

Capstone Project: Simulated Incident Response - Advanced Phishing Attacks at EuroTrans Logistics

EuroTrans Logistics Phishing Incident — Final Incident Response Report

Executive Summary

On **June 10, 2025**, EuroTrans Logistics experienced a phishing attack originating from a spoofed HR email. Malicious Excel attachments enabled macro-based malware that led to multiple endpoint detections, credential theft attempts, keylogger deployment, and outbound connections to attacker-controlled Command and Control (C2) servers. The incident was identified through employee reports and CrowdStrike EDR alerts. The security team conducted a full incident response operation following the NIST framework, containing the attack, eradicating malware artifacts, restoring normal operations, and implementing improved preventive measures.

Timeline of Events

| Time (GMT) | Event |
|------------|--|
| 08:01 | Phishing emails sent from hr@eurotrans-payroll.com |
| 08:11 | Kwame Okyere reported password lockout |
| 08:22 | Mabel Boakye opened a suspicious Excel attachment |
| 08:27 | CrowdStrike EDR detected PowerShell spawned from Excel |
| 08:27 | Admin noticed multiple lockouts |
| 08:35 | Samira Damba's Outlook crashed after opening email |
| 08:42 | Jakarta users reported browser redirects |
| 08:45 | Keylogger detected on ET-JK-01 endpoint |
| 08:46 | Scheduled task UpdateTask.ps1 detected on ET-GH-CS011 |
| 08:50 | Outbound traffic to C2 domains blocked at firewall |

Indicators of Compromise (IOC) Table

| Type | Value |
|--------------|--|
| Sender Email | hr@eurotrans-payroll.com |
| Attachment | StaffComp2025.xlsx |
| C2 IPs | 185.224.128.32, 74.119.201.12 |
| C2 Domain | phish-update365.ru |
| Persistence | PowerShell task <code>UpdateTask.ps1</code> |
| Malware File | %TEMP%\hrdata.exe |

Root Cause and Attack Chain

Root Cause:

- Misconfigured Proofpoint email security (SPF/DKIM/DMARC not enforced)
- Macros enabled in Office documents
- Weak outbound firewall controls
- Lack of phishing-specific incident response playbook

Attack Chain:

1. Phishing emails bypassed email filtering
2. User opened attachment and enabled macros
3. Macros executed PowerShell to download malware
4. Persistence established via scheduled task
5. Keylogger deployed
6. Outbound connections attempted to attacker C2 servers

Email Analysis Table (Parsed Manually)

| Field | Value |
|------------------|--|
| From | hr@eurotrans-payroll.com |
| To | Multiple user inboxes |
| Subject | Staff Payroll Adjustments / Org Chart Update |
| Attachment | StaffComp2025.xlsx |
| SPF Result | FAIL |
| DKIM Result | FAIL |
| DMARC Result | None |
| Verdict | Delivered |
| Return-Path | hr@eurotrans-payroll.com |
| Received from IP | 185.224.128.32 |

Note: Only one unique phishing email sent to multiple recipients.

Containment & Eradication Strategy

Containment Actions:

- Isolated compromised endpoints via CrowdStrike EDR
- Disabled affected user accounts in Active Directory
- Blocked outbound traffic to malicious IPs
- Quarantined phishing emails in Proofpoint
- Suspended external attachments temporarily

Eradication Actions:

- Removed malicious scheduled tasks

- Deleted keylogger malware %TEMP%\hrdata.exe
- Cleared malicious registry entries
- Reimaged compromised systems
- Reset passwords and enforced MFA

Recovery Checklist

- Reimage and patch compromised systems
- Restore affected accounts post-phishing awareness briefing
- Reactivate attachments after security filtering revalidation
- Update outbound firewall and DNS egress policies
- Extend EDR policies for macro-originated PowerShell executions
- Monitor affected systems for 14 days post-incident
- Perform tabletop incident response drill within 30 days

Lessons Learned and Recommendations

Lessons Learned:

- Email security controls were insufficient
- Poor phishing awareness among staff
- Incident response lacked playbook for phishing scenarios
- Limited visibility into remote office threats

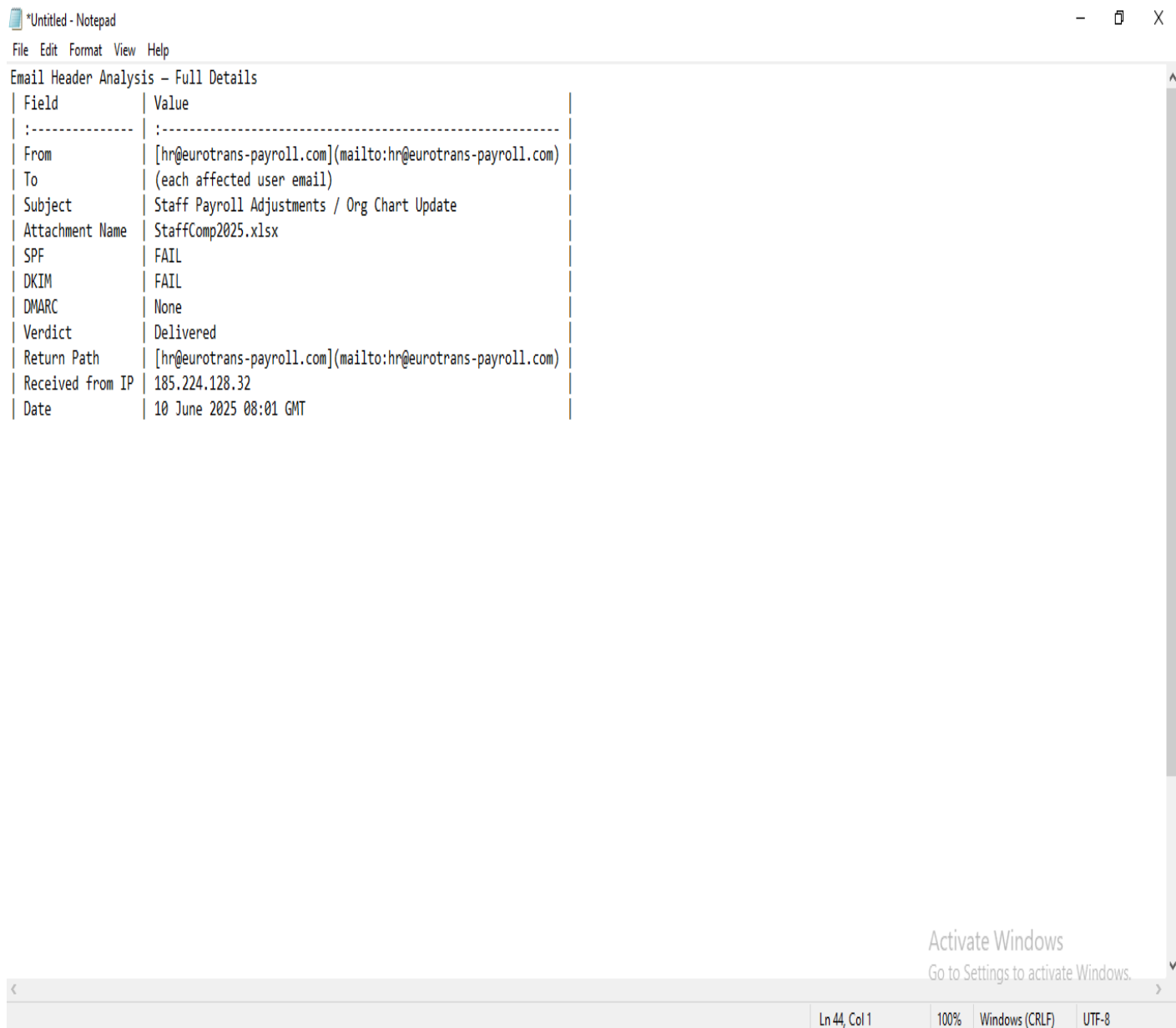
Recommendations:

- Enforce SPF, DKIM, DMARC with strict quarantine policies
- Disable macros in Office by default
- Strengthen firewall egress controls and DNS protection
- Deliver quarterly phishing awareness and simulation training

- Develop phishing-specific IR playbook and automate EDR containment
- Schedule annual tabletop exercises

Screenshots of Logs (Email Header Analysis, EDR Console, etc.)

Screenshot 1: Email Header Analysis (showing SPF: FAIL, DKIM: FAIL, Verdict: Delivered, etc.)



The screenshot shows a Notepad window titled "*Untitled - Notepad" with a menu bar (File, Edit, Format, View, Help). The text content is an email header analysis report titled "Email Header Analysis - Full Details". The report is presented as a table with two columns: "Field" and "Value". The fields and their corresponding values are: From: hr@eurotrans-payroll.com, To: (each affected user email), Subject: Staff Payroll Adjustments / Org Chart Update, Attachment Name: StaffComp2025.xlsx, SPF: FAIL, DKIM: FAIL, DMARC: None, Verdict: Delivered, Return Path: hr@eurotrans-payroll.com, Received from IP: 185.224.128.32, and Date: 10 June 2025 08:01 GMT. At the bottom right of the window, there is a watermark that says "Activate Windows Go to Settings to activate Windows." The status bar at the very bottom indicates "Ln 44, Col 1", "100%", "Windows (CRLF)", and "UTF-8".

| Field | Value |
|------------------|---|
| From | hr@eurotrans-payroll.com |
| To | (each affected user email) |
| Subject | Staff Payroll Adjustments / Org Chart Update |
| Attachment Name | StaffComp2025.xlsx |
| SPF | FAIL |
| DKIM | FAIL |
| DMARC | None |
| Verdict | Delivered |
| Return Path | hr@eurotrans-payroll.com |
| Received from IP | 185.224.128.32 |
| Date | 10 June 2025 08:01 GMT |

Screenshot 2: EDR Console Detection Logs

- PowerShell spawned by Excel
- Outbound connections to C2 IPs
- Keylogger detection
- Scheduled task persistence alert

The screenshot shows a Microsoft Word document titled "Document1 - Microsoft Word (Product Activation Failed)". The ribbon is set to "Home" with the "Font" and "Paragraph" groups visible. The document content is centered and titled "EDR Console Detection Log — Full List". Below the title is a table with 5 columns: Hostname, Detection Summary, Process, Verdict, and Action Taken. The table contains 5 rows of data. The status bar at the bottom indicates "Page: 1 of 2", "Words: 53", and "English (U.S.)". A watermark "Activate Windows" is visible in the bottom right corner.

| Hostname | Detection Summary | Process | Verdict | Action Taken |
|-------------|---|----------------|-----------|--------------|
| ET-GH-CS007 | PowerShell spawned by Excel.exe | powershell.exe | Malicious | Quarantined |
| ET-GH-CS009 | Outbound connection to 185.224.128.32 | powershell.exe | Malicious | Blocked |
| ET-GH-CS009 | Outbound connection to 74.119.201.12 | powershell.exe | Malicious | Blocked |
| ET-GH-CS011 | Scheduled Task: UpdateTask.ps1 | schtasks.exe | Malicious | Deleted Task |
| ET-JK-01 | Keylogger detected in %TEMP%\hrdata.exe | hrdata.exe | Malicious | Deleted |

Screenshot 3: Helpdesk Ticket Summary

- All user incident reports documented by time and issue

The screenshot shows a Microsoft Word document titled "Document1 - Microsoft Word (Product Activation Failed)". The ribbon is set to "Home", and the "Styles" section is expanded, showing "Normal" as the selected style. The document content is a "Helpdesk Ticket Summary — Full List" table with 4 columns: Ticket ID, Time, User, and Issue. The table contains 7 rows of data. The status bar at the bottom indicates "Page: 1 of 1", "Words: 64", and "English (U.S.)". A watermark "Activate Windows" is visible in the bottom right corner.

Helpdesk Ticket Summary — Full List

| Ticket ID | Time | User | Issue |
|-----------|-------|-----------------|--|
| #4561 | 08:11 | Kwame Okvere | Password lockout |
| #4562 | 08:22 | Mabel Boakye | Opened HR email attachment |
| #4563 | 08:27 | Admin (SOC) | Multiple lockout alerts |
| #4564 | 08:35 | Samira Damba | Outlook crash after opening email |
| #4565 | 08:42 | Jakarta Users | Redirects to unknown websites |
| #4566 | 08:45 | CrowdStrike EDR | Keylogger detected on ET-JK-01 |
| #4567 | 08:46 | CrowdStrike EDR | Scheduled task UpdateTask.ps1 detected |

Page: 1 of 1 Words: 64 English (U.S.) 120%