



Incident handler's journal

Maria Audu

| | |
|---------------------|--|
| Date: July 20, 2022 | Entry: #2 |
| Description | Final Alert Ticket Closure <i>Ticket Status: Closed</i> |
| Tool(s) used | N/A |
| Ticket Comments | Final Closure Entry The phishing alert was triggered by an email containing a malicious executable attachment (bfsvc.exe). The attachment's SHA256 hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) was verified as malicious through threat intelligence sources. Email security controls successfully quarantined the attachment prior to execution. Review of email, endpoint, and user activity logs confirmed no user interaction, no file execution, and no system or registry changes. The sender's domain and email content exhibited clear phishing indicators, including impersonation and social engineering tactics. |
| Additional notes | The threat was fully contained with no impact to the user or corporate environment. No escalation or remediation actions were required. The ticket is closed as Phishing – Malicious Attachment (Blocked / No Impact). |