Midnight Blizzard: Microsoft Breach

C-Suite level threat review by applicable business area addressing active threats.

Midnight Blizzard, a Russian-linked advanced persistent threat group recently accessed Microsoft's internal systems and source code repositories. With this information, Midnight Blizzard could discover zero-day vulnerabilities within Microsoft's services. Already Midnight Blizzard is exploiting customer secrets discovered during the attack and is increasing its targeting of Microsoft. Thus, organizations should be on high alert for indicators of compromise from Midnight Blizzard.

Midnight Blizzard (APT29 and Cozy Bear):

Midnight Blizzard is associated with Russia's external intelligence agency and is thus motived by Russian-state interests. Midnight Blizzard is linked to high-profile cyberattacks such as the SolarWinds attack and the breach of the U.S. Democratic National Committee's computer networks.

Midnight Blizzard

Threat Level: High

Attack:

Midnight Blizzard conducted a successful password spray attack on a Microsoft non-production test tenant account. Since the test account did not have multi-factor authentication (MFA), the attackers subsequently gained access to the test tenant. The compromised account had access to an OAuth application with elevated privileges, enabling lateral movement to Microsoft's corporate environment. Once inside the corporate environment, Midnight Blizzard elevated its privileges and maintained persistence by creating an admin account and malicious OAuth applications. Ultimately, the attackers accessed source code repositories and exfiltrated data which contained customer secrets.

Remediation:

- Ensure proper security measures are in place for non-production systems
- Implement data masking on test systems
- Ensure password best practices and MFA are in place for human and service accounts

Midnight Blizzard Microsoft Breach Mapped to MITRE ATT&CK*

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Description
Reconnaissance	Gather Victim Network Information (T1590) *Speculative*	Midnight Blizzard identified a legacy, non-production test tenant in Microsoft's environment
Reconnaissance	Gather Victim Identity Information (T1589) *Speculative*	Utilized a list of valid accounts, usernames, and / or email addresses to conduct the password spray attack
Initial Access	Valid Accounts: Cloud Accounts (T1078.004)	Obtained credentials to the non-production test tenant (via password spray attack)
Persistence	Account Manipulation (T1098)	Elevated permissions on the test tenant, expanding control and enabling lateral movement.
Persistence	Create Account (T1136)	Created an admin user in the corporate tenant.
Defense Evasion	Use Alternate Authentication Material (T1550)	Created malicious OAuth apps
Defense Evasion	Impersonation (T1656)	Used the malicious OAuth apps to impersonate Exchange users
Credential Access	Brute Force: Password Spraying (T1110.003)	Conducted a password spray attack on the test tenant
Command and Control	External Proxy (T1090.002)	This threat actor used residential proxies to attack the test tenant while avoiding detection
Exfiltration	Exfiltration over C2 Channel (T1041) *Speculative*	Exfiltrated data from corporate mailboxes

**This is based on the best information available for use at the time (3/21/24) and is subject to change as facts come to light.*

Midnight Blizzard:

- **Overview of Midnight Blizzard tactics, techniques, and procedures:** https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a?&web_view=true
- **Microsoft blog post on the attack:** https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Response (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
- Threat Intelligence
  - Notification to customers of threats
  - On-demand briefings
  - Threat exposure workshops
  - User awareness training seminars
  - Monthly and quarterly threat intelligence reports