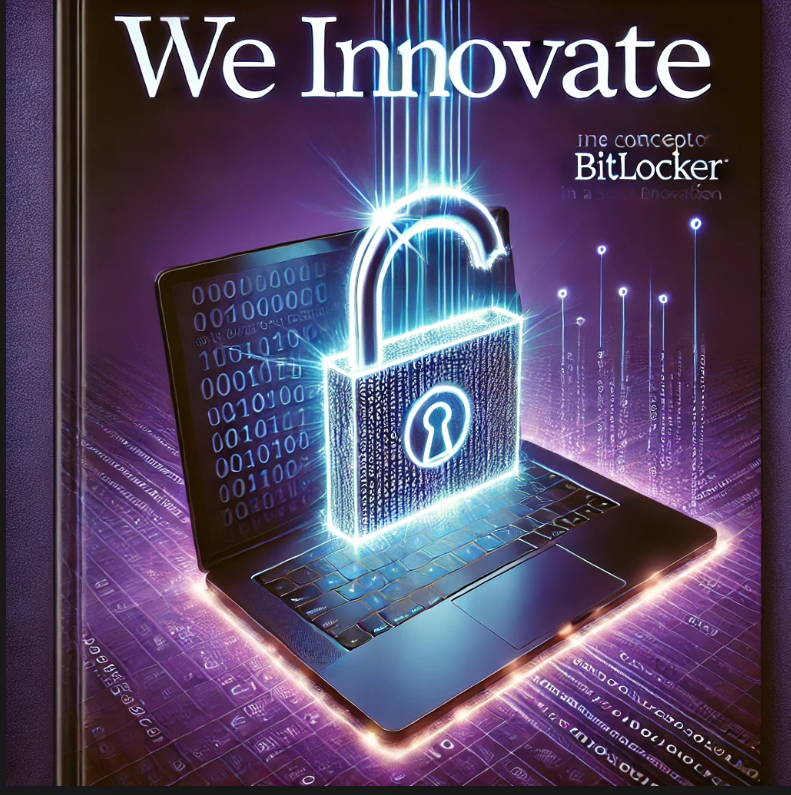
****

**IRON MAN TEAM**

**Incident Response Report**

**for an Unauthorized access attack**

**prepared by:**

**Shahd Baher (L1)**

**Mohamed Ibrahim (L1)**

**Nour Omar (L2)**

**Abdelrahman Zaki (L2)**

**Abdullah Ahmed (L3)**

**Mohamed Yousry (L3)**

**Executive Summary**

* **Incident ID: INC2024-0905-06**
* **Incident Severity: Medium (P3)**
* **Incident Status: Resolved**
* **Incident Report Date: September 05, 2024**
* **Incident Overview: On the morning of September 03, 2024, Iron Man's Security Operations Center (SOC) was alerted to the theft of an IT Officer's laptop. The stolen laptop contained access credentials for various internal systems, which posed a significant security risk. The IT Officer reported the laptop stolen from their vehicle. Due to the sensitive nature of the data and access credentials stored on the device, an immediate investigation and containment effort were launched to prevent potential misuse.**
  + **Iron Man's SOC team worked with the Digital Forensics and Incident Response (DFIR) unit to mitigate any risks associated with the stolen laptop. Key actions included revoking access credentials, performing forensic analysis on backup data, and tightening system access controls to ensure no unauthorized use of the laptop’s credentials occurred.**
* **Incident Timeline**
  + **08:45 AM, September 03, 2024 – IT Officer reports laptop stolen from a vehicle.**
  + **09:00 AM – SOC escalates the incident and initiates a security response, assessing the potential risk from the loss of credentials stored on the device.**
  + **09:15 AM – Immediate password resets and revocation of access tokens for all systems accessed via the stolen laptop begin.**
  + **10:00 AM – Forensic analysis of recent system logs is conducted to ensure no suspicious activity was performed prior to the theft.**
  + **10:30 AM – Remote device wiping initiated to clear all stored data on the laptop once it reconnects to the internet.**
  + **11:00 AM – Access audits are performed across all systems the IT Officer had access to, identifying potential areas of exposure.**
  + **12:00 PM – SOC confirms that no unauthorized access occurred following the theft, and additional security measures are implemented to safeguard against any future credential theft.**
  + **03:00 PM, September 03, 2024 – Incident response is completed, and the incident is marked as resolved with follow-up actions planned.**

Contents

[**L1 Detection** 4](#_Toc176408098)

[**1.Detection Overview** 4](#_Toc176408099)

[**2.Analysis** 4](#_Toc176408100)

[**2.1 Incident details:** 4](#_Toc176408101)

[**2.2 Information About the Device** 4](#_Toc176408108)

[**2.3 Impact assessment** 4](#_Toc176408117)

[**L2 Response** 6](#_Toc176408118)

[**1. Containment** 6](#_Toc176408119)

[**1.1 Mobile Device Management (MDM)** 6](#_Toc176408120)

[**1.2 Account Lockdown** 6](#_Toc176408121)

[**1.3 Device Deactivation** 6](#_Toc176408122)

[**1.4 Password Reset** 7](#_Toc176408123)

[**1.5 Data Backup Check** 7](#_Toc176408124)

[**1.6 Data Encryption via Lockbit Tool** 7](#_Toc176408125)

[**1.7 Multi-Factor Authentication (MFA) Reconfiguration** 7](#_Toc176408126)

[**1.8 Endpoint Detection and Response (EDR) Monitoring** 8](#_Toc176408127)

[**2. Investigation** 8](#_Toc176408128)

[**2.1 Log Analysis** 8](#_Toc176408129)

[**2.2 IP and Location Identification** 8](#_Toc176408130)

[**2.3 Account Activity Review** 9](#_Toc176408131)

[**2.4 System Check** 9](#_Toc176408132)

[**L3 Hunt & Utilize** 10](#_Toc176408133)

[**1.** **Overview** 10](#_Toc176408134)

[**2.** **Threat Hunting** 10](#_Toc176408135)

[**2.1** **Log Analysis** 10](#_Toc176408136)

[**2.2** **Network Traffic Monitoring** 10](#_Toc176408137)

[**2.3** **Account Activity Review** 10](#_Toc176408138)

[**3.** **Utilization of Intel** 10](#_Toc176408139)

[**4.** **Security Posture Enhancement** 11](#_Toc176408140)

[**5.** **Findings and Improvements** 12](#_Toc176408141)

[**6.** **recommendations** 12](#_Toc176408142)

# **L1 Detection**

## **1.Detection Overview**

* **The IT officer reported his laptop stolen.**

## **2.Analysis**

### **2.1 Incident details:**

|  |  |
| --- | --- |
| Place of theft? | Cafe Bucharest in Zamalek |
| Was the laptop powered? | No |
| Was any physical deity found at the scene? | No |

### 

### **2.2 Information About the Device**

|  |  |
| --- | --- |
| Type of installed system device? | Windows 11 |
| Sensitive data stored on the device? | Employee accounts (passwords and username) |
| Is the device encrypted with a password? | Yes |
| Is the device connected to any private or public networks? | No |

### **2.3 Impact assessment**

* **Data exposure**
  + **Action: Determine if any sensitive or confidential data stored on the stolen laptop was accessed, altered, or exfiltrated. The search was focused on the IT department’s files, company documents, and access credentials stored on the device.**
  + **Rationale: Understanding the scope of the data exposure helps gauge the potential damage to the organization and informs the next steps in incident response.**
* **Operational Impact**
  + **Action:** **We Evaluated the impact of the stolen laptop on business operations, including any disruptions caused by the loss of the device or the security response (e.g., account lockouts, system monitoring).**
  + **Rationale:** **Assessing the operational impact is critical to understanding the broader implications of the theft, such as delays in IT projects or a potential drop in employee productivity.**
* **Compliance and Legal Implications**
  + **Action:** **Assess whether the theft of the laptop and the resulting data exposure violate any regulatory or legal obligations like GDPR, internal security policies.**
  + **Rationale: Failure to comply with regulatory requirements can result in significant legal consequences, including fines, lawsuits, or reputational damage.**

# **L2 Response**

## **1. Containment**

### **1.1 Mobile Device Management (MDM)**

* **Action:** **Use MDM tools to lock the stolen laptop remotely, preventing unauthorized access to the system. This measure also buys time to initiate other security responses.**
* **Rationale:** **Locking the laptop remotely limits the attacker’s ability to access or extract data and ensures no further activities can be performed on the device.**

### **1.2 Account Lockdown**

* **Action:** **Immediately lock the IT department member’s account across all systems to prevent further unauthorized access.**
* **Rationale:** **Locking the user account reduces the risk of the attacker using the stolen credentials to gain access to corporate systems.**

### **1.3 Device Deactivation**

* **Action:** **Remove the stolen device from the list of trusted devices connected to the organization's network.**
* **Rationale:** **This ensures that the stolen laptop is no longer able to connect to the company’s network, reducing the attack surface.**

### **1.4 Password Reset**

* **Action:** **Reset the IT staff member’s password across the entire environment, including all services they accessed (e.g., email, VPN, internal tools).**
* **Rationale:** **Resetting the password prevents the attacker from exploiting saved credentials to access any company resources.**

### **1.5 Data Backup Check**

* **Action:** **Ensure that all the data belonging to the IT staff member is backed up and that no critical information has been lost.**
* **Rationale:** **This step safeguards against permanent data loss and ensures that the employee can continue their work without interruption upon device replacement.**

### **1.6 Data Encryption via bit-locker Tool**

* **Action:** **Activate the encryption tool (e.g., bit-locker) to encrypt all sensitive data stored on the laptop’s hard drive.**
* **Rationale:** **Encrypting the data ensures that, even if the attacker accesses the device, they cannot retrieve any valuable information without the decryption key.**

### **1.7 Multi-Factor Authentication (MFA) Reconfiguration**

* **Action:** **Re-enforce and reconfigure multi-factor authentication (MFA) to block any attempts to bypass authentication using the stolen laptop.**
* **Rationale:** **Strengthening MFA prevents the attacker from successfully authenticating even if they have stolen login credentials.**

### **1.8 Endpoint Detection and Response (EDR) Monitoring**

* **Action: If the device reconnects to the internet, use EDR tools to monitor all activities, including login attempts, data transfers, and abnormal behavior.**
* **Rationale:** **Continuous monitoring through EDR allows for real-time detection of any unauthorized access attempts, providing opportunities to block malicious actions.**

## **2. Investigation**

### **2.1 Log Analysis**

* **Action:** **Review all login access logs to trace the attacker’s activities since the laptop was stolen. Focus on identifying if the laptop was connected to the internet and which systems were accessed.**
* **Rationale:** **Log analysis provides insight into the attacker’s movements and can help in determining the severity of the breach.**

### **2.2 IP and Location Identification**

* **Action:** **Analyze the logs generated by the stolen laptop to identify the IP address and potential location of the attacker.**
* **Rationale:** **Identifying the attacker’s IP and location can assist law enforcement efforts and guide future containment measures.**

### **2.3 Account Activity Review**

* **Action:** **Analyze recent activities performed using the IT staff member’s account. Review any access to confidential emails, sensitive documents, or company systems.**
* **Rationale:** **This helps to determine the extent of the data exposure and assess the potential risks to the organization.**

### **2.4 System Check**

* **Action:** **Conduct a thorough examination of the stolen laptop’s last known state, including installed applications, open sessions, and any malware or suspicious tools that might have been used by the attacker.**
* **Rationale:** **Identifying any pre-installed malicious software or tools helps in understanding how the attacker might have leveraged the stolen laptop. This analysis can reveal potential attack vectors.**

# **L3 Hunt & Utilize**

## **Overview**

* Following the incident involving the theft of the IT officer's laptop, we focused on threat hunting, utilizing intelligence gathered during the incident, and enhancing the organization's security posture.

## **Threat Hunting**

* Identifying any ongoing threats or suspicious activities related to the stolen laptop.

### **Log Analysis**

* + Reviewed all login access logs from the time of the theft to the present, focusing on any unusual access patterns or connections made by the stolen laptop.
  + Identified IP addresses and locations associated with the laptop's last known activity to track potential unauthorized access attempts.

### **Network Traffic Monitoring**

* + - * Implemented real-time monitoring of network traffic to detect any attempts by the stolen laptop to connect to the corporate network or access sensitive systems.
      * Utilized Network Intrusion Detection Systems (NIDS) to flag any suspicious activity originating from known IP addresses associated with the theft.

### **Account Activity Review**

* + analysis of the IT officer’s account activity, focusing on any unauthorized access to confidential emails, documents, or systems post-theft.
  + Investigated any attempted logins from unfamiliar locations and flagged them for further investigation.

## **Utilization of Intel**

* Leverage insights gained from the incident to enhance security measures.

**Actions**:

* + **Threat Intelligence Gathering**:
    - Collected data from the incident, including stolen device details, user behavior patterns, and any identified attacker IP addresses.
    - Shared this information with relevant cybersecurity threat intelligence platforms to enhance the organization's awareness of potential vulnerabilities.
  + **Collaboration with Law Enforcement**:
    - Provided law enforcement with the collected IP addresses and any other pertinent information to assist in tracking down the stolen device.
    - Engaged with local authorities to report the incident and seek guidance on any additional security measures that could be implemented.

## **Security Posture Enhancement**

* Strengthen the organization’s defenses against similar incidents in the future.

**Actions**:

* + **Policy Review and Updates**:
    - Reviewed and updated the organization's security policies, particularly concerning mobile devices and remote access.
    - Implemented stricter guidelines for the use of personal devices for work purposes to mitigate risks associated with lost or stolen equipment.
  + **Multi-Factor Authentication (MFA)**:
    - Reinforced the requirement for MFA across all sensitive systems to add an additional layer of security and reduce the risk of unauthorized access using stolen credentials.
    - Conducted training sessions for all employees on the importance of MFA and how to set it up effectively.
  + **Regular Security Audits**:
    - Established a schedule for regular security audits and penetration testing to identify and remediate vulnerabilities in the organization's infrastructure.
    - Focused on areas exposed during the incident, such as remote access and data handling practices.
  + **Employee Training and Awareness**:
    - Launched a mandatory security awareness training program for all employees, emphasizing the risks associated with physical device security and data protection.
    - Included practical guidance on how to respond to lost or stolen devices and the importance of reporting incidents promptly.

## **Findings and Improvements**

• Threat Detection: Real-time monitoring and log analysis successfully identified several unauthorized access attempts related to the stolen laptop.

• Improved Collaboration: Enhanced communication with law enforcement and threat intelligence agencies has strengthened the organization’s response capabilities.

• Enhanced Policies: Updated security policies and procedures have decreased potential vulnerabilities related to mobile device management.

## **recommendations**

1. Continuous Threat Monitoring : Implement ongoing threat hunting and monitoring to quickly identify potential security incidents.

2. Regular Training Refreshers : Schedule periodic refresher courses on security awareness for all employees to keep them informed of evolving threats.

3. Advanced Security Technologies: Explore the adoption of advanced security solutions, such as Endpoint Detection and Response (EDR) and Data Loss Prevention (DLP) tools, to further protect sensitive information.