SOC ALERT TICKET A-2703

Malicious Email Campaign Analysis & Threat Response

ALERT SEVERITY	CURRENT STATUS
HIGH	ESCALATED
CLASSIFICATION	**ASSIGNED ANALYST**
MALWARE	Lydiah Muigwa
DETECTION TIME	**RESPONSE SLA**
2025-07-20 09:30 UTC	4 hours (Met)

Executive Summary

Threat Type: Spear-phishing campaign with malicious executable attachment targeting HR personnel

Attack Vector: Social engineering via fake job application email containing password-protected malware

Impact Assessment: Single endpoint compromise with confirmed malware execution

Escalation Reason: Confirmed malicious file hash match with known threat actor infrastructure

Technical Analysis

Social Engineering Indicators

- **Display Name Spoofing:** "Def Communications" vs actual sender
- **Urgency Tactics:** Job application response pressure
- **Authority Exploitation:** Targeting HR department
- **Trust Building:** Password protection premise for "privacy"

Technical Indicators

- **Suspicious Domain:** .su TLD (Soviet Union legacy)
- **Email Inconsistencies:** Multiple identity mismatches
- **Grammar Anomalies:** Non-native English patterns
- **Executable Disguise:** .exe masquerading as document

🚩 Indicators of Compromise (IOCs)

IOC Type	Value	Confidence	Source
Email Address	76tguyhh6tgftrt7tg.su	High	Email Header Analysis
IP Address	114.114.114.114	High	SMTP Logs
File Hash (SHA-256)	`54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`		
Filename	bfsvc.exe	High	Email Attachment
Password	paradise10789	Medium	Social Engineering

Email Evidence Analysis

FROM: Def Communications <76tguyhh6tgftrt7tg.su> [114.114.114.114] **TO:** hr@inergy.com [176.157.125.93] **SUBJECT:** Re: Infrastructure Egnieer role **DATE:** Wednesday, July 20, 2022 09:30:14 AM **ATTACHMENT:** bfsvc.exe (password: paradise10789) **BODY:** Dear HR at Ingergy, I am writing for to express my interest in the engineer role posted from the website. There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open. Thank you, Clyde West

MITRE ATT&CK Techniques: T1566.001 Spear-phishing Attachment T1204.002 User Execution: Malicious File T1027.002 Obfuscated Files: Software Packing T1036.002 Masquerading: Right-to-Left Override

Escalation Justification

> **Severity Upgrade:** Medium → High based on confirmed malware execution

> **Threat Intelligence Match:** File hash correlates with known APT campaign infrastructure

> **Business Impact:** HR system access potential for lateral movement to employee data

> **Required Actions:** Advanced forensics, network hunting, and incident response

coordination needed

Immediate Response Actions

L2 Analyst Actions Required:

- **Endpoint Isolation:** Quarantine affected workstation (hr@inergy.com user)
- **Network Hunting:** Search for lateral movement indicators across domain
- **Memory Analysis:** Capture volatile artifacts before system shutdown
- **Credential Reset:** Force password change for affected user account
- **IOC Deployment:** Push indicators to all security tools for hunting

Investigation Priorities:

- Analysis of network connections post-execution
- Registry and file system artifacts collection
- Email system logs for additional campaign indicators
- Assessment of data exfiltration potential

📊 Risk Assessment Matrix

Risk Factor	Level	Justification	Mitigation Priority
Data Exfiltration	HIGH	HR system access to employee PII	Critical
Lateral Movement	HIGH	Domain-joined system compromise	Critical
Persistence	MEDIUM	Unknown payload capabilities	High
Compliance Impact	HIGH	Potential PII/PHI exposure	Critical

Ticket Metadata:
Created: 2025-07-20 09:35:00 UTC | Updated: 2025-07-20 11:45:00 UTC