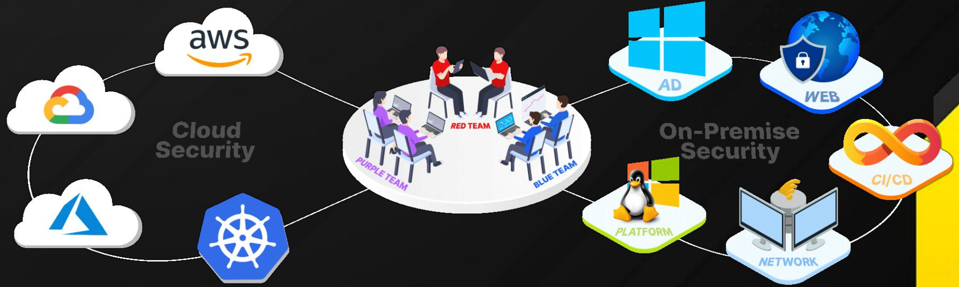
CWL
CyberWarFare Labs

# Emulating & Detecting Microsoft Breach [Midnight Blizzard] in CWL Cyber Range Lab

# About CW Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions:



INFINITE LEARNING EXPERIENCE

**1. Cyber Range Labs**

**2. Up-Skilling Platform**

CWL
CyberWarFare Labs

# About Speaker :

## Manish Gupta

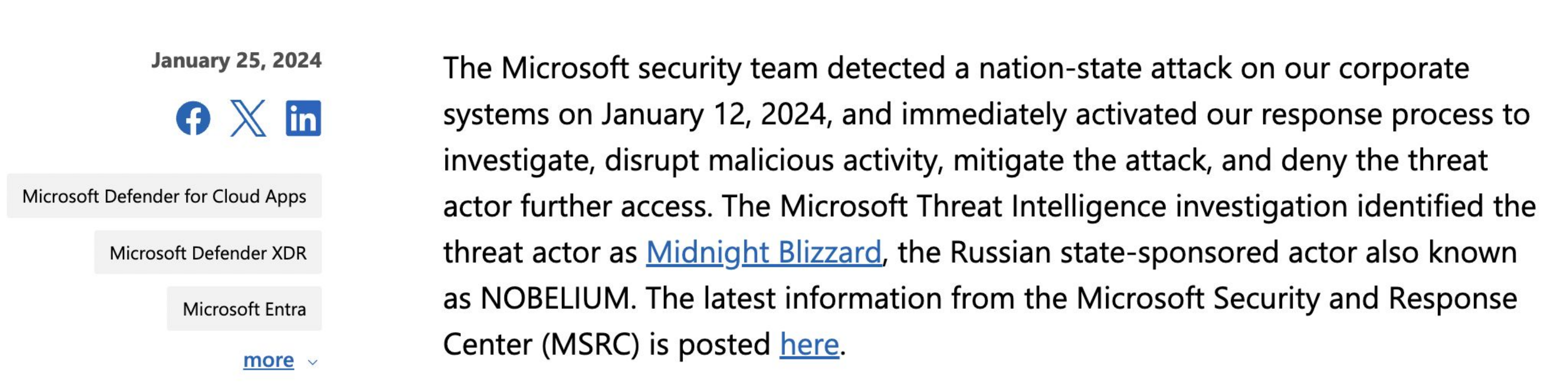
Co-Founder & CEO at CW Labs Pvt. Ltd.

**Manish Gupta** is CEO of CyberWarFare Labs. Where he specializes in Red Teaming Activities on enterprise Environment. His Research interest includes Real World Cyber Attack Simulation and Advanced persistent Threat (APT). Previously he has presented his research at reputed conferences like **Blackhat USA, DEFCON, Nullcon, BSIDES Chapters, X33fcon, NorthSec, CanSecWest & other corporate trainings** etc.

# Agenda

- About Midnight Blizzard Breached
- Emulation
- Detection
- Thank You :)

# About Midnight Blizzard Breached



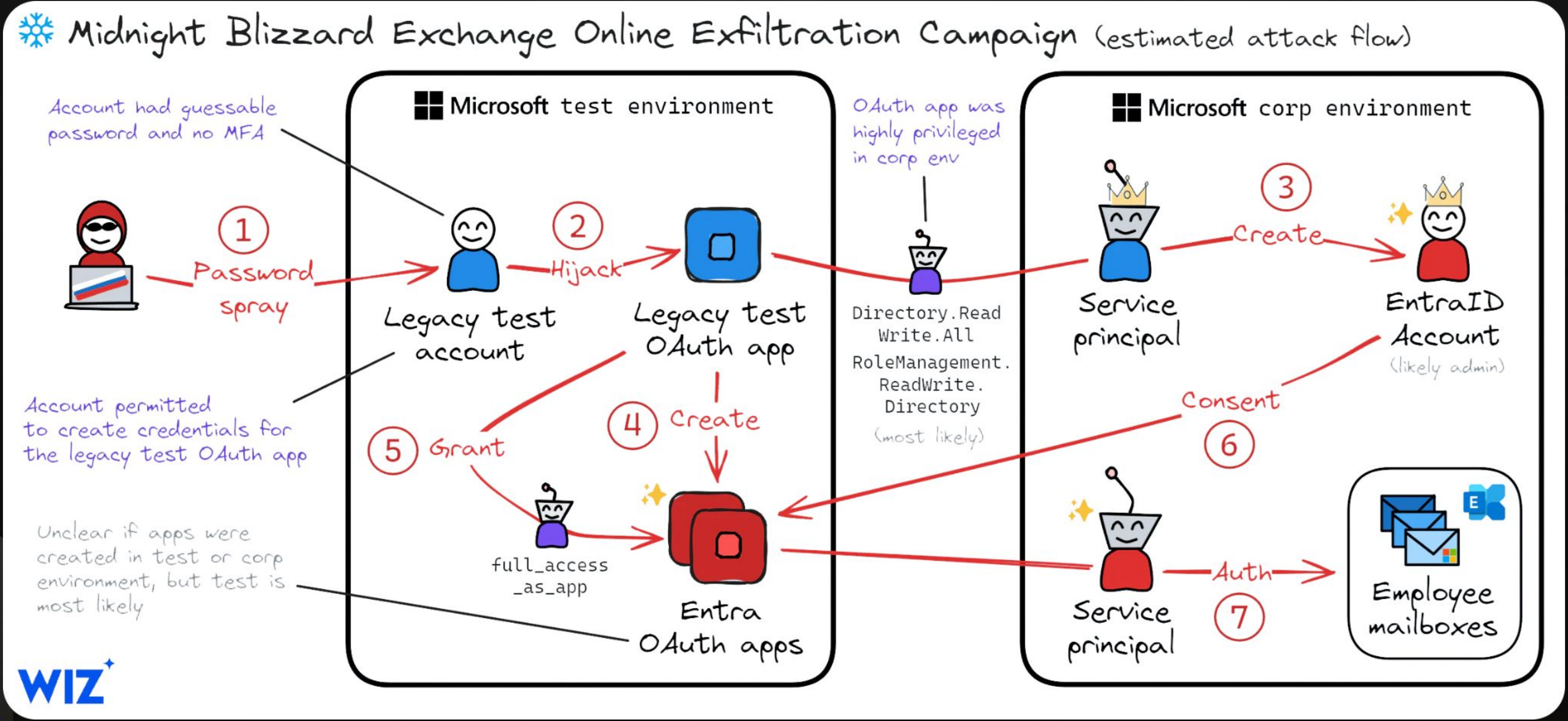
January 25, 2024

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.

# Emulation

- Initial Access - Password Spray
- Persistence - New App Register
- Privilege Escalation - App API Permission
- Lateral Movement - Azure OAuth App Credential

# Emulation


Midnight Blizzard Exchange Online Exfiltration Campaign (estimated attack flow)
Microsoft test environment
Microsoft corp environment
Account had guessable password and no MFA
1 Password spray
Legacy test account
2 Hijack
Legacy test OAuth app
OAuth app was highly privileged in corp env
Directory.Read Write.All
RoleManagement. ReadWrite. Directory
(most likely)
Service principal
3 Create
EntraID Account
(likely admin)
Account permitted to create credentials for the legacy test OAuth app
4 Create
5 Grant
full_access _as_app
Entra OAuth apps
Consent
6
Unclear if apps were created in test or corp environment, but test is most likely
Service principal
Auth
7
Employee mailboxes
WIZ

Ref https://www.wiz.io/blog/midnight-blizzard-microsoft-breach-analysis-and-best-practices

# Detection

- Creating new password of high privileged app
- Creating a new user and assigning  high privilege role.
- Tenant wide admin consent

CWL
CyberWarFare Labs

# Thank You

**For Professional Cyber Penetration Testing / Red Team / Blue Team / Purple Team,**
**Cloud Cyber Range labs / Courses / Trainings**, please email

**info@cyberwarfare.live**

**To know more about our offerings, please visit:**

https://cyberwarfare.live