## **Parking lot USB exercise**

You are part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There’s no one else around who might have dropped it, so you decide to pick it up out of curiosity.

You bring the USB drive back to your office where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it’s one of the only ways to safely investigate an unfamiliar USB stick. The software works by running a simulated instance of the computer on the same workstation. This simulation isn’t connected to other files or networks, so the USB drive can’t affect other systems if it happens to be infected with malicious software.

|  |  |
| --- | --- |
| **Contents** | *In USB we found PII data for example “JB\_Resume.gdoc”. There are organization’s sensitive data like “Employee budget’s..”. It isn’t safe to store personal data with work data.* |
| **Attacker mindset** | *Attacker may use obtained PII data to target Jorge or his relatives. He may employ social engineering attack using this knowledge.*  *There is also risk that USB stick is distraction, attacker may used already stolen data to create fake Jorge drive and targeted him or someone he knows hoping that someone will plug device to workstation to install malware on device* |
| **Risk analysis** | * *Promoting employees awareness by additional training* * *Setting up antivirus scans* * *Disabling AutoPlay function on workstations to prevent computers from executing malware when device is plugged in.* |