## **Parking lot USB exercise**

Scenario: 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** | This drive contains documents that have his personal details which he doesn’t want to share with anyone. It also includes other people details including SPII and PII details |
| **Attacker mindset** | The attacker can edit the new hire letter to his name and join the organization and modify the vacation details and he can cancel or go for vacation for free and Employee budget can be uploaded into dark web and ask for ransomware to avoid reputation exploitation for organization |
| **Risk analysis** | Promoting employee awareness about these types of attacks and what to do when a suspicious USB drive is a managerial control that can reduce the risk of a negative incident. Setting up routine antivirus scans is an operational control that can be implemented. Another line of defense could be a technical control, like disabling AutoPlay on company PCs that will prevent a computer from automatically executing malicious code when a USB drive is plugged in. Encrypting or setting passcodes to open files in USB drive |