## **Parking lot USB exercise**

| **Contents** | * *Are there files that can contain PII?*   *The files on the USB drive contain information about the employee and the head of Jorge Hospital. Obviously, files like photos of their family and data about the company, with him being the owner, are PII.*   * *Are there sensitive work files?*   *Yes, these are sensitive work file about, employee’s budget, shift schedules, jb\_resume, new hire letter…etc*   * *Is it safe to store personal files with work files?*   *No, we should separate our personal and work files into different accounts to avoid putting all information at risk.* |
| --- | --- |
| **Attacker mindset** | * *Could the information be used against other employees?*   *If the USB were infected with a virus, the employee who connects the device within the Hospital's facilities could infect the entire system and carry out a large number of malicious actions, such as encrypting system files, creating backdoors, unauthorized remote access, information gathering and so on.*   * *Could the information be used against relatives?*   *An attacker can review the information on the USB drive pertaining to relatives and identify valuable data to then conduct a deep analysis of these individuals and launch attacks on their accounts.*  *The attacks we can carry out are quite numerous, including* ***phishing****,* ***impersonation****,* ***emotional manipulation****,* ***access to shared accounts****, and so on.*   * *Could the information provide access to the business?*   *Having Jorge's information, we can perform a* ***brute-force attack*** *on his work account. Since we know a good deal about his personal life, this could help us relate it to one of his passwords. As he's responsible for Human Resources, we're sure to gain permissions to obtain valuable information about employees and related parties.* |
| **Risk analysis** | * *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?*   *Keylogger - Attack simulating a brute force attack with a keyboard.*  *Autorun Files - Autorun Files with malicious code*  *Firmware attacks - It's hard for antivirus software to detect because the malware resides in the controller's hardware, not in the disk's files.*   * *What sensitive information could a threat actor find on a device like this?*   *A threat actor could find highly sensitive* ***Personally Identifiable Information (PII)****,* ***Protected Health Information (PHI)****, and* ***confidential Corporate/Proprietary Information*** *on such a device. This includes names, addresses, financial details, patient records, internal IT infrastructure details, and strategic business plans.*   * *How might that information be used against an individual or an organization?*   ***Individuals:*** *Identity theft, financial fraud, targeted phishing/scams, blackmail, and reputational damage.*  ***Organizations:*** *Data breaches, financial losses (fines, lawsuits), intellectual property theft, corporate espionage, ransomware attacks, reputational damage, and disruption of operations.* |