This is a technical bulletin intended for technical audiences

****

Number: AL23-013
Date: August 3, 2023

Title

Midnight Blizzard conducts targeted social engineering over Microsoft Teams

Audience

This Alert is intended for IT professionals and managers of notified organizations.

Purpose

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional detection and mitigation advice to recipients. The Canadian Centre for Cyber Security ("Cyber Centre") is also available to provide additional assistance regarding the content of this Alert to recipients as requested.

Details

On August 2, 2023, Microsoft Threat Intelligence published an advisory [1] highlighting details of targeted social engineering activity by threat actor Midnight Blizzard (previously tracked by Microsoft as NOBELIUM) taking place over Microsoft Teams. Using previously compromised Microsoft 365 tenants renamed to appear as technical support entities, Midnight Blizzard steals credentials by sending messages over Teams to engage with users and bypass multifactor authentication (MFA) prompts.

While this campaign has affected fewer than 40 organizations globally, the Cyber Centre has received reports of attempts within Canada.

Suggested Actions

The Cyber Centre recommends organizations:

- Review the Microsoft advisory and look for indicators of compromise to determine if related activity has occurred. If activity has been detected and a compromise has occurred:
    - Reimage compromised systems.
    - Reset all potentially compromised credentials.

In addition, the Cyber Centre strongly recommends that organizations review and implement the Cyber Centre's Top 10 IT Security Actions [2] with an emphasis on the following topics.

- Phishing Awareness. This includes both identification of phishing but also procedures on what to do if a phishing email is received.
- The Cyber Centre has several publications available on Phishing Awareness [3] [4] [5].
- Phishing Technical Controls.

- Multi-factor Authentication.
    - Where feasible, implement phishing-resistant MFA like FIDO2 security keys, Windows Hello,
      and Certificate Based Auth.

- Enforcing the Management of Administrative Privileges.
    - Minimize the number of administrators and privileged roles.
    - Conduct administrative activities on managed, hardened, and dedicated devices with restricted access to email, web browsing and outside connectivity.
    - Enable two-person integrity when resetting administrative accounts to minimize successful
      social engineering activities.

- Remote Access Management and Controls.
    - Network segmentation and demilitarized zones (DMZs).

- Configure firewalls to selectively control and monitor traffic passed between zones.

- Implementing location and device based conditional access policies.

- Software Management and Deployment Controls.

- Business continuity planning, which is tested and validated.

References

[1] Midnight Blizzard conducts targeted social engineering over Microsoft Teams
https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

[2] Top 10 IT Security Actions
https://cyber.gc.ca/en/top-10-it-security-actions

[3] Don't Take the Bait: Recognize and Avoid Phishing Attacks
https://cyber.gc.ca/en/guidance/dont-take-bait-recognize-and-avoid-phishing-attacks

[4] Spotting Malicious Email Messages
https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100

[5] Spear phishing: What it is and how you can protect yourself
https://www.getcybersafe.gc.ca/en/blogs/spear-phishing-what-it-and-how-you-can-protect-yourself

****