Threat Hunting Report

Name: [Alexander Focsha]
Date: [5/23/25]
Role: Junior Cybersecurity Analyst

Executive Summary

This report details a cyber incident involving unauthorized network access attempts. We've identified **Indicators of Compromise (IOCs)**, attributed the attack to **APT41**, and propose mitigation strategies. Findings include suspicious network traffic, SMB scans, RDP brute force attempts, and use of legitimate system tools. The incident highlights potential data breaches and lateral movement risks, emphasizing the need for immediate and proactive security enhancements.

Indicators of Compromise (IOCs)

- **Suspicious Traffic:** Unusual outbound connections from internal hosts, signaling potential Command and Control (C2) communication and data exfiltration.
- **SMB Scans:** Firewall logs show internal SMB port (445/tcp) scans, indicating internal reconnaissance and lateral movement attempts.
- **RDP Brute Force Attempts:** Numerous failed RDP logins (3389/tcp) suggest attempts to gain interactive access.
- **Legitimate Utility Use:** Endpoint logs show `ipconfig` and `netstat` executed unusually, pointing to attacker discovery.
- **Credential Dumper:** Presence or execution of `pwdump` indicates credential theft, risking privilege escalation and wider compromise.

These IOCs collectively point to **data breach risk, lateral movement, and system compromise.**

Threat Actor Group Attribution

The attack is attributed to **APT41**.

Justification: The observed TTPs align strongly with APT41's known methods:

- **Software Use:** The logs show `ipconfig`, `netstat`, and `pwdump` (S0100, S0104, S0006), all explicitly listed as APT41 tools.
- **Techniques:** The observed RDP brute force attempts lead to **Valid Accounts (T1078)**, a key APT41 technique. Additionally, evidence of **Windows Service (T1543.003)**, **Windows Command Shell (T1059.003)**, and **WMI (T1047)** abuse for persistence and execution directly matches APT41's documented TTPs. While some overlaps exist with APT29, the specific combination of observed tool use and techniques points more directly to APT41, especially given the financial sector target.

Mitigation Strategies

Remediation:

- **Suspicious Traffic:** Implement strict firewall egress filtering and DNS sinkholing to block C2.
- **SMB Scans:** Segment the network, limit SMB communication, disable SMBv1, and enforce SMB signing.
- **RDP Brute Force:** Use account lockout policies, RDP gateways/VPNs, and Network Level Authentication (NLA).
- **Legitimate Utility Use:** Deploy EDR with behavioral analytics and implement application whitelisting.
- **Credential Dumper:** Use credential guard solutions (e.g., Windows Defender Credential Guard) and implement LAPS for local admin passwords.

Proactive Security:

- Implement **Multi-Factor Authentication (MFA)** for all critical access.
- Enhance **logging and retention** for better visibility.
- Conduct **regular security audits and penetration tests**.
- Provide **ongoing security awareness training** for employees.
- Strictly enforce the **Principle of Least Privilege**.
- Maintain a **timely patch management program**.

These strategies align with **NIST Cybersecurity Framework** (Identify, Protect, Detect, Respond) and **CIS Benchmarks** (e.g., Secure Configurations, Continuous Vulnerability Management, Data Protection).

Analysis Process Summary

Tools and Methodologies:

We used **Wazuh SIEM** for centralized log ingestion and analysis, deployed via **Docker**. The **MITRE ATT&CK Framework** guided our TTP mapping and threat attribution.

Steps Taken:

Logs from various sources were ingested into Wazuh. We reviewed alerts, identified attack patterns (e.g., RDP brute force, SMB scans), extracted specific IOCs (IPs, timestamps, commands), and performed contextual analysis. Finally, we mapped behaviors to MITRE ATT&CK and attributed the attack to APT41.

Challenges and Observations:

High log volume was managed using Wazuh's filtering. We noted challenges with granular endpoint logging, highlighting a need for better configuration. Differentiating legitimate activity from malicious also required careful analysis.

Reflection and Recommendations

Reflection: The systematic analysis using Wazuh and MITRE ATT&CK was very effective. Correlating diverse logs provided a comprehensive view of the incident. This reinforced the need for more granular endpoint logging.

Lessons Learned: Centralized logging with a SIEM is crucial. MITRE ATT&CK is invaluable for understanding threats. Basic cybersecurity hygiene and fundamentals remain critical. Attackers often "live off the land" using legitimate tools, stressing behavioral analysis.

Ongoing Security Recommendations: Implement **automated vulnerability management**. Plan and implement a **Zero Trust Architecture**. Enhance **EDR deployment**. Conduct **regular tabletop exercises**. Deploy **Privileged Access Management (PAM)**. Continue **security awareness training**. Establish **threat hunting**. Perform **regular configuration audits**. Integrate **external threat intelligence**.