

The use of DGAs makes it difficult for security teams and automated systems to predict and block malicious domains because the domains change frequently and can appear random. This technique is a form of domain fluxing, which helps the threat actor evade detection by blocklists, signature filters, reputation systems, and other security controls.

By using a DGA, Star Blizzard can systematically switch between domains during their attacks, making it harder for defenders to track and remove these domains. This tactic is part of their sophisticated approach to maintaining their malicious operations and avoiding disruption by cybersecurity measures.

E. Password-protected PDF lures or links to cloud-based file-sharing platforms

Star Blizzard has been using password-protected PDF lure documents or links to cloud-based file-sharing platforms as part of their spear-phishing campaigns. These tactics serve multiple purposes:

- **Password-Protected PDF Lure Documents**: By using password-protected PDFs, Star Blizzard can bypass some automated email scanning systems that cannot analyze the content of encrypted documents. The passwords for these documents are typically provided in the same phishing email or in a follow-up email.
- **Links to Cloud-Based File-Sharing Platforms**: These links lead to cloud-based platforms where the protected PDFs are stored. The use of legitimate file-sharing services can lend an air of credibility to the phishing attempt and may also evade detection by security systems that trust content hosted on these platforms.

The PDFs often contain a call to action, such as a button or link, which when clicked, redirects the user to a malicious site designed to steal credentials or other sensitive information. This technique is effective because it exploits the user's trust in familiar file-sharing services and the expectation of receiving legitimate documents.

VI. ATTACKS IMPACT

Microsoft did fall victim to a cyberattack by threat actor known as Blizzard, also referred to as Nobelium, APT29, or Cozy Bear. The attack was detected on January 12, 2024, and began in late November 2023.

The threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold. They then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of the senior leadership team and employees in cybersecurity, legal, and other functions.

The attackers exfiltrated some emails and attached documents, and the investigation indicates they were initially targeting email accounts for information related to Blizzard itself. The attack was not the result of a vulnerability in Microsoft products or services, and there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems.

A. Actions Taken by Microsoft in Response to the Blizzard Cyberattack and Secure Future Initiative

In response to the Blizzard cyberattack, Microsoft took immediate action to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. They have begun notifying employees whose email accounts were compromised during the attack.

Microsoft assured staff and the world that the attack was not due to any specific vulnerability in Microsoft products or services, and there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems.

Microsoft announced that they will apply their current security standards to Microsoft-owned legacy systems, even when these changes might cause disruption to existing business processes. They also plan to make significant changes to their internal security practices.

Microsoft's response underscores its commitment to addressing the threat posed by nation-state actors like Blizzard and its commitment to responsible transparency as recently affirmed in their Secure Future Initiative (SFI).

The Secure Future Initiative (SFI) is a program introduced by Microsoft in November 2023. The SFI rests on three key pillars:

- The development of AI-based cyber defenses.
- Advancements in fundamental software engineering.
- A strategic shift in the balance between security and business risk, acknowledging that the traditional calculus is no longer sufficient

VII. Defense (Microsoft Advisory)

A. Defense and protection guidance

In response to the ' Blizzard' cyberattack, Microsoft has provided guidance for defense and protection against such nation-state attacks. This guidance includes:

- **Multi-Factor Authentication (MFA)**: Microsoft emphasized the importance of enabling MFA, as the test tenant account compromised in the attack did not have MFA enabled.
- **Monitoring OAuth Applications**: Threat actors like Blizzard often use OAuth applications to help hide their activities. Microsoft recommends monitoring for suspicious OAuth applications and revoking any that are not recognized or needed.
- **Awareness of Social Engineering Attacks**: Microsoft Threat Intelligence has identified highly targeted social engineering attacks using credential theft phishing lures sent as Microsoft Teams chats by Blizzard. Awareness and training can help users recognize and avoid these attacks.
- **Network Traffic Analysis**: Blizzard used residential proxy networks to launch their attacks, routing traffic through a vast number of IP addresses also used by legitimate users. Monitoring and analyzing network traffic for suspicious patterns can help detect such activities.
- **Regular Patching and Updating**: Keeping systems and software up-to-date is crucial in defending against attacks that exploit known vulnerabilities.

Defend Against Malicious OAuth Applications

- **Audit Privilege Levels**: Use the Microsoft Graph Data Connect authorization portal to audit the privilege level of all identities, both users and service principals, in your tenant. Scrutinize privileges, especially if they belong to unknown identities, are attached to identities no longer in use, or are excessive.
- **Review ApplicationImpersonation Privileges**: Audit identities with ApplicationImpersonation privileges in Exchange Online, as these allow a service principal to impersonate a user. Use the PowerShell command Get-ManagementRoleAssignment -Role ApplicationImpersonation -GetEffectiveUsers to review these permissions.
- **Identify Malicious OAuth Apps**: Use anomaly detection policies to detect malicious OAuth apps that make sensitive Exchange Online administrative activities. Investigate and remediate any risky OAuth apps through App governance.
- **Conditional Access App Control**: Implement conditional access app control for users connecting from unmanaged devices to monitor and control how they access cloud apps.
- **Review Permissions**: Review any applications that hold EWS.AccessAsUser.All and EWS.full_access_as_app permissions. Remove them if they are no longer required.
- **Role-Based Access Control**: Implement granular and scalable role-based access control for applications in Exchange Online to ensure they are only granted access to the specific mailboxes required.

Protect Against Password Spray Attacks

- **Eliminate Insecure Passwords**: Encourage the use of strong, unique passwords and eliminate common or weak passwords that are easily guessable.
- **Educate Users**: Train users to review sign-in activity and report suspicious attempts as "This wasn't me".
- **Reset Compromised Passwords**: Reset passwords for any accounts targeted during a password spray attack, and investigate further if those accounts had system-level permissions.
- **Use Microsoft Entra ID Protection**: Detect, investigate, and remediate identity-based attacks with solutions like Microsoft Entra ID Protection.
- **Microsoft Purview Audit**: Investigate compromised accounts using Microsoft Purview Audit (Premium).
- **Enforce Password Protection**: Use Microsoft Entra Password Protection for Microsoft Active Directory Domain Services on-premises.
- **Risk Detections for User Sign-Ins**: Utilize risk detections to trigger multifactor authentication or password changes.
- **Password Spray Investigation Playbook**: Investigate any potential password spray activity using the password spray investigation playbook.

B. Detection and hunting guidance

In the wake of the Blizzard cyberattack, Microsoft has provided detailed guidance for detection and hunting of such threats. Hunting for Indicators of Compromise

- **Log Data Analysis**: Microsoft has provided detailed guidance on what to look for in log data to hunt and detect malicious activity associated with Blizzard
- **Posture Management** Tools: These tools can help organizations inventory all non-human identities and highlight unused OAuth applications, especially those with over-permissive access to impersonate every user when authenticating to Office 365 Exchange.

Microsoft's detection and hunting guidance for the Blizzard cyberattack involves reviewing Exchange Web Services (EWS) activity and using Microsoft Entra ID Protection, which has several relevant detections that help organizations identify these techniques or additional activity that may indicate anomalous activity. The use of residential proxy network infrastructure by threat actors is generally more likely to generate Microsoft Entra ID Protection alerts due to inconsistencies in patterns of user behavior compared to legitimate activity.

Microsoft Entra ID Protection alerts that can help indicate threat activity associated with this attack include:

- **Unfamiliar sign-in properties**: This alert flags sign-ins from networks, devices, and locations that are unfamiliar to the user.
- **Password spray**: This risk detection is triggered when a password spray attack has been successfully performed.
- **Threat intelligence**: This alert indicates user activity that is unusual for the user or consistent with known attack patterns.
- **Suspicious sign-ins (workload identities)**: This alert indicates sign-in properties or patterns that are unusual for the related service principal.

C. XDR and SIEM alerts and protection

Microsoft Defender for Cloud Apps and Microsoft Defender XDR also provide alerts that can help indicate associated threat activity. These alerts include indications of a significant increase in calls to the Exchange Web Services API, suspicious metadata associated with mail-related activity, and the creation of an OAuth application that accessed mailbox items.

Microsoft Defender XDR and Microsoft Sentinel customers can also use specific hunting queries and analytic rules to find related activity in their networks. These include queries to find sign-ins by a labeled password spray IP and rules to identify password spray attempts, the granting of full_access_as_app permission to an OAuth application, and the addition of services principal/user with elevated permissions

Once an actor decides to use OAuth applications in their attack, a variety of follow-on activities can be identified in alerts to help organizations identify and investigate suspicious activity.

The following Microsoft Defender for Cloud Apps alerts can help indicate associated threat activity:

- App with application-only permissions accessing numerous emails – A multi-tenant cloud app with application-only permissions showed a significant increase in calls to the Exchange Web Services API specific to email enumeration and collection. The app might be involved in accessing and retrieving sensitive email data.
- Increase in app API calls to EWS after a credential update – This detection generates alerts for non-Microsoft OAuth apps where the app shows a significant increase in calls to Exchange Web Services API within a few days after its certificates/secrets are updated or new credentials are added.
- Increase in app API calls to EWS – This detection generates alerts for non-Microsoft OAuth apps that exhibit a significant increase in calls to the Exchange Web Services API. This app might be involved in data exfiltration or other attempts to access and retrieve data.
- App metadata associated with suspicious mail-related activity – This detection generates alerts for non-Microsoft OAuth apps with metadata, such as name, URL, or publisher, that had previously been observed in apps with suspicious mail-related activity. This app might be part of an attack campaign and might be involved in exfiltration of sensitive information.
- Suspicious user created an OAuth app that accessed mailbox items – A user that previously signed on to a medium- or high-risk session created an OAuth application that was used to access a mailbox using sync operation or multiple email messages using bind operation. An attacker might have compromised a user account to gain access to organizational resources for further attacks.

The following Microsoft Defender XDR alert can indicate associated activity:

- Suspicious user created an OAuth app that accessed mailbox items – A user who previously signed in to a medium- or high-risk session created an OAuth application that was used to access a mailbox using sync operation or multiple email messages using bind operation. An attacker might have compromised a user account to gain access to organizational resources for further attacks

Extended Detection and Response (XDR) and Security Information and Event Management (SIEM) systems can provide alerts and protection against malicious activities such as those carried out by the Blizzard threat group.

Microsoft Defender for Cloud Apps can generate alerts for various suspicious activities, including:

- An app with application-only permissions accessing numerous emails.

- An increase in app API calls to Exchange Web Services (EWS) , especially after a credential update.
- App metadata associated with suspicious mail-related activity.
- A suspicious user creating an OAuth app that accessed mailbox items.
- Microsoft Defender XDR can also generate an alert when a suspicious user creates an OAuth app that accesses mailbox items.

According to Microsoft guidances these alerts can help organizations identify and investigate suspicious activities related to OAuth applications, which are often used in attacks like those carried out by Blizzard. By monitoring for these types of activities, organizations can better protect themselves against similar threats

- To detect password spray attacks, security teams can use various hunting queries that analyze log data for signs of such attacks. Here are some examples of hunting queries and techniques that can be used:
- Failed Authentication Attempts Across Multiple Accounts: Look for sudden spikes in the number of failed login attempts or locked accounts, which can indicate a password spray attack
- Sign-in Attempts from Suspicious Locations: Monitor sign-in attempts from locations that are unusual for the user, as attackers may use IP addresses from different geographic regions
- Unusual Sign-in Times: Password spray attacks often occur at odd hours when fewer users are likely to be active, so monitoring for authentication attempts during these times can be useful
- Low and Slow Attack Indicators: Detect password spray attacks that attempt to stay under the radar by not triggering account lockouts or bad password thresholds
- Advanced Hunting Queries: Use a query-based threat hunting tool like Microsoft Defender's Advanced Hunting to inspect events in your network and gather more information related to password spray alerts
- Alert Classification: Check whether the user received other alerts before the password spray activity, such as impossible travel alerts, activity from infrequent countries/regions, or suspicious email deletion activity

Here are some specific hunting queries provided by Microsoft:

```
// Find sign-ins by a labeled password spray IP
IdentityLogonEvents
| where Timestamp between (startTime .. endTime)
| where isnotempty(IPTags) and not(IPTags has_any('Azure','Internal Network IP','branch office'))
| where IPTags has_any ("Brute force attacker", "Password spray attacker", "malicious", "Possible Hackers")
```

```
// Find MailItemsAccessed or SaaS actions performed by a labeled password spray IP
CloudAppEvents
| where Timestamp between (startTime .. endTime)
| where isnotempty(IPTags) and not(IPTags has_any('Azure','Internal Network IP','branch office'))
| where IPTags has_any ("Brute force attacker", "Password spray attacker", "malicious", "Possible Hackers")
```

Network traffic analysis can be a powerful tool in detecting password spray attacks. Here are some methods that organizations can use:

- Intrusion Detection Systems (IDS): IDS tools monitor network traffic and flag suspicious login activities. They analyze login attempts, account lockouts, and authentication failures to identify potential password spraying attacks
- Security Monitoring: Continuous monitoring of user login activities and abnormal patterns can help identify potential attacks. Monitoring tools can track login attempts from unusual locations, or at unusual times, which could indicate a password spraying attack
- User Behavior Analysis: Analyzing user behavior can help detect suspicious activities. Deviations from normal behavior, such as login attempts outside of regular working hours or simultaneous login attempts from multiple locations, can be red flags for password spraying attacks
- Configure Security Password Settings: If your organization utilizes a Security Logging Platform, ensure that it's configured to identify or detect failed login attempts across all systems. This will help you detect those tell-tale signs of password spraying attacks in the future
- Monitoring and Logging: These are some of the best proactive ways to detect password-spraying attacks. They help to detect failed login attempts and inform the IT Administrator accordingly. For example, if there are 5 unsuccessful login attempts, the password policy locks out the user account, and the network monitoring solution triggers an alarm to the IT Administrator
- SIEM (Security Information and Event Management): In case there is unusual behavior in your organization, your SIEM will pick it up. SIEM solutions aggregate and analyze event data in real time from network devices, servers, domain controllers and more, providing security intelligence for real-time analysis of security alerts generated by applications and network hardware

Organizations can use OAuth application permissions to detect potential security vulnerabilities in several ways:

- Investigate and Remediate Risky OAuth Apps: Organizations can use tools like Microsoft Defender for Cloud Apps to investigate and remediate risky OAuth apps. This involves scrutinizing apps that have not been updated recently, apps that have irrelevant permissions,

and apps that appear suspicious based on their name, publisher, or URL. The OAuth app audit can be exported for further analysis of the users who authorized an app

- Create Policies to Control OAuth Apps: Organizations can set permission policies to get automated notifications when an OAuth app meets certain criteria. For example, alerts can be set up for apps that require a high permission level. OAuth app policies enable organizations to investigate which permissions each app requested and which users authorized those permissions
- Identify Vulnerabilities in OAuth Implementation: Vulnerabilities can arise in the client application's implementation of OAuth as well as in the configuration of the OAuth service itself. Identifying and exploiting these vulnerabilities can help organizations protect their own applications against similar attacks
- Monitor for Malicious OAuth Applications: Threat actors can misuse OAuth applications to automate financially driven attacks. Monitoring for such misuse can help organizations detect and respond to potential security vulnerabilities. For example, Microsoft provides queries that can be used to identify high outbound email senders and suspicious email events
- Understand the Impact of Malicious OAuth Application Consent: If a user grants access to a malicious third-party application, the application can access the user's data and perform actions on their behalf. Understanding the impact of such actions can help organizations develop strategies to detect and mitigate potential security vulnerabilities