**Attack vector of a USB drive**

**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.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

**Scenario**

Review the following scenario. Then complete the step-by-step instructions.

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 question below to complete the activity.

**Step 1: Access the template**

Parking lot USB exercise

|  |  |
| --- | --- |
| Contents | Write 2-3 sentences about the types of information found on this device.  . Are there files that can contain PII?  . Are there sensitive work files?  . Is it safe to store personal files with work files?  Yes, some files can potentially contain personally identifiable information (PII). In this case, the new hire letter may contain the PII of the newly hired employee, and the employee shift schedule may contain PII of the hospital's staff, such as their names, work schedules, and potential contact information. Sensitive work files are present on the USB drive, such as the new hire letter and employee shift schedule. These files contain confidential information related to the hospital's operations, employees, and possibly their contact details. Storing personal files alongside work files on the same USB drive is not safe from a security perspective. It is generally recommended to keep personal and work-related data separate to minimize the risk of data breaches and unauthorized access. |
| Attacker Mindset | Write 2-3 sentences about the types of information found on this device.  . Are there files that can contain PII?  . Are there sensitive work files?  . Is it safe to store personal files with work files?  Yes, some files can potentially contain personally identifiable information (PII). In this case, the new hire letter may contain the PII of the newly hired employee, and the employee shift schedule may contain PII of the hospital's staff, such as their names, work schedules, and potential contact information. Sensitive work files are present on the USB drive, such as the new hire letter and employee shift schedule. These files contain confidential information related to the hospital's operations, employees, and possibly their contact details. Storing personal files alongside work files on the same USB drive is not safe from a security perspective. It is generally recommended to keep personal and work-related data separate to minimize the risk of data breaches and unauthorized access. |
| Risk analysis | Write 2-3 sentences about the types of information found on this device.  . Are there files that can contain PII?  . Are there sensitive work files?  . Is it safe to store personal files with work files?  Yes, some files can potentially contain personally identifiable information (PII). In this case, the new hire letter may contain the PII of the newly hired employee, and the employee shift schedule may contain PII of the hospital's staff, such as their names, work schedules, and potential contact information. Sensitive work files are present on the USB drive, such as the new hire letter and employee shift schedule. These files contain confidential information related to the hospital's operations, employees, and possibly their contact details. Storing personal files alongside work files on the same USB drive is not safe from a security perspective. It is generally recommended to keep personal and work-related data separate to minimize the risk of data breaches and unauthorized access. |

mitigate these types of 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?*

To mitigate these types of attacks, several controls can be implemented:

Technical Controls: The hospital should implement endpoint security solutions that can scan and detect malicious software on USB drives before they are accessed. This would help prevent the infection of the hospital's network or other devices. Regular software updates and patch management can also help reduce vulnerabilities.

Operational Controls: It is essential to educate employees about the risks associated with plugging in unknown USB drives and promote a culture of security awareness. Employees should be trained not to use unfamiliar USB drives and to report them to the IT department. Additionally, the hospital should establish strict data handling policies to segregate personal and work-related data.

Managerial Controls: Access controls and encryption should be implemented to protect sensitive data. Managers should enforce policies that restrict the storage of sensitive work files on personal USB drives and promote secure data sharing practices. Incident response plans should also be in place to address potential data breaches.

Step 2: Inspect the contents of the USB stick

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.

Review the types of information that Jorge has stored on this device. Then, in the **Contents** row of the activity template, write **2-3 sentences** (40-60 words) about the type of information that's stored on the USB drive.

***Note:*** *USB drives often contain an assortment of personally identifiable information (PII). Attackers can easily use this sensitive information to target the data owner or others around them.*

Step 3: Apply an attacker mindset to the contents of the USB drive

Step 4: Analyze the risks of finding a parking lot USB

Contents: found on the USB stick appear to be a mix of personal and work-related files. The personal files include family and pet photos, while the work-related files consist of a new hire letter and an employee shift schedule.

Yes, there are files that can potentially contain personally identifiable information (PII). In this case, the new hire letter may contain PII of the newly hired employee, and the employee shift schedule may contain PII of the hospital's staff, such as their names, work schedules, and potentially contact information.

Sensitive work files are present on the USB drive, such as the new hire letter and employee shift schedule. These files contain confidential information related to the hospital's operations, employees, and possibly their contact details.

Storing personal files alongside work files on the same USB drive is not safe from a security perspective. It is generally recommended to keep personal and work-related data separate to minimize the risk of data breaches and unauthorized access.

Attacker Mindset: The information found on this USB drive could be used against Jorge or the

hospital by an attacker. If an attacker gains access to PII on the drive, they could potentially engage in identity theft or launch phishing attacks against Jorge. The information could also be used against the hospital's employees if their personal data is exposed. Additionally, if the information on the drive provides details about the hospital's operations, it could potentially be used for targeted attacks or corporate espionage.

Risk Analysis: To mitigate these types of attacks, several controls can be implemented: