

**Incident handler's journal**  
  
**Incident Handler’s Journal**

**Date:** February 19, 2025

**Entry ID:** 002

### **Incident Overview**

* **Incident Type:** Phishing Attempt with Malicious Attachment
* **Affected System:** Employee Workstation on Internal Network
* **Ticket ID:** A-2703
* **Severity Level:** Medium
* **Incident Status:** Closed

### **Incident Details**

#### **The 5 W’s of the Incident:**

* **Who caused the incident?**
  + The phishing email originated from **Def Communications (76tguyhh6tgftrt7tg.su)**, an untrusted source. The email impersonated a job applicant and targeted an HR email address ([hr@inergy.com](mailto:hr@inergy.com)).
* **What happened?**
  + The phishing email contained a password-protected **malicious attachment (bfsvc.exe)**. Upon investigation, the attachment was identified as malware attempting to establish persistence and exfiltrate credentials.
* **When did the incident take place?**
  + The email was received on **July 20, 2022, at 09:30:14 AM**. The incident response process began immediately upon detection.
* **Where did the incident occur?**
  + The attack targeted the HR department’s email system within the company’s internal network.
* **Why did it happen?**
  + The phishing email exploited social engineering tactics, disguising itself as a job application with a **password-protected attachment** to bypass security filters.

### **Investigation Findings**

* **Malware Analysis:**
  + The **file hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b)** was confirmed malicious using **VirusTotal**.
  + Behavioral analysis indicated **execution of malicious scripts, persistence mechanisms, and credential theft** attempts.
* **Indicators of Compromise (IoCs):**
  + **File Hash:** 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
  + **Sender’s IP Address:** 114.114.114.114
  + **Targeted Email:** [hr@inergy.com](mailto:hr@inergy.com)
  + **Malicious Domain Contacted:** org.misecure.com

### **Incident Response Actions Taken**

✅ Quarantined the affected system to prevent further exposure.

✅ Blocked the sender's email and **malicious attachment** across security filters.

✅ Updated firewall and security tools to block **malicious IP (104.115.151.81) and domain (org.misecure.com)**.

✅ Conducted an endpoint scan to verify no residual malware remained.

✅ Reset relevant credentials to mitigate credential theft risks.

✅ Conducted **user awareness training** for HR employees on phishing recognition.

### **Final Assessment & Closure Justification**

* The phishing email was **successfully mitigated**, and no further escalation was required.
* Security controls have been reinforced to prevent similar attacks.
* The incident has been **marked as closed**, and continuous monitoring has been implemented.

**Next Steps:**

* Enhance **phishing detection mechanisms** for similar threats.
* Update **incident response playbooks** with newly observed TTPs (Tactics, Techniques, and Procedures).
* Continue monitoring for any further related activity.

**Status:** ✅ **Closed**

**Escalation Required:** No