**🧑‍💻 Informe de Laboratorio – CyberDefenders: Oski Lab**

**📄 Información General**

* **Nombre del laboratorio:** Oski Lab
* **Plataforma:** CyberDefenders
* **Fecha de realización:** 27/05/2025
* **Duración estimada:** 45 minutos
* **Dificultad percibida:** Media

**🎯 Objetivo del Laboratorio**

Un contador de la empresa recibió un correo electrónico titulado "Nuevo pedido urgente" de un cliente a última hora de la tarde. Al intentar acceder a la factura adjunta, descubrió que contenía información falsa sobre el pedido. Posteriormente, la solución SIEM generó una alerta sobre la descarga de un archivo potencialmente malicioso. Tras una investigación inicial, se descubrió que el archivo PPT podría ser el responsable de esta descarga. La tarea consiste en realizar un análisis detallado de este archivo para identificar su comportamiento malicioso y las técnicas utilizadas.

**🛠️ Herramientas Utilizadas**

* **VirusTotal:** Para análisis de hash y comportamiento del archivo.
* **ANY.RUN:** Para análisis dinámico del malware.
* **Recorded Future Triage:** Para obtener información adicional sobre el malware.

**🧪 Análisis y Desarrollo**

**🔍 Q1 – Familia de malware**

**Pregunta:** ¿Cuál es el nombre de la familia de malware del ejecutable malicioso que se encuentra en el PPT?  
**Respuesta:** **Stealc**

**Análisis:**  
Se proporcionó un hash MD5 del archivo malicioso. Al consultar este hash en VirusTotal, se identificó que pertenece a la familia de malware **Stealc**, conocida por utilizar DLLs legítimas para exfiltrar archivos, información confidencial y monederos de criptomonedas desde el host infectado.

**🕒 Q2 – Fecha de creación del malware**

**Pregunta:** ¿Cuándo se creó el malware?  
**Respuesta:** **2022-09-28 17:40:46 UTC**

**Análisis:**  
En la pestaña "Details" de VirusTotal, dentro de la sección "History", se encontró la fecha de creación del archivo malicioso, lo que proporciona información sobre su origen temporal.

**🌐 Q3 – Servidor C2C**

**Pregunta:** ¿Con qué servidor C2C se comunica el malware en el archivo PPT?  
**Respuesta:** **http://171.22.28.221/5c06c05b7b34e8e6.php**

**Análisis:**  
En la pestaña "Relations" de VirusTotal, específicamente en "Contacted URLs", se identificó que el malware se comunica con el servidor mencionado, actuando como su centro de comando y control (C2C).

**📚 Q4 – Primera biblioteca solicitada**

**Pregunta:** ¿Cuál es la primera biblioteca que solicita el malware después de la infección?  
**Respuesta:** **sqlite3.dll**

**Análisis:**  
Utilizando la herramienta ANY.RUN, se observó que la primera biblioteca solicitada por el malware tras la infección es **sqlite3.dll**, lo que indica su intento de acceder a bases de datos SQLite en el sistema comprometido.

**🔑 Q5 – Clave RC4 utilizada**

**Pregunta:** ¿Cuál es la clave RC4 específica que utiliza este malware?  
**Respuesta:** **5329514621441247975720749009**

**Análisis:**  
A través de la herramienta Recorded Future Triage, se accedió a la configuración del malware, donde se identificó la clave RC4 utilizada para descifrar cadenas codificadas en base64.

**🛡️ Q6 – Técnica MITRE ATT&CK empleada**

**Pregunta:** ¿Qué técnica de MITRE ATT&CK están utilizando para robar la contraseña de un usuario?  
**Respuesta:** **T1555: Credentials from Password Stores**

**Análisis:**  
En el informe de ANY.RUN, al acceder a la sección ATT&CK Matrix, se identificó que el malware emplea la técnica **T1555**, que implica la extracción de credenciales desde almacenes de contraseñas del sistema.

**🗑️ Q7 – Directorio objetivo para eliminación**

**Pregunta:** ¿A qué directorio o ruta apunta el malware para su eliminación?  
**Respuesta:** **C:\ProgramData**

**Análisis:**  
Observando el árbol de procesos en ANY.RUN, se detectó que el malware ejecuta un proceso CMD que, tras un breve retraso, elimina el archivo ejecutable malicioso y otras DLLs asociadas ubicadas en el directorio **C:\ProgramData**.

**⏱️ Q8 – Tiempo hasta autoeliminación**

**Pregunta:** Después de exfiltrar con éxito los datos del usuario, ¿cuántos segundos tarda el malware en autoeliminarse?  
**Respuesta:** **5 segundos**

**Análisis:**  
El análisis dinámico en ANY.RUN mostró que el malware espera **5 segundos** después de la exfiltración de datos antes de proceder a su autoeliminación, como parte de sus técnicas de evasión.

**✅ Conclusión**

El laboratorio Oski Lab proporcionó una experiencia práctica en el análisis de malware, desde la identificación de su familia hasta la comprensión de sus técnicas de evasión y exfiltración de datos. Se destacó la importancia de herramientas como VirusTotal y ANY.RUN para realizar análisis estáticos y dinámicos, respectivamente. Además, se evidenció cómo los atacantes emplean técnicas sofisticadas, como el uso de DLLs legítimas y la autoeliminación post-exfiltración, para evitar la detección y el análisis foren