Incident handler's journal

Date: 24/02/2025.	**Entry:** 001/02/25
Description	Suspicious email.
Tool(s) used	Sandbox to open attachment
The 5 W's	• **Who**??>> Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> • **What** happened? Employee received an email from an unknown source with a message pretending to be a response to a job offer with CV in attachment, which is passworded. The attachment seems to be a malicious executing file. The employee probably opened it. • **When** ??>> Wednesday, July 20, 2022 09:30:14 AM • **Where** ??>> employee's company email address [<hr@inergy.com> <176.157.125.93>] • **Why** ? This is probably a phishing scam
Additional notes	Attachment: filename="bfsvc.exe"
