## **USN Baiting Report**

|  |  |
| --- | --- |
| **Contents** | *There are multiple cases of PII on this device including finances, work schedules and family names. Sensitive files such as shift schedules showcase who is where and when as well as a new hire form. These should not be stored on the same USB and work files especially sensitive ones should be secured in a vault or password or encryption protected.* |
| **Attacker mindset** | *This information could be used to threaten and blackmail the individual as well as the friends, family and colleagues all detailed within the USB. This could in turn lead to Jorge being manipulated into becoming a security threat within himself either with or even without his knowledge.* |
| **Risk analysis** | *Many different forms of malware could be hidden on this device. Ransomware, remote access tools, worms, root kits, key loggers are some to name a few. If this device was in fact infected with malware and found by another employee and inserted into a standard workstation there the malware may have been activated.*  *There is clearly PII on this device but pending further investigation I would make a reasonable assumption that SPII would be uncovered on the work-related documents on the removed device.*  *This information could be used to manipulate the individual to carry out illegal and actions towards the organization.* |