## **Parking lot USB exercise**

| **Contents** | The USB belongs to the human resource manager (Jorge) in the company and it contains a mixture of personally identifiable information such as family photos and plans. It also contains sensitive work related information like shift schedules, employee budget, a new hire letter and a resume. |
| --- | --- |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.  The shift schedule could contain sensitive information like the names of other employees who work for the same hospital or even the names of specific patients they might have been assigned to. With this information, attackers might target other employees who work for the hospital. Potential targets might include the social media accounts of individuals related to the owner of the drive such as relative and family members.  Interestingly, files contained in the drive might be a distraction, relying on a curious employee to lower their guard and plug the USB into their company system. This might automatically activate a malware installed on the USB thus granting the threat actor remote access and control over the device and unfettered access into the company’s systems.  By passing the company’s perimeter defences will allow the attacker access to internal-only systems or even restricted data like SPII, PII and PHI. This can quickly escalate to a ransomware attack, data exfiltration or APT. |
| **Risk analysis** | The device might contain malicious code in files that when clicked might direct the user to phishing websites where their credentials are exposed and harvested. It might also give the attacker outright remote access to the system through HID - human interface device spoofing. This happens when the computer is tricked into believing the USB is a keyboard.  A threat actor can find information related to company secrets. They could gain potential access to employee and patient data.  This attack can be mitigated using the PoLP security control. Having antiviruses installed on systems can detect malware in the USB and initiate a deletion process. Employees should be educated to return any of such found devices to the IT department who can follow best practice in evaluating the safety of the drive. For example, they might use a virtualised instance to scanning the drive for potential viruses and malware before handing it over to the legitimate owner, in case of lost property. Disabling AutoPlay will also prevent a compute from automatically executing malicious clode on USBs. |