Incident Report: Hands-on Keyboard Attack via Credential Misuse

Findings

Time:

- Initial activity: **November 22, 2025 – 11:48 UTC**
- Final observed activity: **November 24, 2025 – 11:29 UTC**

Host:

- mydfir-ndean-vm

Impacted User(s):

- AzureAD\JennySmith (jsmith)

Key Alert Types:

- Hands-on Keyboard Activity
- Credential Theft (Mimikatz)
- Risky Sign-in / Impossible Travel
- Suspicious PowerShell Activity
- Privilege Escalation Attempt (Blocked)

Tools / Techniques Observed:

- Mimikatz (multiple variants)
- Interactive PowerShell
- Active Directory Discovery (AdFind, SOAPHound)
- Privilege Escalation Attempt (BadPotato)
- Attempted RDP Lateral Movement (Blocked)

External Entities (Domains / IPs):

- 45.76.129.144 — Foreign IP (London, UK)
- 76.31.117.80 — Expected region IP

Investigation

On **November 22, 2025 at 11:48 UTC**, Microsoft Defender XDR detected a high-severity incident involving a successful **RemoteInteractive login from a foreign IP**, followed by hands-on-keyboard activity on host mydfir-ndean-vm. The activity involved credential theft attempts using **Mimikatz**, interactive **PowerShell execution**, **Active Directory reconnaissance**, and a **blocked privilege-escalation attempt**. Based on the incident details and attack progression, this behavior is consistent with a **credential misuse–driven hands-on-keyboard intrusion** following likely credential compromise. At this time, **we cannot confirm any ongoing malicious activity**, and the incident appears fully contained.

Incident Report: Hands-on Keyboard Attack via Credential Misuse

WHO

- Activity was performed under the compromised user account AzureAD\JennySmith (jsmith).
- The attacker authenticated using valid credentials from an external IP not associated with the legitimate user.
- All observed actions were executed under this identity following the unauthorized login.

WHAT

- The attacker attempted credential theft, environment discovery, and privilege escalation.
- Multiple malicious tools were created or executed but were blocked or remediated by Defender.
- No persistence, lateral movement, or data access was achieved.

WHEN

- **Nov 22, 2025 – 11:48 UTC:** Foreign RemoteInteractive login detected
- **Nov 22, 2025 – 12:55 UTC:** First activity wave (Mimikatz, PowerShell)
- **Nov 22, 2025 – 13:10 UTC:** RDP lateral movement attempt blocked
- **Nov 24, 2025 – 11:12–11:29 UTC:** Second activity wave (recon + escalation attempts)
- **Nov 24, 2025 – 11:48 UTC:** No further malicious activity observed

WHERE

- All malicious activity was confined to a single endpoint: mydfir-ndean-vm.
- Tools were executed via interactive PowerShell sessions following remote logon.
- Files were staged and executed from user and temporary directories on the host.

WHY

- The attacker’s likely objectives were to harvest credentials, enumerate the environment, and gain elevated privileges.
- These actions align with early-stage intrusion behavior following credential compromise.

HOW

- The incident likely began with credential exposure via phishing.
- The attacker authenticated using valid credentials from a foreign location.
- Post-authentication actions included PowerShell execution, credential dumping attempts, discovery tooling, and a blocked privilege-escalation attempt.
- Microsoft Defender XDR prevented further progression of the attack.

Recommendations

1. Enforce **multi-factor authentication (MFA)** for all users (especially remote and privileged access).
2. Review and restrict **PowerShell usage** for non-admin users and ensure advanced logging.
3. Audit and monitor **remote access and identity sign-ins** (impossible travel and risky sign-in).