

Case Study:

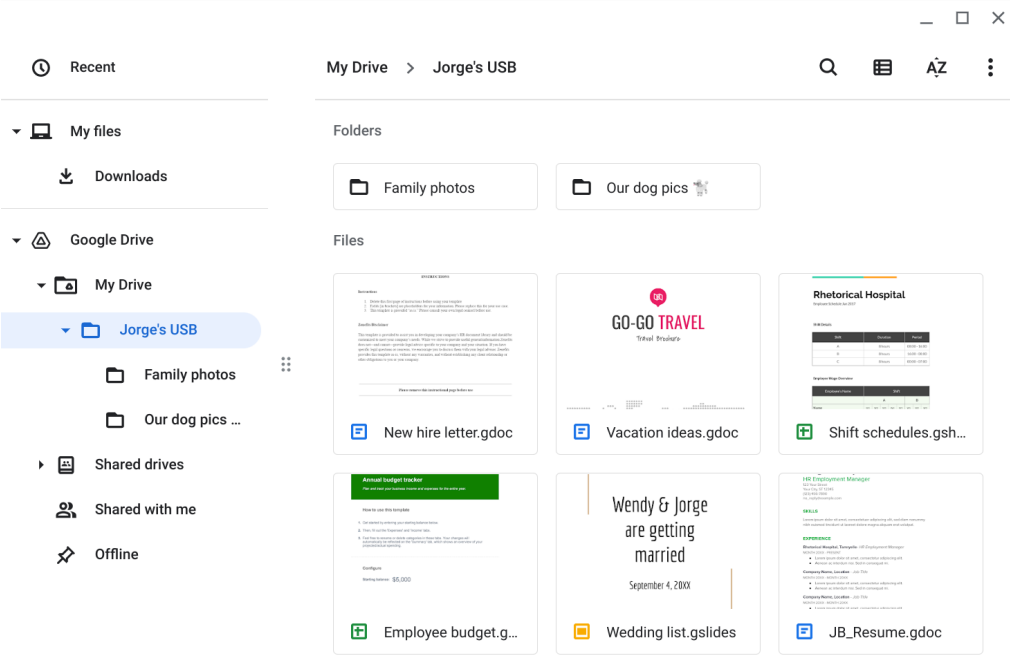
Identify The Attack Vectors of a Found USB Drive

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.

Parking Lot USB Exercise

<p>Contents</p>	 <p>After creating a virtual environment and plugging the USB drive into the workstation, the contents of the device appear to belong to Jorge Bailey, the human resource manager at Rhetorical Hospital. 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.</p>
<p>Attacker mindset</p>	<p>The timesheets can provide an attacker intel about other people that Jorge works with. Either work or personal information could be used in a social engineering phishing attack to trick Jorge. For example, a malicious email can be designed to look as though it comes from a coworker or relative.</p>

Risk analysis	<p>Technical, operational and managerial controls to mitigate attacks:</p> <ul style="list-style-type: none">- Technical Control: Disabling AutoPlay on company PCs that will prevent a computer from automatically executing malicious code when a USB drive is plugged in.- Operational Control: Setting up routine antivirus scans.- Managerial Control: Promoting employee awareness about these types of attacks and what to do when a suspicious USB drive is found.
----------------------	---