Midnight Blizzard conducts targeted social engineering over Microsoft Teams

microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

August 2, 2023

By

Microsoft Threat Intelligence has identified highly targeted social engineering attacks using credential theft phishing lures sent as Microsoft Teams chats by the threat actor that Microsoft tracks as Midnight Blizzard (previously tracked as NOBELIUM). This latest attack, combined with past activity, further demonstrates Midnight Blizzard's ongoing execution of their objectives using both new and common techniques. In this latest activity, the threat actor uses previously compromised Microsoft 365 tenants owned by small businesses to create new domains that appear as technical support entities. Using these domains from compromised tenants, Midnight Blizzard leverages Teams messages to send lures that attempt to steal credentials from a targeted organization by engaging a user and eliciting

approval of multifactor authentication (MFA) prompts. As with any social engineering lures, we encourage organizations to reinforce security best practices to all users and reinforce that any authentication requests not initiated by the user should be treated as malicious.

Our current investigation indicates this campaign has affected fewer than 40 unique global organizations. The organizations targeted in this activity likely indicate specific espionage objectives by Midnight Blizzard directed at government, non-government organizations (NGOs), IT services, technology, discrete manufacturing, and media sectors. Microsoft has mitigated the actor from using the domains and continues to investigate this activity and work to remediate the impact of the attack. As with any observed nation-state actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to secure their environments.

Midnight Blizzard (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-government 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. 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, exploitation of service providers' trust chain to gain access to downstream customers, as well as the Active Directory Federation Service (AD FS) malware known as FOGGYWEB and MAGICWEB. Midnight Blizzard (NOBELIUM) is tracked by partner security vendors as APT29, UNC2452, and Cozy Bear.

Midnight Blizzard's latest credential phishing attack

Midnight Blizzard regularly utilizes token theft techniques for initial access into targeted environments, in addition to authentication spear-phishing, password spray, brute force, and other credential attacks. The attack pattern observed in malicious activity since at least late May 2023 has been identified as a subset of broader credential attack campaigns that we attribute to Midnight Blizzard.

Use of security-themed domain names in lures

To facilitate their attack, the actor uses Microsoft 365 tenants owned by small businesses they have compromised in previous attacks to host and launch their social engineering attack. The actor renames the compromised tenant, adds a new onmicrosoft.com

subdomain, then adds a new user associated with that domain from which to send the outbound message to the target tenant. The actor uses security-themed or product name-themed keywords to create a new subdomain and new tenant name to lend legitimacy to the messages. These precursory attacks to compromise legitimate Azure tenants and the use of homoglyph domain names in social engineering lures are part of our ongoing investigation. Microsoft has mitigated the actor from using the domains.

Social engineering attack chain

In this activity, Midnight Blizzard either has obtained valid account credentials for the users they are targeting, or they are targeting users with passwordless authentication configured on their account – both of which require the user to enter a code that is displayed during the authentication flow into the prompt on the Microsoft Authenticator app on their mobile device.

After attempting to authenticate to an account where this form of MFA is required, the actor is presented with a code that the user would need to enter in their authenticator app. The user receives the prompt for code entry on their device. The actor then sends a message to the targeted user over Microsoft Teams eliciting the user to enter the code into the prompt on their device.

Step 1: Teams request to chat

The target user may receive a Microsoft Teams message request from an external user masquerading as a technical support or security team.

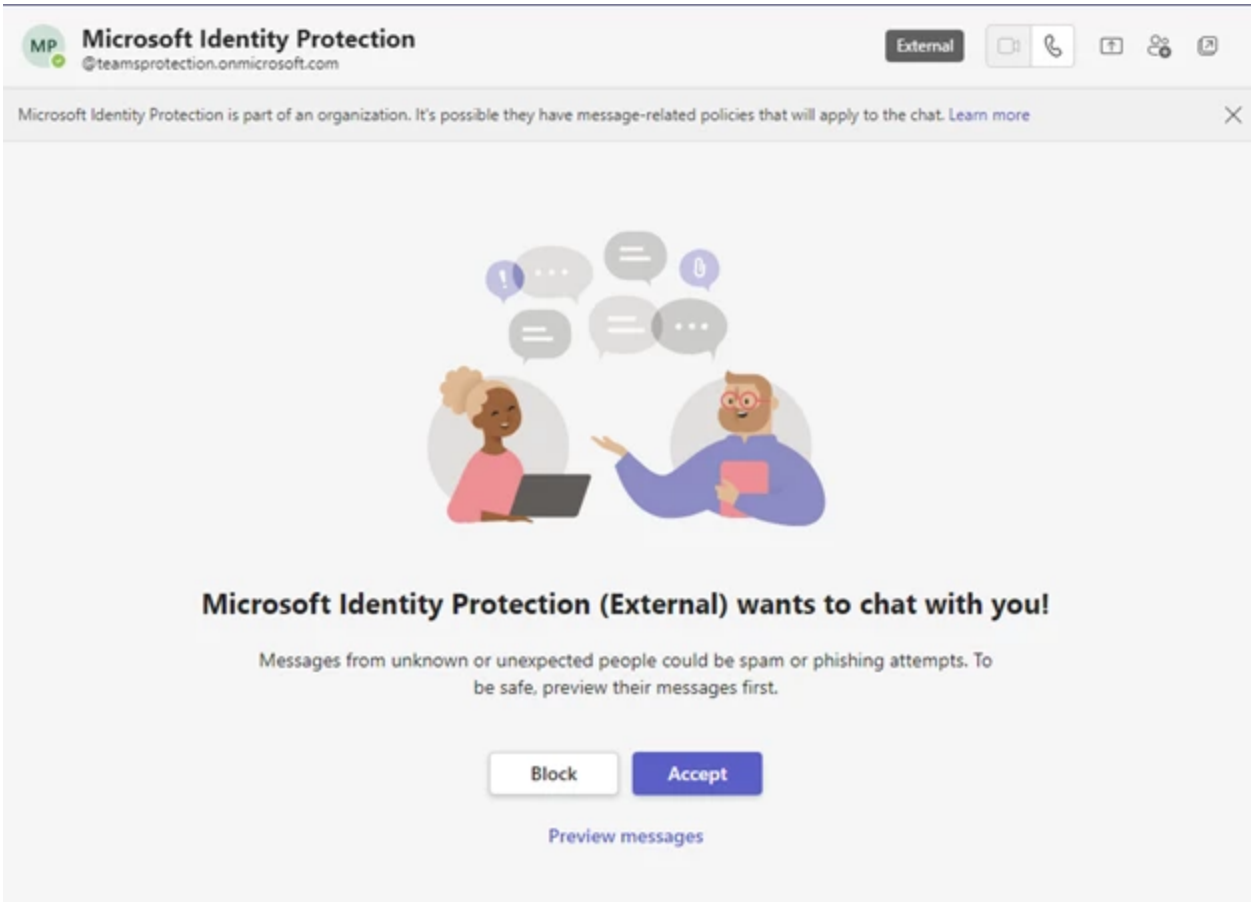


Figure 1: Screenshot of a Microsoft Teams message request from a Midnight Blizzard-controlled account

Step 2: Request authentication app action

If the target user accepts the message request, the user then receives a Microsoft Teams message from the attacker attempting to convince them to enter a code into the Microsoft Authenticator app on their mobile device.

Figure 2: A Microsoft Teams prompt with a code and instructions.

Step 3: Successful MFA authentication

If the targeted user accepts the message request and enters the code into the Microsoft Authenticator app, the threat actor is granted a token to authenticate as the targeted user. The actor gains access to the user's Microsoft 365 account, having completed the authentication flow.

The actor then proceeds to conduct post-compromise activity, which typically involves information theft from the compromised Microsoft 365 tenant. In some cases, the actor attempts to add a device to the organization as a managed device via Microsoft Entra ID

(formerly Azure Active Directory), likely an attempt to circumvent conditional access policies configured to restrict access to specific resources to managed devices only.

Recommendations

Microsoft recommends the following mitigations to reduce the risk of this threat.

- Pilot and start deploying phishing-resistant authentication methods for users.
- Implement Conditional Access authentication strength to require phishing-resistant authentication for employees and external users for critical apps.
- Specify trusted Microsoft 365 organizations to define which external domains are allowed or blocked to chat and meet.
- Keep Microsoft 365 auditing enabled so that audit records could be investigated if required.
- Understand and select the best access settings for external collaboration for your organization.
- Allow only known devices that adhere to Microsoft's recommended security baselines.
- Educate users about social engineering and credential phishing attacks, including refraining from entering MFA codes sent via any form of unsolicited messages.
- Educate Microsoft Teams users to verify 'External' tagging on communication attempts from external entities, be cautious about what they share, and , and never share their account information or authorize sign-in requests over chat.
- Educate users to review sign-in activity and mark suspicious sign-in attempts as "This wasn't me".
- Implement Conditional Access App Control in Microsoft Defender for Cloud Apps for users connecting from unmanaged devices.

Indicators of compromise

Indicator	Type	Description
mlcrosoftaccounts.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
msftonlineservices.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
msonlineteam.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
msftservice.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
noreplyteam.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain

accounteam.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
teamsprotection.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
identityverification.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
msftprotection.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
accountsverification.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
azuresecuritycenter.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain

Hunting guidance

Microsoft Purview

Customers hunting for related activity in their environment can identify users that were targeted with the phishing lure using content search in Microsoft Purview. A content search can be created for selected Exchange mailboxes (which include Teams messages) using the following keywords (remove the [] around the "." before use):

- *mlcrosoftaccounts.onmicrosoft[.]com*
- *msftonlineservices.onmicrosoft[.]com*
- *msonlineteam.onmicrosoft[.]com*
- *msftservice.onmicrosoft[.]com*
- *noreplyteam.onmicrosoft[.]com*
- *accounteam.onmicrosoft[.]com*
- *teamsprotection.onmicrosoft[.]com*
- *identityverification.onmicrosoft[.]com*
- *msftprotection.onmicrosoft[.]com*
- *accountsverification.onmicrosoft[.]com*
- *azuresecuritycenter.onmicrosoft[.]com*
- *We detected a recent change to your preferred Multi-Factor Authentication (MFA)*

The search results will include the messages that match the criteria. The first result will appear to be from *<threadid>@unq.gbl.spaces* addressed to the target user and the threat actor (i.e., the request to chat as described in Step 1), followed by the message sent by the threat actor, as shown in the Microsoft Purview image below:

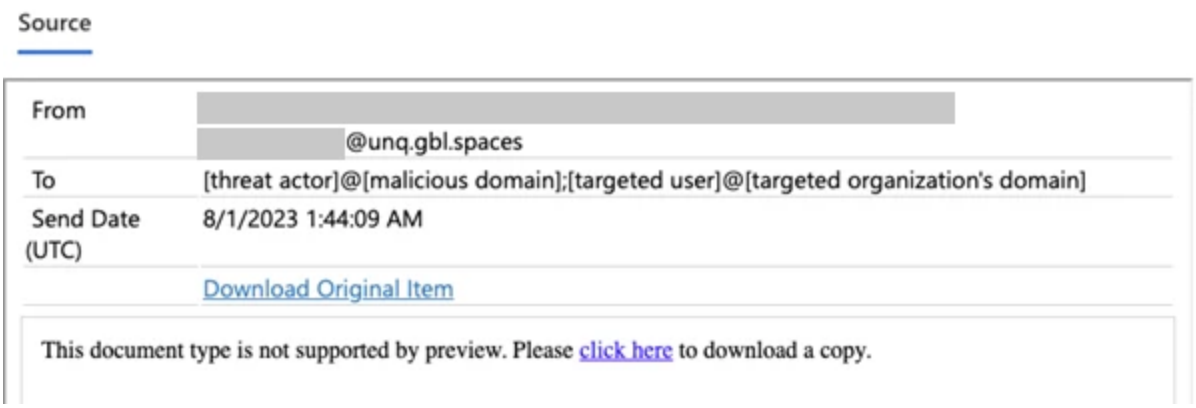


Figure 3: Message sent by the threat actor, as shown in Microsoft Purview

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with “TI map”) to automatically match indicators associated with Midnight Blizzard in Microsoft Defender Threat Intelligence 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 Defender Threat Intelligence connector and analytics rule deployed in their Sentinel workspace. Learn more about the Content Hub.

Microsoft Sentinel also has a range of detection and threat hunting content that customers can use to detect activity related to the activity described in this blog:

Further reading

Read about the threat actor Midnight Blizzard (formerly tracked as NOBELIUM).

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

To get notified about new publications and to join discussions on social media, follow us on Twitter at https://twitter.com/MsftSecIntel.

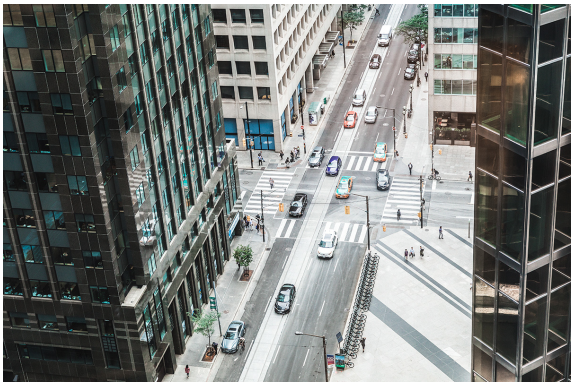
Related Posts

MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone

Microsoft security researchers have discovered a post-compromise capability we're calling MagicWeb, which is used by a threat actor we track as NOBELIUM to maintain persistent access to compromised environments.

New sophisticated email-based attack from NOBELIUM

Microsoft Threat Intelligence Center (MSTIC) has uncovered a wide-scale malicious email campaign operated by NOBELIUM, the threat actor behind the attacks against SolarWinds, the SUNBURST backdoor, TEARDROP malware, GoldMax malware, and other related components. The campaign, initially observed and tracked by Microsoft since January 2021, evolved over a series of waves demonstrating significant experimentation.



FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor

In-depth analysis of newly detected NOBELIUM malware: a post-exploitation backdoor that Microsoft Threat Intelligence Center (MSTIC) refers to as FoggyWeb. NOBELIUM uses FoggyWeb to remotely exfiltrate the configuration database of compromised AD FS servers, decrypted token-signing certificate, and token-decryption certificate, as well as to download and execute additional components.

Breaking down NOBELIUM's latest early-stage toolset

In this blog, we highlight four tools representing a unique infection chain utilized by NOBELIUM: EnvyScout, BoomBox, NativeZone, and VaporRage. These tools have been observed being used in the wild as early as February 2021 attempting to gain a foothold on a variety of sensitive diplomatic and government entities.