### **USB Attack Scenario Report**

#### **Contents**

The USB device contains a mix of personal and work-related files, including family and pet photos, a letter of new hire, and employee shift schedules. These files could contain personally identifiable information (PII), such as names and contact details. Sensitive work files, like the new hire letter and shift schedules, should not be stored with personal files due to the risk of data breaches and misuse.

#### **Attacker Mindset**

An attacker could use the information on the USB to target Jorge or the hospital. The work-related files could facilitate attacks against other employees by revealing their schedules or new hires. Personal information, such as family photos, could be used to create phishing emails or social engineering attacks aimed at Jorge's relatives or colleagues. Additionally, the information could provide attackers with enough details to gain unauthorized access to the hospital's systems.

#### **Risk Analysis**

USB baiting attacks can introduce various types of malicious software, such as keyloggers, ransomware, or spyware, onto a network. If an infected device were discovered by another employee and connected to the network, it could lead to widespread infection and data breaches. Sensitive information found on such a device could be used for identity theft, unauthorized access to systems, or to launch targeted attacks against the hospital or its employees.

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

1. **Technical Controls:** Implement endpoint security solutions that can detect and block malicious software from external devices. Regularly update and patch software to protect against known vulnerabilities.
2. **Operational Controls:** Establish policies that prohibit the storage of personal files on work devices. Encourage employees to use secure cloud storage for work-related files and to avoid using USB drives for sensitive information.
3. **Managerial Controls:** Conduct regular security training to educate employees about the risks associated with unknown USB devices and the importance of following data handling policies. Implement procedures for securely managing and disposing of USB drives.

**Professional Tips from CISA:**

1. Keep personal and work USB drives separate to minimize the risk of cross-contamination.
2. Always scan USB drives for malware before use.
3. Use encryption on USB drives to protect sensitive information.

Implementing these controls can significantly reduce the risk of such incidents and protect both individuals and the organization from potential harm.

### **Informe del Escenario de Ataque con USB (spanish)**

#### **Contenido**

El dispositivo USB contiene una mezcla de archivos personales y relacionados con el trabajo, incluidos fotos de familiares y mascotas, una carta de una nueva contratación y horarios de turnos de empleados. Estos archivos podrían contener información de identificación personal (PII), como nombres y detalles de contacto. Archivos de trabajo sensibles, como la carta de nueva contratación y los horarios de turnos, no deberían almacenarse junto con archivos personales debido al riesgo de filtraciones de datos y uso indebido.

#### **Mentalidad del Atacante**

Un atacante podría utilizar la información del USB para atacar a Jorge o al hospital. Los archivos relacionados con el trabajo podrían facilitar ataques contra otros empleados al revelar sus horarios o nuevas contrataciones. La información personal, como fotos familiares, podría usarse para crear correos electrónicos de phishing o ataques de ingeniería social dirigidos a los familiares o colegas de Jorge. Además, la información podría proporcionar a los atacantes detalles suficientes para obtener acceso no autorizado a los sistemas del hospital.

#### **Análisis de Riesgo**

Los ataques de cebo con USB pueden introducir varios tipos de software malicioso, como keyloggers, ransomware o spyware, en una red. Si un empleado descubriera un dispositivo infectado y lo conectara a la red, podría llevar a una infección generalizada y brechas de datos. La información sensible encontrada en un dispositivo como este podría usarse para el robo de identidad, acceso no autorizado a sistemas o para lanzar ataques dirigidos contra el hospital o sus empleados.

Para mitigar estos tipos de ataques, se deben implementar varios controles:

1. **Controles Técnicos:** Implementar soluciones de seguridad en los puntos finales que puedan detectar y bloquear software malicioso de dispositivos externos. Actualizar y parchear regularmente el software para protegerse contra vulnerabilidades conocidas.
2. **Controles Operativos:** Establecer políticas que prohíban el almacenamiento de archivos personales en dispositivos de trabajo. Fomentar el uso de almacenamiento en la nube seguro para archivos relacionados con el trabajo y evitar el uso de unidades USB para información sensible.
3. **Controles Administrativos:** Realizar capacitaciones de seguridad regularmente para educar a los empleados sobre los riesgos asociados con dispositivos USB desconocidos y la importancia de seguir las políticas de manejo de datos. Implementar procedimientos para gestionar y eliminar de manera segura las unidades USB.

**Consejos Profesionales de CISA:**

1. Mantener las unidades USB personales y de trabajo separadas para minimizar el riesgo de contaminación cruzada.
2. Siempre escanear las unidades USB en busca de malware antes de su uso.
3. Utilizar cifrado en las unidades USB para proteger la información sensible.

Implementar estos controles puede reducir significativamente el riesgo de tales incidentes y proteger tanto a las personas como a la organización de posibles daños.