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 Técnica

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

Introducción

Kaspersky Security Endpoint es una solución de seguridad diseñada para proteger dispositivos y redes empresariales contra amenazas cibernéticas, incluyendo malware, ataques de phishing, ransomware y más. Para detectar y mitigar estas amenazas, Kaspersky Security Endpoint lleva a cabo protección adaptativa de última generación que incluye:

Protección en tiempo real: Kaspersky Security Endpoint opera en tiempo real para detectar amenazas a medida que ocurren. Monitorea constantemente la actividad en el dispositivo o en la red y busca signos de comportamiento sospechoso. El cual logra detectar gracias a su base de datos actualizada de firmas de malware, sus técnicas heurísticas avanzadas para identificar amenazas desconocidas y su protección contra exploits de vulnerabilidades conocidas.

Aprendizaje automático y análisis de comportamiento: Kaspersky Security Endpoint emplea algoritmos de aprendizaje automático para identificar patrones y comportamientos anómalos en el sistema. Lo cual le permite detectar amenazas nuevas que su base de datos de firmas de malware todavía no incluye.

Análisis de reputación: Kaspersky Security Endpoint evalúa la reputación de archivos y sitios web. Si un archivo o sitio se considera sospechoso, se somete a un análisis más detenido y si se considera inseguro, puede bloquearse.

Actualizaciones frecuentes: Kaspersky se asegura de mantener su base de datos de firmas y técnicas de detección actualizadas para hacer frente a las amenazas más recientes.

Atención activa: Los administradores reciben informes y notificaciones en tiempo real sobre actividades sospechosas o incidentes de seguridad para que puedan tomar medidas rápidas y adecuadas.

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

Máquina Virtual

Por cuestiones de seguridad, todos los virus analizados se descargaron en una máquina virtual. 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.

Imagen 1. Máquina Virtual Windows 11 en VirtualBox

En la Imagen 1 se observa los ajustes necesarios para arrancar la máquina virtual de Windows 11 como fueron mencionados con anterioridad.

Kaspersky Security Endpoint

Creamos un workspace en Kaspersky Endpoint Security Cloud, 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 máquina virtual, y se ligó subsecuentemente el sistema operativo de Windows 11 al portal web de Kaspersky.

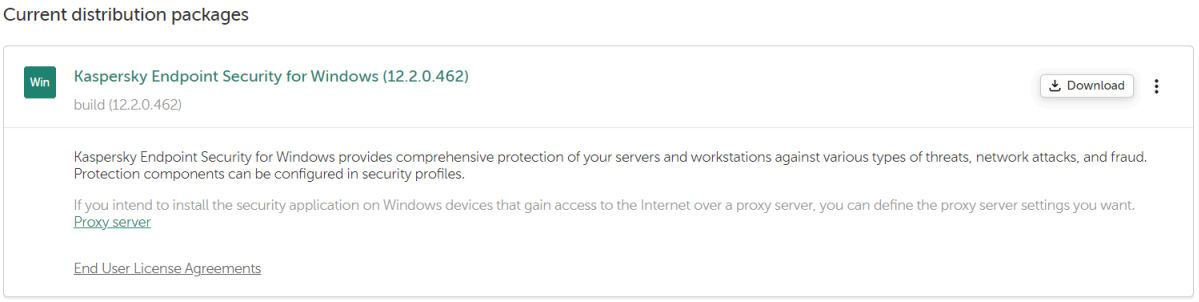

Imagen 2. Distribución de Kaspersky Endpoint Security instalada en la máquina virtual

Como se muestra en la Imagen 2, el programa Kaspersky Endpoint Security aparece accesible para descargarse por medio de la página de Kaspersky Endpoint Security Cloud.

Varios miembros del equipo intentaron realizar este proceso, pero encontraron problemas en diferentes etapas del proceso. Algunos tuvieron problemas en instalar o correr la máquina virtual, mientras que otros no lograron conectar su máquina virtual al workspace compartido incluso después de haber descargado Kaspersky Endpoint Security en esta. No obstante, sí se logró hacer la configuración completa en una de las computadoras, y esta fue la que se utilizó para el análisis de virus.

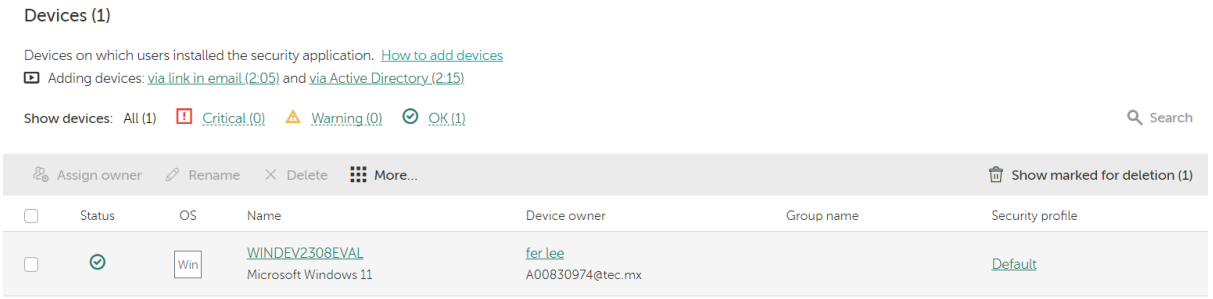

Imagen 3. Dispositivos conectados al workspace de Kaspersky Endpoint Security Cloud. Se puede observar la máquina virtual Windows 11

En la Imagen 3 tenemos la identificación del dispositivo “WINDEV2308EVAL”, del usuario “fer lee”. Este dispositivo está enlazado con la aplicación de “Kaspersky Endpoint Security.” Ya que se conectó al mismo servidor, el sitio web es capaz de mostrar qué dispositivos se conectaron con éxito.

Virus

Se analizaron 3 amenazas:

- EICAR
- ytisf/theZoo
- HEUR Trojan

Para cada una de estas amenazas se ingresó a su sitio web correspondiente en la máquina virtual. En todos los casos, se desplegaba un mensaje de advertencia de Kaspersky el cuál bloqueaba el acceso al sitio. Una vez que aparecía este mensaje de advertencia, el workspace de Kaspersky Business Hub detectaba la anomalía y la registraba en el portal web. A partir de la información recopilada se realizó el análisis en la siguiente sección.

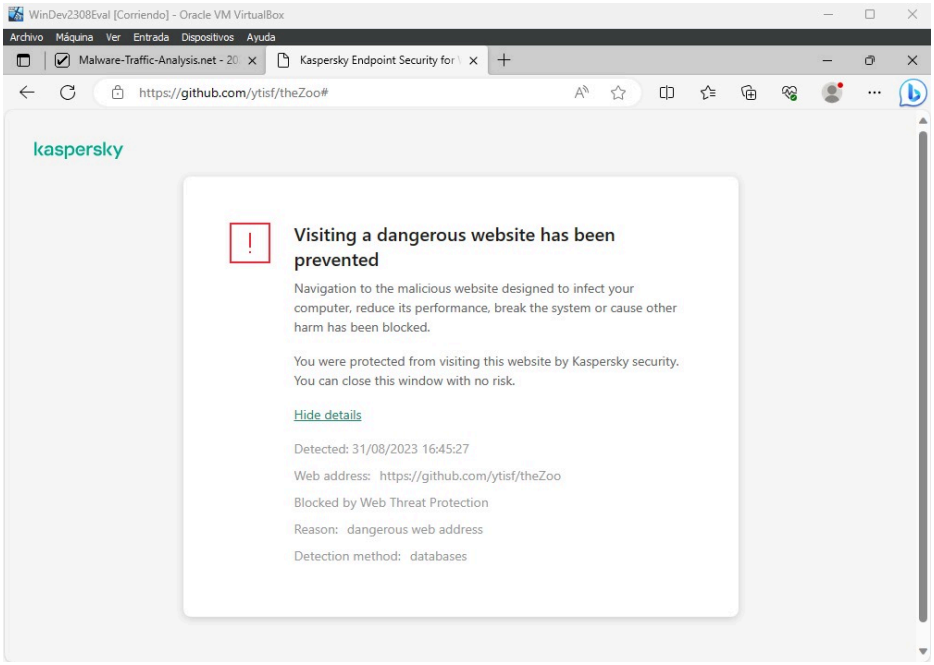

Imagen 4. Advertencia de Kaspersky Endpoint Security al tratar de ingresar al sitio de The Zoo

En la Imagen 4 observamos lo que ocurre cuando se accede a alguno de los códigos maliciosos mencionados con anterioridad. Se utiliza como ejemplo “The Zoo”, el cuál se identificó como una amenaza y por lo tanto se bloqueó el proceso para ejecutarse y provocar un ataque cibernético que afecte a la máquina.

Resultados

Usando la herramienta “Kaspersky Endpoint Security Cloud” específicamente la opción de “Endpoint Detection and Response” proporcionada por el socio formador IPC Services pudimos hacer un análisis profundo de cada uno de los ataques que simulamos en nuestra máquina virtual. Este análisis nos proporcionó información de los ataques, especialmente nos brindó información sobre las acciones efectuadas, la categoría de la amenaza detectada, el origen del archivo, usuario que descargó el archivo entre otros. Toda esta información es presentada de manera visual en una gráfica de cadena de desarrollo de la amenaza, lo cual nos permitió tener un mejor entendimiento de lo sucedido en el ataque para su posterior análisis.

Cada amenaza probada presentó sus propias particularidades y su propia forma de interacción. Por ello, cada gráfico de cadena de desarrollo fue diferente ya que esto caracteriza al malware en sí.

Descripción de las evidencias

Amenaza 1 EICAR

La primera amenaza fue la proporcionada por el socio formador en el link “https://secure.eicar.org/eicar.com” el cual ejecutamos en nuestra máquina virtual y Kaspersky detectó.

Origen de la amenaza

Proceso 1:

Aquí tenemos la información obtenida en Kaspersky sobre el proceso que dio origen al ataque:

Parámetro de Inicio	Tipo	PID del sistema	Crítico	Nivel de Integridad
C:\Windows\explorer.exe	Proceso	4752	No	Integridad media

Usuario	Hora
WINDEV2308EVAL\User	29/08/2023 8:41:00

Tabla 1. Información Proceso 1 amenaza 1

Se puede apreciar que el primer bloque en el diagrama de proceso es el correspondiente a la primera acción, en este caso un proceso hecho por el usuario principal del sistema:

Imagen 5. Diagrama Amenaza 1 Proceso 1

En la Imagen 5 se visualiza el primer diagrama, conocido como “chain graph” o gráfica de cadena. Se indica el proceso y los 2 subprocesos detectados por la primera amenaza “EICAR”.

Kaspersky capturó este proceso y nos proporciona la siguiente información:

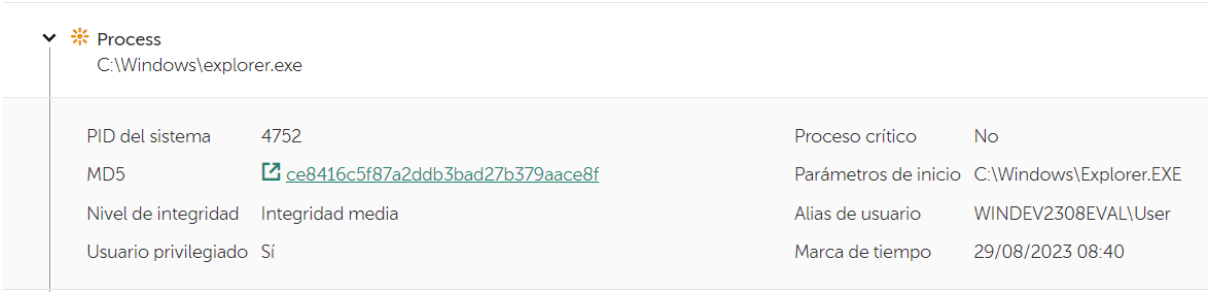

Imagen 6. Información Kaspersky Proceso 1 Amenaza 1

Como se puede visualizar en la Imagen 6, el proceso muestra parámetros que nos permiten conocer detalles acerca de la amenaza. Sin embargo, al ser simplemente un proceso, no se revela aún todo el desglose, sino hasta que se lleguen a los subprocesos.

Desarrollo de Amenaza

En el desarrollo de la amenaza tuvimos 2 subprocesos en total.

Child process 1:

El primer subproceso fue un proceso hijo del proceso principal, aquí se ve la información obtenida de este en kaspersky:

Parámetro de Inicio	Número	PID del sistema	Tipo	Crítico	Nivel de Integridad
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start /prefetch:5	1	2556	Child Process	No	Integridad media

Tabla 2. Información Subproceso 1 Amenaza 1

El siguiente diagrama nos muestra la relación que tuvo este proceso durante el ataque:

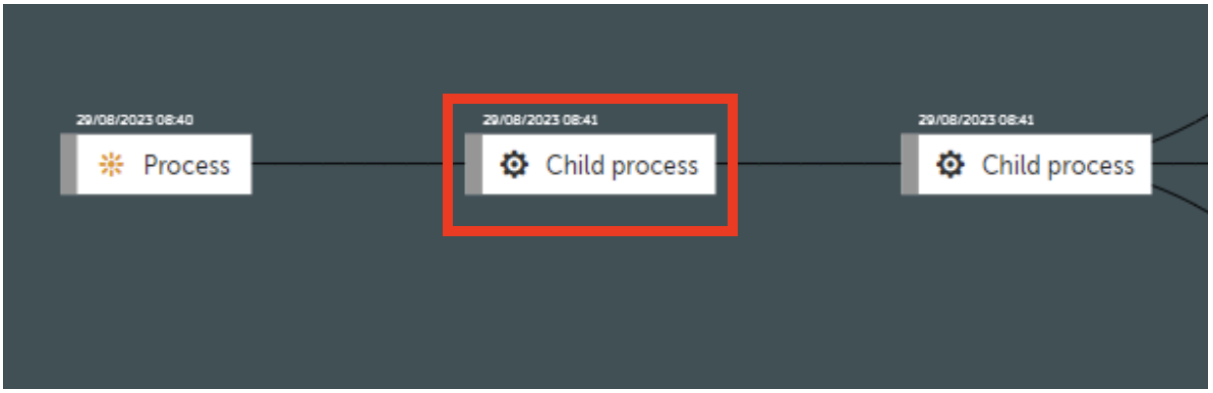

Imagen 7. Diagrama Subproceso 1 Amenaza 1

La imagen 7 muestra el primer subproceso siendo señalado por un recuadro rojo. De esta manera, señala su localización en el diagrama.

Y el siguiente resumen nos dice los detalles del proceso.

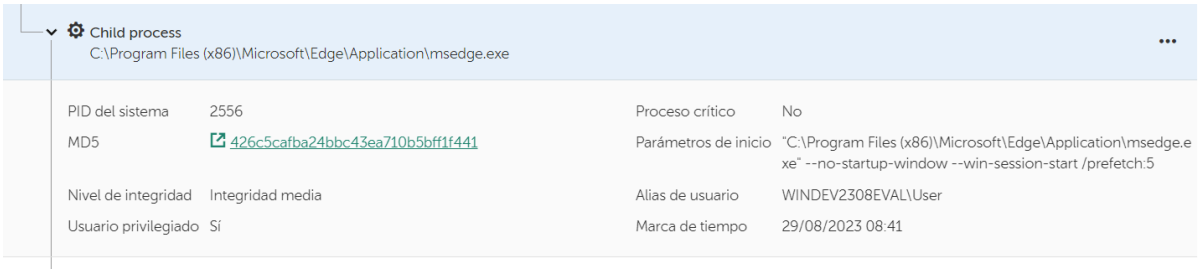

Imagen 8. Información Subproceso 1 Amenaza 1

La Imagen 8 nos muestra de manera detallada la información que representa al subproceso 1 de esta amenaza.

Child process 2:

El segundo subproceso fue un proceso hijo del proceso hijo anterior, aquí se ve la información obtenida de este en kaspersky:

Parámetro de Inicio	Número	PID del sistema	Tipo	Crítico	Nivel de Integridad
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2068 --field-trial-handle=1988,i,14367486399260472272,16595257938813403381,262144 /prefetch:3	1	7388	Child Process	No	Integridad media

Tabla 3. Información Subproceso 2 Amenaza 1

Aquí se destaca este proceso en el diagrama de Kaspersky:

Imagen 9. Diagrama Subproceso 2 Amenaza 1

Y se puede ver cómo Kaspersky clasificó el proceso:

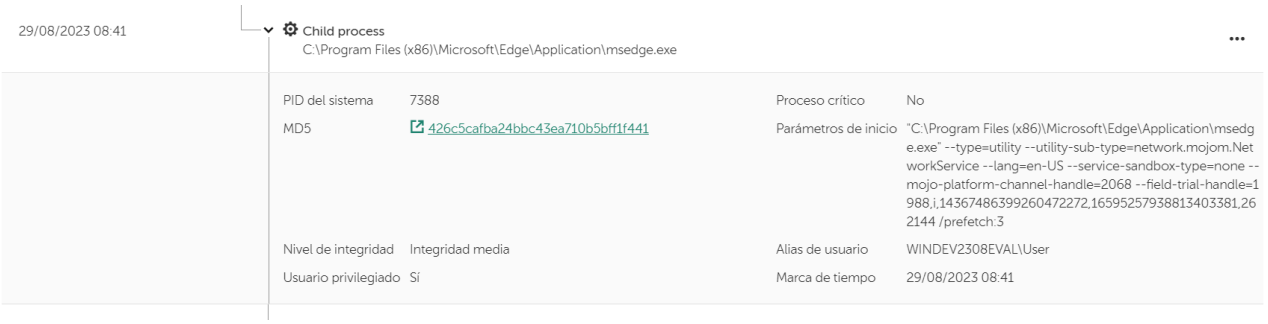

Imagen 10. Información Subproceso 2 Amenaza 1

Este subproceso dio como resultado 3 subprocesos consiguientes:

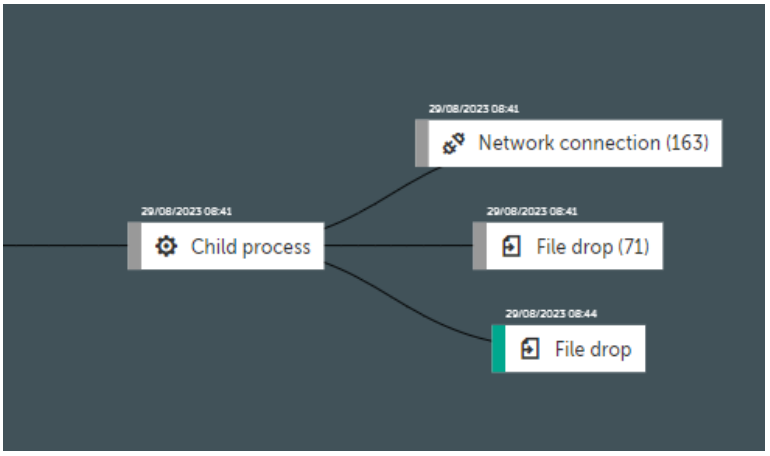

Imagen 11. Diagrama de resultados del Subproceso 2

Network Connection:

El primer subproceso que se dio fue una conección a internet el cual se conectó con 163 direcciones IP las cuales se enlistan a continuación una muestra representativa de las primeras 5:

Parámetro	**Número**	**Tipo**	**Resultados de la comprobación de fiabilidad**	**Hora de detección**
Network Connection	163	Conexiones Remotas	No fiable	29/08/2023 8:41
Dirección remota			**Dirección Local**	
35.213.89.133:443			10.0.2.15:49782	
20.127.253.7:443			10.0.2.15:49781	
20.127.253.7:443			10.0.2.15:49780	
35.213.89.133:443			10.0.2.15:49779	
52.38.56.225:443			10.0.2.15:49776	

Tabla 4.Conexión a Red Amenaza 1

El subproceso se resalta en el siguiente diagrama:

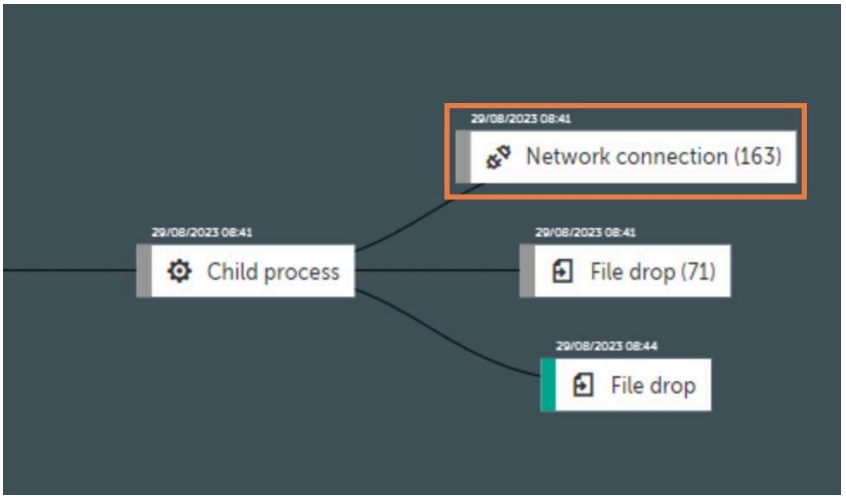

Imagen 12. Diagrama Conexión a Red Amenaza 1

Y se puede ver parte de la lista de direcciones IP en la siguiente imagen:

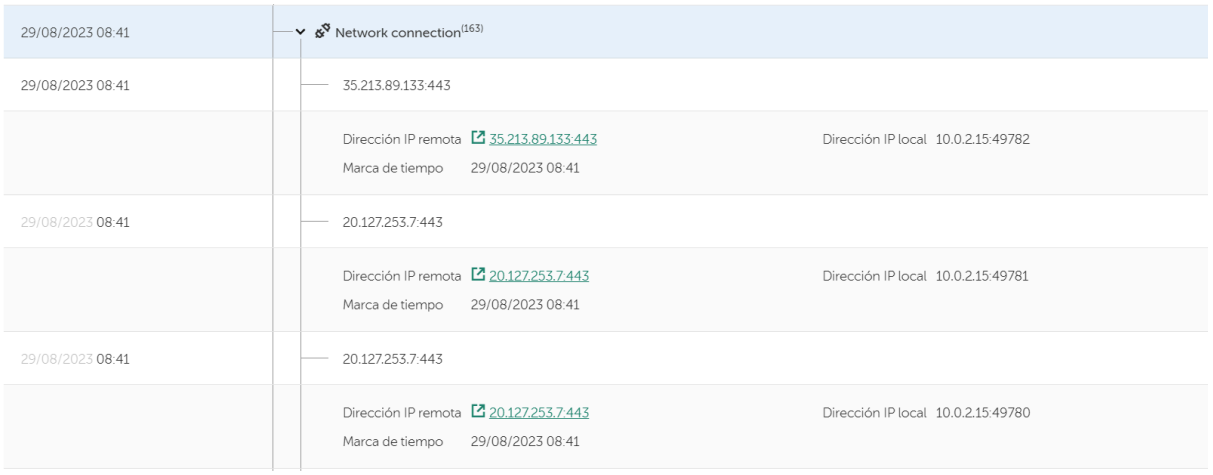

Imagen 13. Información Conexión a Red Amenaza 1

File drop:

El segundo subproceso de este fue un filedrop o una creación de archivos, los cuales fueron archivos temporales creados en las rutas listadas a continuación:

Parámetro	**Número**	**Tipo**	**Resultados de la comprobación de fiabilidad**	**Hora de detección**
File drop	71	Archivos Temporales	No fiable	29/08/2023 8:41
Rutas				
C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00005a				
C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00005b				
C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00005c				
C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00005d				
C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00005e				
C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00005f				
C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000060				

Tabla 5. Creación de Archivos Amenaza 1

Kaspersky da los detalles de los archivos creados de la siguiente manera:

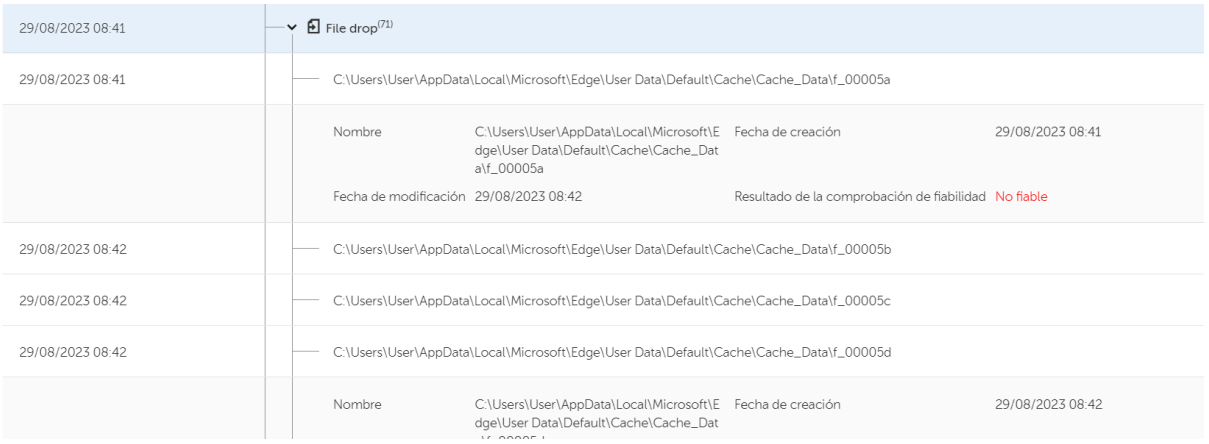

Imagen 14. Información Creación de Archivos Amenaza 1

Este subproceso se destaca en el siguiente diagrama:

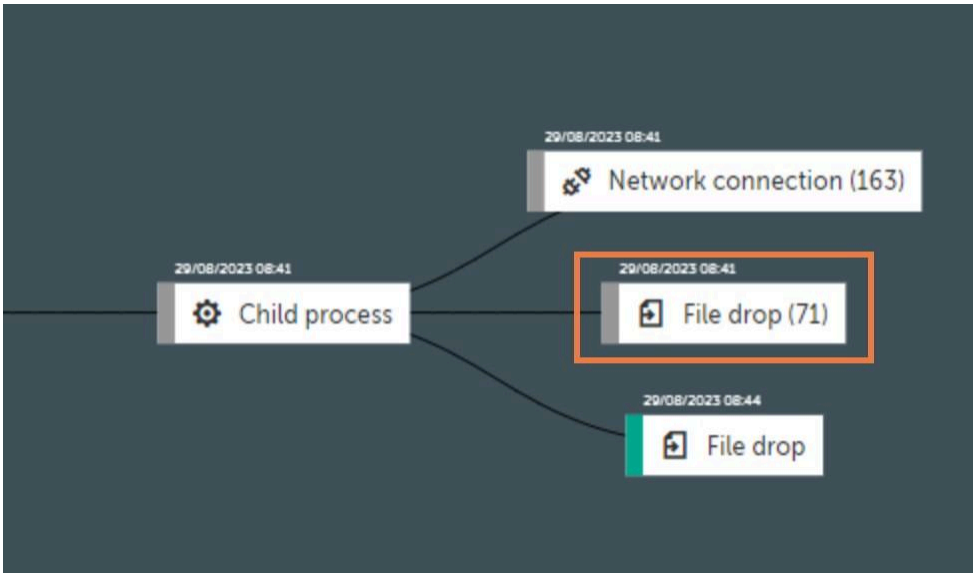

Imagen 15. Diagrama de la creación de archivos Amenaza 1

Indicadores de compromiso

El tercer subproceso, la creación del archivo "EICAR-Test-File", fue el que Kaspersky Endpoint Security Cloud-EDR detectó como un archivo malicioso por lo que bloqueó la acción y nos proporcionó la siguiente información:

URL de Descarga	**Amenaza**	**Tipo**	**Acción**	**Hora de detección**
https://secure.eicar.org/eicar.com	EICAR-Test-File	File-Drop	Bloqueada	29/08/2023 8:44
Indicadores				
MD5		**SHA-256**		
44d88612fea8a8f36de82e1278abb02f		275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f		
Descargador MD5		**Descargador SHA-256**		
426c5cafba24bbc43ea710b5bff1f441		869d62ca6f1ec17cda74aa091f8c5be4361ab473ed8077fdfdecf8482671630a		

Tabla 6. Información EICAR-Test-File

La información del archivo "EICAR-Test-File" también se puede ver en la siguiente captura de Kaspersky.

Imagen 16. Información EICAR-Test-File Amenaza 1

La creación de este archivo fue la acción del último subproceso que se generó del proceso hijo:

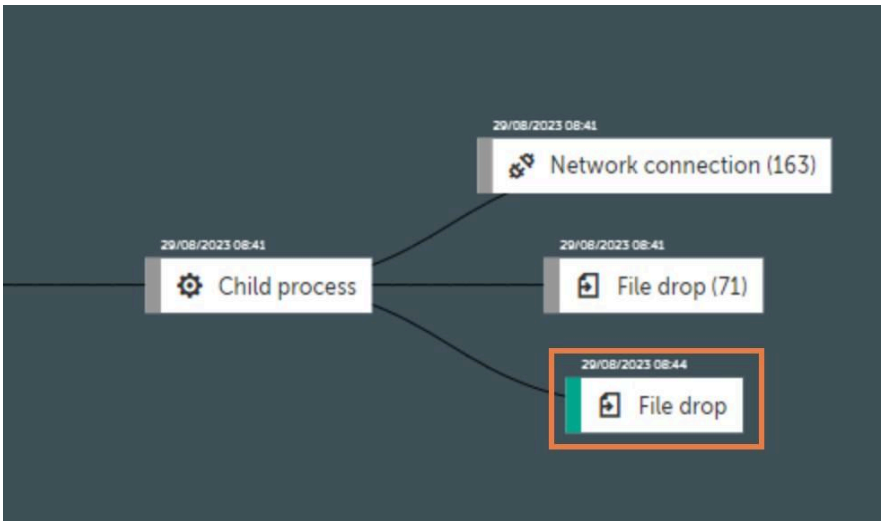

Imagen 17. Diagrama EICAR-Test-File Amenaza 1

Cabe aclarar que para obtener más información acerca de esta amenaza en particular se puede acceder a su "MD5" o su "SHA-256" con lo cual se puede ver en la base de datos de Kaspersky como se a clasificado con anterioridad, que medidas se pueden tomar, cuando fue la última vez detectado, etc.

Amenaza 2: TheZoo

La segunda amenaza surgió del link "https://github.com/ytisf/theZoo" proporcionado por el socio formador el cual se ejecutó en nuestra máquina virtual y Kaspersky bloqueó de manera inmediata.

Amenaza	**Tipo**	**Acción**	**Hora de detección**
https://github.com/ytisf/theZoo	Detect Proceso	Bloqueada	06/09/2023 8:59
Indicadores			
MD5	**SHA-256**		
177dc89bd51467ac4c771960c7cf994e	ef2a0f2614c79c781cf36724aa3d097196dfd9284d4616225f7ce66e283891d1		

Tabla 7. Información Proceso 1 Amenaza 2

Aquí se puede ver la manera en la que Kaspersky visualizó esta amenaza:

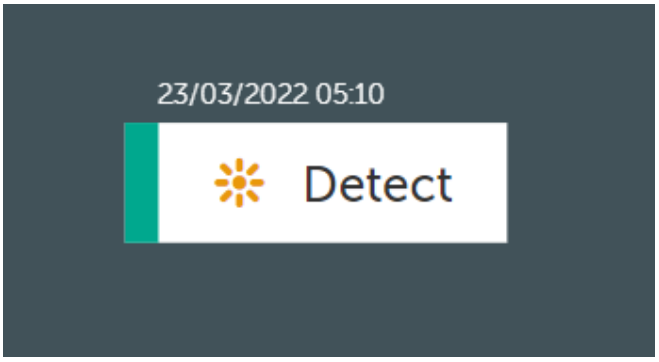

Imagen 18. Diagrama Proceso 1 Amenaza 2

Amenaza 3 HEUR Trojan

La tercera amenaza vino 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.

Origen de la amenaza

Proceso 1:

Aquí tenemos la información obtenida en Kaspersky sobre el proceso que dio origen al ataque:

Parámetro de Inicio	Tipo	PID del sistema	Crítico	Nivel de Integridad
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window /prefetch:5	Proceso	8068	No	Integridad media

Usuario	Hora
WINDEV2308EVAL\User	07/09/2023 11:19

Tabla 8. Información Proceso 1 Amenaza 3

Y aquí podemos ver el diagrama que muestra los procesos hijo que surgieron del proceso que inició el ataque:

Imagen 19. Diagrama Proceso 1 Amenaza 3

El proceso se puede ver descrito en la siguiente imagen:

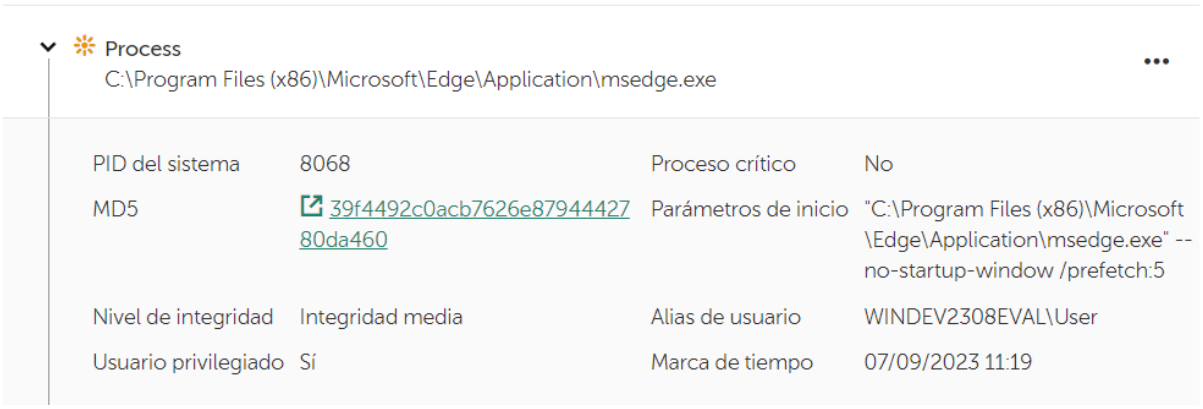

Imagen 20. Información Proceso 1 Amenaza 3

Desarrollo de Amenaza

En el desarrollo de la amenaza tuvimos 1 subprocesos en total.

Child process 1:

El primer subproceso fue un proceso hijo del proceso principal, aquí se ve la información obtenida de este en kaspersky:

Parámetro de Inicio	Número	PID del sistema	Tipo	Crítico	Nivel de Integridad
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2068 --field-trial-handle=1908,i,2988695898937731 41,13477618556145221816,262144 /prefetch:3	1	8000	Child Process	No	Integridad media

Tabla 9. Información Proceso Hijo 1 Amenaza 3

Este subproceso se resulta en el siguiente diagrama:

Imagen 21. Información Proceso Hijo 1 Amenaza 3

Y Kaspersky muestra los detalles del subproceso en la siguiente imagen:

Imagen 22. Información Proceso Hijo 1 Amenaza 3

Indicadores de compromiso

Despues de subproceso se creo un archivo con nombre:

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

que se identificó como una amenaza de tipo: “HEUR:Trojan.MSOffice.SAgent.gen”

URL de Descarga	Amenaza	Tipo	Acción	Hora de detección
https://raw.githubusercontent.com/Da2dalus/The-MALWARE-Repo/master/Spyware/Kakwa.doc//JIM	HEUR:Trojan.MSOffice.SAgent.gen	File-Drop	Bloqueada	07/09/2023 11:39
Indicadores				
MD5		**SHA-256**		
09148a50e00d77132d1f4f4de4afa590		d0a76710d23ad79be2dfe76ddf70e683df1c66048c231df5ec097e4b492d1f00		
Descargador MD5		**Descargador SHA-256**		
39f4492c0acb7626e8794442780da460		b8defb82250a3fa81f4894ef4bf0f31583b4b7daa628f7f1c95e04e681972f8a		

Tabla 10. Información Filedrop 1 Amenaza 3

El siguiente diagrama muestra en qué parte del ataque sucedió el file drop.

Imagen 23. Diagrama FileDrop 1 Amenaza 3

Y los detalles del archivo creado son:

Imagen 24. Información FileDrop 1 Amenaza 3

Conclusiones, recomendaciones y evaluación final desde el punto de vista técnico

Amenaza 1 EICAR

Con la información reunida de kaspersky pudimos obtener información del ataque, entre ello que la conección se hizo desde el “Microsoft Edge” el cual ejecutó 2 sub-procesos y creó 71 archivos temporales con 163 intentos a conexiones remotas desde la IP Origen: “10.0.2.15” desde el Alias Usuario: “WINDEV2308EVAL\User” con privilegios de Administrador.

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 deducir que la anteriormente la amenaza fue detectada como un malware de tipo worm.

Cisco define un malware tipo gusano como un tipo de malware o software malicioso que puede replicarse rápidamente y propagarse a través de dispositivos dentro de una red. A medida que se propaga consume ancho de banda, sobrecargando los sistemas infectados y haciéndolos poco fiables o inaccesibles. Además se menciona que sus actividades características incluyen creación de archivos temporales y conexiones a la red. (“What Is a Worm?”)

Pero esta amenaza en específico es un EICAR, de la plataforma “ACAD”, que suele ser utilizado para el software de AutoCAD.

Amenaza 2

Kaspersky nos proporcionó información de este ataque, aunque no tan extensa como en el ataque anterior. Esto se debe a la naturaleza del mismo, ya que Kaspersky pudo detectar como amenaza desde el primer proceso del malware.

Vemos que en este caso solo obtuvimos 1 proceso que se descargó de la página “https://github.com/ytisf/theZoo” el cual se bloqueó de manera satisfactoria y no se permitió que se hicieran más subprocesos consiguientes.

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.

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

En esta amenaza usando la herramienta de Kaspersky nos dio información sobre este ataque con el cual nos podemos hacer una mejor idea de como fue el ataque. La conexión se hizo desde el "Microsoft Edge" el cual ejecutó 1 sub-procesos y creó 1 archivo con el nombre "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 para Microsoft Office.

Fortinet define un troyano como un tipo de malware que generalmente se oculta como un archivo adjunto de un correo electrónico o un archivo de descarga gratuita y que, luego, se transfiere al dispositivo del usuario. Una vez descargado, el código malicioso ejecutará la tarea para la que el atacante lo diseñó, como obtener acceso de puerta trasera a los sistemas corporativos, espiar la actividad en línea de los usuarios o robar datos sensibles. ("¿Qué es un troyano? Virus troyanos y software malware").

Recomendaciones

Existen varias acciones que se pueden realizar para proteger nuestras maquinas de software malicioso como el anteriormente mencionado algunas de las que consideramos más importantes son:

Mantener el software actualizado. Al asegurarse de que tu sistema operativo, programas y aplicaciones estén siempre actualizados con los últimos parches de seguridad, se evitan vulnerabilidades conocidas ya que los desarrolladores suelen lanzar actualizaciones para corregir estas.

Ser cauteloso con los correos electrónicos y descargas. Recomendamos no abrir correos electrónicos o archivos adjuntos sospechosos. Los worms y troyanos a menudo se distribuyen a través de archivos adjuntos de correo electrónico o descargas de sitios web no confiables. Verificar la autenticidad de los remitentes antes de abrir archivos adjuntos promueve la seguridad en el sistema operativo y evita que software no deseado tenga acceso a esta.

Nuestra última recomendación es utilizar software de seguridad confiable y actualizado para escanear y proteger tu sistema contra amenazas, incluyendo worms y troyanos. A lo largo de este documento pudimos demostrar la importancia de la herramienta "Kaspersky Endpoint Security Cloud" para la obtención de información relevante para los ataques así como para la respuesta ante estos que nos permita proteger nuestro sistema operativo de diversas amenazas. Por ello hacemos la fuerte recomendación de obtener software que cumpla esta función y asegurarse de mantenerlo siempre actualizado.

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.