Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

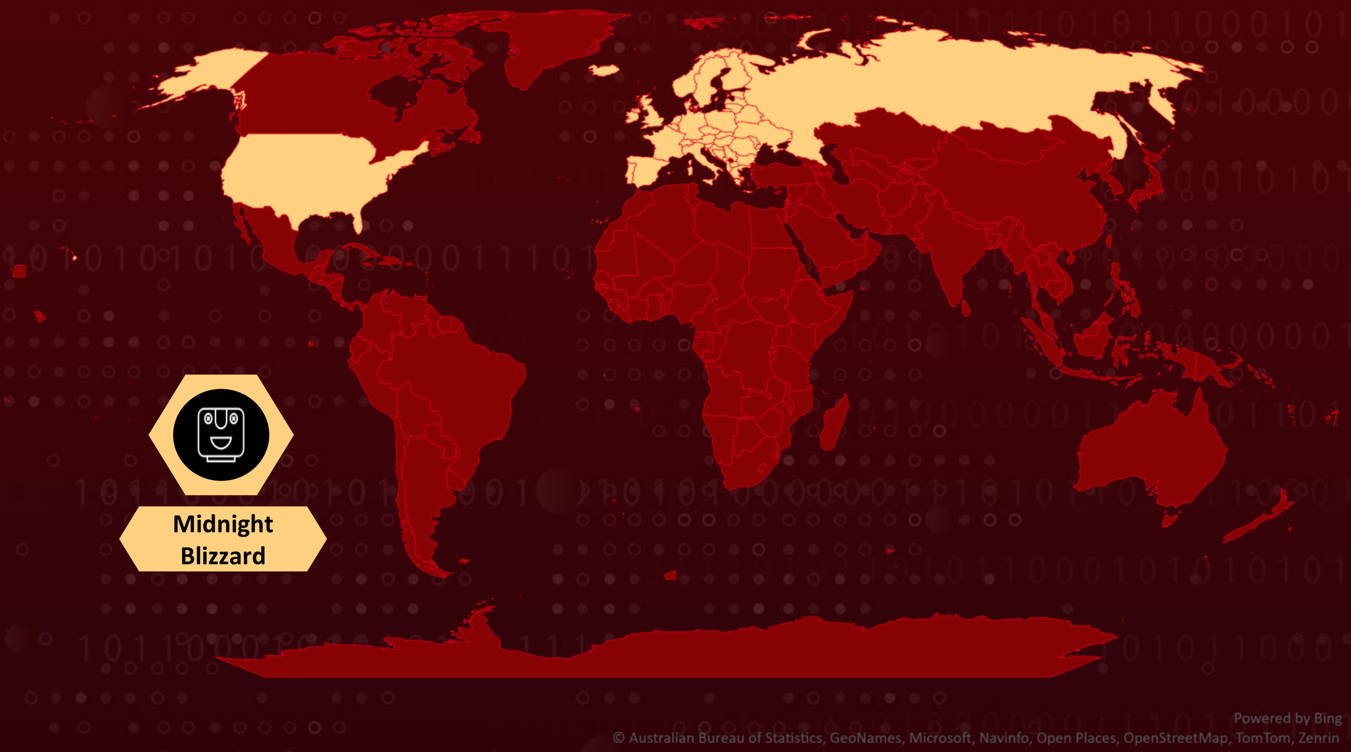
Midnight Blizzard Exploiting Legacy OAuth for Lateral Movement

Date of Publication	Admiralty Code	TA Number
January 29, 2024	A1	TA2024036

Summary

Attack Began: November 2023
Targeted Countries: US and Europe
Threat Actor: Midnight Blizzard (aka APT 29, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo)
Targeted Industries: Governments, Diplomatic entities, Non-Governmental Organizations (NGOs) and IT service providers
Attack: Midnight Blizzard exploited a legacy test OAuth application with elevated access due to a common password and lack of multi-factor authentication (MFA). The attackers leveraged this access to move laterally within Microsoft's network, potentially exfiltrating data and gaining broader control.

Attack Regions


Midnight Blizzard
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Microsoft confirmed that the Russian state-backed cyberespionage group Midnight Blizzard, also known as Nobelium or APT29, breached its systems in November 2023, stealing emails from executives' accounts. Microsoft discovered this breach on January 12, 2024, and identified the malicious activity through Exchange Web Services logs and knowledge of Russian state-sponsored hacking techniques.

#2 The attack involved password spray attacks targeting a non-production test tenant account without multifactor authentication (MFA). Midnight Blizzard employed evasion techniques, such as launching attacks from distributed residential proxy infrastructure, to avoid detection. The threat actor also misused OAuth application for lateral movement and post-compromise activities. OAuth is exploited to move laterally across cloud environments, especially for email collection.

#3 Midnight Blizzard, tracked as APT29, UNC2452, and Cozy Bear, primarily focuses on governments, diplomatic entities, NGOs, and IT service providers in the US and Europe. Their operations involve a variety of techniques, including compromise of valid accounts, supply chain attacks, and exploitation of service providers' trust chains. The investigation is ongoing, and the use of residential proxies complicates traditional indicators of compromise-based detection.

#4 In May 2023, Midnight Blizzard employed targeted social engineering via Microsoft Teams to steal credentials, utilizing compromised domains and convincing users to enter authentication codes for espionage. In September 2023, the group exploited a critical vulnerability (CVE-2023-42793) in JetBrains TeamCity, allowing full server compromise.

Recommendations

OAuth Application Management: Regularly audit and review OAuth applications in use within the organization. Limit permissions for OAuth applications to the minimum required for their functionality.
Monitor and restrict access to sensitive data or systems granted through OAuth applications.

Enable Multi-Factor Authentication (MFA): Ensure that MFA is enabled for all user accounts, especially those with elevated privileges. Regularly review and update MFA policies to align with the latest security recommendations.

Legacy Account Security: Identify and secure legacy accounts, ensuring they have proper security controls, including MFA. Regularly review and update access permissions for legacy accounts, minimizing unnecessary privileges.

Password Policy and Monitoring: Implement strong password policies, enforcing complex and unique passwords. Monitor for unusual login activity, especially multiple failed login attempts or suspicious patterns indicative of password spraying attacks

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0006** Credential Access	**TA0042** Resource Development	**TA0005** Defense Evasion
T1110.003 Password Spraying	**T1110** Brute Force	**T1027** Obfuscated Files or Information	**T1586** Compromise Accounts
T1190 Exploit Public-Facing Application	**T1583** Acquire Infrastructure	**T1583.006** Web Services	**T1586.002** Email Accounts

References

https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

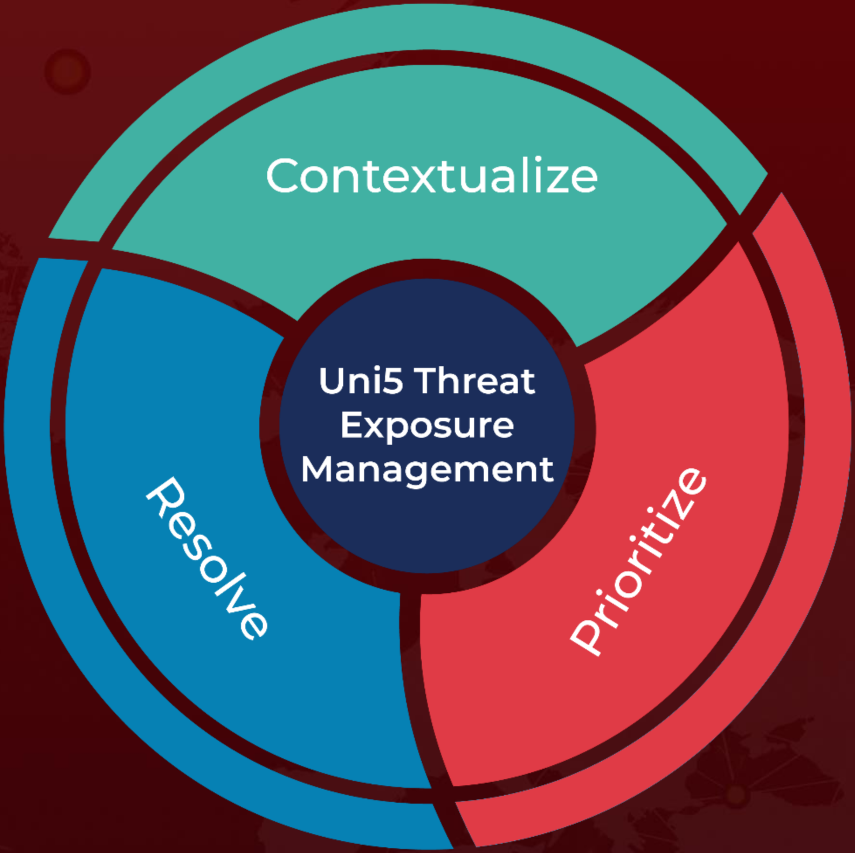
https://www.hivepro.com/threat-advisory/new-apt-29-campaign-targets-organizations-through-microsoft-teams/

https://www.hivepro.com/threat-advisory/russian-svr-exploits-critical-teamcity-vulnerability-globally/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 29, 2024 • 4:30 AM

More at www.hivepro.com