

Scenario :: Identify attack vectors of a USB drive

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.

Addendum -

You 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.

Jorge's drive contains a mix of personal and work-related files. For example, it contains folders that appear to store family and pet photos. There is also a new hire letter and an employee shift schedule.

 Offline

JB_Rsume.

Report

<i>Contents</i>	<i>Some documents appear to contain personal information that Jorge wouldn't want to be made public. The work files include the PII of other people. Also, the work files contain information about the hospital's operations.</i>
<i>Attacker mindset</i>	<i>The timesheets can provide an attacker intel about other people that Jorge works with. Either work or personal information could be used to trick Jorge. For example, a malicious email can be designed to look as though it comes from a coworker or relative.</i>
<i>Risk analysis</i>	<i>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.</i>