Parking lot USB exercise

Contents	The information found of this USB device appears to be a mix of personal and professional data. There is PII like like family photos pet photos, wedding list, work schedule and resume. There's also work information about hires and budgets that could be added as more PII data.
Attacker mindset	*This information could be used again Jorge to impersonate him both on his work and also in his personal life. An example could be cancelling his wedding reservations or exposing him with sensitive data. Regarding his work, and attacker could use the information to contact the new hire or stalk Jorge on his way to work.*
Risk analysis	*These USB devices could have malware on them, usually made to infect and to perpetrate into the victim's computer or network. This could be his person machine on a work network containing sensitive information.* *This sensitive information would be "PII": names, addresses, phone numbers, Social Security numbers, bank cards, passwords… it also could be "SPII": like health information, biometric data.* *This information could be used for Identity Theft, Black Mailing, Targeting Attacks and to Gaing Unauthorized access (impersonation).*