**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  04/02/2025 | **Entry:**  03 |
| Description | This entry documents the investigation of a confirmed phishing attack involving a malicious email attachment. |
| Tool(s) used | VirusTotal |
| The 5 W's | * **Who** caused the incident?   The threat actor behind the attack behind the phishing attack used the email address Def Communications <76tguyhh6tgfrt7tg.su> and the IP address 114.114.114.114 to send a malicious email.   * **What** happened?   A phishing email was sent to an employee with a malicious attachment  (bfsvc.exe).   * **When** did the incident occur?   The incident occurred on Wednesday, July 2022 at 09:30:14   * **Where** did the incident happen?   Inergy organization at the recipient cooperate inbox and work station   * **Why** did the incident happen?   The attacker crafted a convincing phishing email with a fake job application to trick the recipient into downloading the malicious file. |
| Additional notes | The email included misspelled word which indicates a sign of phishing attack.  The incident could have been prevented if staffs and workers were properly educated on phishing attacks. |