**SUBJECT: URGENT: Major Security Incident - Multiple Malware Infections Detected**

TO: CISO, IT Management

FROM: SOC Team

**URGENT ACTION REQUIRED**

Dear Management,

The Security Operations Center has identified a significant security incident requiring immediate attention.

**INCIDENT OVERVIEW:**

- 🚨 11 MALWARE DETECTIONS across 5 user accounts

- 🔴 Multiple infection types: Trojan, Rootkit, Ransomware, Spyware

- ⚠️ 5 failed login attempts from suspicious external IPs

- 👥 All monitored users (Alice, Bob, Charlie, David, Eve) affected

**CRITICAL SYSTEMS IMPACTED:**

- Multiple endpoints compromised

- Potential data exfiltration risk

- Ransomware threat detected on the critical system

**IMMEDIATE ACTIONS TAKEN:**

1. Incident response procedures activated

2. Initial containment measures in progress

3. Investigation underway to determine scope

**REQUESTED SUPPORT:**

- Approval for emergency password resets

- Resources for comprehensive system scans

- Management communication to affected teams

We are containing the situation and will provide a detailed update within 2 hours.

Best regards,

SOC Team.