# **Activity: Identify the attack vectors of a USB drive**

**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.

**Step 1. Inspect the contents of the USB stick**

create a virtual environment and plug the USB drive into the workstation. The contents of the device appear to belong to Jorge Bailey, the human resource manager at Rhetorical Hospital.

A screenshot of a computer

Description automatically generated

Step 2. Apply an attacker mindset to the content of the USB drive.

Step 3. Analyse the risks of finding a parking lot USB

Consider some of the risks associated with USB baiting attacks:

* What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?
* What sensitive information could a threat actor find on a device like this?
* How might that information be used against an individual or an organization?

**Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | Some documents appear to contain personal information that Jorge would not want to be made public. The work files include the PII of other people. Also, the work files contain information about a hospital’s operations. |
| **Attacker mindset** | The timesheet can provide an attacker intel about other people that Jorge works with. Either work or personal information could be used to trick Jorge, a malicious email could be designed to look as it comes from a coworker or relative. |
| **Risk analysis** | Promoting employee awareness about these type 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. Disabling AutoPlay on company PCs could also be implemented to prevent a computer from automatically executing malicious code when a USB drive is plugged in. |