## **Parking lot USB exercise**

| **Contents** | The USB contains all types of information: vacation ideas, wedding list, pet’s photos, JB’s resume, shift schedules, employees budget and a new hire letter. There are a few documents that contain PII and sensitive work files, info that doesn’t only include the owner of the USB, but other employees too. |
| --- | --- |
| **Attacker mindset** | The info that appears in the USB could be used against other employees because there is a document claiming “Employee budget..” so I imagine that’s a usable document for financial matters. They could also use the family photos to publish them on social media, etc. |
| **Risk analysis** | It could be that any type of malicious software was hidden in this USB, something like a virus infecting all the workstation devices and getting all the data the attacker wanted. If the device was infected and another employee discovered it and used it, it would infect all the systems of the Hospital and all the data would be exposed (customers, patients data). A threat actor will find names, ID, telephone number, financial account numbers, addresses… of various employees including the ones of human resource manager. This info could be used against an individual or organization asking for a bounty in exchange of not posting this personal info, like a ransomware, or they can use this info to impersonate the individual and take advantage of this to get money or break the individual’s reputation. |