Parking Lot USB Drive - Attack Vector Analysis

# Activity Overview

In this activity, you will assess the attack vectors of a USB drive. You will consider a scenario of finding a USB drive in a parking lot from both the perspective of an attacker and a target.  
  
USBs, or flash drives, are commonly used for storing and transporting data. However, some characteristics of these small, convenient devices can also introduce security risks. Threat actors frequently use USBs to deliver malicious software, damage other hardware, or even take control of devices. USB baiting is an attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network. It relies on curious people to plug in an unfamiliar flash drive that they find.

# 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-By-Step Instructions

Follow the instructions and answer the questions below to complete the activity.

## Contents

The USB drive contains a mix of personal and work-related files, including family and pet photos, a new hire letter, and an employee shift schedule. These files indicate that the drive belongs to Jorge Bailey, the human resource manager at Rhetorical Hospital. This combination of personal and professional data increases the risk if the drive were to fall into the wrong hands.

## Attacker Mindset

An attacker could use the information on the USB drive to craft targeted phishing attacks or social engineering campaigns. The inclusion of work-related documents might help an attacker impersonate Jorge or exploit his role within the hospital. It’s also possible the attacker planted the USB intentionally, making it a staged baiting attempt.

## Risk Analysis

USB baiting presents several security risks, including the potential delivery of malware such as keyloggers, ransomware, or remote access tools. If an infected device were used by an unsuspecting employee, it could compromise entire networks. Sensitive data like shift schedules and personal photos could also be exploited to impersonate staff. To mitigate these risks, organizations should train employees not to use unknown USB drives, implement endpoint detection tools, and use virtualization environments for safe analysis.