Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencias de Datos y Matemáticas

Aplicación de Criptografía y Seguridad

Kaspersky Endpoint Security Cloud

Versión Ejecutiva

Samantha Ruelas Valtierra	A01704564
Ángel David Ávila Pérez	A01562833
Héctor David Bahena Garza	A01284661
Manzur Macías Pineda	A01198234
María Fernanda Lee Ponce	A00830974
Gonzalo Garza Moreno	A01284950

Profesores Óscar E. Labrada Gómez y Alberto F. Martínez Herrera

Socio Formador IPC Services

Monterrey, Nuevo León.

07/09/2023

Índice

Índice **2**
Introducción: **3**
Desarrollo: **4**
Instalación de software 4
Virus 4
Resultados: **5**
Descripción de las Amenazas 5
Amenaza 1 EICAR 5
Amenaza 2 The Zoo 5
Amenaza 3 Kakwa.doc 6
Conclusiones **7**
Amenaza 1 EICAR 7
Amenaza 2 The Zoo 7
Amenaza 3 Kakwa.doc 7
Recomendaciones **8**
Referencias **8**

Introducción:

Kaspersky Endpoint Security Cloud es una solución de seguridad informática diseñada para proteger las redes y dispositivos de una organización contra una amplia variedad de amenazas cibernéticas. El propósito principal de utilizar **Kaspersky Endpoint Security Cloud** es garantizar la seguridad de los sistemas, datos y activos de una empresa o institución, y esto se logra a través de varias funciones clave:

- Protección contra malware y virus: **Kaspersky Endpoint Security Cloud** Es una herramienta que utiliza tecnología avanzada de detección y eliminación de malware para detectar y proteger dispositivos contra virus, troyanos, ransomware y otros tipos de software malicioso.
- Gestión centralizada: **Kaspersky Endpoint Security Cloud** permite a los administradores de TI gestionar la seguridad de todos los dispositivos desde una única consola de administración basada en la nube. Esto simplifica la gestión y el monitoreo de la seguridad informática.
- Control de aplicaciones y dispositivos: Los administradores pueden establecer políticas para controlar qué aplicaciones y dispositivos pueden utilizarse en alguna red en específico. Esto ayuda a regular la ejecución de software no autorizado y por lo tanto aumenta la protección contra amenazas potenciales.
- Actualizaciones automáticas: **Kaspersky Endpoint Security Cloud** se actualiza automáticamente para mantenerse al día con las últimas amenazas y vulnerabilidades de seguridad, lo que garantiza una protección continua efectiva y relevante.
- Informes y auditoría: **Kaspersky Endpoint Security Cloud** proporciona herramientas de generación de informes y auditorías que permiten realizar un seguimiento de la actividad de seguridad, identificar posibles brechas y cumplir con los requisitos de cumplimiento normativo.
- Escalabilidad: **Kaspersky Endpoint Security Cloud** es escalable y puede adaptarse a las necesidades de las organizaciones o usuarios que lo deseen utilizar, ya sean pequeñas, medianas o grandes.

En resumen, Kaspersky Security Endpoint utiliza una combinación de firmas conocidas, análisis heurístico, aprendizaje automático y análisis de comportamiento para detectar y mitigar una amplia gama de amenazas cibernéticas en tiempo real, lo que ayuda a mantener seguros los dispositivos y redes empresariales. Además, ofrece herramientas de gestión y control que permite personalizar las políticas de seguridad de acuerdo al ambiente en el que se necesite.

Desarrollo:

Utilizamos la herramienta **Kaspersky Endpoint Security Cloud** dentro de una máquina virtual para poder analizar amenazas artificiales que introducimos en el sistema y así obtener un mayor entendimiento de amenazas de este tipo en un escenario del mundo real. Luego procedimos a utilizar la herramienta para analizar 3 escenarios diferentes, con el fin de llegar a una conclusión sobre su nivel de amenaza, sus consecuencias y las recomendaciones que podemos ofrecer para evitar tales amenazas, o en caso de ser inevitable, cómo lidiar con las consecuencias.

Instalación de software

Instalamos una máquina virtual para que cualquier ataque artificial u otro tipo de amenaza que pudiéramos provocar dentro de la máquina no afectará significativamente ninguno de nuestros dispositivos personales o escolares. Para este propósito se utilizó el software Oracle VM Virtualbox, en el cuál se instaló una versión de evaluación de Windows 11 (WinDev2307Eval) de 64-bit. A esta se le asignaron 4096 MB de memoria RAM. Ese fue el entorno en el cuál se descargaron los virus.

Descargamos el archivo que contiene la herramienta **Kaspersky Endpoint Security Cloud** y creamos un workspace en al cuál se añadieron las cuentas de todos los miembros del equipo. Se descargó Kaspersky Endpoint Security for Windows 12.2.0.462 en la maquina virtual, y se ligó subsecuentemente el entorno de Windows 11 al portal web de Kaspersky.

Virus

Se analizaron 3 amenazas:

- EICAR
- ytisf/theZoo
- HEUR Trojan

En cada caso, al intentar acceder a estos sitios, se activaba una advertencia de Kaspersky que bloqueaba el acceso. Posteriormente, se registraban estas anomalías en el portal web del workspace de Kaspersky Business Hub. La información recopilada se utilizaría para un análisis posterior en la siguiente sección del informe.

Resultados:

Descripción de las Amenazas

Analizamos 3 amenazas artificiales para familiarizarnos con la herramienta de análisis y la respuesta al ataque.

Amenaza 1 EICAR

Ejecutamos la primera amenaza artificial proporcionada por el OSF, lo que resultó en varios subprocesos secundarios que establecieron conexiones con varias direcciones IP desconocidas pero detectadas y posteriormente se empezó la descarga de varios archivos temporales, uno de los cuales fue detectado por **Kaspersky Endpoint Security Cloud** como un malware malicioso, por lo que detuvo su descarga y señaló una amenaza potencial.

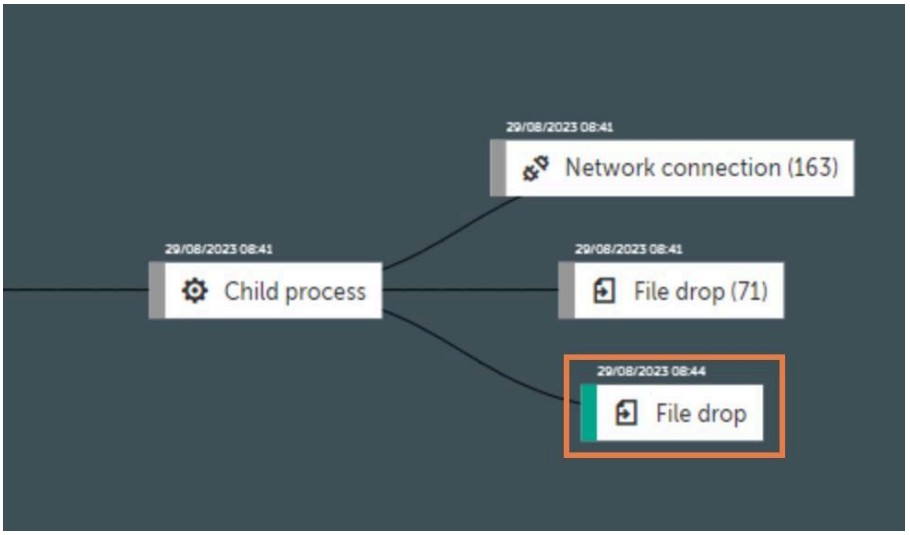

Imagen 1. Diagrama EICAR-Test-File Amenaza 1

Amenaza 2 The Zoo

La segunda amenaza que probamos con Kaspersky Endpoint Security Cloud fue detectada y bloqueada de manera rápida, de tal manera que la información que Kaspersky pudo proporcionar sobre la amenaza simplemente indicaba que se detectó y bloqueó una amenaza, que no se tomaron acciones adicionales, simplemente que se bloqueó un malware malicioso de realizar acciones dentro del sistema.

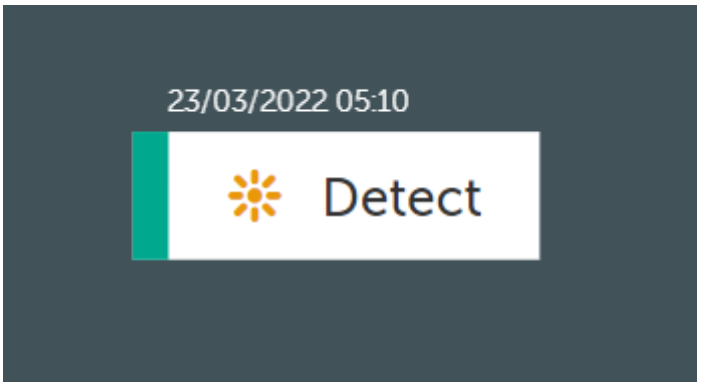

Imagen 2. Diagrama Proceso 1 Amenaza 2

Amenaza 3 Kakwa.doc

La Tercera amenaza se obtuvo del link:

“https://raw.githubusercontent.com/Da2dalus/The-MALWARE-Repo/master/Spyware/Kakwa.doc//JIM”

El cual es un repositorio de github en donde hay gran cantidad de software malicioso para hacer pruebas y poder probar la ciberseguridad de diferentes sistemas.

Esta amenaza consistió en 1 subproceso y creó 1 archivo denominado “HEUR:Trojan.MSOffice.SAgent.gen” con los comportamientos de la amenaza, el nombre proporcionado por Kaspersky y su clasificación en “SHA-256” y “MD5” podemos deducir que este fue un ataque tipo troyano.

Imagen 3. Diagrama de Proceso Amenaza 3

Conclusiones

Amenaza 1 EICAR

La primera amenaza ejecutó 2 subprocesos y creó 71 archivos temporales con 163 intentos de conexiones remotas desde la IP de origen con permisos de administrador que luego fueron bloqueados y puestos en cuarentena por Kaspersky Endpoint Security Cloud. Con Kaspersky Endpoint Security Cloud-EDR pudimos detectar y bloquear de manera satisfactoria el Archivo EICAR-Test-File.

Analizando el comportamiento del malware y basándo nos en la documentación obtenida por Kaspersky en su base de datos del “SHA-256” y “MD5” podemos observar que antes la amenaza fue detectada como un malware de tipo worm, pero este específicamente es un EICAR-Test-File, para el software de AutoCAD.

Amenaza 2 The Zoo

Investigando en la información obtenida por en la base de datos de Kaspersky solo pudimos deducir que este malware se podría tratar de un troyano por su clasificación en ocasiones anteriores. Con su SHA-256 se pudo obtener que es un Adware y otros, su plataforma es un WIN32, siendo su clase un Hacktool o Troyano, pero sin asegurar cual de los dos es.

Aun así, podemos estar seguros que las acciones de Kaspersky demuestran su gran capacidad para manejar amenazas de cualquier tipo y de proteger la computadora de estos malwares desde el primer proceso, así salvaguardando nuestras máquinas.

Amenaza 3 Kakwa.doc

La amenaza se detectó como un ataque cibernético analizado con la herramienta de Kaspersky. Se identificó que la conexión se realizó desde el navegador "Microsoft Edge" y que se generó un archivo llamado "HEUR:Trojan.MSOffice.SAgent.gen". Según la información proporcionada por Kaspersky, se clasifica como un ataque de tipo troyano para Microsoft Office. Los troyanos son malware que se camuflan como archivos adjuntos de correo electrónico o descargas gratuitas y, una vez en el dispositivo del usuario, realizan acciones maliciosas como crear puertas traseras, espiar la actividad en línea o robar datos sensibles.

Recomendaciones

Al concluir con el análisis se pueden sugerir las siguientes recomendaciones para mantener un ambiente seguro y limpio para trabajar.

1. Mantener el software actualizado: Es esencial asegurarse de que el sistema operativo y las aplicaciones estén siempre actualizados con los últimos parches de seguridad para evitar vulnerabilidades conocidas.
2. Ser cauteloso con los correos electrónicos y descargas: Se recomienda no abrir correos electrónicos o archivos adjuntos sospechosos, ya que los worms y troyanos a menudo se distribuyen de esta manera. Verificar la autenticidad de los remitentes antes de abrir archivos adjuntos es una práctica segura.
3. Utilizar software de seguridad confiable y actualizado: Se insta a emplear software de seguridad confiable que pueda escanear y proteger el sistema contra amenazas, incluyendo worms y troyanos. Se destaca la importancia de herramientas como "Kaspersky Endpoint Security Cloud" para obtener información relevante sobre ataques y tomar medidas para proteger el sistema.

En resumen, mantener el software actualizado, ser cauteloso con los correos electrónicos y las descargas, y utilizar software de seguridad confiable son medidas esenciales para proteger las computadoras contra amenazas de software malicioso. Se recomienda encarecidamente mantener el software de seguridad actualizado para una protección efectiva.

Referencias

Kaspersky. “.” . - *YouTube*, 2 October 2022, https://opentip.kaspersky.com/09148a50e00d77132d1f4f4de4afa590/results. Accessed 7 September 2023.

Kaspersky. “Ejemplo de análisis de un gráfico de cadena de desarrollo de la amenaza.” *Kaspersky support*, https://support.kaspersky.com/Cloud/1.0/es-ES/231627.htm. Accessed 7 September 2023.

“¿Qué es un troyano? Virus troyanos y software malware.” *Fortinet*, https://www.fortinet.com/lat/resources/cyberglossary/trojan-horse-virus. Accessed 7 September 2023.

“What Is a Worm?” *Cisco*, https://www.cisco.com/c/en/us/products/security/what-is-a-worm.html. Accessed 7 September 2023.