|  |  |
| --- | --- |
| C:\user-pjpf\Briefcase-SO\so\so-12-13\slides\logo-IST-Tecnico.JPG | INSTITUTO SUPERIOR TÉCNICO  Departamento de Engenharia Informática  Forensics Cyber Security  MEIC / METI 2018-2019 – 1st Semester |

Digital Forensics Report

**83531 - Miguel Belém**

**83567 - Tiago Gonçalves**

**83576 - Vítor Nunes**

# Can you determine how the malware has taken over Sally's computer?

The most common ways to get infected by ransomware is by network or by plugging a infected USB drives. The team found a **thunderbird** profile account with one gmail account setted up. We manage to retrieve the INBOX msf file.

The team suspects that Sally received a phishing email which the sender was identified as “**Biochemistry Campus IT Department** <jason\_halloween@protonmail.com>”.

This clearly sound suspicious, even the attachment we found on the message.

# Can you recover Sally's original files? If you do not succeed at retrieving the original files, can you at least extract some of its fragments?

…

# What can you tell about the identity of the attacker?

…

# Elaborate a timeline of the most significant events of the case.

…

Can also attach appendices, e.g., displaying relevant evidence, timelines, etc.