### **SOC Investigation Report**

**Date of Incident:** 10/1/2025

**Analyst Name:** Abdelrahman Salem

**Tool Used:** IBM QRadar

**Incident ID:** QRadar101-001

#### **1. Executive Summary**

On 10/1/2025, IBM QRadar detected multiple security events indicating a potential insider-assisted compromise within the corporate network. The investigation revealed that an attacker exploited a malicious document to gain initial access, used lateral movement techniques, and exfiltrated sensitive project data. Immediate containment and mitigation steps were implemented to address the threat.

#### **2. Incident Details**

**Incident Description:** QRadar flagged multiple security events, including unauthorized data exfiltration, suspicious process execution, and lateral movement attempts.

**Affected Systems:**

* **Initial Compromised Host:** 192.168.10.15
* **Domain Controller:** 192.168.20.21
* **Additional Host:** MGNT-01

**Incident Timeline:**

* **10/1/2025 11:02:** Malicious document executed on 192.168.10.15.
* **10/1/2025 11:14:** Unauthorized access to domain controller 192.168.20.21.
* **10/1/2025 11:20:** Lateral movement to MGNT-01 using wmiexec.py.
* **10/1/2025 11:36:** Data exfiltration to external IP 192.20.80.25.

#### 

#### 

#### **3. Investigation Steps**

**Logs Analyzed:**

* Sysmon Logs (swift on security configuration)
* PowerShell Logs
* Windows Event Logs
* Suricata IDS Alerts
* Zeek Logs (conn, HTTP)

**Rules Triggered:**

* Suricata Alert: ET MALWARE Possible Malicious Document Download (SID: 2027865)
* Windows Event Log: New User Account Created

**Suspicious Activities Identified:**

1. Execution of a malicious document ("important\_instructions.docx") on 192.168.10.15.
2. Creation of unauthorized user account "Rambo."
3. Lateral movement using wmiexec.py targeting MGNT-01.
4. Data exfiltration using curl to IP 192.20.80.25.

#### **4. Root Cause Analysis**

**Cause:** The incident was initiated through a phishing email containing a malicious document, "important\_instructions.docx," opened by an employee ("nour") on host 192.168.10.15. This allowed the attacker to gain an initial foothold.

**Impact:**

* Unauthorized access to sensitive project data ("project48").
* Exfiltration of data to external IP 192.20.80.25.
* Compromise of multiple internal systems, including MGNT-01.

#### **5. Mitigation and Recommendations**

**Actions Taken:**

1. Isolated compromised systems (192.168.10.15 and MGNT-01) from the network.
2. Reset credentials for all affected user accounts.
3. Conducted a network-wide scan to identify additional indicators of compromise (IoCs).

**Recommendations:**

1. **Enhance Email Security:** Deploy advanced email filtering to detect and block malicious attachments.
2. **Strengthen Endpoint Security:** Implement endpoint detection and response (EDR) tools for real-time monitoring.
3. **Improve Logging:** Enable detailed PowerShell logging and enforce log retention policies.
4. **User Training:** Conduct regular phishing awareness training for employees.
5. **Network Segmentation:** Implement strict network segmentation to limit lateral movement.
6. **Patch Management:** Ensure all systems and software are regularly updated and patched.

#### **6. Conclusion**

The investigation confirmed that the attacker exploited a malicious document to compromise the network. The incident involved lateral movement, data exfiltration, and the use of malicious tools. Remediation steps have been implemented to address the threat and prevent future incidents. Ongoing monitoring and user education will be critical to maintaining the organization’s security posture.

**Prepared by:** Abdelrahman Salem **Date:** 17/1/2024