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

1 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.

An interesting fact that reveals that Sally downloaded the infected attachment to her Downloads folder.

Sally clearly executed the file as we can find two processes running from that exact file.

2 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?

Yes, we recovered all image (PNG files), a PDF document and a text file. We used the **128-bit AES** symmetric key, found in memory dump to decrypt the files.

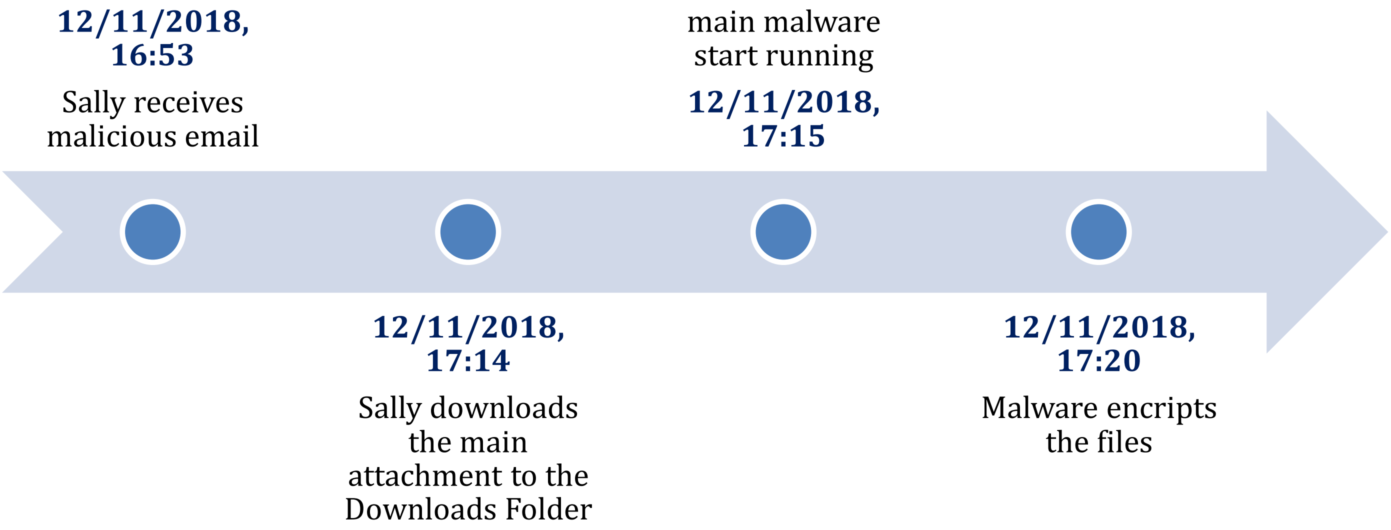
3 What can you tell about the identity of the attacker?

After inspecting the memory, we observed two IP addresses. The first one to be discovered (194.210.229.58) we think it is the IP from the last computer that accessed the machine that was logged in by the virus. ("Last login...). Nothing can ensure us that IP is from the attacker although it gives us strong suspicions that it could the attack origin.

The second one was found next to popup message in memory (146.193.41.57) with a possible userID "jason" and a possible password "friday13th". We think it might be the IP of the attacker as it was found next to references of sally/Documents right before the popup appears (it seems like the popup came from the IP).

We cannot confirm the identity of the attacker but we can do further investigations with a warrant to search for the origin of the IPs.

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



12/11/2018, 16:53

Sally receives malicious email

12/11/2018, 17:14

Sally downloads the main attachment to the Downloads Folder

main malware start running

12/11/2018, 17:15

12/11/2018, 17:20

Malware encripts the files