Midnight Blizzard: Guidance for responders on nation-state attack | Microsoft Security Blog

Clip source: Midnight Blizzard: Guidance for responders on nation-state attack | Microsoft Security Blog

Midnight Blizzard: Guidance for responders on nation-state attack

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM. The latest information from the Microsoft Security and Response Center (MSRC) is posted here.

As stated in the MSRC blog, given the reality of threat actors that are well resourced and funded by nation states, we are shifting the balance we need to strike between security and business risk – the traditional sort of calculus is simply no longer sufficient. For Microsoft, this incident has highlighted the urgent need to move even faster.

If the same team were to deploy the legacy tenant today, mandatory Microsoft policy and workflows would ensure MFA and our active protections are enabled to comply with current policies and guidance, resulting in better protection against these sorts of attacks.

Microsoft was able to identify these attacks in log data by reviewing Exchange Web Services (EWS) activity and using our audit logging features, combined with our extensive knowledge of Midnight Blizzard. In this blog, we provide more details on

Midnight Blizzard, our preliminary and ongoing analysis of the techniques they used, and how you may use this information pragmatically to protect, detect, and respond to similar threats in your own environment.

Using the information gained from Microsoft's investigation into Midnight Blizzard, Microsoft Threat Intelligence has identified that the same actor has been targeting other organizations and, as part of our usual notification processes, we have begun notifying these targeted organizations.

It's important to note that this investigation is still ongoing, and we will continue to provide details as appropriate.

Midnight Blizzard

Midnight Blizzard (also known as NOBELIUM) is a Russia-based threat actor attributed by the US and UK governments as the Foreign Intelligence Service of the Russian Federation, also known as the SVR. This threat actor is known to primarily target governments, diplomatic entities, non-governmental organizations (NGOs) and IT service providers, primarily in the US and Europe. Their focus is to collect intelligence through longstanding and dedicated espionage of foreign interests that can be traced to early 2018. Their operations often involve compromise of valid accounts and, in some highly targeted cases, advanced techniques to compromise authentication mechanisms within an organization to expand access and evade detection.

Midnight Blizzard is consistent and persistent in their operational targeting, and their objectives rarely change. Midnight Blizzard's espionage and intelligence gathering activities leverage a variety of initial access, lateral movement, and persistence techniques to collect information in support of Russian foreign policy interests. They utilize diverse initial access methods ranging from stolen credentials to supply chain attacks, exploitation of on-premises environments to laterally move to the cloud, and exploitation of service providers' trust chain to gain access to downstream customers. Midnight Blizzard is also adept at identifying and abusing OAuth applications to move laterally across cloud environments and for post-compromise activity, such as email collection. OAuth is an open standard for token-based authentication and

authorization that enables applications to get access to data and resources based on permissions set by a user.

Midnight Blizzard is tracked by partner security vendors as APT29, UNC2452, and Cozy Bear.

Midnight Blizzard observed activity and techniques

Initial access through password spray

Midnight Blizzard utilized password spray attacks that successfully compromised a legacy, non-production test tenant account that did not have multifactor authentication (MFA) enabled. In a password-spray attack, the adversary attempts to sign into a large volume of accounts using a small subset of the most popular or most likely passwords. In this observed Midnight Blizzard activity, the actor tailored their password spray attacks to a limited number of accounts, using a low number of attempts to evade detection and avoid account blocks based on the volume of failures. In addition, as we explain in more detail below, the threat actor further reduced the likelihood of discovery by launching these attacks from a distributed residential proxy infrastructure. These evasion techniques helped ensure the actor obfuscated their activity and could persist the attack over time until successful.

Malicious use of OAuth applications

Threat actors like Midnight Blizzard compromise user accounts to create, modify, and grant high permissions to OAuth applications that they can misuse to hide malicious activity. The misuse of OAuth also enables threat actors to maintain access to applications, even if they lose access to the initially compromised account. Midnight Blizzard leveraged their initial access to identify and compromise a legacy test OAuth application that had elevated access to the Microsoft corporate environment. The actor created additional malicious OAuth applications. They created a new user account to grant consent in the Microsoft corporate environment to the actor controlled malicious OAuth applications. The threat actor then used the legacy test OAuth application to

grant them the Office 365 Exchange Online *full_access_as_app* role, which allows access to mailboxes.

Collection via Exchange Web Services

Midnight Blizzard leveraged these malicious OAuth applications to authenticate to Microsoft Exchange Online and target Microsoft corporate email accounts.

Use of residential proxy infrastructure

As part of their multiple attempts to obfuscate the source of their attack, Midnight Blizzard used residential proxy networks, routing their traffic through a vast number of IP addresses that are also used by legitimate users, to interact with the compromised tenant and, subsequently, with Exchange Online. While not a new technique, Midnight Blizzard's use of residential proxies to obfuscate connections makes traditional indicators of compromise (IOC)-based detection infeasible due to the high changeover rate of IP addresses.

Defense and protection guidance

Due to the heavy use of proxy infrastructure with a high changeover rate, searching for traditional IOCs, such as infrastructure IP addresses, is not sufficient to detect this type of Midnight Blizzard activity. Instead, Microsoft recommends the following guidance to detect and help reduce the risk of this type of threat:

Defend against malicious OAuth applications

- Audit the current privilege level of all identities, both users and service principals, in your tenant using Microsoft Graph Data Connect authorization portal to understand which identities are highly privileged. Privilege should be scrutinized more closely if it belongs to an unknown identity, is attached to identities that are no longer in use, or is not fit for purpose. Identities can often be granted privilege over and above what is required. Defenders should pay attention to apps with app-only permissions as those apps may have over-privileged access.

- Audit identities that hold *ApplicationImpersonation* privileges in Exchange Online. *ApplicationImpersonation* allows a caller, such as a service principal, to impersonate a user and perform the same operations that the user themselves could perform. Impersonation privileges like this can be configured for services that interact with a mailbox on a user's behalf, such as video conferencing or CRM systems. If misconfigured, or not scoped appropriately, these identities can have broad access to all mailboxes in an environment. Permissions can be reviewed in the Exchange Online Admin Center, or via PowerShell:

```
Get-ManagementRoleAssignment -Role ApplicationImpersonation -GetEffectiveUsers
```

- Identify malicious OAuth apps using anomaly detection policies. Detect malicious OAuth apps that make sensitive Exchange Online administrative activities through App governance. Investigate and remediate any risky OAuth apps.
- Implement conditional access app control for users connecting from unmanaged devices.
- Midnight Blizzard has also been known to abuse OAuth applications in past attacks against other organizations using the *EWS.AccessAsUser.All* Microsoft Graph API role or the Exchange Online ApplicationImpersonation role to enable access to email. Defenders should review any applications that hold *EWS.AccessAsUser.All* and *EWS.full_access_as_app* permissions and understand whether they are still required in your tenant. If they are no longer required, they should be removed.
- If you require applications to access mailboxes, granular and scalable access can be implemented using role-based access control for applications in Exchange Online. This access model ensures applications are only granted to the specific mailboxes required.

Protect against password spray attacks

- Eliminate insecure passwords.

- Educate users to review sign-in activity and mark suspicious sign-in attempts as "This wasn't me".
- Reset account passwords for any accounts targeted during a password spray attack. If a targeted account had system-level permissions, further investigation may be warranted.
- Detect, investigate, and remediate identity-based attacks using solutions like Microsoft Entra ID Protection.
- Investigate compromised accounts using Microsoft Purview Audit (Premium).
- Enforce on-premises Microsoft Entra Password Protection for Microsoft Active Directory Domain Services.
- Use risk detections for user sign-ins to trigger multifactor authentication or password changes.
- Investigate any possible password spray activity using the password spray investigation playbook.

Detection and hunting guidance

By reviewing Exchange Web Services (EWS) activity, combined with our extensive knowledge of Midnight Blizzard, we were able to identify these attacks in log data. We are sharing some of the same hunting methodologies here to help other defenders detect and investigate similar attack tactics and techniques, if leveraged against their organizations. The audit logging that Microsoft investigators used to discover this activity was also made available to a broader set of Microsoft customers last year.

Identity alerts and protection

Microsoft Entra ID Protection has several relevant detections that help organizations identify these techniques or additional activity that may indicate anomalous activity that needs to be investigated. 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 (such as location, diversity of IP addresses, etc.) that may be beyond the control of the threat actor.

The following Microsoft Entra ID Protection alerts can help indicate threat activity associated with this attack:

- **Unfamiliar sign-in properties** – This alert flags sign-ins from networks, devices, and locations that are unfamiliar to the user.
- **Password spray** – A password spray attack is where multiple usernames are attacked using common passwords in a unified brute force manner to gain unauthorized access. This risk detection is triggered when a password spray attack has been successfully performed. For example, the attacker has successfully authenticated in the detected instance.
- **Threat intelligence** – This alert indicates user activity that is unusual for the user or consistent with known attack patterns. This detection is based on Microsoft's internal and external threat intelligence sources.
- **Suspicious sign-ins (workload identities)** – This alert indicates sign-in properties or patterns that are unusual for the related service principal.

XDR and SIEM alerts and protection

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 Serves API. This app might be involved in data exfiltration or other attempts to access and retrieve data.

- **App metadata associated with suspicious mal-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.

Related hunting queries

Microsoft Defender XDR customers can run the following query to find related activity in their networks:

- 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")
```

Microsoft Sentinel customers can use the following analytic rules to find related activity in their network.

- Password spray attempts – This query helps identify evidence of password spray activity against Microsoft Entra ID applications.
- OAuth application being granted full_access_as_app permission – This detection looks for the *full_access_as_app* permission being granted to an OAuth application with Admin Consent. This permission provides access to Exchange mailboxes via the EWS API and could be exploited to access sensitive data. The application granted this permission should be reviewed to ensure that it is necessary for the application's function.

- Addition of services principal/user with elevated permissions – This rule looks for a service principal being granted permissions that could be used to add a Microsoft Entra ID object or user account to an Admin directory role.
- Offline access via OAuth for previously unknown Azure application – This rule alerts when a user consents to provide a previously unknown Azure application with offline access via OAuth. Offline access will provide the Azure app with access to the resources without requiring two-factor authentication. Consent to applications with offline access should generally be rare.

Microsoft Sentinel customers can also use this hunting query:

- OAuth apps reading mail both via GraphAPI and directly – This query returns OAuth Applications that access mail both directly and via Graph, allowing review of whether such dual access methods follow expected user patterns.

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

Microsoft customers can use the following reports in Microsoft Defender Threat Intelligence to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments:

- Midnight Blizzard
- Midnight Blizzard credential attacks
- Threat overview: Cloud identity abuse
- Techniques profile: Password spray attacks