🛡️EDR Investigation Report

# 1. Investigation Summary

Incident Name: Phishing Email – Malicious Attachment Execution

Date/Time Identified: 20250603

Reported By: [Insert name or role, e.g., SOC Analyst, User]

Brief Description: A phishing email was sent by a malicious actor posing as Jeff Johnson, with an attachment labeled 'Payslip.pdf'. Upon execution, the file delivered malware to multiple hosts.

# 2. Timeline of Events

|  |  |
| --- | --- |
| Time | Event |
| 00:00 | Malicious email received by users |
| 00:07 | Email downloaded by Host-IOPE |
| 00:57 | File executed on Host-HKNV |
| 01:43 | Email downloaded by Host-ATYU |
| 02:00 | Malware communication or activity observed on HKNV |
| 02:10 | Incident response team notified |
| 02:15 | Containment actions applied (Quarantine, Investigate) |

# 3. Affected Systems

-Host-ATYU

- Host-IOEP

- Host-HKNV

# 4. Root Cause Analysis

Root Cause: User(s) downloaded and executed a malicious email attachment from an external sender pretending to be a trusted contact.

Threat Vector: Email attachment ('Payslip.pdf')

Indicators of Compromise (IOCs):

- Sender email: j.johnson@ppc.com

- File: Payslip.pdf

- Suspicious processes or outbound traffic logs

# 5. Actions Taken

- Isolated affected devices from the network

- Deleted the malicious file

- Scanned all systems for malware

- Updated endpoint protection tools

- Reset affected user credentials

# 6. Recovery

- Verified integrity of restored systems

- Monitored for abnormal behavior for 48 hours

- Reconnected cleaned systems to the network

# 7. Lessons Learned & Recommendations

- Train users to identify phishing emails

- Implement email attachment filtering

- Enable attachment sandboxing

- Conduct regular phishing simulation tests

- Enforce least privilege on endpoints

# 8. Prepared By

Name: Jessica Stovall

Date: [Insert date]

Role: Aspiring Cybersecurity Analyst