



Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencias de Datos y Matemáticas

Kaspersky Endpoint Security Cloud

Reporte Técnico

Aplicación de criptografía y seguridad - MA2005B.201

Ángel Azahel Ramírez Cabello	A01383328
Annette Pamela Ruiz Abreu	A01423595
Luis Angel López Chávez	A01571000
Jorge Raúl Rocha	A01740816
Franco Mendoza Muraira	A01383399

Profesores:

Óscar E. Labrada Gómez

Alberto F. Martínez Herrera

Socio Formador: IPC Services

Monterrey, Nuevo León

19 de octubre de 2023

CONTENIDOS

1. INTRODUCCIÓN	3
1.1. Problema	3
1.2. Justificación	4
1.3. Objetivo	4
2. ANTECEDENTES	5
2.1. Máquina virtual	5
2.2. Sistema operativo	5
2.3. Malware	5
2.4. Virus informático	5
2.5. Troyano	6
2.6. Ransomware	6
3. DESARROLLO	7
3.1. Herramientas	7
3.1.1. Creación de la máquina virtual con Windows	7
3.1.2. Configuración para tener acceso a una red	8
3.1.3. Kaspersky	9
3.1.4. Instalación	10
3.2. Metodología	11
3.2.1. EICAR	11
3.2.2. WannaCry	12
3.2.3. IllusionBot	13
3.2.4. AsproxOld	14
3.2.5. Dyre Original	15
4. RESULTADOS	16
4.1. EICAR	18
4.1.1. Resumen ejecutivo	18
4.1.2. Objetivos	18
4.1.3. Alcance	18
4.1.4. Metodología	19
4.1.5. Hallazgos	21
4.1.6. Conclusiones	24
4.1.7. Recomendaciones	25
4.2. WannaCry	26
4.2.1. Resumen ejecutivo	26
4.2.2. Objetivos	26

4.2.3.	Alcance	26
4.2.4.	Metodología	26
4.2.5.	Hallazgos	31
4.2.6.	Conclusiones	33
4.2.7.	Recomendaciones	34
4.3.	IllusionBot	34
4.3.1.	Resumen ejecutivo	34
4.3.2.	Objetivos	35
4.3.3.	Alcance	35
4.3.4.	Metodología	35
4.3.5.	Hallazgos	36
4.3.6.	Conclusiones	39
4.3.7.	Recomendaciones	39
4.4.	AsproxOld	39
4.4.1.	Resumen ejecutivo	39
4.4.2.	Objetivos	40
4.4.3.	Alcance	40
4.4.4.	Metodología	40
4.4.5.	Hallazgos	42
4.4.6.	Conclusiones	44
4.4.7.	Recomendaciones	44
4.5.	Dyre Original	44
4.5.1.	Resumen ejecutivo	45
4.5.2.	Objetivos	45
4.5.3.	Alcance	45
4.5.4.	Metodología	45
4.5.5.	Hallazgos	47
4.5.6.	Conclusiones	54
4.5.7.	Recomendaciones	54
5.	CONCLUSIONES	56
REFERENCIAS		57

1. INTRODUCCIÓN

En un mundo cada vez más interconectado, la seguridad de la información se ha convertido en un tema crítico y desafiante. Según IDC Research, cada día se producen 350 000 ataques de malware en el mundo. (IT Digital Media Group 2021) Con la creciente sofisticación de las amenazas ciberneticas, la necesidad de herramientas eficaces para proteger sistemas y redes es innegable. Conceptos como el análisis forense digital se han vuelto esenciales para comprender y mitigar los ataques ciberneticos. Un análisis forense digital implica la recopilación, análisis y documentación de evidencia digital relacionada con actividades ilegales o incidentes de seguridad. Esto no solo ayuda a comprender la naturaleza de los ataques, sino que también permite tomar medidas adecuadas para prevenir futuros incidentes y proporcionar pruebas en caso de litigios o investigaciones legales. En este contexto, Kaspersky Endpoint Security Cloud emerge como una solución valiosa, permitiendo la documentación detallada de incidentes, la generación de informes forenses, y la implementación de medidas de protección ágiles en dispositivos analizados. Para evaluar la eficacia de esta herramienta, llevamos a cabo pruebas exhaustivas en un entorno controlado, aplicando códigos maliciosos de diversa naturaleza, como EICAR, WannaCry, IlusionBot, AsproxOld y Dyre Original. Esto permitió una evaluación completa de la capacidad de Kaspersky Endpoint Security Cloud para detectar, bloquear y documentar dichas amenazas.

El alcance de las pruebas abarcó la simulación de situaciones realistas de ataques ciberneticos y la observación del comportamiento de la herramienta en respuesta a estas amenazas. Se recopilaron datos detallados y se generaron informes forenses para cada caso de estudio. La fortaleza de las pruebas radicó en la representación precisa de escenarios de ataques potenciales y en la evaluación rigurosa de las capacidades de detección y respuesta de Kaspersky Endpoint Security Cloud. Los resultados de estas pruebas proporcionarán información crítica para comprender el desempeño de esta solución de seguridad en la detección y mitigación de amenazas ciberneticas. Este reporte técnico abordará el uso de Kaspersky Endpoint Security Cloud, su relevancia en la actualidad y su aplicación en la fase de evaluación de códigos maliciosos.

1.1. Problema

La constante evolución de las amenazas ciberneticas y la creciente complejidad de los ataques representan un riesgo significativo para la seguridad de la información y los sistemas. La falta de herramientas efectivas de monitoreo, análisis y respuesta a incidentes puede exponer a organizaciones a pérdidas de datos y vulnerabilidades. En 2021, el Informe Anual de Ciberseguridad de Kaspersky registró un promedio de 360,000 nuevos archivos maliciosos diarios. Este número es solo una fracción de la vasta cantidad de amenazas ciberneticas que circulan en el ciberespacio. La variedad de estas amenazas va desde virus y ransomware hasta troyanos y ataques de phishing, y su propósito puede ser desde el robo de datos confidenciales hasta el secuestro de sistemas informáticos. (Kaspersky 2021)

1.2. Justificación

La justificación para la evaluación de Kaspersky Endpoint Security Cloud radica en su capacidad para abordar los desafíos de seguridad en un entorno digital en constante cambio. La herramienta promete la generación de informes forenses detallados, la automatización de tareas repetitivas y la protección de dispositivos sin necesidad de inversión adicional en hardware. Evaluar su desempeño en la detección y análisis de códigos maliciosos es fundamental para comprender su utilidad y su potencial impacto en la seguridad de las organizaciones. (Kaspersky s.f.(a)) La importancia de la ciberseguridad es aún más evidente al observar el impacto económico de los ataques cibernéticos. Un informe publicado por Cybersecurity Ventures estima que, para 2021, los costos globales de ciberdelincuencia ascenderían a más de 6 billones de dólares anuales. Estos costos incluyen gastos asociados con la mitigación de amenazas, pérdida de ingresos, daño a la reputación de la empresa y costos legales. (Morgan 2016) Además, la ciberseguridad no es una preocupación exclusiva de las empresas. En un mundo cada vez más digital, los individuos también están expuestos a riesgos significativos. Un informe de la empresa de seguridad Norton reveló que en 2020, el 46 % de los adultos en los Estados Unidos experimentaron algún tipo de ciberdelincuencia. Esto incluye desde el robo de información personal hasta el acoso en línea. (Norton 2021)

1.3. Objetivo

El objetivo principal de este reporte técnico es evaluar la eficacia y las capacidades de Kaspersky Endpoint Security Cloud en la detección y análisis de códigos maliciosos. A lo largo de múltiples fases, se instalará la herramienta en máquinas virtuales, se realizará una capacitación sobre su uso y se analizará el comportamiento de códigos maliciosos en un entorno controlado. A partir de los resultados obtenidos, se buscará identificar cuál de los códigos maliciosos es el más complejo de analizar, cuál se considera el más peligroso y qué códigos maliciosos requieren más pasos para dañar el objetivo, proporcionando una base para evaluar la utilidad de Kaspersky Endpoint Security Cloud en la seguridad cibernética.

2. ANTECEDENTES

Para comprender a fondo el contenido y las implicaciones de este reporte, es esencial establecer una base de conocimiento sólida en torno a ciertos conceptos críticos en el ámbito de la ciberseguridad y el análisis forense digital. Los siguientes conceptos servirán como pilares fundamentales para comprender las evaluaciones y análisis presentados a lo largo de este informe.

2.1. Máquina virtual

Una máquina virtual no es diferente que una computadora física como una laptop o un celular, en el sentido que tiene una CPU, memoria para guardar archivos, además de que se puede conectar a internet. Mientras que las partes que hacen a una computadora física son físicas y tangibles (hardware) en las máquinas virtuales estas partes son pensadas como software, existen solo como código. Las máquinas virtuales están separadas del resto del sistema, lo que significa que el software que está dentro de las máquinas virtuales no tendría por qué intervenir con el sistema operativo primario de la computadora anfitriona. (Microsoft s.f.)

2.2. Sistema operativo

Es un programa de software que después de ser cargado a la computadora a través de un programa de arranque (boot program), gestiona todos los otros programas de aplicaciones que hay en la computadora. Los programas de aplicación utilizan el sistema operativo solicitando servicios a través de una interfaz de programa de aplicación. Además, que los usuarios pueden interactuar directamente con el sistema operativo a través de diferentes interfaces como la línea de comandos o una interfaz gráfica. (Bigelow 2023)

2.3. Malware

Es cualquier código de software o programa de computadora que esté hecho intencionalmente con el propósito de dañar a una computadora o a sus usuarios. Casi todos los ciberataques de hoy en día, involucran algún tipo de malware. Existen diferentes tipos de malware dependiendo de qué es lo que buscan los cibercriminales. Ocurren miles de millones de ataques de malware cada año y estas infecciones pueden ocurrir en cualquier sistema operativo. Una tendencia en aumento, es que los ataques de malware están dirigidos a negocios sobre los usuarios porque los hackers han aprendido que es más lucrativo ir por las organizaciones, ya que guardan información personal sobre sus clientes que puede ser utilizada para el robo de identidad o vendida en la 'dark web'. (IBM s.f.(b))

2.4. Virus informático

Es un tipo de malware que está diseñado para propagarse de un dispositivo anfitrión a otro y tiene la habilidad de replicarse, son diseñados para modificar el funcionamiento de un equipo. Los virus se insertan a un archivo o un documento que admite macros para ejecutar su código. La manera en como ataca es que una vez que se adjunta al archivo se mantiene inactivo hasta que alguna circunstancia hace que se ejecute su

código. Pueden realizar acciones devastadoras como robar contraseñas o datos, registrar las pulsaciones del teclado, dañar archivos, enviar spam a los contactos guardados y hasta tomar el control del equipo. (Norton 2018)

2.5. Troyano

Es un tipo de malware que se disfraza como un software legítimo. Los ciberdelincuentes a menudo emplean troyanos para intentar acceder a los sistemas de los usuarios. A menudo se utiliza el término virus troyano, sin embargo, esto es ligeramente engañoso, ya que a diferencia de los virus, estos no se autorreplican. Un programa troyano se propaga simulando ser un software o un contenido útil. (kaspersky 2023)

2.6. Ransomware

Es un tipo de malware que se usa para cifrar archivos de una computadora o dispositivo, impidiendo acceso de los usuarios a sus propios archivos. Típicamente, se exige un pago a los atacantes para poder acceder nuevamente a los archivos. Este tipo de malware fue creado a finales de los 80. En los últimos años, los ataques de ransomware han evolucionado para ser ataques de doble y triple extorsión; esto quiere decir que además de que encriptan tu información y solicitan un pago, te amenazan con filtrar tus datos si es que no cumples con el pago o atacar a los clientes de la víctima. (IBM s.f.(a))

3. DESARROLLO

3.1. Herramientas

La creación de un entorno virtual de pruebas es esencial para evaluar y experimentar con diferentes configuraciones de software, sistemas operativos y aplicaciones sin afectar nuestro entorno de producción. VirtualBox es una herramienta de virtualización que permite crear máquinas virtuales (VM) en las cuales podemos ejecutar sistemas operativos y aplicaciones aislados de nuestro sistema anfitrión (Red Hat 2022). En este informe técnico, exploraremos los pasos necesarios para instalar y configurar VirtualBox con el propósito de crear un entorno virtual de pruebas. La descarga del instalador de VirtualBox se debe hacer desde el sitio web oficial de Oracle: <https://www.virtualbox.org/wiki/Downloads>. Su instalación es sencilla, simplemente se entra a la página, se descarga el paquete que corresponde a la máquina operativa (en este caso fue Windows) y se siguen los pasos que se indican. Al final, obtienes el entorno que se observa en la Figura 1.

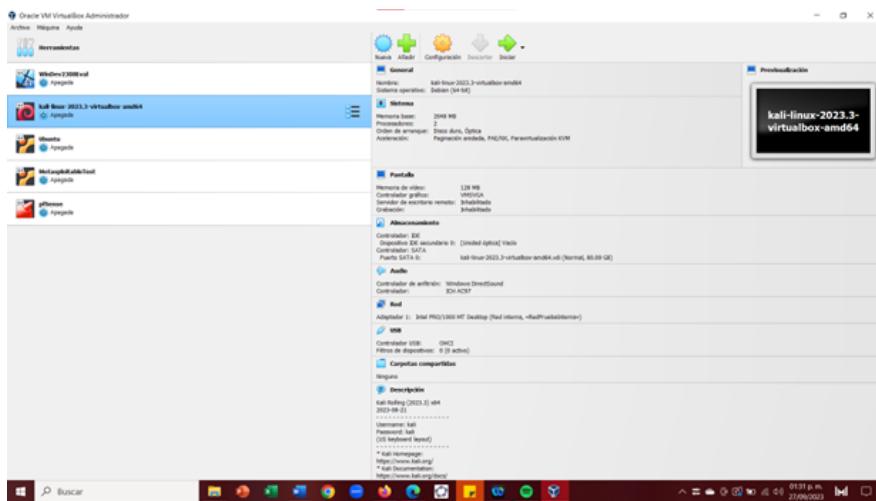


Figura 1: Demostración de instalación de VirtualBox en el equipo de cómputo

3.1.1. Creación de la máquina virtual con Windows

Una vez teniendo la máquina virtual que nos ayudará a crear nuestro entorno controlado, se tiene que popular con los ambientes adecuados para realizar pruebas de varios códigos maliciosos. Para emular de la mejor manera un entorno común se elige utilizar una máquina virtual con sistema operativo Windows 11. Para computadoras de escritorio, el sistema operativo Windows acapara la gran mayoría del mercado, representando un 68 % de los usuarios totales, seguido por macOS con un 20 % (Statcounter Global Stats 2023). Dentro de los mismos dispositivos Windows, una de las versiones más populares es la versión más reciente: Windows 11. Se eligió utilizar esta versión del sistema operativo para mejor representar el equipo de un consumidor promedio que haya comprado un equipo de cómputo en la actualidad, pues una gran cantidad de estos dispositivos vienen con esta versión preinstalada (MiniTool 2021). Para descargar Windows 11 se siguieron la serie de pasos descrita a continuación y el resultado de su instalación se puede visualizar en la

Figura 2.

1. Se descargó la máquina virtual de Windows desde el enlace proporcionado, y se descomprimió el archivo en el equipo local.
2. Luego, se importó la máquina virtual de Windows en VirtualBox. En la configuración de la máquina virtual, se asignó un mínimo de 4 GB de memoria y se creó un disco duro virtual con un tamaño predeterminado de 10 GB.
3. Se inició la máquina virtual de Windows en VirtualBox, y se llegó a la página de inicio del sistema operativo.

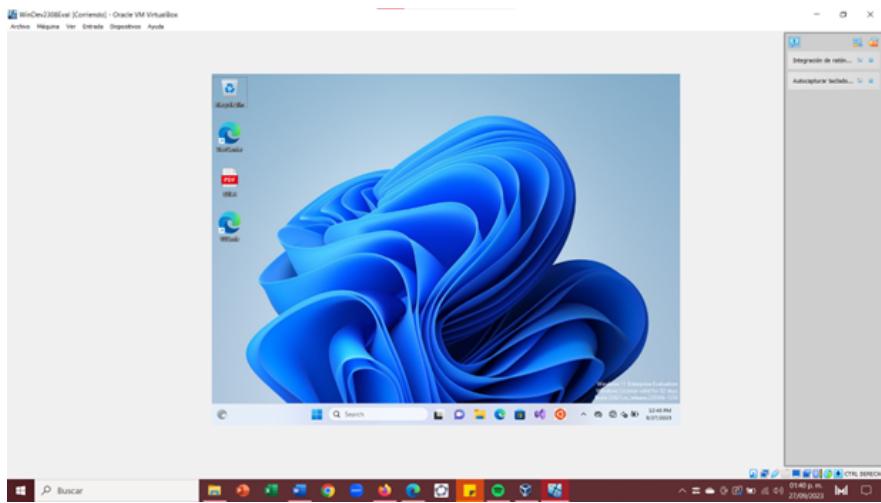


Figura 2: Demostración de instalación de Windows 11 en el equipo de cómputo

3.1.2. Configuración para tener acceso a una red

La mayoría de los usuarios tienen acceso al internet. La red es uno de los principales medios por el cual se propagan los códigos maliciosos. Es por esto que, usando la misma herramienta de VirtualBox, se integra un ambiente virtual para emular el uso de un router para la conexión a internet. Es importante mencionar que se realiza de esta manera para evitar que el daño de uno de estos programas se filtre a nuestra red real. El software utilizado para cumplir este requisito es *pfSense*, un software de uso libre con implementaciones incluyendo *firewall* y servicios de router para emular la conexión de un usuario promedio (Netgate 2023), recordando que algunos de estos sirven para controlar y manejar el tráfico de la red por razones de seguridad como es el firewall (Cisco 2023). Con las dos máquinas virtuales, una emulando el equipo de cómputo de un usuario promedio, y otro emulando la conexión al internet, se tiene un ambiente controlado donde la máquina virtual de Windows se conectará al router de *pfSense*. El resultado de la instalación se muestra en la Figura 3. Para la configuración del router se siguieron los siguientes pasos:

1. Se procedió a descargar la máquina virtual de *pfSense* desde el enlace suministrado y se descomprimió el archivo en la ubicación local.

2. A continuación, se importó la máquina virtual de *pfSense* en el software de virtualización VirtualBox. En la configuración de esta máquina virtual, se asignaron 1024 MB de memoria, y se creó un disco duro virtual con un tamaño de 6 GB.
3. Se configuró el adaptador de red de la máquina virtual de *pfSense* de manera que el Adaptador 1 operara en modo Bridge, y el Adaptador 2 en modo NAT. Esta configuración permitió a la máquina virtual de *pfSense* conectarse a la red local y tener acceso a Internet.
4. Se procedió a iniciar la máquina virtual de *pfSense* y se configuraron los parámetros iniciales, lo que incluyó la configuración de DNS con las direcciones 8.8.8.8 y 8.8.4.4. Se aceptaron las opciones por defecto y se completó la instalación.
5. Desde la máquina virtual de Windows, se accedió a la interfaz web de *pfSense* mediante el navegador web Mozilla Firefox. Se utilizó la dirección IP del router (192.168.1.1) y se ingresaron las credenciales de acceso (Usuario: admin, Contraseña: *pfSense*).
6. Se aceptaron todas las opciones predeterminadas en la configuración de *pfSense* y se procedió a aceptar la licencia de uso.
7. Finalmente, se verificó la conexión a Internet desde la máquina virtual de Windows al navegar por un sitio web.

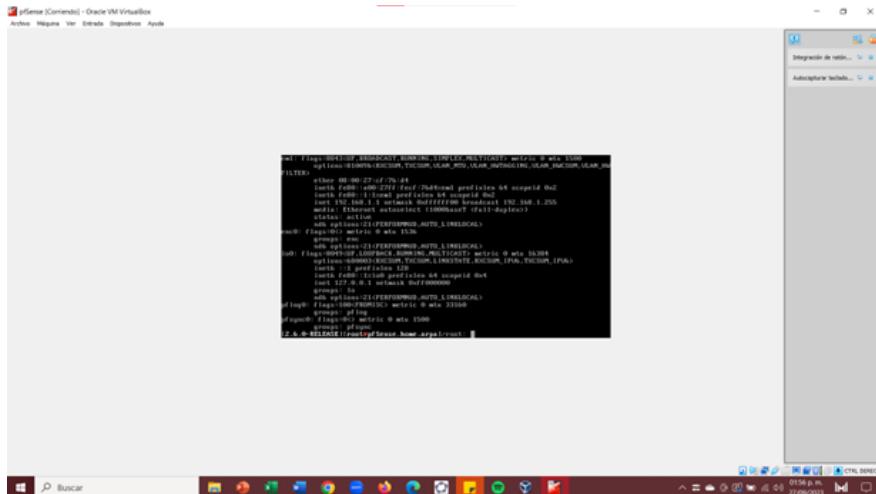


Figura 3: Uso de ifconfig para mostrar la IP del router

3.1.3. Kaspersky

Para llevar a cabo un análisis exhaustivo, hemos empleado la potente herramienta Kaspersky Endpoint Security Cloud, la cual se revela como un recurso esencial en la protección de dispositivos frente a códigos maliciosos y comportamientos anómalos. Kaspersky Endpoint Security Cloud, dirigida principalmente a empresas con recursos limitados, se distingue por un conjunto de características que la posicionan como una solución integral de ciberseguridad (Kaspersky 2023a). Una de sus notables características radica en la

implementación de la inteligencia artificial, específicamente el empleo de modelos de aprendizaje supervisado (*machine learning*) en el proceso de detección de anomalías. Este enfoque revolucionario se basa en la recopilación y análisis de datos de actividad en dispositivos supervisados por la herramienta Kaspersky en ventanas de tiempo previas. La inteligencia artificial utiliza estos datos para entrenar modelos que, posteriormente, intentarán predecir valores de parámetros en una ventana de tiempo futura. La esencia de este método consiste en comparar la media de la diferencia al cuadrado entre los valores observados y los predichos, estableciendo un umbral para identificar cualquier discrepancia significativa, lo que se cataloga como una anomalía (*Kaspersky Machine Learning for Anomaly Detection s.f.*).

Kaspersky Endpoint Security Cloud también cuenta con un sólido núcleo de funcionamiento respaldado por una extensa base de datos de firmas de código malicioso, lo que permite una identificación y eliminación efectiva de amenazas conocidas y previamente documentadas. Este enfoque se complementa con un análisis heurístico avanzado, capaz de detectar comportamientos inusuales y patrones desconocidos en tiempo real. La combinación de estas técnicas tradicionales y modernas confiere a la herramienta la versatilidad necesaria para combatir tanto amenazas ya identificadas como nuevas y emergentes, ofreciendo una sólida defensa contra códigos maliciosos y actividades sospechosas. (usa.kaspersky.com 2023)

3.1.4. Instalación

La evidencia de la instalación se puede observar en la Figura 4. Para descargar la herramienta, se siguió esta serie de pasos:

1. Se registró una cuenta en el sitio web oficial de Kaspersky Endpoint Security Cloud y se inició sesión en la cuenta de Kaspersky.
2. Se configuraron los detalles de la organización, como el nombre y la ubicación.
3. Se descargó el instalador desde la consola de administración.
4. El instalador del agente de seguridad se descargó en la máquina virtual que se deseaba proteger, y se ejecutó en ella.
5. El agente de seguridad se instaló en la máquina virtual y se configuró automáticamente, asegurándose de que la máquina estuviera conectada a Internet durante este proceso.
6. Desde la consola de administración en línea, se configuraron las políticas de seguridad que se deseaban aplicar a los dispositivos, como las políticas de escaneo, cortafuegos y otras configuraciones de seguridad.
7. Se repitieron los pasos 4 y 5 para todos los dispositivos que se deseaban proteger en la organización.
8. Se utilizó la consola de administración para supervisar la seguridad de los dispositivos y realizar un seguimiento de las amenazas detectadas. También se realizaron actualizaciones periódicas del agente de seguridad y las políticas para mantener la protección actualizada.

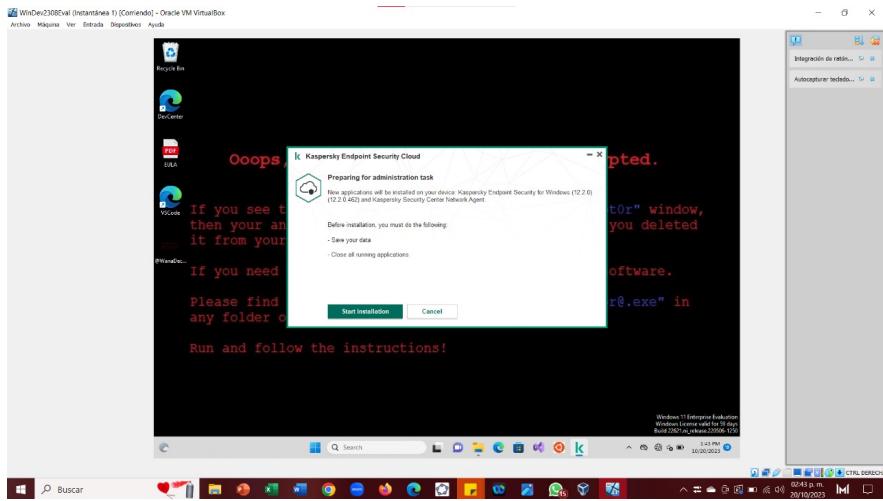


Figura 4: Demostración de instalación de la herramienta Kaspersky en la máquina virtual de Windows

3.2. Metodología

Una vez teniendo la configuración descrita anteriormente, se probará cada uno de los códigos o programas maliciosos para analizar y documentar sus comportamientos para ponderar el posible daño que pudieran infiligr a un usuario promedio o a cualquier institución que no tome las medidas de ciberseguridad necesaria.

3.2.1. EICAR

El término EICAR se refiere a un malware de prueba, creado específicamente para evaluar la capacidad de detección y respuesta de las soluciones antivirus y antimalware. Fue desarrollado por el Instituto Europeo para la Investigación de los Antivirus Informáticos o por sus siglas (EICAR). Este virus de prueba no es malicioso y no contiene código ejecutable para el dispositivo, pero la mayoría de las aplicaciones antivirus lo detectan como una posible amenaza. El archivo que tiene este virus de prueba se puede descargar desde el sitio web de EICAR: <https://www.eicar.org/download-anti-malware-testfile/>. (kaspersky s.f.) El malware EICAR no debe ser considerado como una amenaza real; en cambio, es un archivo de prueba diseñado para simular una infección de malware. Carece de código ejecutable y, por lo tanto, no representa un riesgo para los dispositivos en los que se encuentra. Este malware de prueba es esencialmente una cadena de caracteres que se almacena en un archivo con extensión '.com.'; por lo general se suele ver de la siguiente manera:

X5O!P%@AP[454(P)7CC)7}\$.EICAR – STANDARD – ANTIVIRUS – TEST – FILE!\$H + H*

Algunas de las razones por las cuales se utiliza este tipo de malware de prueba son las siguientes:

- Probar la detección de malware: El archivo EICAR es un archivo de prueba que se utiliza a menudo para verificar que los sistemas de antivirus y antimalware estén funcionando correctamente.
- Ayudar a los investigadores de seguridad a desarrollar nuevos métodos de detección de malware: El archivo EICAR se puede utilizar para probar nuevos métodos de detección de malware. Si un nuevo método de detección lo puede detectar, significa que tiene el potencial de detectar malware real.

- Educar a los usuarios sobre el malware: El archivo EICAR puede ser utilizado para enseñar a los usuarios sobre el malware y cómo protegerse de él.

3.2.2. WannaCry

WannaCry, un ransomware que apareció por primera vez en 2017, se caracteriza por su capacidad para cifrar los archivos del usuario en un sistema infectado, haciendo que estos sean inaccesibles para el usuario legítimo. La particularidad de este ransomware es que exige un pago en Bitcoin a cambio de la clave de descifrado necesaria para recuperar los archivos. Es importante destacar que WannaCry se propaga de manera eficiente al buscar sistemas vulnerables en una red local y, mediante un mecanismo de propagación automática, infecta múltiples máquinas con rapidez. Los ataques perpetrados por WannaCry resultaron especialmente dañinos debido a una vulnerabilidad en sistemas Windows que, aunque había sido corregida por el fabricante, afectó a más de 200,000 máquinas debido a la falta de actualizaciones (Kaspersky 2023b). *EternalBlue*. La singularidad de esta vulnerabilidad reside en su origen, ya que fue desarrollada por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) como una herramienta de explotación de seguridad. Sin embargo, *EternalBlue* se filtró en línea, cayendo en manos de actores maliciosos que aprovecharon su potencial para orquestar ataques masivos. Aprovechando esta vulnerabilidad, WannaCry no solo cifra los archivos de la víctima, sino que también busca de manera activa sistemas vulnerables en la red local, propagándose de forma automática, lo que contribuyó a la rápida propagación del malware (Labs 2019). El orden de las tareas que realiza es el siguiente:

1. Cifrado de archivos: El ransomware utiliza cifrado de alto nivel para bloquear el acceso a los archivos de la víctima, lo que resulta en la pérdida de datos críticos.
2. Rescate en Bitcoin: Una vez que los archivos se encuentran encriptados, WannaCry presenta una nota de rescate que exige un pago en Bitcoin a cambio de la clave de descifrado. Este acto extorsivo es una característica distintiva de este malware.
3. Propagación automática: WannaCry busca y explota activamente sistemas vulnerables en la red local, utilizando la vulnerabilidad *EternalBlue* para propagarse de forma automática. Esto le permite infectar máquinas en la misma red con gran velocidad, lo que lo convierte en un ransomware altamente efectivo en términos de propagación.

Si las herramientas antivirus están desactualizadas o configuradas de manera incorrecta, la infección por WannaCry conlleva una serie de consecuencias y problemas potenciales como:

- Pérdida de datos críticos: Dado que WannaCry cifra los archivos del usuario, las víctimas pueden enfrentar la pérdida de datos valiosos. La recuperación de estos archivos a menudo depende de pagar un rescate, lo que no garantiza que se recuperarán todos los datos intactos.
- Repercusiones financieras: El ransomware impone un rescate en Bitcoin, lo que puede resultar en costos significativos para las organizaciones y los individuos. Además de los rescates que se exigen a cambio

de la clave de descifrado, las organizaciones pueden enfrentar costos adicionales, como la inversión en servicios forenses para investigar la intrusión, así como la inversión en medidas de ciberseguridad mejoradas para prevenir futuros ataques.

- Problemas con herramientas antivirus desactualizadas o configuradas incorrectamente: Cuando las herramientas antivirus no están actualizadas o configuradas de manera incorrecta, se presentan problemas como la falta de detección de ransomware, el fracaso en la eliminación efectiva y la propagación continua de la infección.
- Impacto en la productividad: Cuando una organización o un individuo se ven afectados por WannaCry, la pérdida de acceso a archivos críticos y la necesidad de lidiar con la recuperación de datos pueden resultar en una disminución significativa de la productividad. Las operaciones comerciales pueden detenerse o ralentizarse considerablemente.
- Reputación dañada: La infección por WannaCry puede tener un impacto negativo en la reputación de una organización. Las brechas de seguridad y las interrupciones en el servicio pueden erosionar la confianza de los clientes y socios comerciales.
- Riesgo de sanciones legales: Dependiendo de la jurisdicción y las circunstancias específicas, las organizaciones que sufren una infección por ransomware pueden enfrentar riesgos legales y sanciones. La gestión inadecuada de la seguridad de la información puede dar lugar a consecuencias legales y regulatorias.

(Ghafur et al. 2019)

La implementación de un software antivirus rigurosamente actualizado y debidamente configurado se convierte en una medida esencial en la lucha contra la infección por ransomware, con ejemplos emblemáticos como WannaCry. Esta estrategia no solo actúa como un escudo preventivo, sino que también desempeña un papel crítico en la reducción del impacto potencial en caso de un intento de infección, al detectar y bloquear proactivamente amenazas, además de posibilitar respuestas rápidas y efectivas para la mitigación de riesgos. La actualización constante de firmas y patrones de malware, junto con una configuración precisa que se ajuste a las necesidades específicas de la organización, fortalece la postura de seguridad cibernética y reduce la exposición a amenazas de cifrado de datos y posibles consecuencias adversas.

3.2.3. IllusionBot

Es un malware que se presenta como un bot de comercio binario legítimo, pero en realidad es un programa malicioso que puede robar información personal o causar daños a la computadora y está diseñado para operar de manera sigilosa y perjudicial en sistemas informáticos. Desde el punto de vista técnico, IllusionBot se origina en la programación y el desarrollo de cibercrimen con conocimientos avanzados en seguridad informática. Este malware generalmente se propaga a través de vectores de ataque como correos electrónicos de phishing, descargas de archivos adjuntos infectados, o explotación de vulnerabilidades en sistemas operativos. Además, puede utilizar técnicas de evasión para evitar la detección por parte de soluciones de seguridad. La fecha de compilación de este malware es del 22/04/2006 (aunque la fecha puede ser falsa). (Ka1d 2021)

Algunas de las tareas que puede realizar este malware son:

- Recopilación de datos sensibles: IllusionBot tiene la capacidad de robar información confidencial, como contraseñas, datos bancarios, documentos personales, y más, de los dispositivos infectados.
- Creación de puertas traseras: Establece una puerta trasera en el sistema comprometido, permitiendo a los atacantes el acceso remoto para llevar a cabo acciones maliciosas adicionales.
- Distribución de malware adicional: IllusionBot puede servir como punto de entrada para otros tipos de malware, lo que complica aún más la situación de seguridad.

Entre algunas de las consecuencias que puede traer este malware a un equipo se encuentran:

- Robo de datos personales: El malware puede robar información personal como contraseñas, números de tarjetas de crédito y direcciones de correo electrónico.
- Amenaza a la continuidad del negocio: En el caso de organizaciones, una infección por IllusionBot puede interrumpir las operaciones normales, causando pérdidas financieras y dañando la reputación.
- Daños a la computadora: El malware puede causar pérdida de datos o ralentización de rendimiento. Además de que también puede instalar otros programas maliciosos.
- Infección de otras computadoras: El malware puede propagarse a otras computadoras a través de redes compartidas o archivos adjuntos de correo electrónico.

(Ka1d 2021)

3.2.4. AsproxOld

El malware AsproxOld, también conocido como Asprox o W32/Asprox, es un ejemplo notorio de software malicioso que ha estado activo durante varios años y se ha utilizado para llevar a cabo ataques ciberneticos devastadores. AsproxOld es un tipo de malware diseñado para infectar sistemas informáticos con el objetivo de realizar una variedad de actividades maliciosas, como el robo de información sensible y la propagación de otros tipos de malware. Se clasifica como un troyano, lo que significa que se oculta en programas o archivos legítimos para infiltrarse en sistemas sin el conocimiento del usuario. El malware Asprox fue descubierto aproximadamente en el 2008 y llega a máquinas a través de phishing e inyecciones SQL para infectar páginas web. Este malware obtiene cualquier tipo de información personal o financiera que esté disponible en línea, a través de búsquedas random en Google. También tiene un segundo método de función, llamado Kuluz, el cual descarga e instala más malware a la máquina. (Infosec Institute s.f.)

La infección por AsproxOld puede tener graves consecuencias y problemas, que incluyen:

- Robo de datos sensibles: El malware puede llevar a la exposición y el robo de datos personales y financieros, lo que plantea riesgos de robo de identidad y fraude.
- Propagación de malware adicional: Como puerta trasera, AsproxOld puede facilitar la entrada de otros tipos de malware, lo que complica aún más la seguridad del sistema.

- Vulneración de la privacidad: La capacidad de AsproxOld para espiar la actividad en línea y las comunicaciones pone en peligro la privacidad de los usuarios.
- Daño a la integridad del sistema: El malware puede causar daños a la funcionalidad y estabilidad del sistema infectado, lo que puede llevar a bloqueos y mal funcionamiento.

(NHS Digital 2018)

3.2.5. Dyre Original

Dyre Original, también conocido como Dyreza, es un malware notorio y peligroso que ha sido utilizado en ataques cibernéticos dirigidos a robar información financiera y datos sensibles que apareció por primera vez en junio del 2014. Dyre Original es un tipo de troyano bancario, una categoría de malware diseñada específicamente para robar información financiera, como credenciales bancarias, tarjetas de crédito y detalles de cuentas en línea. Se presenta en varias versiones y ha sido parte de campañas de ciberdelincuencia dirigidas a bancos y otras instituciones financieras. A diferencia de los troyanos bancarios comunes, no utiliza inyecciones web para modificar el contenido del navegador, lo que hace es que redirige el tráfico de interés a sus propios servidores. Este troyano se distribuyó más durante el 2014 y el 2016, y se propagaba a través de otro malware llamado Upatre, el cual a su vez se propagaba a través de mensajes de phishing y sitios web comprometidos (Kaspersky s.f.(b)). Algunas de las actividades que puede realizar este malware son:

- Keylogging (registro de pulsaciones de teclas): Dyre Original registra las pulsaciones de teclas del usuario, lo que le permite capturar contraseñas, nombres de usuario y otra información confidencial.
- Inyección de formularios falsos: El malware puede modificar las páginas web legítimas de bancos y otros servicios financieros para incluir formularios falsos que capturan los datos ingresados por el usuario.
- Suplantación de sitios web: Dyre Original puede redirigir a los usuarios a sitios web falsos que imitan a los sitios legítimos de instituciones financieras para robar información.

Algunas de las consecuencias que puede tener en caso de que no se cuente con un buen antivirus son las siguientes:

- Robo de datos bancarios: Puede robar las credenciales de acceso bancario de los usuarios, los números de las tarjetas de crédito y los números de identificación.
- Transferencias bancarias fraudulentas: Con el uso de las credenciales robadas puede hacer transferencias bancarias a cuentas controladas por ciberdelincuentes.
- Instalación de otro malware: Puede instalar otro malware en el sistema afectado, como troyanos de acceso remoto o ransomware.
- Daño a la reputación: Las víctimas pueden sufrir daños a su reputación, especialmente las empresas si se utiliza la información personal de sus clientes para cometer fraudes o actividades delictivas.

(Stone-Gross y Khandhar 2014)

4. RESULTADOS

Con el propósito de presentar de manera efectiva los resultados obtenidos tras la ejecución de los códigos maliciosos, abordaremos cada caso como un escenario de ciberseguridad y seguiremos un proceso metodológico basado en el análisis forense digital. Este proceso nos permitirá analizar detalladamente cada incidente, identificar posibles amenazas y examinar la secuencia de eventos que rodea a cada código malicioso. El enfoque en un análisis forense digital garantiza la recopilación rigurosa de evidencia digital y una comprensión profunda de las actividades maliciosas, lo que a su vez respalda la toma de decisiones informadas para la mitigación de amenazas y la implementación de salvaguardias futuras. Haremos dos modificaciones a la estructura común de un análisis forense: omitiremos la sección de 'antecedentes' dado que, como pusimos a prueba los códigos, no hay historial de ataques en alguna empresa; en la parte de 'metodología' de cada caso, reportaremos los pasos técnicos que se llevaron a cabo para ejecutar los códigos maliciosos y utilizar la herramienta de Kaspersky.

Es importante mencionar que antes de la ejecución de cada uno de los códigos maliciosos se debe desactivar previamente el funcionamiento del agente de Kaspersky Endpoint dentro de la máquina virtual, con el objetivo de permitir la generación de una cadena de acciones para posterior análisis, como se puede ver en la Figura 5.

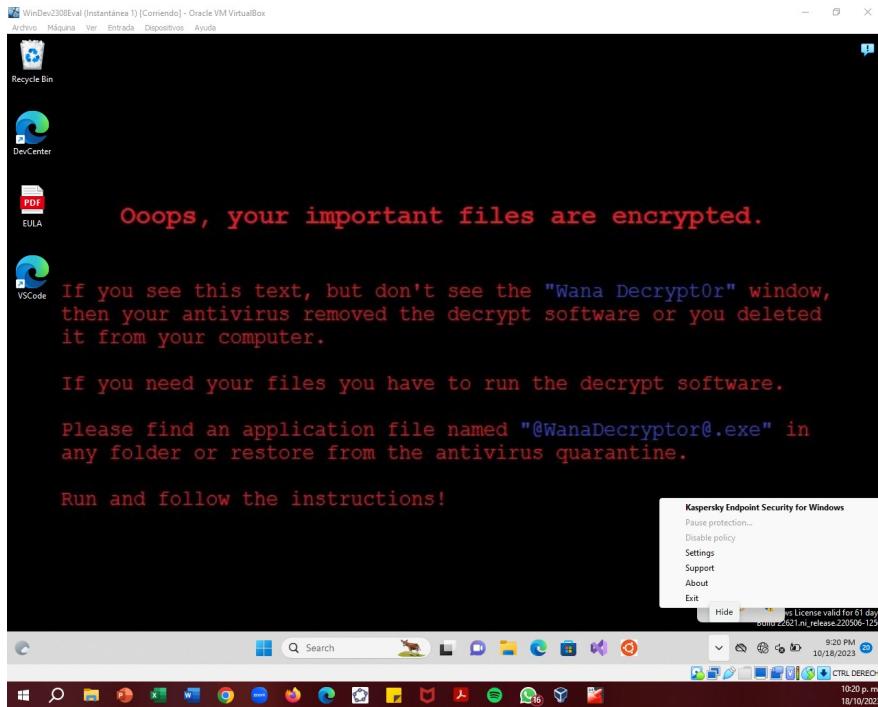


Figura 5: Anulación de servicios del agente de Kaspersky en la VM de Windows

Posteriormente, se desactivaron las opciones de seguridad inherentes en el sistema operativo de Windows 11 (Windows Defender), las opciones anuladas se pueden visualizar en las Figuras 6 y 7. De igual manera, cabe mencionar que cada vez que se ejecutaba un código malicioso nuevo se necesitaba agregar como exclusión (como se observa en la Figura 8); ya que, el software de Windows Defender no permitía su plena ejecución.

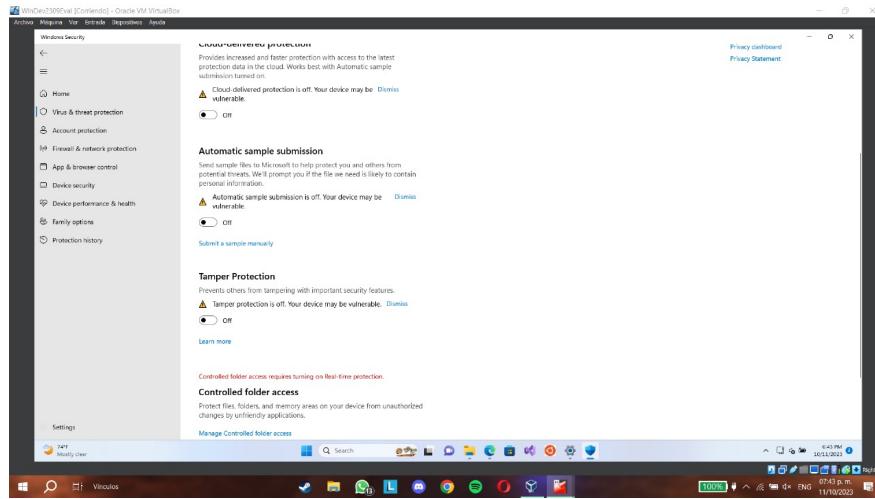


Figura 6: Primera parte de opciones desactivadas en el antivirus Windows Defender

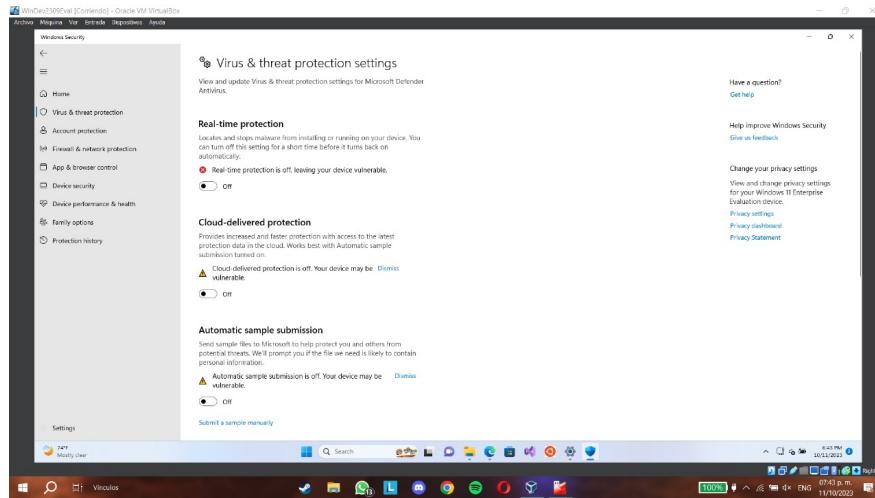


Figura 7: Segunda parte de opciones desactivadas en el antivirus Windows Defender

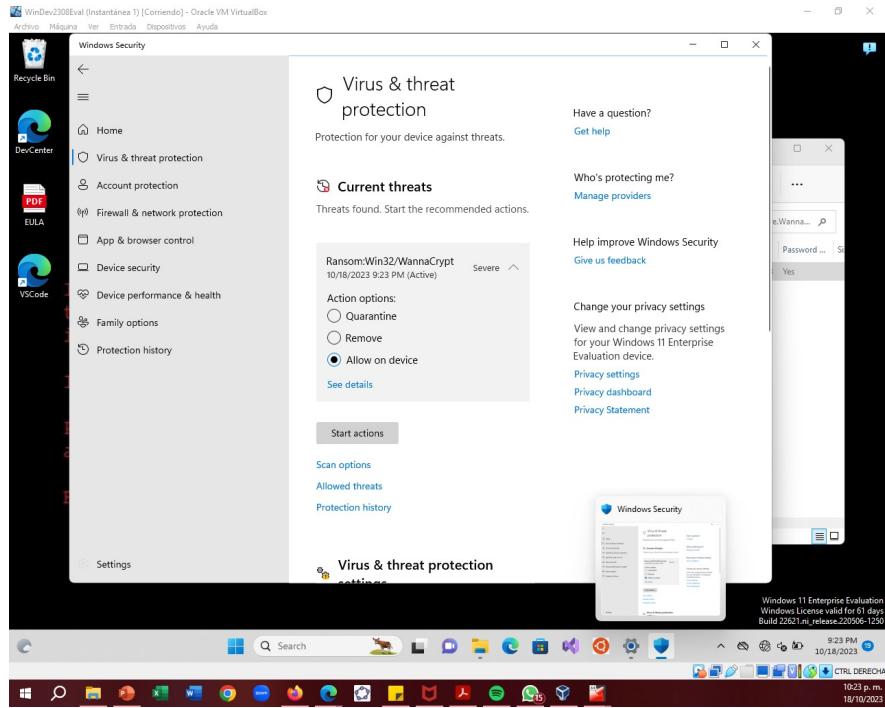


Figura 8: Opción de exclusión nueva para permitir la ejecución de código malicioso

4.1. EICAR

Caso: 1

Fecha del incidente: 14 octubre de 2023

Hora: 17:22

Nombre del incidente: Implementación de EICAR

4.1.1. Resumen ejecutivo

Se llevó a cabo una investigación forense digital relacionada con la implementación de EICAR (Instituto Europeo de Investigación en Ciencias de la Computación Aplicada), una organización que establece estándares para la evaluación de software antivirus. El objetivo principal de esta evaluación fue determinar si Kaspersky puede detectar y neutralizar amenazas basadas en el archivo EICAR de manera eficiente.

4.1.2. Objetivos

Determinar si la solución de Kaspersky es capaz de detectar y neutralizar el archivo EICAR de manera eficaz. Además, se buscó evaluar la capacidad de Kaspersky para detectar y responder a amenazas similares en tiempo real.

4.1.3. Alcance

Este informe se centra en la evaluación de la capacidad de Kaspersky para detectar y neutralizar el archivo EICAR. No abarca una evaluación exhaustiva de todas las funcionalidades de Kaspersky ni de la seguridad

en general del entorno. Además, se limita a las funcionalidades y habilidades de la máquina virtual instalada, pero se demuestra el funcionamiento del agente dentro de la máquina virtual de Windows 11.

4.1.4. Metodología

Para comenzar con la prueba EICAR, primero se accedió a la dirección URL <https://www.eicar.org/download-anti-malware-testfile/>, cuyo destino está marcado como peligroso por el navegador Edge, como se puede ver en la Figura 9. Una vez dentro de la página, se navegó para encontrar la tabla que contiene las cuatro pruebas de malware de EICAR, como se observa en la Figura 10.

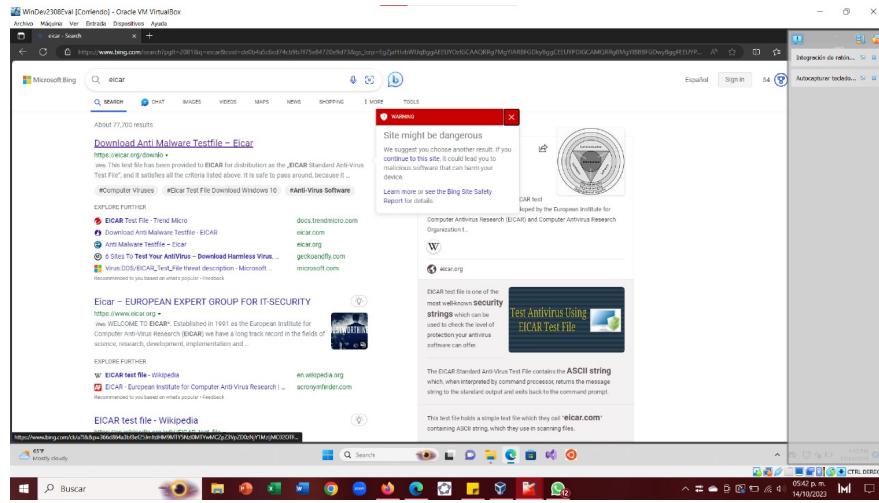


Figura 9: Investigación en motor de búsqueda Bing por la prueba EICAR

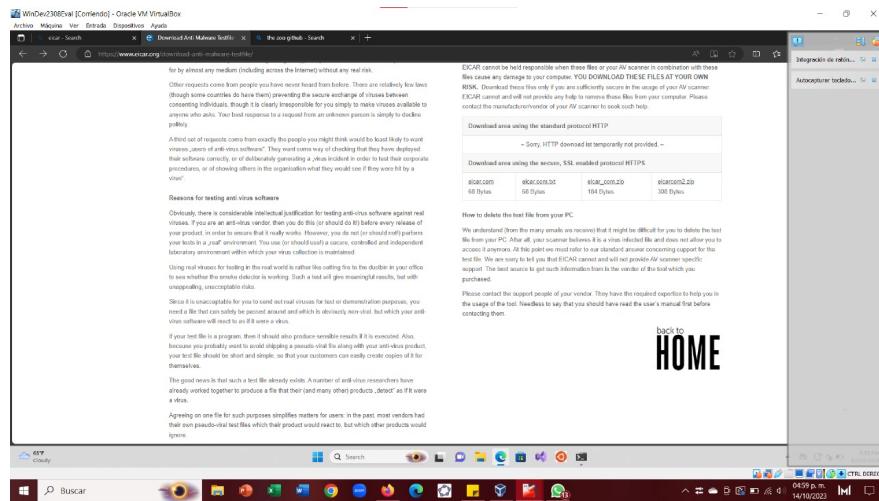


Figura 10: Sección de descargas del código malicioso de prueba de EICAR

Cada una de las cuatro pruebas consiste en distintas formas de comprobar el funcionamiento de un agente de antivirus, pero consisten en realidad en solamente dos archivos de malware distintos. El primero se comparte vía web con una dirección URL donde se muestra el mensaje de la Figura 11 (esto aplica al hacer clic

en los hipervínculos eicar.com y eicar.com.txt); por otro lado, el segundo se trata de una carpeta comprimida donde está un ejecutable que al activarse simplemente realiza un proceso que debería ser detectado por el antivirus como sospechoso (lo cual aplica para los hipervínculos **eicar_com.zip** y **eicarcom2.zip**). La visualización de los archivos descargados se puede ver en las Figuras 12 y 13.

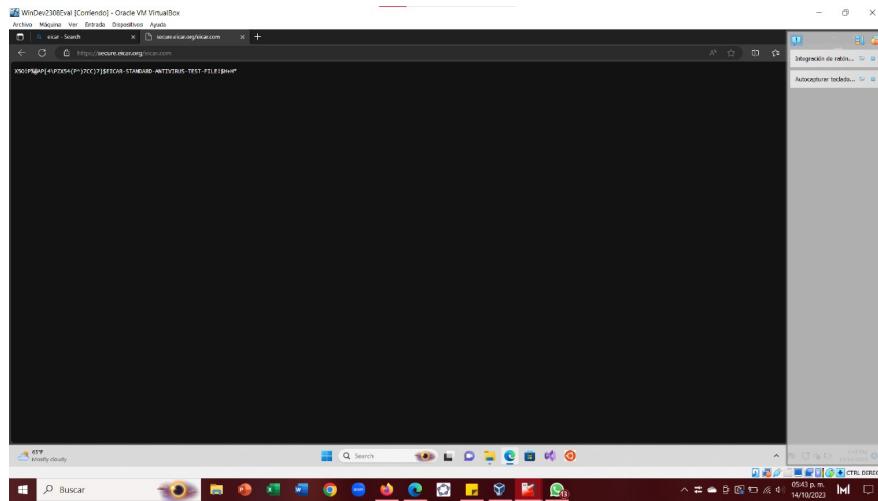


Figura 11: Captura del mensaje mostrado por el código malicioso vía URL web de la prueba EICAR

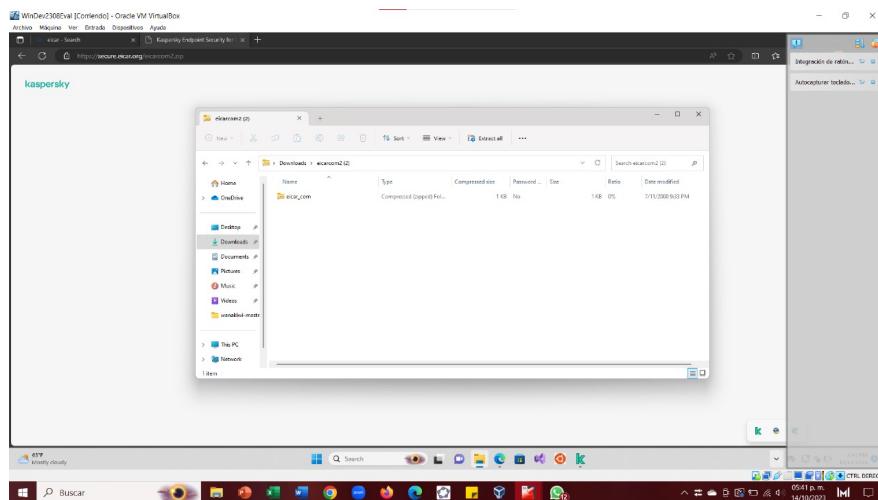


Figura 12: Evidencia de descarga del código malicioso en forma de carpeta comprimida de la prueba EICAR

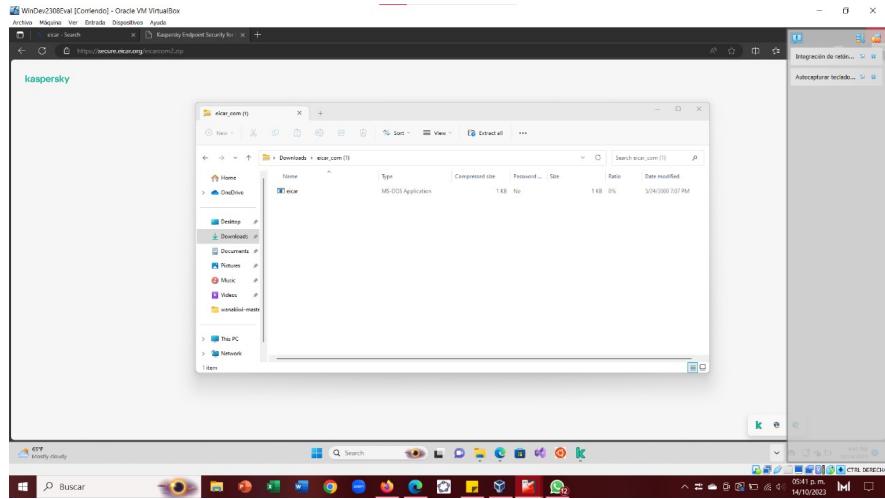


Figura 13: Contenido de la carpeta comprimida de la prueba EICAR

4.1.5. Hallazgos

Después de haber probado cada uno de los cuatro ejemplos de malware, se generaron distintos reportes por parte de Kaspersky Endpoint Security Cloud EDR; sin embargo, nunca se llegó a generar una cadena de desarrollo completa en ninguno de los casos, pero al menos se comprobó el funcionamiento del software con esta herramienta básica. En primer lugar, en las Figuras 14 y 15 se puede observar cómo se bloqueó un archivo durante su descarga en la VM y el malware llegó hasta ahí por la activación del agente antimalware.

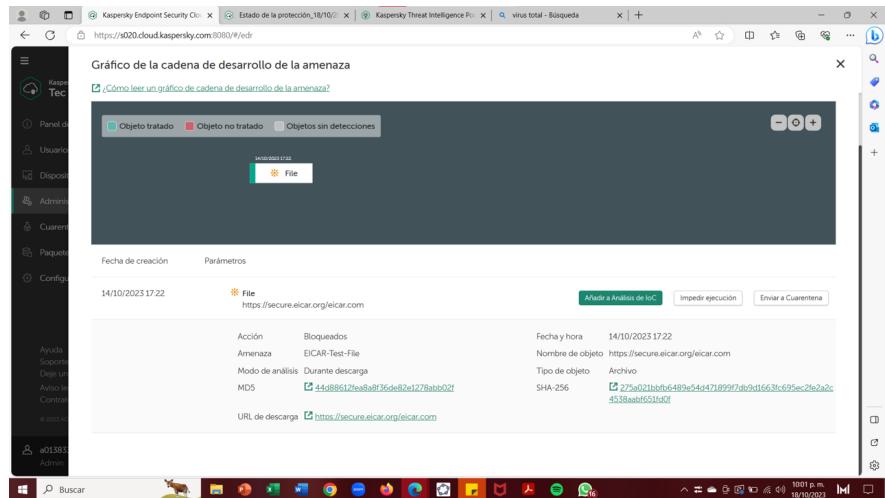


Figura 14: Captura del reporte de la consola de Kaspersky del código malicioso .com de la prueba EICAR

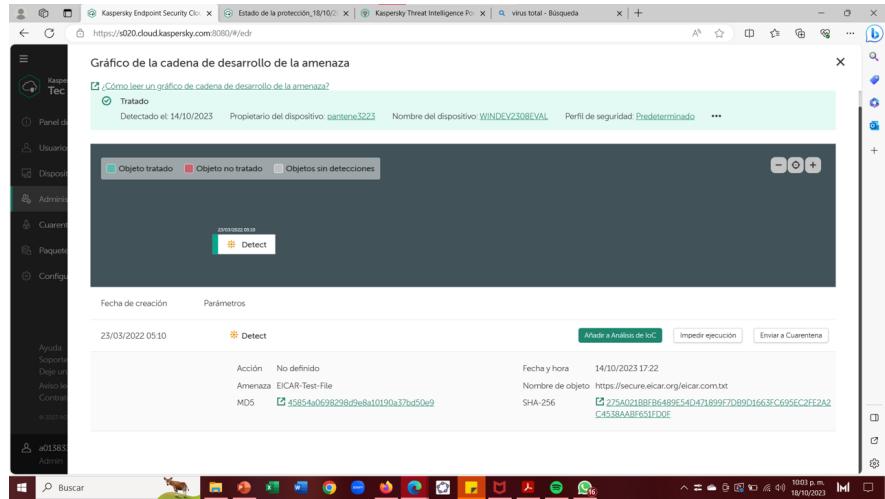


Figura 15: Captura del reporte de la consola de Kaspersky del código malicioso .com.txt de la prueba EICAR

Por otra parte, en las Figuras 16 y 17 se puede observar cómo los archivos ZIP tampoco prosperaron lo suficiente como para que el agente generara una cadena de desarrollo de la amenaza. No obstante, estos dos análisis nos dejan bastante claro que el agente no es capaz de identificar qué tipo de archivo es el malware al tratarse de una compresión (zip).

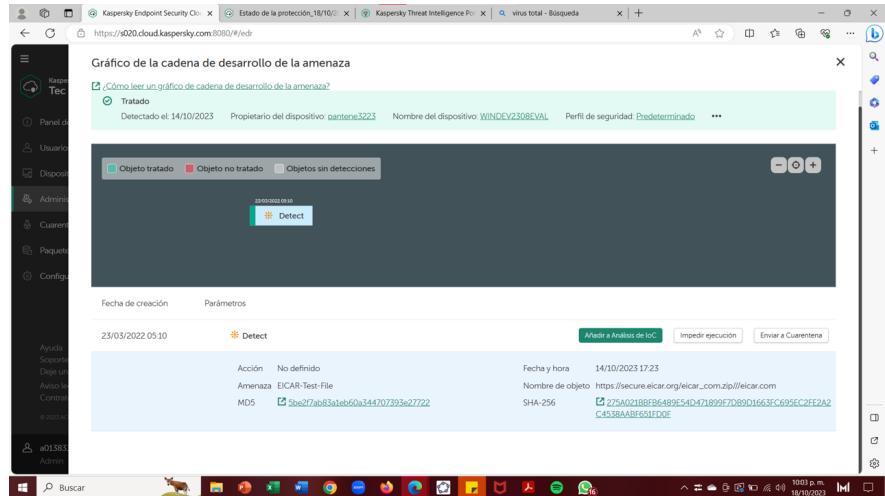


Figura 16: Captura del reporte de la consola de Kaspersky del código malicioso ZIP de la prueba EICAR

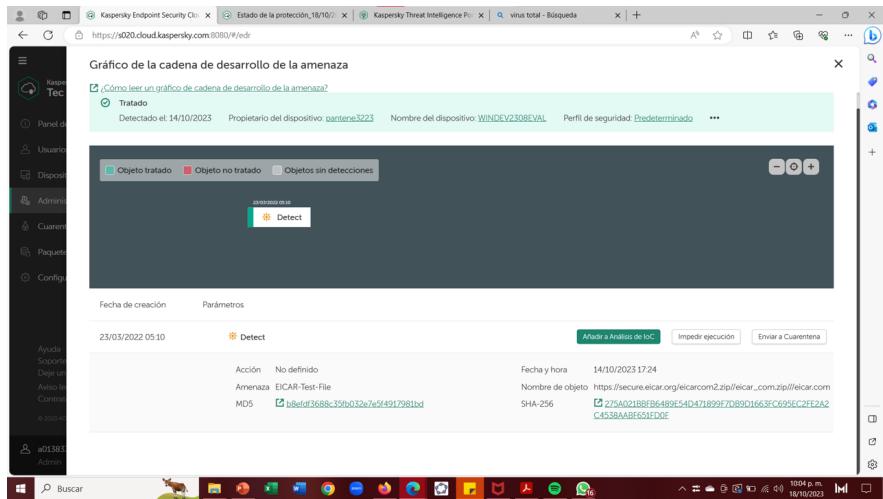


Figura 17: Captura del reporte de la consola de Kaspersky del código malicioso ZIP de la prueba EICAR

Para resumir los indicadores de compromiso de un malware se utiliza una tabla como la que se muestra en el Cuadro 1, donde aparecen las principales características señaladas por el agente antimalware, en este caso se dió más importancia a la versión .com del malware de EICAR dado que solamente será usado como ejemplo, ya que, no hay un peligro real en ninguna de las cuatro versiones de la prueba.

Nombre de objeto	Amenaza	Tipo	Acción	Hora de detección
https://secure.eicar.org/eicar.com	EICAR-Test-File	Archivo	Eliminado	14/10/2023 17:22
Indicadores				
MD5	SHA-256			
44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c453aabf651fd0f9			

Cuadro 1: Indicadores de compromiso del malware Eicar en su versión .com

Posteriormente, con el objetivo de tener mayor información de este malware, se decidió analizar su función hash SHA-256 en la base de datos de Kaspersky, donde aparece un gran número de hits (Figura 18). Esto indica que es un archivo que ha sido reportado frecuentemente como malicioso. De igual manera, se comprobó si los principales proveedores de ciberseguridad conocen sobre este malware usando la página <https://www.virustotal.com/gui/home/upload>, donde se encontró que 63 de los 75 lo detecta como peligroso, con lo que se reafirma lo común que es este malware alrededor de las distintas bases de datos que hay en la web (Figura 19).

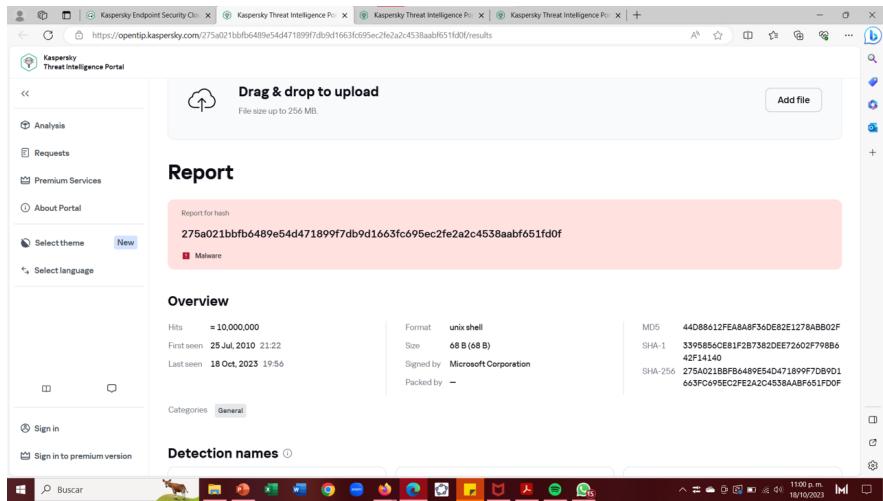


Figura 18: Búsqueda de información sobre el hash del código malicioso de la prueba EICAR en la base de datos de Kaspersky

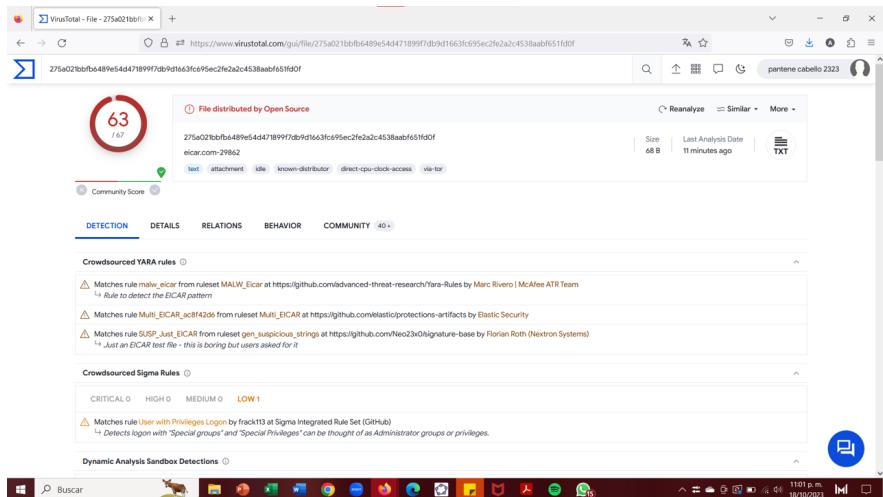


Figura 19: Búsqueda de información sobre el hash del código malicioso de la prueba EICAR en la base de datos de virustotal.com

4.1.6. Conclusiones

La prueba EICAR es una valiosa herramienta para evaluar la efectividad de los programas antivirus al simular un ataque de malware. Al emplearla regularmente, los usuarios pueden identificar brechas de seguridad y fortalecer sus defensas cibernéticas. La importancia de la prueba EICAR radica en su capacidad para ayudar a los usuarios y a las empresas a identificar posibles brechas de seguridad y a fortalecer sus defensas cibernéticas. Al emplear esta prueba de forma regular, se puede garantizar que los sistemas de seguridad estén funcionando correctamente y que estén preparados para hacer frente a posibles ataques de malware comunes, pero no todos los existentes.

4.1.7. Recomendaciones

Es esencial tener en cuenta que la prueba EICAR no puede ser considerada como una evaluación exhaustiva de la capacidad de un sistema para protegerse contra todas las amenazas ciberneticas. A pesar de su utilidad, las organizaciones y los usuarios deben complementar el uso de la prueba EICAR con otras medidas de seguridad robustas, como actualizaciones regulares de software, políticas de acceso seguras y capacitación continua del personal. Solo mediante la implementación de un enfoque integral y multidimensional de la ciberseguridad se puede garantizar una protección sólida y efectiva contra las amenazas digitales en constante evolución.

Nota: Los siguientes códigos maliciosos provienen del repositorio de GitHub llamado 'theZoo' cuyo enlace se encuentra en el siguiente sitio web: <https://github.com/ytisf/theZoo>. En su página principal, vista en la Figura 20, se incluye un archivo README.md donde se incluyen las instrucciones para clonarlo en el equipo (en este caso se realizó sobre la VM). Cabe resaltar que este sitio es altamente peligroso, a tal grado de haber sido bloqueado por el agente de Kaspersky antes de apagarlo, así como se observa en la Figura 21.

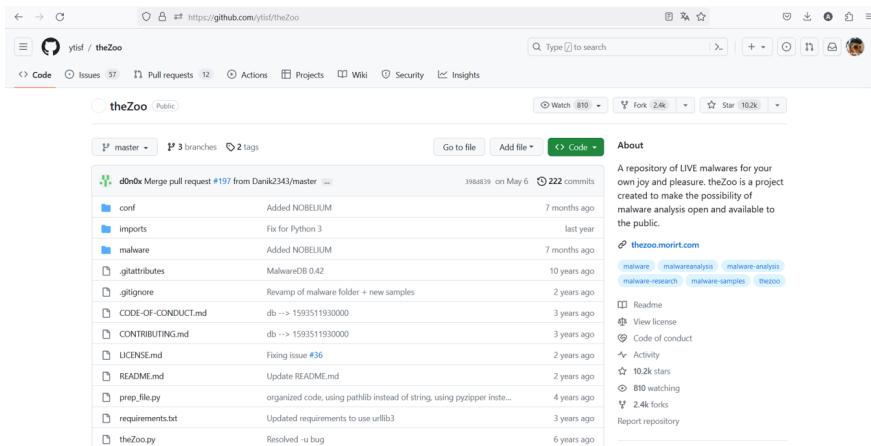


Figura 20: Página principal del repositorio theZoo en GitHub

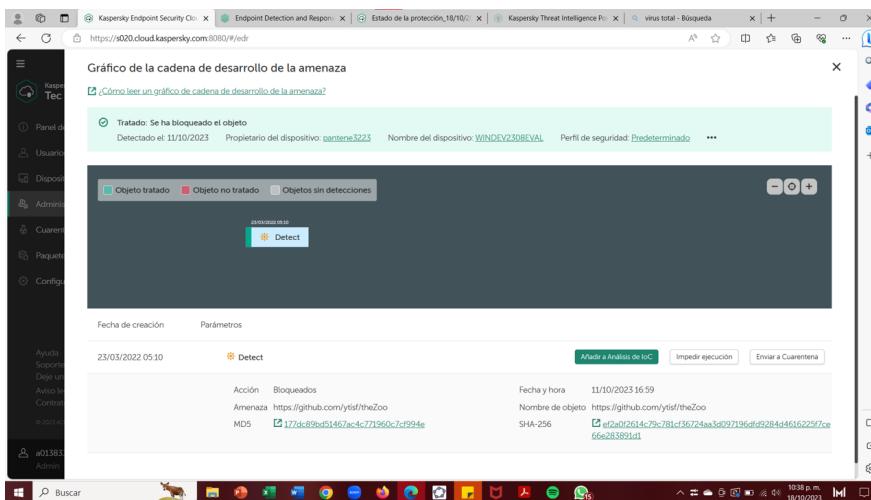


Figura 21: Demostración de que el antivirus de Kaspersky detecta al repositorio como un sitio peligroso

4.2. WannaCry

Caso: 2

Fecha del incidente: 11 de octubre de 2023

Hora: 14:28

Nombre del incidente: taskdl.exe

4.2.1. Resumen ejecutivo

En el marco de una investigación forense digital, se ha llevado a cabo una evaluación relacionada con la capacidad de Kaspersky para detectar y neutralizar el malware WannaCry. WannaCry es un ransomware que se dio a conocer en 2017 y causó estragos en sistemas informáticos de todo el mundo por su habilidad para encriptar archivos. El objetivo principal de esta evaluación es determinar si la solución de Kaspersky puede abordar eficazmente las amenazas asociadas con WannaCry.

4.2.2. Objetivos

Los objetivos de esta evaluación son los siguientes:

1. Determinar la capacidad de Kaspersky para detectar la presencia de WannaCry en un entorno controlado.
2. Evaluar la eficacia de Kaspersky en la neutralización y eliminación de WannaCry.
3. Analizar la respuesta de Kaspersky ante amenazas similares en tiempo real.

4.2.3. Alcance

Este informe se enfoca en la evaluación de la capacidad de Kaspersky para detectar y neutralizar el malware WannaCry en un entorno controlado. No abarca una evaluación exhaustiva de todas las funcionalidades de Kaspersky ni de la seguridad general del entorno. La evaluación se limita a las capacidades de la máquina virtual instalada, pero se demuestra el funcionamiento del agente de Kaspersky dentro de un entorno simulado para comprender su respuesta frente a WannaCry y amenazas similares.

4.2.4. Metodología

Para comenzar con la prueba del ransomware WannaCry, primero se accedió a la carpeta con el nombre 'Ransomware_WannaCry' dentro del archivo ZIP del repositorio de 'theZoo'. Dentro de esta carpeta se encontró un solo ejecutable, como se puede ver en la Figura 22. Se intentó abrir el ejecutable, pero nos arrojó una alerta Windows Defender sobre los contenidos del ejecutable (Figura 23).

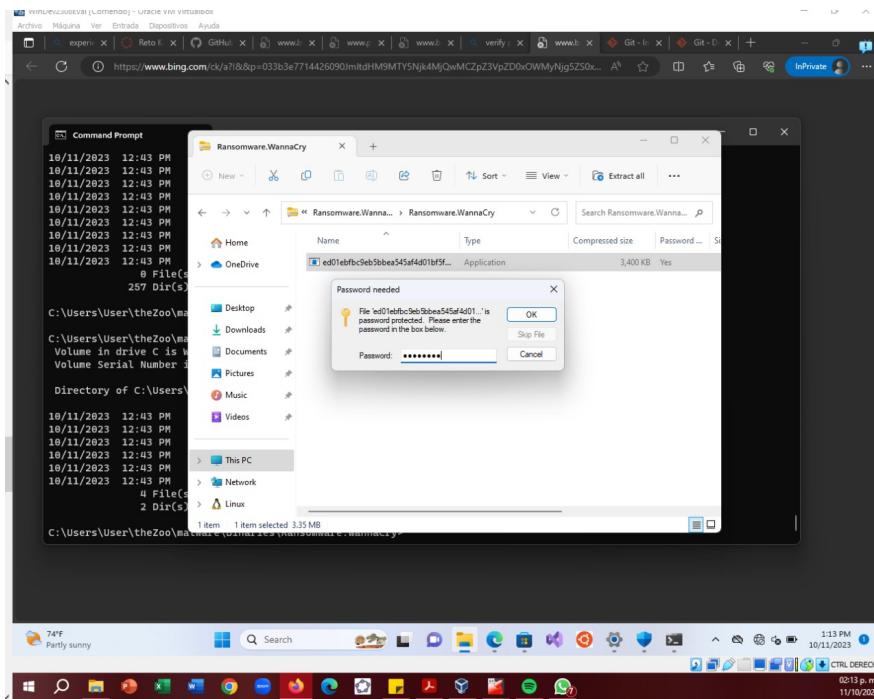


Figura 22: Descompresión de ZIP de WannaCry

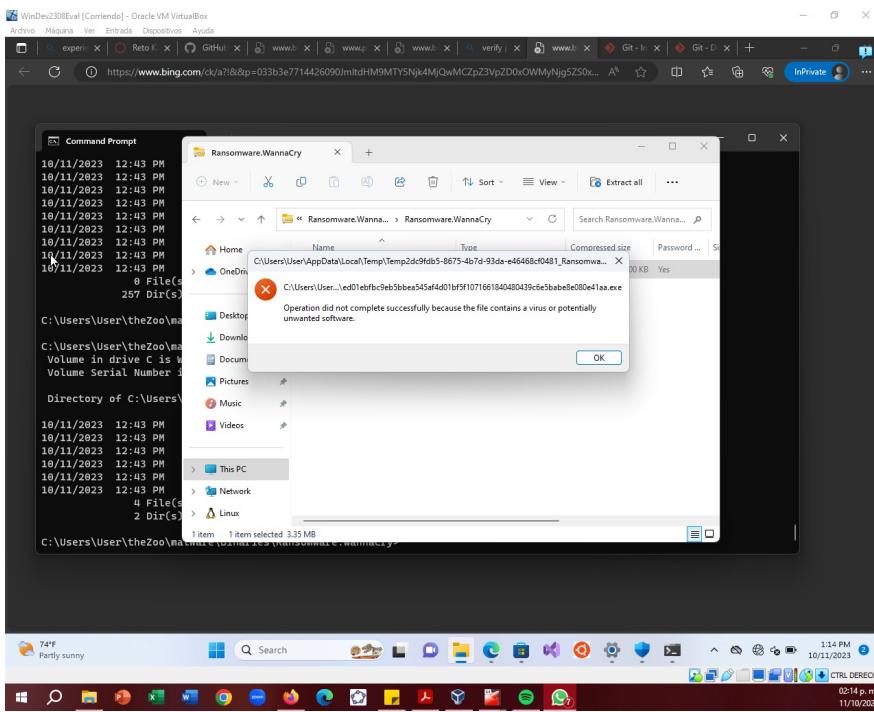


Figura 23: Alerta de Windows Defender sobre la carpeta que contiene WannaCry

Después de desactivar correctamente los antivirus de Windows, se corrió el ejecutable. Este nos desplegó la pantalla de alerta de la Figura 24, la cual nos avisó que los archivos de la máquina habían sido encriptados. Además, nos dio los pasos para desencriptarlos, pidiendo un rescate con un valor de \$300 USD en bitcoin

para poder acceder nuevamente a los archivos. Todo esto se debía realizar dentro de un límite de tiempo específico.

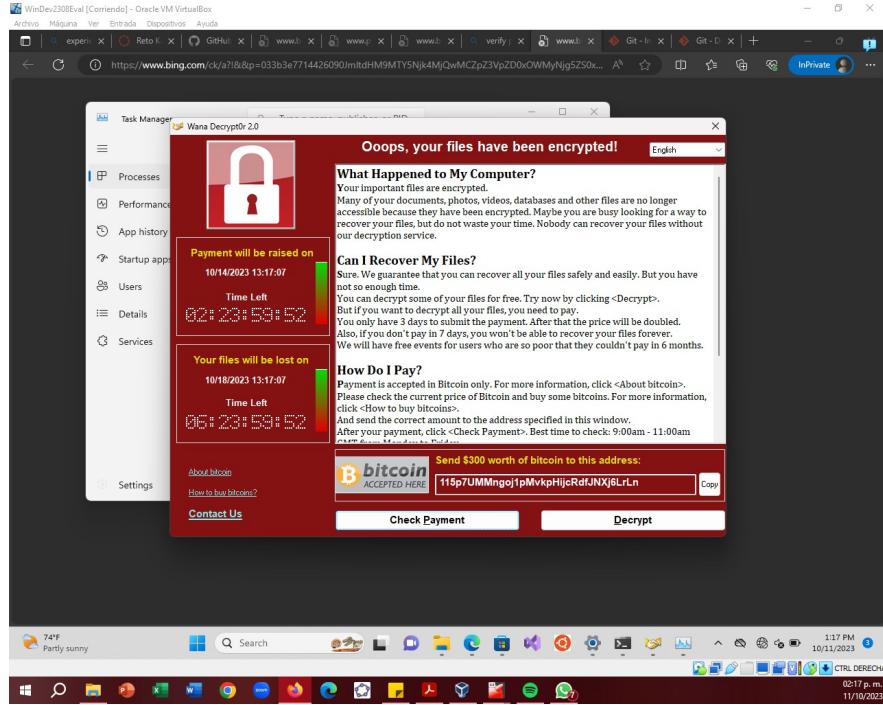


Figura 24: Pantalla de alerta con pasos a realizar para desencriptar la información

Este aviso es acompañado de cambios en la máquina, como se puede ver en las Figuras 25 y 26. Aquí se pueden observar que se agregaron archivos a la computadora y se cambió el fondo de pantalla para poder desplegar las instrucciones al usuario, asegurando que vea la alerta mostrada por el virus.

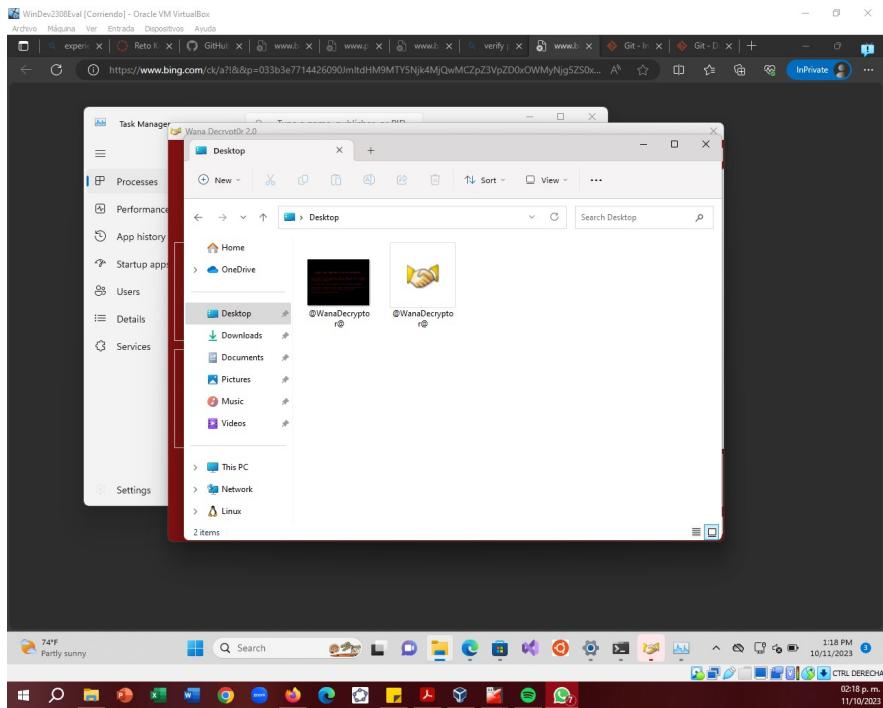


Figura 25: Captura de archivos descargados en la carpeta de escritorio por WannaCry

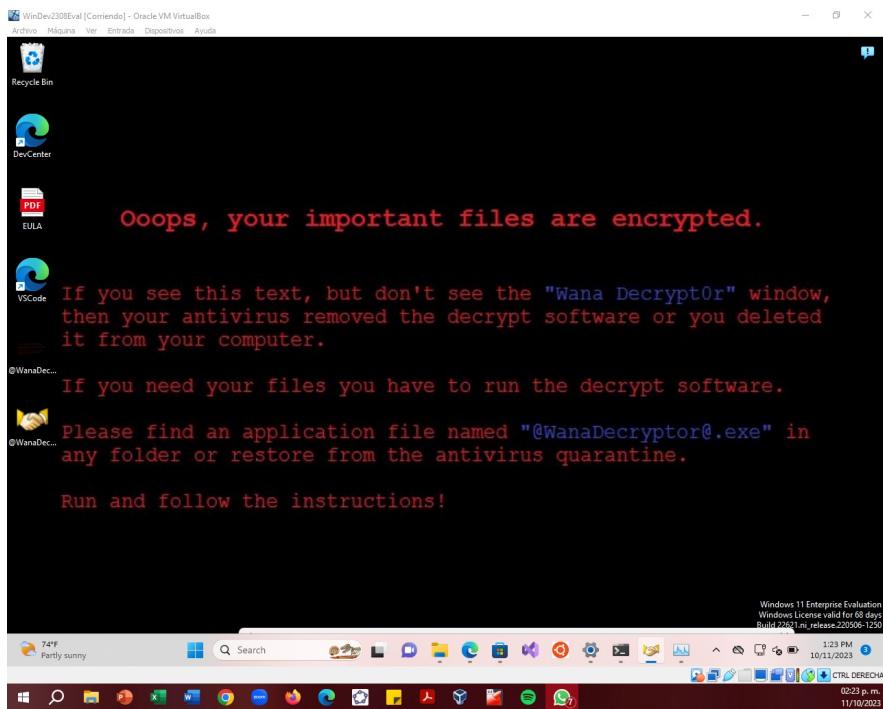


Figura 26: Evidencia de cambios en el escritorio por WannaCry

Se encendió la herramienta de Kaspersky, y se puede ver en la Figura 27 que detectó el ransomware; sin embargo, lo hizo ya muy tarde para poder detener el virus. En las Figuras 28 y 29 se puede ver la prueba de la encriptación de los archivos.

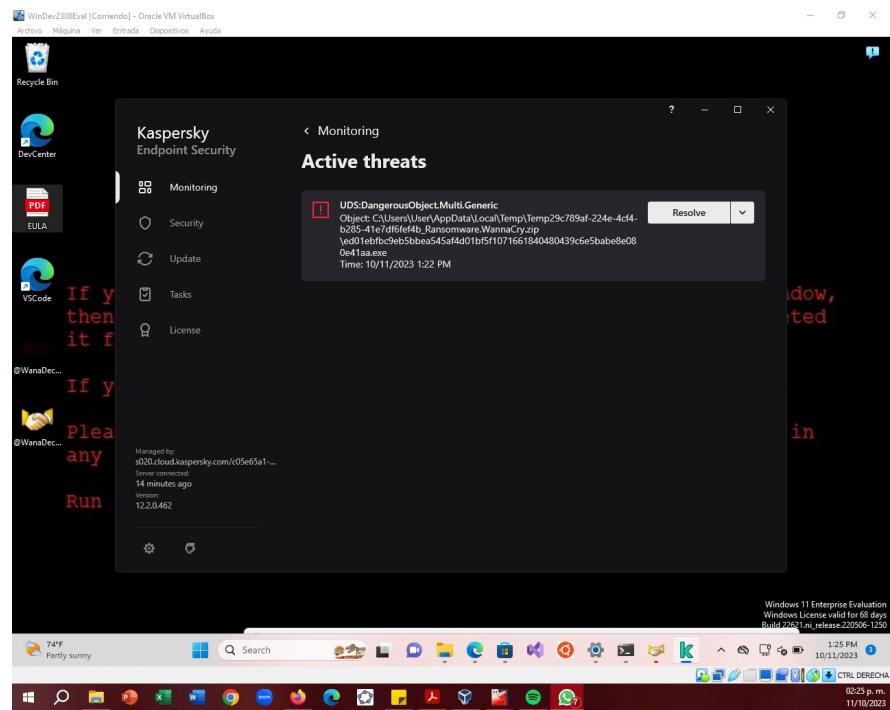


Figura 27: Detección de objeto sospechoso proveniente de WannaCry por parte de la herramienta de Kaspersky

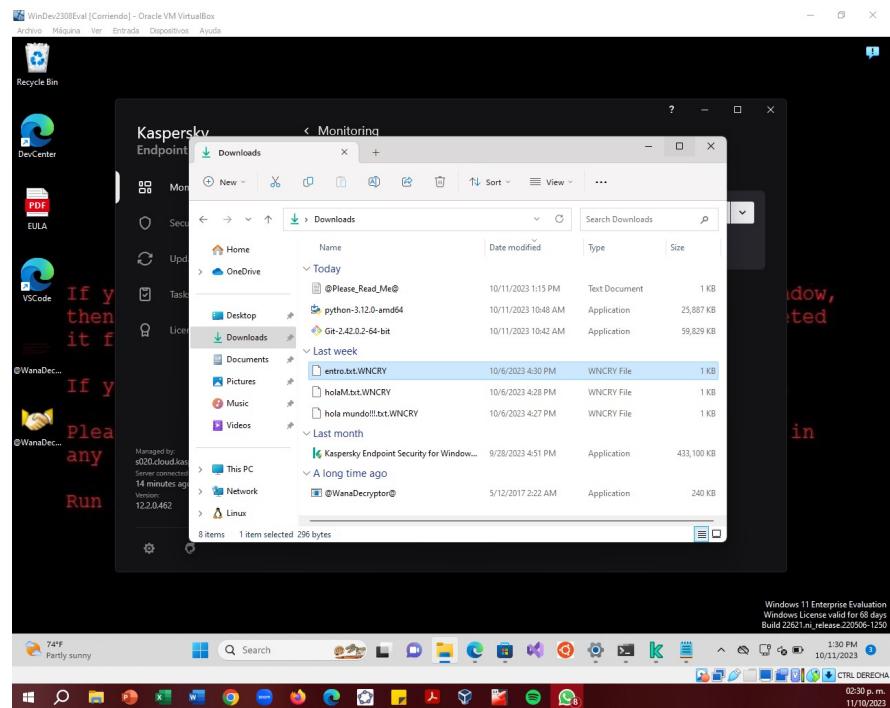


Figura 28: Evidencia de archivos encriptados por el Ransomware

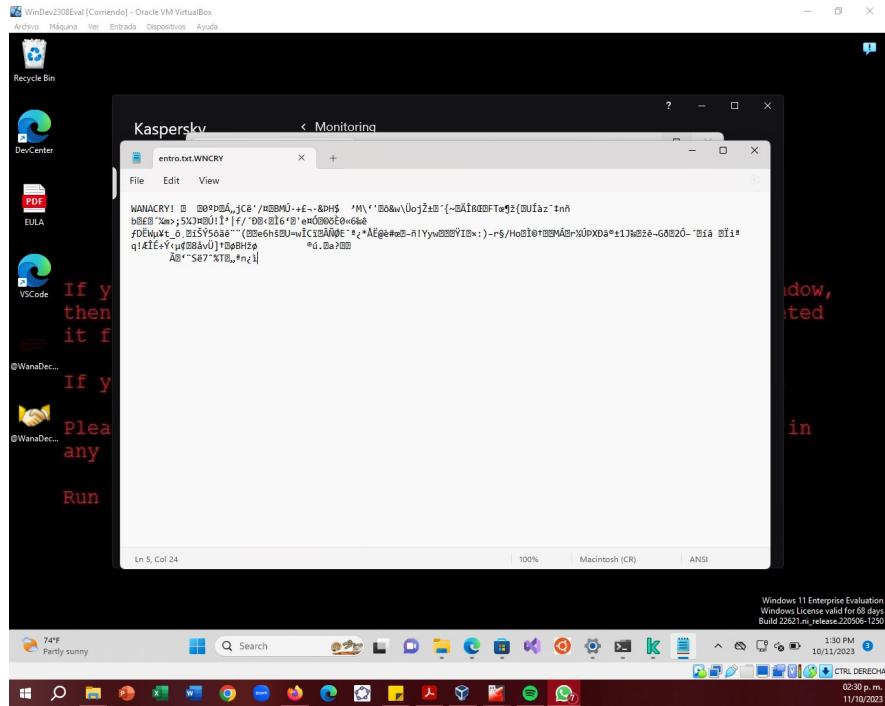


Figura 29: Evidencia de encriptado de un archivo específico por parte de WannaCry

4.2.5. Hallazgos

Después de haber descargado y corrido el ejecutable dentro de la máquina virtual, la herramienta de Kaspersky lo detectó y se puede observar en las Figuras 30, 31 y 32 que no prosperó lo suficiente para desarrollar una cadena completa; puesto que la herramienta bloqueó al archivo durante su descarga y lo eliminó, el resumen de los indicadores de compromiso de esta operación se pueden ver en el Cuadro 2.

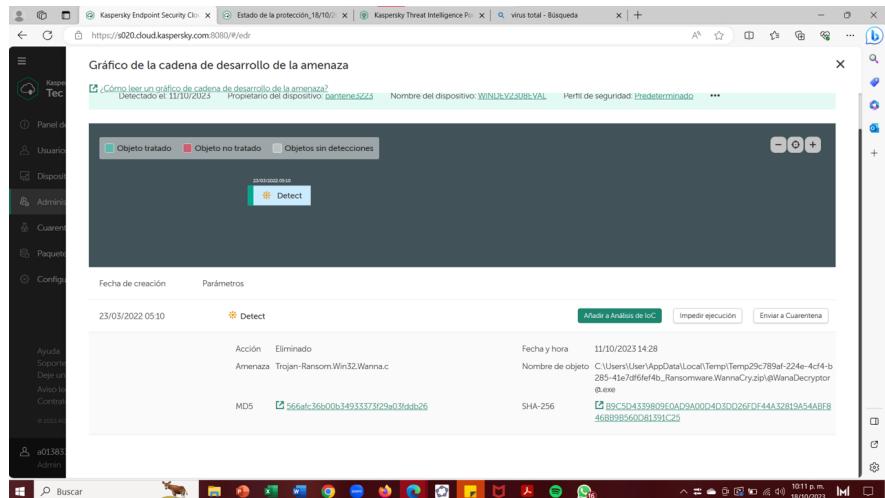


Figura 30: Detección de archivo que contiene el aviso para desencriptar los archivos

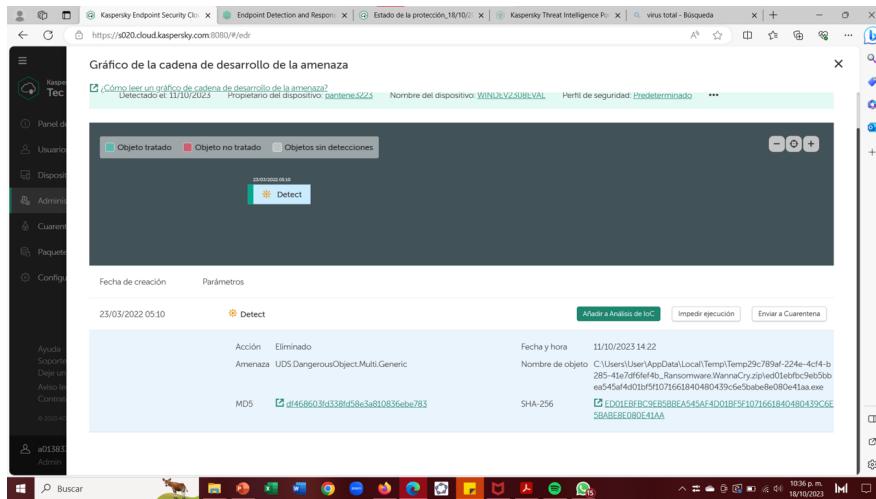


Figura 31: Detección de archivo ejecutable encriptado de WannaCry

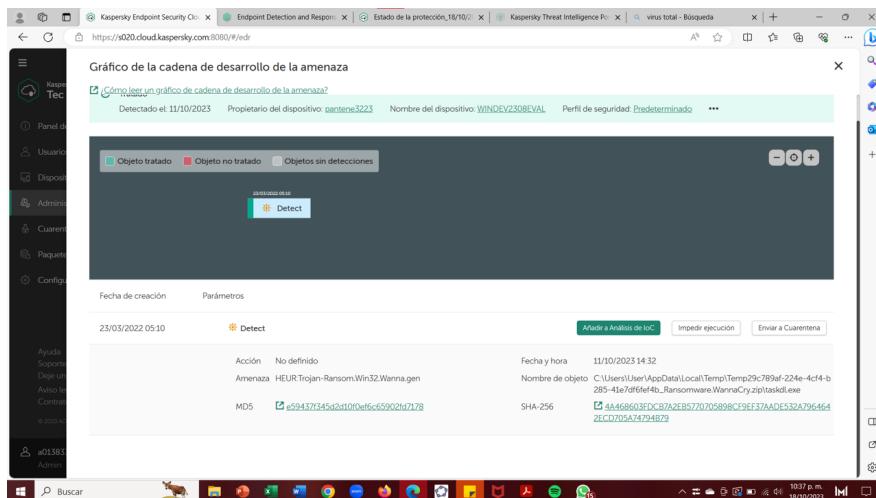


Figura 32: Detección de archivo troyano de WannaCry

Nombre de objeto	Amenaza	Tipo	Acción	Hora de detección
C:\Users\...\taskdl.exe	HEUR:Trojan-Ransom.Win32.Wanna.gen	Archivo	Eliminado	11/10/2023 14:32
Indicadores				
MD5		SHA-256		
e59437f345d2d10f0ef6c65902fd7178		4A468603FDCB7A2EB5770705898CF9EF3ADE532A7964642ECD705A74794B79		

Cuadro 2: Indicadores de compromiso del malware Wanna Cry

Después, con la información del reporte que genera la herramienta de Kasperky, se pudo analizar el resultado de la función hash SHA-256 del archivo para poder ver qué es lo que había en la base de datos de Kaspersky. Aquí se encontró un gran número de hits, lo cual nos indica que este archivo ya ha sido reportado

por más usuarios, como se puede observar en la Figura 33. Luego, con la finalidad de obtener más información en la detección de este malware, se revisó la página [Virustotal](#), en donde se subió el archivo y se pudo ver que 63 de los 72 proveedores de ciberseguridad conocen y detectan este malware, lo cual se puede ver en la Figura 34.

Figura 33: Búsqueda de información sobre el hash del código malicioso de WannaCry en la base de datos de Kaspersky

Figura 34: Búsqueda de información sobre el hash del código malicioso de WannaCry en la base de datos de virustotal.com

4.2.6. Conclusiones

La simulación del ransomware WannaCry en un entorno virtual de Windows aislado resalta la importancia de la preparación y la concienciación en ciberseguridad. Esta prueba ha demostrado la velocidad y la facilidad con la que el ransomware puede propagarse y encriptar archivos sensibles, lo que subraya la necesidad de implementar medidas preventivas sólidas, como actualizaciones de seguridad y copias de seguridad regulares.

Al realizar pruebas de este tipo en un entorno virtual, se puede comprender mejor el impacto potencial de un ataque real y se pueden desarrollar estrategias efectivas de mitigación y recuperación. Sin embargo, también destaca la importancia de la educación continua sobre seguridad cibernética y la implementación de políticas de seguridad sólidas en las organizaciones para minimizar la exposición a riesgos cibernéticos y garantizar una respuesta rápida y eficiente en caso de un ataque real.

4.2.7. Recomendaciones

Para evitar caer en el ransomware WannaCry y protegerse de futuros ataques similares, se recomienda seguir estas prácticas de seguridad informática:

- Mantén tu sistema actualizado: Instala regularmente las actualizaciones de software y parches de seguridad proporcionados por tu proveedor de sistema operativo. WannaCry aprovechó una vulnerabilidad en sistemas no actualizados, por lo que mantener tu software al día es crucial.
- Utiliza un software antivirus confiable: Instala un software antivirus confiable y mantenlo actualizado para detectar y bloquear posibles amenazas de ransomware.
- Realiza copias de seguridad regulares: Respaldá tus archivos importantes con regularidad en dispositivos externos o en la nube. Asegúrate de que estas copias de seguridad estén actualizadas y sean accesibles en caso de una infección de ransomware.

De igual manera, se recomienda usar la herramienta Wanakiwi, la cual fue desarrollada para proporcionar una posible solución al ransomware WannaCry. Esta herramienta tiene la capacidad de buscar en la memoria del sistema números primos y reconstruir la clave de cifrado utilizada por el ransomware, con la condición de que el sistema infectado no haya sido reiniciado y que el proceso del ransomware no haya sido detenido. Aunque la herramienta ha demostrado ser efectiva en entornos de laboratorio, su éxito puede variar según el sistema y la situación específica del usuario. Se sugiere utilizarla con precaución, ya que su eficacia puede ser limitada en algunos casos debido a las acciones del malware. El desarrollo de esta herramienta fue posible gracias al trabajo de Adrien Guinet, Benjamin Delpy y Matt Suiche, cuya dedicación y talento merecen reconocimiento en la comunidad de ciberseguridad (Kujawa 2017).

4.3. IllusionBot

Caso: 3

Fecha del incidente: 17 de octubre 2023

Hora: 19:42

Nombre del incidente: BOTBINARY.EXE

4.3.1. Resumen ejecutivo

En el marco de una investigación forense digital, se ha llevado a cabo una evaluación relacionada con la capacidad de Kaspersky para detectar y neutralizar el malware IllusionBot. IllusionBot es un malware famoso

que puede pasar desapercibido y que ha sido utilizado en diversas ciberamenazas y actividades maliciosas en línea. El objetivo principal de esta evaluación es determinar si la solución de Kaspersky puede abordar eficazmente las amenazas asociadas con IllusionBot.

4.3.2. Objetivos

Los objetivos de esta evaluación son los siguientes:

1. Determinar la capacidad de Kaspersky para detectar la presencia de IllusionBot en un entorno controlado.
2. Evaluar la eficacia de Kaspersky en la neutralización y eliminación de IllusionBot.
3. Analizar la respuesta de Kaspersky ante amenazas similares en tiempo real.

4.3.3. Alcance

Este informe se enfoca en la evaluación de la capacidad de Kaspersky para detectar y neutralizar el malware IllusionBot en un entorno controlado. No abarca una evaluación exhaustiva de todas las funcionalidades de Kaspersky ni de la seguridad general del entorno. La evaluación se limita a las capacidades de la máquina virtual instalada, pero se demuestra el funcionamiento del agente de Kaspersky dentro de un entorno simulado para comprender su respuesta frente a IllusionBot y amenazas similares.

4.3.4. Metodología

Para comenzar con la prueba del IllusionBot, primero se accedió a la carpeta con el nombre 'IllusionBot_May2007' dentro del ZIP del repositorio de 'theZoo'. Como se puede ver en la Figura 35, dentro de esta carpeta se encuentra el ejecutable del malware con nombre 'BOTBINARY.exe'. Se activa el ejecutable y se abre el Administrador de Tareas de Windows para verificar su funcionamiento. (Figura 36).

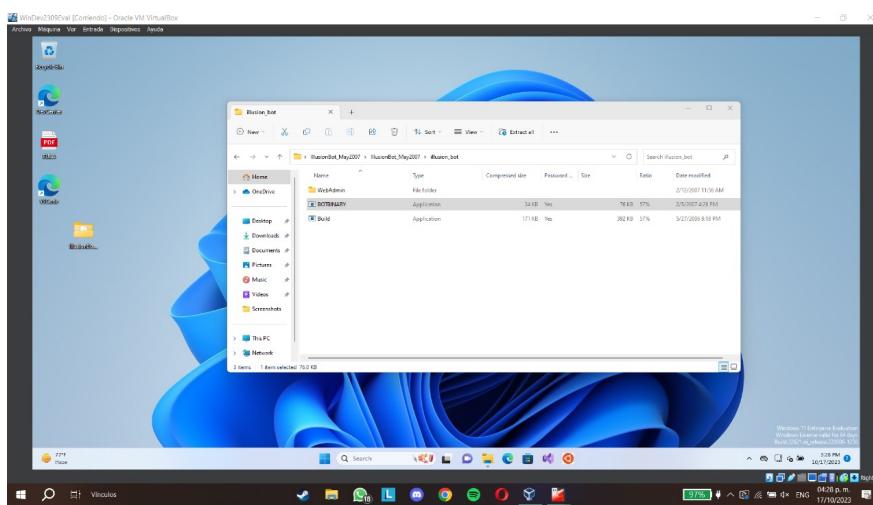


Figura 35: Descompresión de carpeta en formato ZIP con el ejecutable del bot

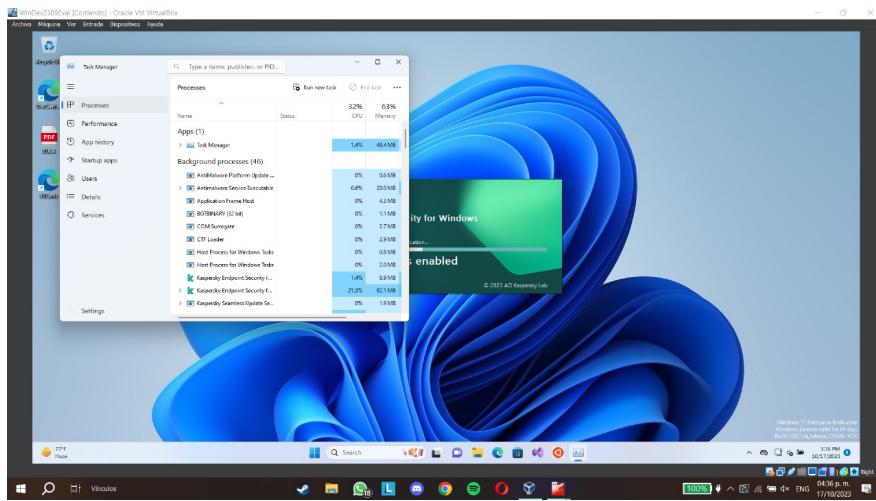


Figura 36: Evidencia del funcionamiento del bot como proceso en el administrador de tareas de Windows

Después de unos minutos y habiendo dejado correr el malware, activamos la herramienta de Kaspersky para que pueda detener el virus. En la Figura 37 se muestra la detección que hace la herramienta.

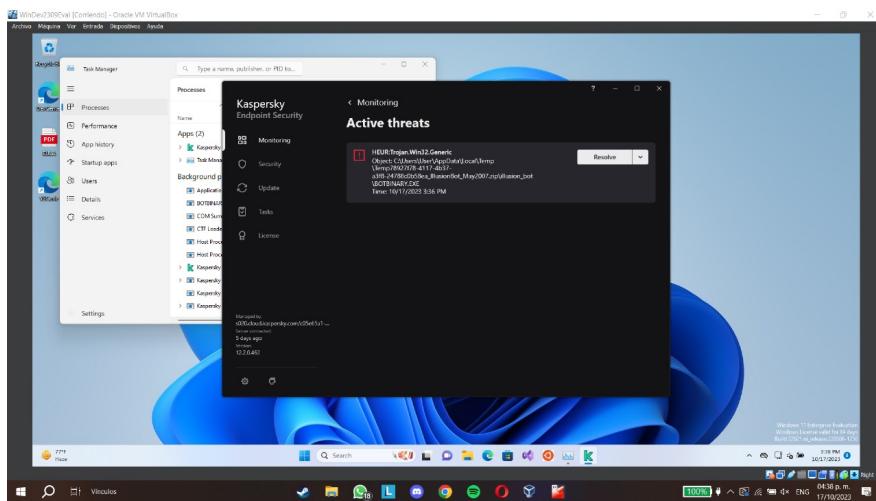


Figura 37: Detención del proceso del ejecutable del bot, por parte de la herramienta de Kaspersky

4.3.5. Hallazgos

Se crea el reporte de parte de Kaspersky y en la Figura 38, se puede ver el gráfico que nos arroja sobre la amenaza que detectó por el IllusionBot. Además, se puede ver que la cadena de desarrollo de amenaza no fue generada en su totalidad debido a la rapidez de actuar por parte de la herramienta, el resumen de los indicadores de compromiso se encuentra en el Cuadro 3. No obstante, se pudo analizar el hash del código malicioso (Figura 39) para posteriormente hacer un análisis a fondo en la base de datos de Kaspersky y en <https://www.virustotal.com>. (Figura 40 y 41)

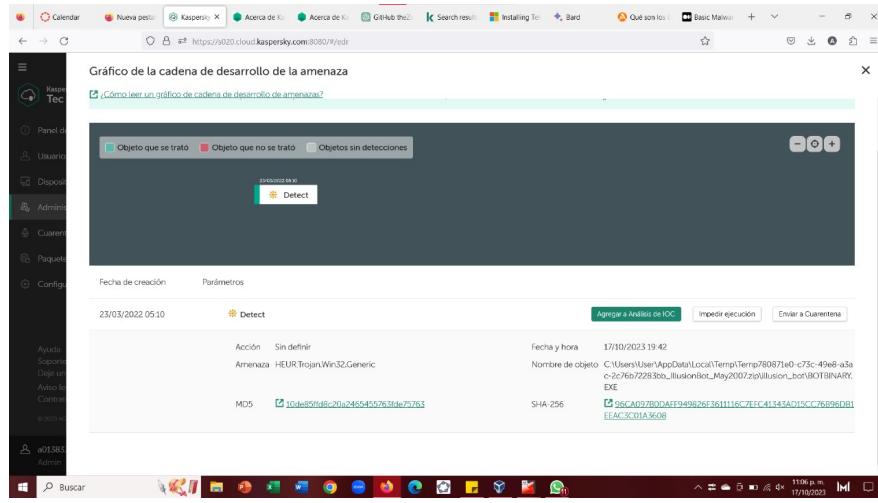


Figura 38: Captura de gráfico de la cadena de desarrollo de la amenaza por parte de Kaspersky Security Cloud Console

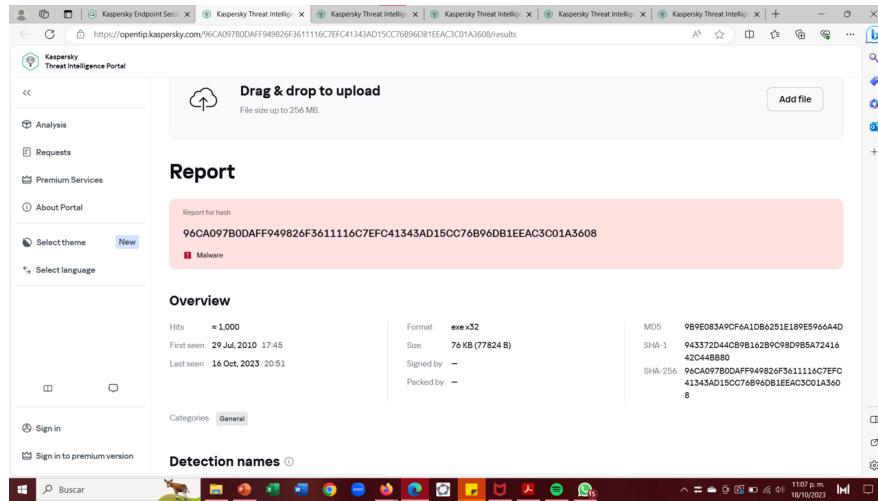


Figura 39: Búsqueda de información sobre el hash del código malicioso de IllusionBot en la base de datos de Kaspersky

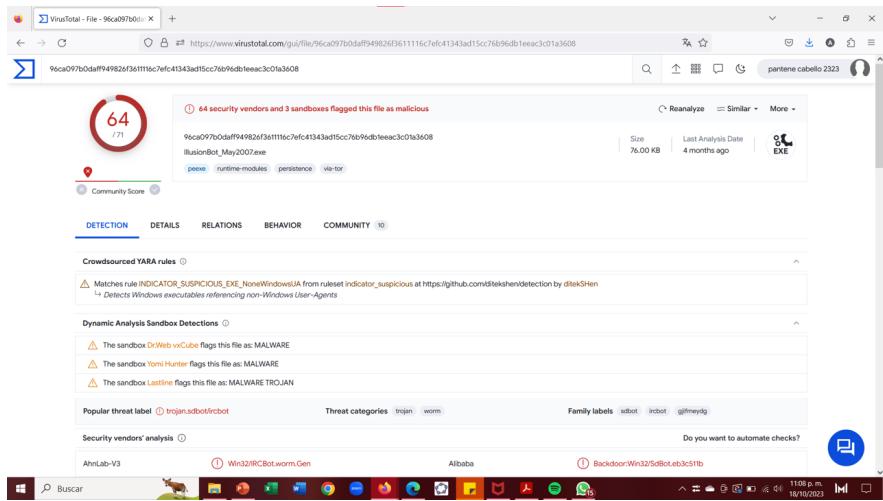


Figura 40: Búsqueda de información sobre el hash del código malicioso de IllusionBot en la base de datos de virustotal.com

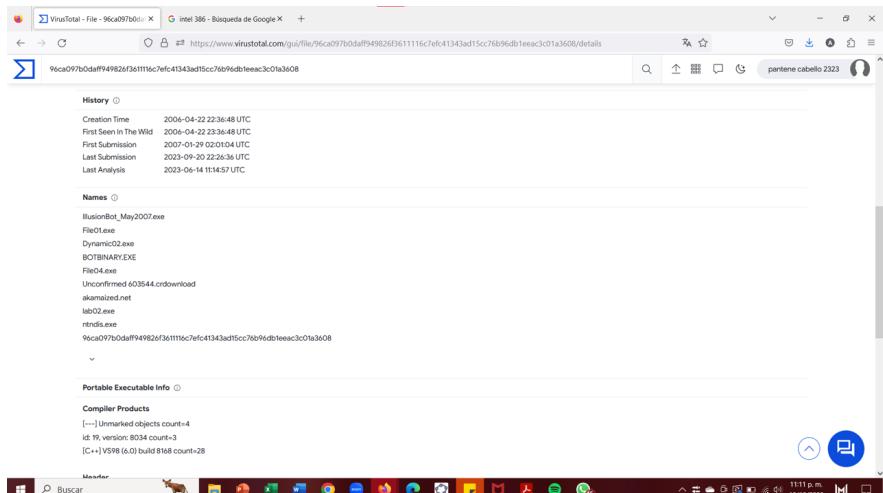


Figura 41: Búsqueda de información sobre el origen del malware de IllusionBot usando su hash en la base de datos de virustotal.com

Nombre de objeto	Amenaza	Tipo	Acción	Hora de detección
C:\Users\User...\BOTBINARY.EXE	HEUR:Trojan.Win32.Generic	Archivo	Eliminado	17/10/2023 19:42
Indicadores				
MD5		SHA-256		
10de85ffd8c20a2465455763fde75763		96CA097B0DAFF949826F3611116C7EFC41343AD15CDB1EEAC3C01A3608		

Cuadro 3: Indicadores de compromiso del malware IllusionBot

4.3.6. Conclusiones

La simulación de IllusionBot ha destacado la sofisticación y la peligrosidad de las amenazas ciberneticas modernas. Esta prueba subraya la importancia de mantener una postura proactiva en ciberseguridad, incluyendo la implementación de soluciones antivirus actualizadas y firewalls robustos. Además, resalta la necesidad de una supervisión constante de la red y la detección temprana de actividades sospechosas, así como de la educación continua de los usuarios para que estén atentos a posibles signos de compromiso de seguridad. Dada la complejidad de IllusionBot y su poca frecuencia en servidores dedicados a la detección de malware, es imperativo fortalecer las defensas ciberneticas y adoptar estrategias de prevención integrales para proteger eficazmente los datos sensibles y los sistemas críticos contra amenazas cada vez más avanzadas y sigilosas.

4.3.7. Recomendaciones

Para prevenir problemas con el malware bot espía IllusionBot y salvaguardar la seguridad de los sistemas, se recomienda implementar una serie de medidas de seguridad efectivas. En primer lugar, es crucial mantener actualizados los programas antivirus y antimalware para detectar y eliminar cualquier instancia de IllusionBot o amenazas similares. Además, se deben fortalecer las defensas de la red mediante la configuración de firewalls avanzados y la segmentación de la red para limitar la propagación del malware en caso de una intrusión. Se recomienda también llevar a cabo auditorías de seguridad periódicas y pruebas de penetración para identificar posibles vulnerabilidades y parchearlas de inmediato. Educar a los usuarios sobre los riesgos potenciales de la ingeniería social y el phishing también es esencial para prevenir la infiltración de IllusionBot a través de métodos de engaño. Por último, se debe implementar una política de acceso restrictiva y privilegios mínimos para reducir la exposición de los datos críticos y restringir el impacto en caso de una posible infección. Mediante la adopción de estas medidas integrales, las organizaciones pueden fortalecer sus defensas contra el malware bot espía IllusionBot y proteger eficazmente la integridad de sus sistemas y datos sensibles.

4.4. AsproxOld

Caso: 4

Fecha del incidente: 18 de octubre de 2023

Hora: 11:13

Nombre del incidente: US_Airways_E-Ticket_Print_Doc.exe

4.4.1. Resumen ejecutivo

Como parte de una investigación forense digital, se ha llevado a cabo una evaluación relacionada con la capacidad de Kaspersky para detectar y neutralizar el malware AsproxOld. El malware AsproxOld es una amenaza que ha estado activa durante varios años y se ha utilizado en diversas campañas de robo de datos en línea. El objetivo principal de esta evaluación es determinar si la solución de Kaspersky puede abordar eficazmente las amenazas asociadas con Asprox.

4.4.2. Objetivos

Los objetivos de esta evaluación son los siguientes:

1. Determinar la capacidad de Kaspersky para detectar la presencia de AsproxOld en un entorno controlado.
2. Evaluar la eficacia de Kaspersky en la neutralización y eliminación de AsproxOld.
3. Analizar la respuesta de Kaspersky ante amenazas similares en tiempo real.

4.4.3. Alcance

Este informe se centra en la evaluación de la capacidad de Kaspersky para detectar y neutralizar el malware Asprox en un entorno controlado. No abarca una evaluación exhaustiva de todas las funcionalidades de Kaspersky ni de la seguridad general del entorno. La evaluación se limita a las capacidades de la máquina virtual instalada, pero se demuestra el funcionamiento del agente de Kaspersky dentro de un entorno simulado para comprender su respuesta frente a Asprox y amenazas similares.

4.4.4. Metodología

Para comenzar se descomprimió el archivo zip, como se puede observar en la Figura 42. Una vez que se descomprimió, se ejecutó el programa adentro de la carpeta y desplegó una ventana tal y como se muestra en la Figura 43.

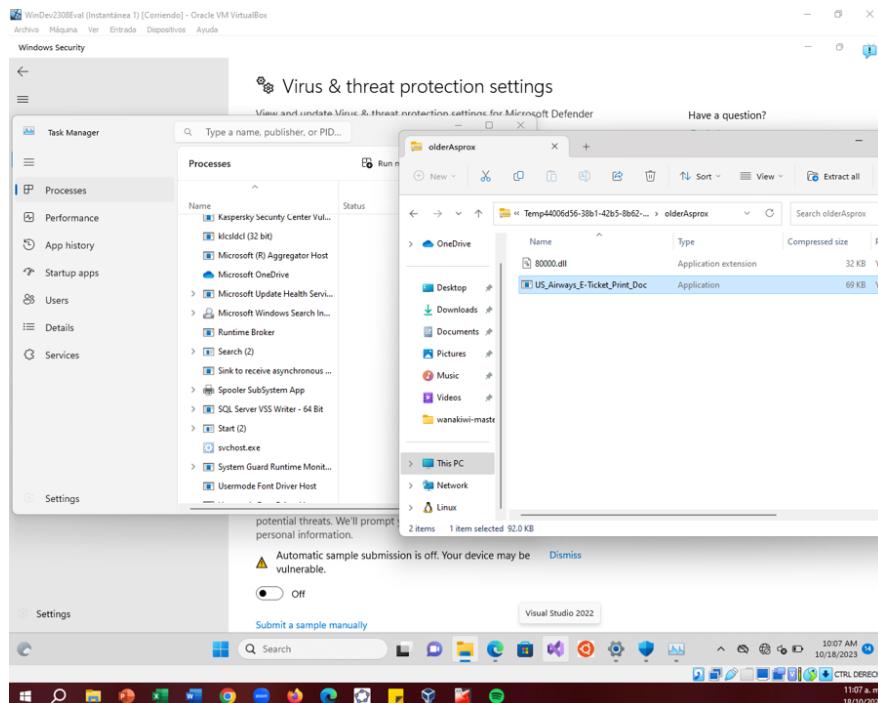


Figura 42: Descompresión de la carpeta ZIP oldAsprox

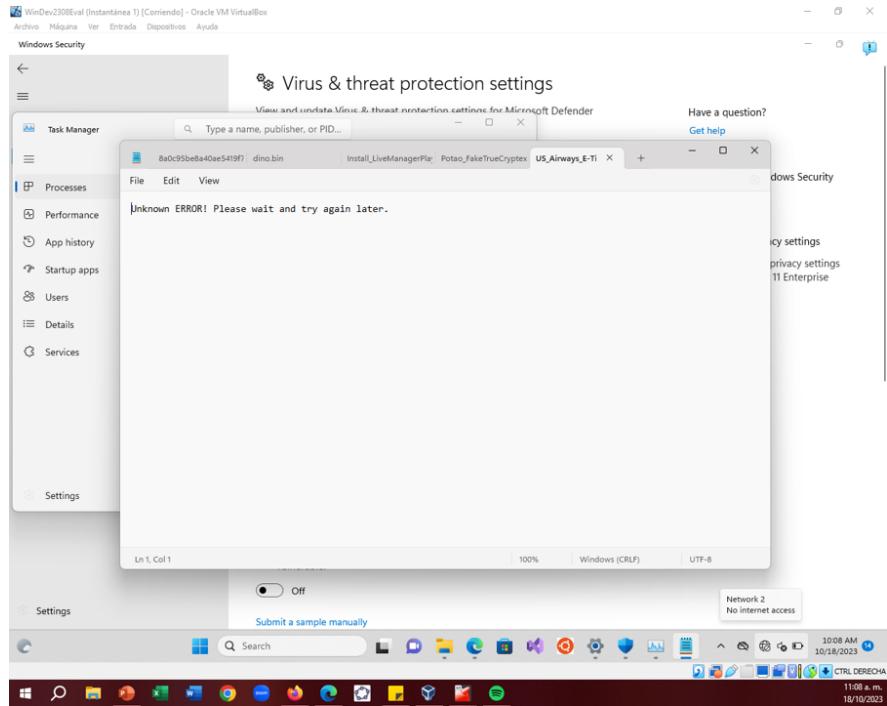


Figura 43: Resultado final de la ejecución del malware oldAsprox

Cabe mencionar que después de la ejecución del código malicioso, AsproxOld al parecer pudo detectar que estaba en una máquina virtual y buscó infectar a la computadora física. El antivirus de la computadora en donde se tienen las máquinas virtuales desplegó una ventana en donde decía que se había evitado una conexión peligrosa, como se puede observar en la Figura 44.

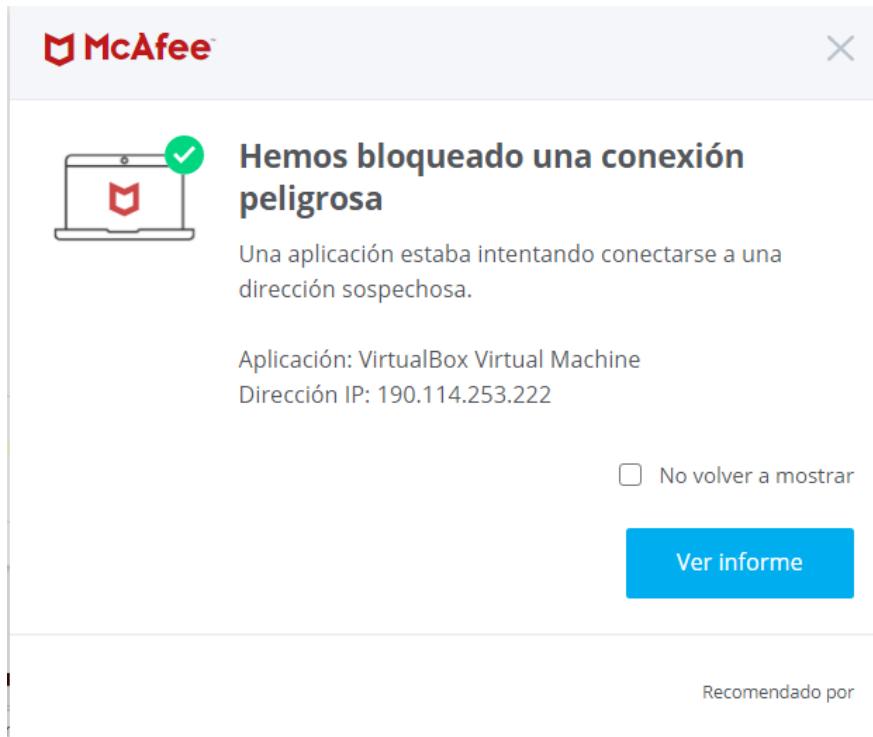


Figura 44: Problemas en equipo local al ejecutar el malware dentro de la VM

4.4.5. Hallazgos

Después de ejecutar el malware en la máquina virtual, se puede observar en la Figura 45 cómo la herramienta de Kaspersky fue capaz de detectarlo y bloquearlo durante su descarga; sin embargo, no lo dejó ejecutar toda la cadena, puesto que lo identificó como un objeto con malware y lo borró, el resumen de los indicadores de compromiso se encuentra en el Cuadro 4.

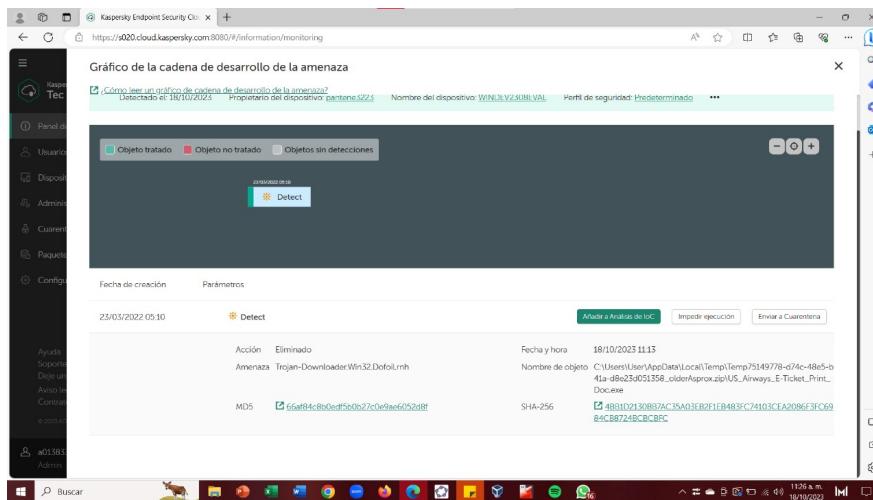


Figura 45: Captura de gráfico de la cadena de desarrollo de la amenaza por parte de Kaspersky Security Cloud Console

Nombre de objeto	Amenaza	Tipo	Acción	Hora de detección
C:\Users\User...Print_Doc.exe	Trojan-Downloader.Win32.Dofoil.rnh	Archivo	Eliminado	18/10/2023 11:13
Indicadores				
MD5				SHA-256
66af84c8b0edf5b0b27c0e9ae6052d8f				4BB1D2130BB7AC35A03EB2F1EB483CEA2086F3FC6984CB8724BCBCBFC

Cuadro 4: Indicadores de compromiso del malware oldAsprox

Luego, con el objetivo de tener más información acerca de este malware y a través del reporte hecho por la herramienta de Kaspersky, se decidió analizar el resultado de la función hash SHA-256 en la base de datos de Kaspersky. Aquí se observó que tiene un número elevado de hits, lo que quiere decir que es un archivo que ha sido reportado muchas veces como un malicioso (Figura 46). Además, para conocer sobre cómo es que responden algunos de los proveedores de ciberseguridad reconocen este malware, se usó el sitio [virustotal](http://virustotal.com). Aquí se subió el ejecutable y se reportó que 63 de los 72 lo detectan como peligroso, lo cual se puede ver en la Figura 46.

The screenshot shows the Kaspersky Threat Intelligence Portal interface. On the left, there's a sidebar with options like Analysis, Requests, Premium Services, About Portal, Select theme, and Select language. The main area has a search bar at the top with the URL https://opentip.kaspersky.com/4BB1D2130BB7AC35A03EB2F1EB483CEA2086F3FC6984CB8724BCBCBFC. Below the search bar, there's a "Report" section with a "Report for hash" input field containing the SHA-256 hash. A red box highlights the "Malware" category. The "Overview" section provides details such as Hits (10,000), Format (exe x32), Size (92 KB), and various MD5 and SHA-256 hash values. At the bottom, there's a "Detection names" section showing logos of various security vendors that have detected the file as malicious.

Figura 46: Búsqueda de información sobre el hash del código malicioso de oldAsprox en la base de datos de Kaspersky

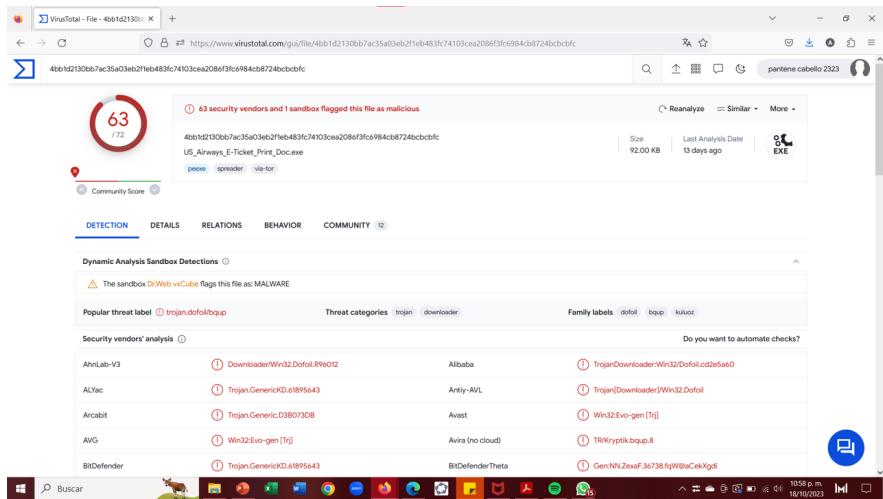


Figura 47: Búsqueda de información sobre el hash del código malicioso de oldAsprox en la base de datos de virustotal.com

4.4.6. Conclusiones

La simulación de AsproxOld nos muestra la importancia de tener un buen sistema de defensa en nuestra computadora (antimalware o antivirus) y el ser más cauteloso con lo que se descarga de internet y se ejecuta. Siempre se tiene que desconfiar de archivos que se bajen de internet y de vez en cuando hacer una inspección sobre la actividad de nuestra computadora para ver si se están ejecutando tareas sospechosas.

4.4.7. Recomendaciones

Dado que existe una tendencia masiva de crear malware, es importante contar con un antivirus que esté avalado o que cuente con algún tipo de certificación como AV-TEST, VB100, entre otras. Además, es importante considerar que las bases de datos de estos antivirus se mantengan actualizadas y los programas que use el usuario en su computadora estén actualizados, ya que constantemente se encuentran diferentes vulnerabilidades en los programas. Hacer diferentes simulaciones de descarga de malware ayuda a probar la eficacia de los diferentes tipos de sistemas de defensa que existen. El tener un respaldo de los equipos que contengan información relevante, ya sea de los clientes o del usuario, es una gran medida de seguridad. Dicho respaldo debe estar guardado en un lugar seguro y debe ser diferente a donde se encuentra el equipo. Además, este debe ser actualizado con cierta regularidad. Sobre todo, es crucial tener un plan de contingencia en el caso de que ocurra algún imprevisto.

4.5. Dyre Original

Caso: 5

Fecha del incidente: 18 de octubre del 2023

Hora: 10:49

Nombre del incidente: fax_390392029_072514.exe

4.5.1. Resumen ejecutivo

Como parte de una investigación forense digital, se ha realizado una evaluación relacionada con la capacidad de Kaspersky para detectar y neutralizar el malware Dyre. Dyre es un troyano bancario notorio que ha sido utilizado en ataques dirigidos a instituciones financieras y usuarios en línea. El objetivo principal de esta evaluación es determinar si la solución de Kaspersky puede abordar eficazmente las amenazas asociadas con Dyre.

4.5.2. Objetivos

Los objetivos de esta evaluación son los siguientes:

1. Determinar la capacidad de Kaspersky para detectar la presencia de Dyre en un entorno controlado.
2. Evaluar la eficacia de Kaspersky en la neutralización y eliminación de Dyre.
3. Analizar la respuesta de Kaspersky ante amenazas similares en tiempo real.

4.5.3. Alcance

Este informe se enfoca en la evaluación de la capacidad de Kaspersky para detectar y neutralizar el malware Dyre en un entorno controlado. No abarca una evaluación exhaustiva de todas las funcionalidades de Kaspersky ni de la seguridad general del entorno. La evaluación se limita a las capacidades de la máquina virtual instalada, pero se demuestra el funcionamiento del agente de Kaspersky dentro de un entorno simulado para comprender su respuesta frente a Dyre y amenazas similares.

4.5.4. Metodología

Para comenzar con la prueba del malware Dyre, primero se accedió a la carpeta con el nombre 'Dyre' dentro del archivo ZIP del repositorio de 'theZoo' (Figura 48). Dentro de esta carpeta se encontró el ejecutable del malware con nombre 'fax_390392029_072514.exe', como se puede ver en la Figura 49. Se activó el ejecutable y se abrió el Administrador de Tareas de Windows para verificar su funcionamiento, como se muestra en la Figura 50.

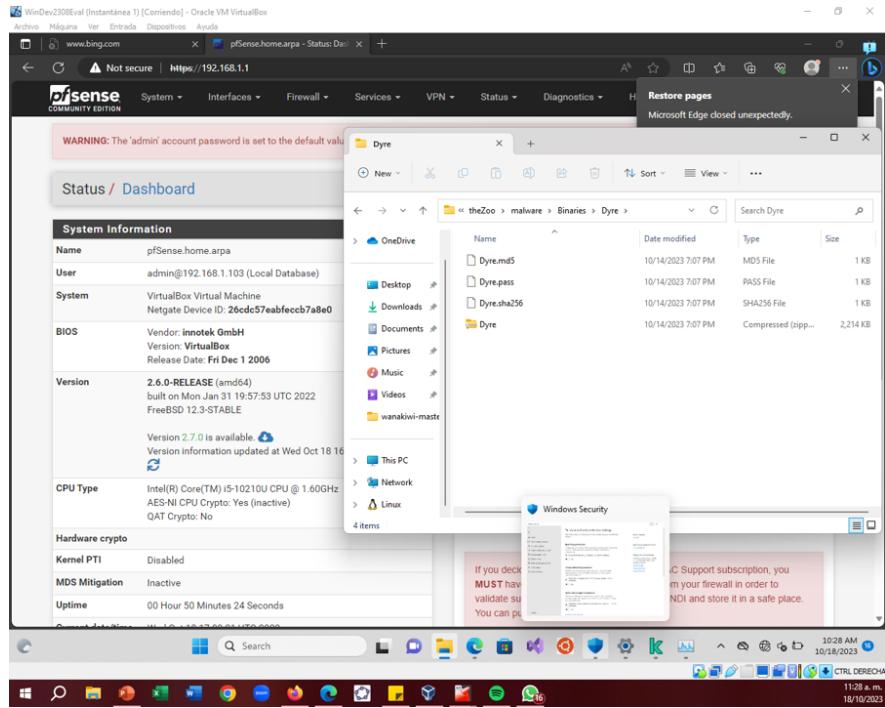


Figura 48: Localización de la carpeta ZIP del malware Dyre

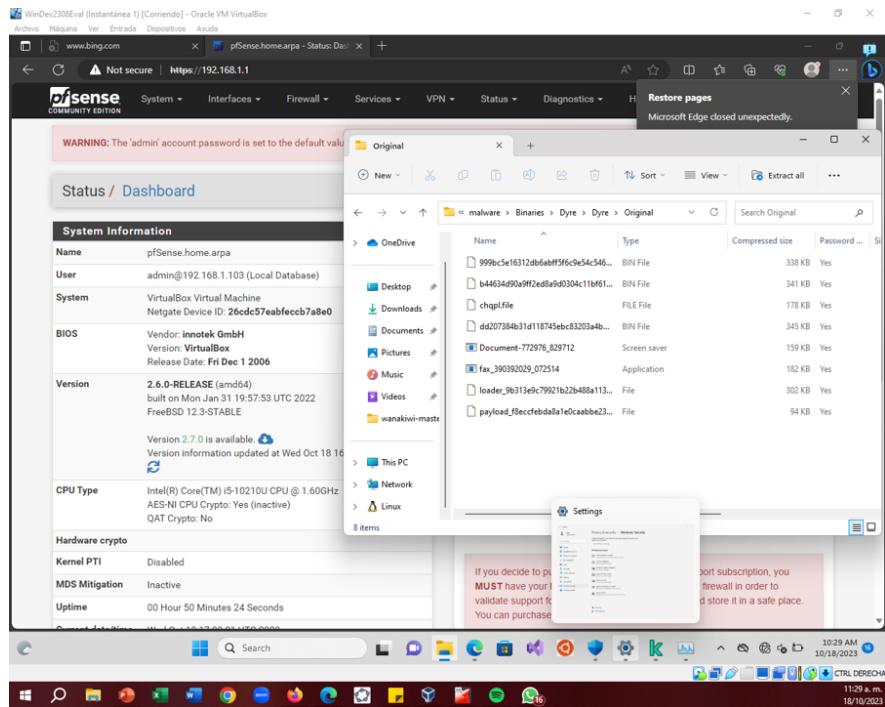


Figura 49: Descompresión del archivo ZIP de la carpeta Dyre en su versión Original

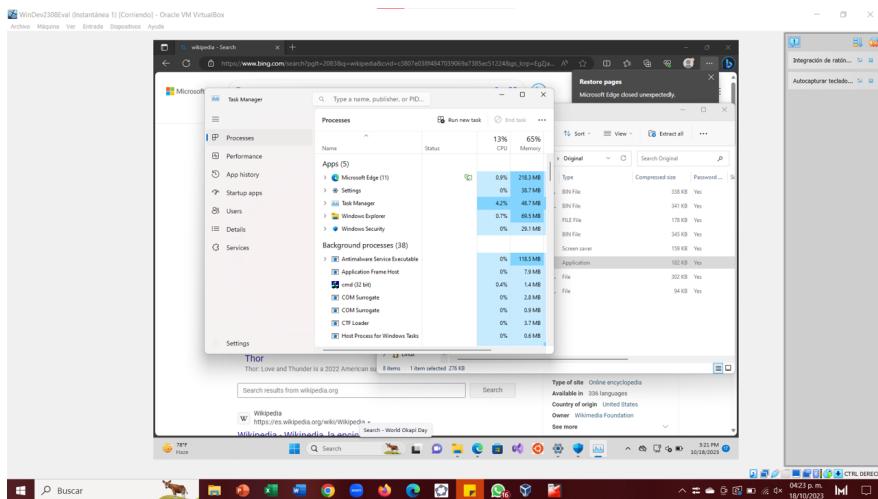


Figura 50: Evidencia del malware ejecutando su proceso dentro de la VM mediante el administrador de tareas

4.5.5. Hallazgos

Después de haber encendido el agente antimalware de la máquina virtual de Kaspersky, se reportó un gráfico de la cadena de desarrollo de la amenaza. Esta fue más desarrollada que los anteriores casos reportados, como se puede ver en la Figura 51. Con esta cadena se pudo detallar con mayor precisión los procesos seguidos por el malware dentro de la máquina virtual.

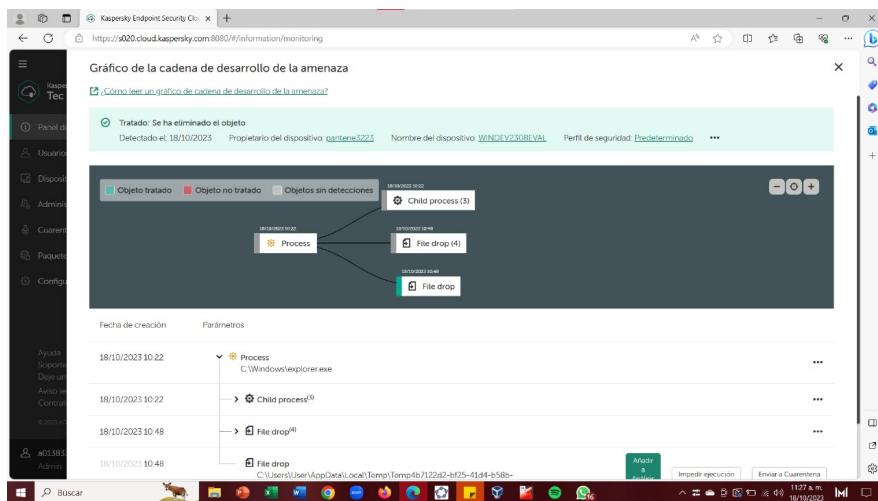


Figura 51: Captura de gráfico de la cadena de desarrollo de la amenaza por parte de Kaspersky Security Cloud Console

Para comenzar con el análisis se debe describir lo acontecido en el proceso primordial, iniciado por el malware, como se puede ver en la Figura 52. Este se trata de C:\.exe, cuya funcionalidad es activar el buscador de archivos de Windows. Se activó primero este proceso para comenzar a revisar detalles del entorno bajo la mirada del malware. Cabe mencionar que este proceso se hace con privilegios de administrador y usando

el usuario principal del sistema operativo `WINDEV2308EVAL\User`, lo cual hará más difícil su detección en este paso. Por otra parte, también es necesario resaltar que el agente antimalware tomó la decisión correcta de no detener este proceso, puesto que esto inhabilitaría a la máquina virtual de hacer búsquedas entre sus archivos, lo cual es una pérdida que no debería de suceder porque deja el sistema operativo sin herramientas para trabajar adecuadamente. El resumen de este inicio de línea de acción se puede observar en los Cuadros 5 y 6.

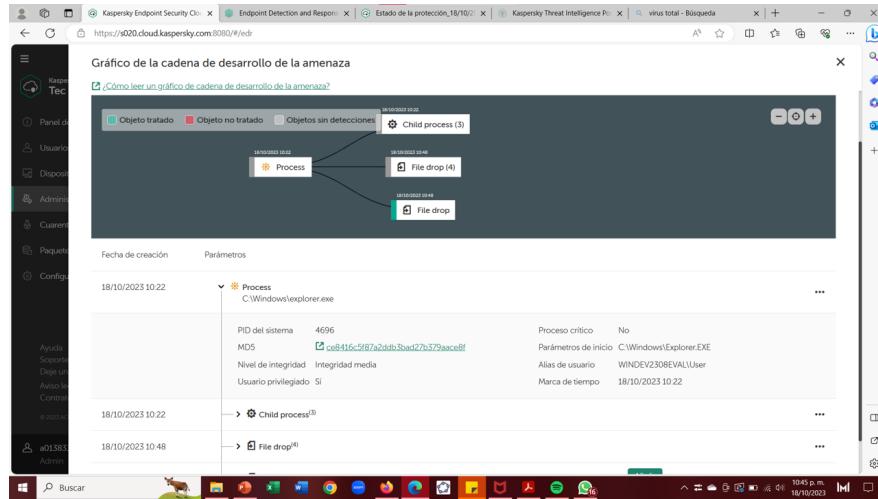


Figura 52: Captura de inicio de la cadena de desarrollo de la amenaza, comenzando por usar el buscador de archivos de Windows

Parámetro de inicio	Tipo	PID del sistema	Crítico	Nivel de Integridad
C:.EXE	Proceso	4696	No	Media

Cuadro 5: Origen de la amenaza

Usuario	Hora
WINDEV2308EVAL	18/10/23 10:22

Cuadro 6: Detalles de la amenaza

De acuerdo con el gráfico de la cadena de desarrollo de la amenaza (Figura 51) se generan tres procesos hijos que ejecutan diversos comandos en la terminal de la máquina virtual. Como se puede ver en la Figura 53, el primero de ellos se trata de la ejecución del archivo `VBoxTray.exe`, el cual es un componente del software Oracle VM VirtualBox y es responsable de proporcionar la bandeja del sistema de VirtualBox, lo que permite a los usuarios acceder rápidamente a ciertas funciones y configuraciones relacionadas con VirtualBox directamente desde la bandeja del sistema. Al identificar la presencia de `VBoxTray.exe`, Dyre podría ajustar su comportamiento y eludir ciertas técnicas de análisis o detección utilizadas por programas antivirus y sistemas de seguridad. El segundo de los procesos hijos se trata de `msedge.exe-no-startup-window`

--win-session-start /prefetch:5" y se refiere a la ubicación del archivo ejecutable 'msedge.exe' del navegador Microsoft Edge en un sistema Windows, seguido de varios modificadores. El comando está diseñado para iniciar el navegador Microsoft Edge con ciertas opciones y parámetros de inicio específicos. En particular, los modificadores '-no-startup-window' indican que el navegador se inicie sin abrir una ventana de navegador, mientras que '--win-session-start' se utiliza para abrir el navegador en la sesión de Windows actual. La opción '/prefetch:5' especifica la cantidad de recursos de precarga que se asignan al inicio del navegador para optimizar el rendimiento y acelerar los tiempos de carga de las páginas web. Esta línea de comandos muy probablemente se refiera a que el malware está buscando iniciar una sesión del navegador para después hacer consultas en la web sobre archivos para descargar. Este segundo proceso junto con el tercero se pueden visualizar en la Figura 54, siendo el tercero el que despierta dudas sobre su objetivo, ya que se accede a OneDrive.exe/background". Esto se refiere a la ubicación del archivo ejecutable 'OneDrive.exe' de Microsoft OneDrive en un sistema Windows, seguido del modificador '/background'. El comando está diseñado para iniciar la aplicación de Microsoft OneDrive en segundo plano al inicio del sistema, lo que permite que la aplicación se ejecute sin mostrar una ventana visible. Es posible que se use este ejecutable para verificar si el usuario tiene una cuenta de OneDrive con la cual respaldar sus archivos o quizás para robar sus credenciales de dicha plataforma. Los detalles de estos tres procesos hijos se resumen en el Cuadro 7.

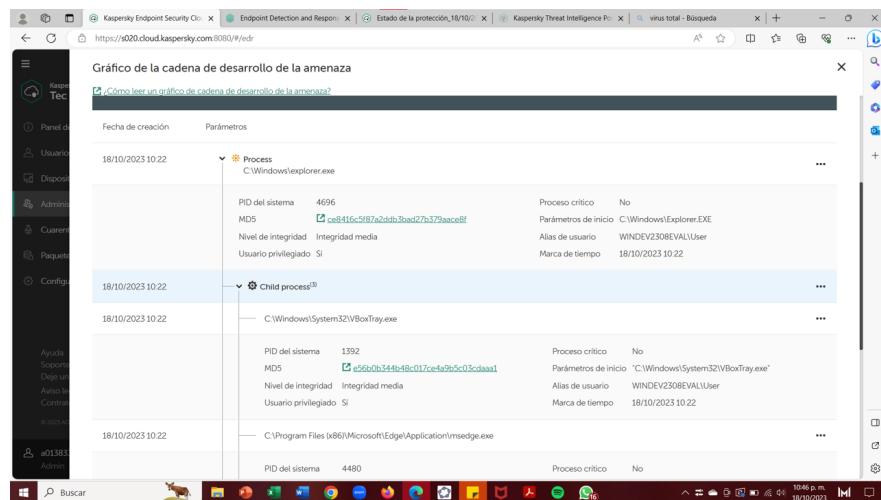


Figura 53: Captura del primer proceso hijo de la cadena de desarrollo del malware Dyre, donde se encuentra al archivo VBoxTray

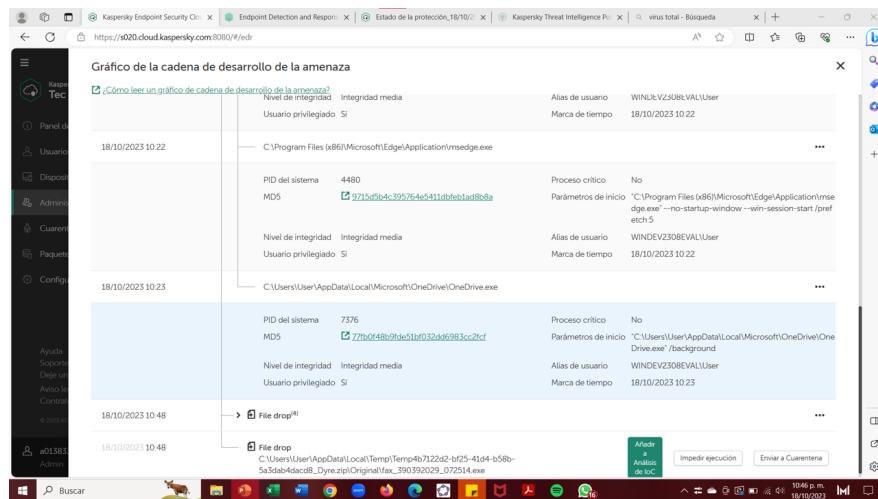


Figura 54: Captura del segundo y tercer proceso hijo de la cadena de desarrollo del malware Dyre

Parámetro	Número	Tipo	Crítico	Nivel de Integridad
C:\Windows\System32\VBoxTray.exe	2	Childrenprocess	No	Media
C:\ProgramFiles(x86)\Microsoft\Edge\Application\msedge.exe--no-startup-window--win-session-start/prefetch:5	2	Childrenprocess	No	Media
C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe/background	2	Childrenprocess	No	Media

Cuadro 7: Lista de procesos hijos

En paralelo a la ejecución de las líneas de comando anteriores, el malware Dyre también genera un proceso **File drop** con el cual carga cuatro archivos que contienen al código malicioso como tal (Figura 55). El origen de estos no parece ser de un equipo remoto, debido a que el agente de Kaspersky no señala ninguna IP remota, así que fueron instalados a partir de la descompresión del archivo ZIP original. Estos cuatro no parecen ser fiables, pero tampoco parecen ser ejecutados. Sus detalles aparecen en el Cuadro 8

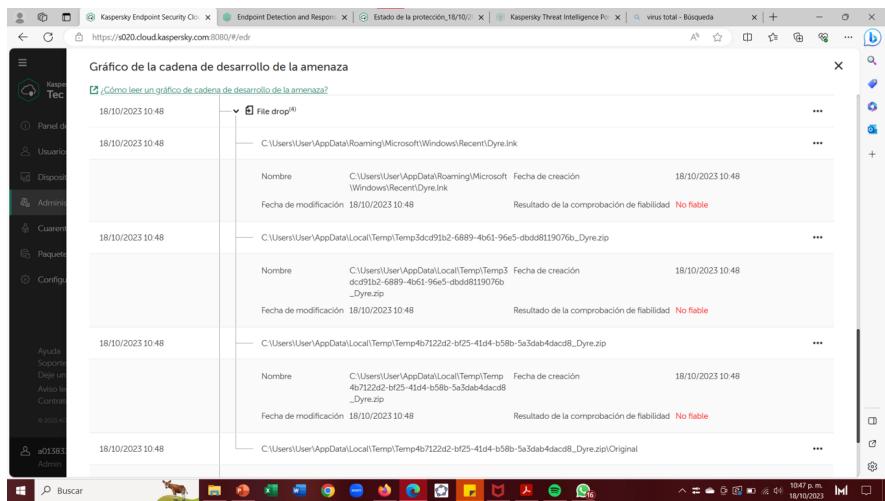


Figura 55: Lista con los archivos insertados en AppData por el malware Dyre

Parámetro	Número	Tipo	Resultado de la comprobación de fiabilidad	Hora de detección
File drop	4	Archivos	No confiable	18/10/2023 10:48

Rutas
<ul style="list-style-type: none"> ■ C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\Dyre.lnk ■ C:\Users\User\AppData\Local\Temp\Temp3dcd91b2-6889-4b61-96e5-dbdd8119076bDyre.zip ■ C:\Users\User\AppData\Local\Temp\Temp4b7122d2-bf25-41d4-b58b-5a3dab4dacd8Dyre.zip ■ C:\Users\User\AppData\Local\Temp\Temp4b7122d2-bf25-41d4-b58b-5a3dab4dacd8Dyre.zip\Original

Cuadro 8: Lista de rutas seguidas por el procesos File drop

Finalmente, en la cadena de desarrollo de la amenaza se selecciona un proceso 'File drop' separado dependiendo si fue tratado por su inminente peligro (Figura 56). En este caso, el archivo aparece con el nombre de **fax_390392029_072514.exe**, lo cual lo hace parecer un archivo inofensivo si es que se mandara por correo electrónico sin la extensión .exe. De hecho, este es el ejecutable que genera el mensaje de aviso visto en la metodología. Los indicadores de compromiso aparecen en el Cuadro 9, pero realmente se trata de un troyano que está robando la información, de acuerdo con los reportes de Kaspersky y virustotal.com (Figuras 57 y 58). No obstante, el agente antimalware lo detuvo antes de que pudiera robar información o

quizás no fue capaz de verificar las direcciones IP con las que se conectó. De cualquier manera, esta cadena de desarrollo de la amenaza añade mucho valor a la investigación de los procesos seguidos por el malware dentro de equipos de cómputo.

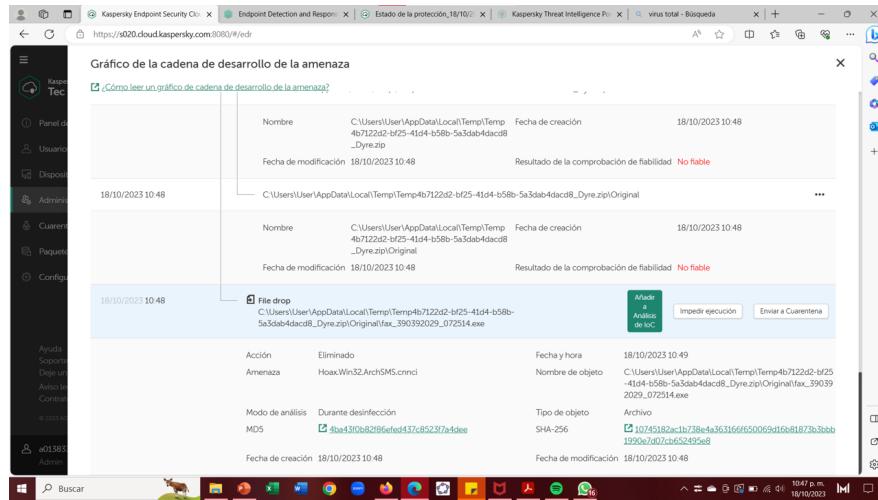


Figura 56: Captura de ejecutable visible del malware Dyre que es el final de la cadena de desarrollo de la amenaza según el análisis de Kaspersky

Nombre de objeto	Amenaza	Tipo	Acción	Hora de detección
C:...fax390392029_072514.exe	Hoax.Win32.ArchSMS.cnnci	Archivo	Eliminado	18/10/2023 10:48
Indicadores				
MD5	SHA-256			
4ba43f0b82f86efed437c8523f7a4dee	10745182ac1b738e4a363166f650069d16b81873b3bbb1990e7d07cb652495e8			

Cuadro 9: Indicadores de compromiso del malware Dyre

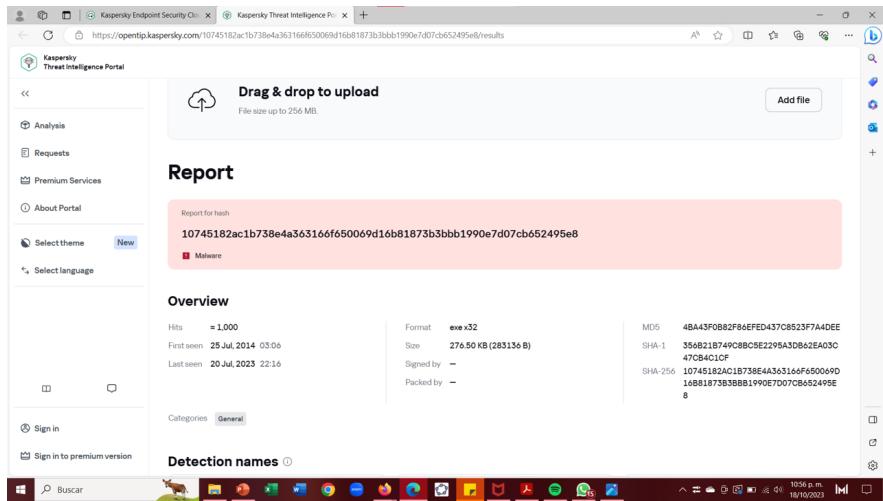


Figura 57: Búsqueda de información sobre el hash del código malicioso de Dyre Original en la base de datos de Kaspersky

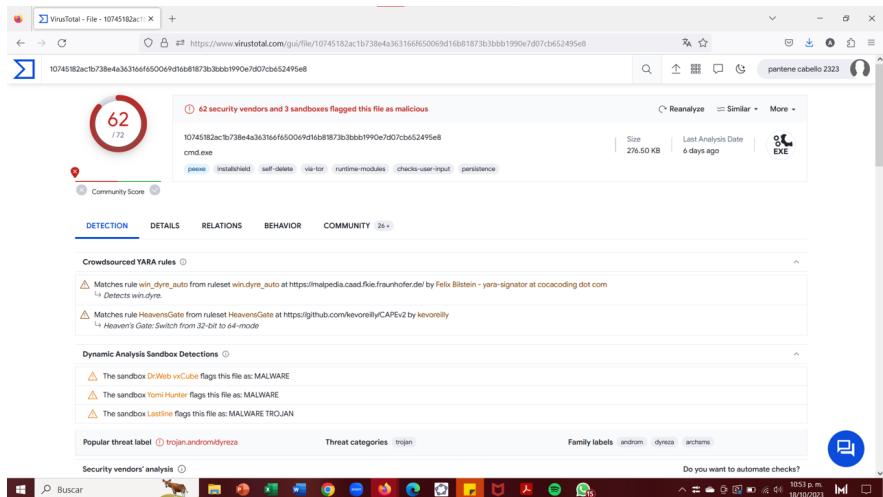


Figura 58: Búsqueda de información sobre el hash del código malicioso de Dyre Original en la base de datos de virustotal.com

Haciendo uso del análisis de los distintos casos de malware mediante la herramienta de Kaspersky y la página web de virustotal.com se logró consolidar la tabla comparativa del Cuadro 10, donde se observa que EICAR sobresale como el malware con más 'hits', principalmente debido a su naturaleza como una prueba de antivirus comúnmente utilizada. Por otro lado, se identifica que los malware IlusionBot y DyreOriginal, a pesar de tener un número limitado de 'hits', son de los más peligrosos en la actualidad, lo que subraya su capacidad para eludir detecciones y comprometer sistemas de forma sigilosa. Es importante destacar que el número de proveedores que detectan estos diferentes tipos de malware es relativamente similar, indicando que muchos de estos proveedores han actualizado sus sistemas para detectar una amplia gama de amenazas, considerando la prevalencia y persistencia de varios tipos de malware en el panorama de la seguridad cibernética.

Malware	# Hits	# Proveedores que lo detectan
EICAR	10,000,000	63
WannaCry	10,000	63
IllusionBot	1,000	64
AsproxOld	10,000	63
Dyre Original	1,000	62

Cuadro 10: Comparativa de registros de ataques de malware en distintas bases de datos de ciberseguridad

4.5.6. Conclusiones

La simulación del malware Dyre en un entorno virtual de Windows aislado ha puesto de manifiesto la sofisticación y el riesgo que representan las amenazas ciberneticas actuales. Esta prueba ha subrayado la capacidad de Dyre para eludir las medidas de seguridad convencionales y para comprometer la integridad de los datos confidenciales. Revela la importancia de una detección temprana y de una respuesta rápida ante posibles ataques de malware, así como la necesidad de implementar capas adicionales de seguridad, como firewalls avanzados y software de detección de intrusos, para mitigar el riesgo de infiltración. Además, resalta la importancia de la concienciación de los usuarios sobre las prácticas de seguridad cibernetica y el fomento de una cultura organizacional proactiva en cuanto a la protección de datos. La prueba del malware Dyre enfatiza la necesidad de una estrategia integral de seguridad cibernetica que abarque no solo medidas técnicas, sino también la educación y la capacitación continua del personal para hacer frente a las amenazas persistentes y en constante evolución.

4.5.7. Recomendaciones

- Mantener el software actualizado: Se recomienda mantener actualizado el software y el sistema operativo, incluyendo aplicaciones de terceros y parches de seguridad relevantes.
- Utilizar software de seguridad confiable: Se aconseja utilizar un software antivirus y antimalware confiable y actualizado, y realizar análisis periódicos para identificar posibles amenazas.
- Implementar soluciones de seguridad de red: Es fundamental implementar firewalls y soluciones de detección de intrusos avanzados para monitorear y controlar el tráfico de la red y prevenir posibles brechas de seguridad.
- Educar a los usuarios: Se recomienda proporcionar capacitación regular a los usuarios sobre prácticas de seguridad cibernetica, como verificar enlaces y archivos adjuntos antes de interactuar con ellos, y fomentar la concienciación sobre posibles riesgos, como el phishing y la ingeniería social.
- Establecer políticas de acceso: Se aconseja establecer políticas de acceso y privilegios adecuados para restringir el acceso a datos confidenciales y minimizar la exposición a posibles amenazas.

- Realizar copias de seguridad periódicas: Se sugiere realizar copias de seguridad regulares de los datos críticos en dispositivos externos o en la nube, y garantizar que las copias de seguridad sean fácilmente recuperables en caso de una intrusión de malware.
- Monitorear la actividad de red y sistema: Se aconseja monitorear de cerca la actividad de la red y del sistema en busca de comportamientos anormales o actividades sospechosas que puedan indicar una posible infiltración de malware.
- Implementar cifrado de datos: Se recomienda implementar soluciones de cifrado para proteger los datos confidenciales en caso de acceso no autorizado.

5. CONCLUSIONES

La evaluación de los códigos maliciosos EICAR, WannaCry, IlusionBot, AsproxOld y Dyre Original arrojó resultados valiosos en términos de su complejidad, nivel de riesgo y eficacia en la ejecución de acciones perjudiciales. Dyre Original destacó por su complejidad en el análisis. Desde la búsqueda de información hasta el análisis del historial del ataque, Dyre Original es un malware difícil de entender debido a la poca información que se encuentra disponible y a su comportamiento elusivo. Además, como este fue el único malware que generó una cadena, se tuvo que realizar un análisis exhaustivo para comprender lo que realizaba. En cuanto al nivel de peligrosidad, Dyre Original nuevamente se destacó como el más perjudicial. Este troyano bancario está diseñado específicamente para robar información financiera y datos sensibles, lo que lo convierte en una amenaza significativa para las víctimas. Dyre Original tiene la capacidad de registrar pulsaciones de teclas, suplantar sitios web y robar credenciales bancarias, lo que puede resultar en pérdidas económicas sustanciales y problemas de privacidad para quienes lo padecen. En términos de eficacia en la ejecución de acciones perjudiciales, IlusionBot se destacó por su rapidez y automatización. Este código malicioso se propaga con facilidad a través de sistemas vulnerables y redes locales, y su propagación automática puede infectar máquinas de manera rápida y efectiva. Sus ataques fueron exitosos debido a la explotación de una vulnerabilidad de Windows, y en cuestión de horas, logró afectar a un gran número de dispositivos, demostrando su capacidad para dañar rápidamente y de manera extensa. Por otro lado, EICAR fue el código malicioso que ejecutó menos pasos. Sin embargo, es importante destacar que EICAR no es un malware real, sino una prueba de detección utilizada para verificar la capacidad de los sistemas antivirus y antimalware. Su simplicidad radica en su propósito de ser detectado por las soluciones de seguridad como un archivo de prueba. Por lo tanto, su capacidad para dañar es nula.

La ciberseguridad es un imperativo en un mundo cada vez más digital. Para protegerse contra ataques cibernéticos, es fundamental mantener software y sistemas actualizados, utilizar software de seguridad confiable y capacitar a los empleados en buenas prácticas de ciberseguridad. La implementación de firewalls, copias de seguridad regulares y autenticación de dos factores añade capas adicionales de seguridad. Además, el monitoreo constante, la gestión de políticas de contraseñas sólidas y la elaboración de planes de respuesta a incidentes son esenciales. El control de acceso, evaluaciones de vulnerabilidades y cumplimiento legal son prácticas adicionales que refuerzan la ciberseguridad. Mantenerse actualizado con la educación y la formación en ciberseguridad es un proceso continuo. Estas acciones en conjunto reducen significativamente la exposición a las amenazas cibernéticas y protegen los datos y la información crítica.

REFERENCIAS

- Bigelow, Stephen J. (abr. de 2023). “Operating System (OS)”. En: *WhatIs.com*. URL: <https://www.techtarget.com/whatis/definition/operating-system-OS>.
- Cisco (2023). *What Is a Firewall?* <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>. Accessed: October 17, 2023.
- Ghafur, S. et al. (2019). “A retrospective impact analysis of the WannaCry cyberattack on the NHS”. En: *npj Digital Medicine* 2.1. DOI: 10.1038/s41746-019-0161-6.
- IBM (s.f.[a]). *¿Qué es el ransomware?* — IBM. URL: <https://www.ibm.com/mx-es/topics/ransomware>.
- (s.f.[b]). *What is malware?* — IBM. URL: <https://www.ibm.com/topics/malware>.
- Infosec Institute (s.f.). *Asprox / Kuluoz Botnet Analysis*. URL: <https://resources.infosecinstitute.com/topics/malware-analysis/asprox-kuluoz-botnet-analysis/>.
- IT Digital Media Group (mar. de 2021). *Cada día se producen en el mundo 350.000 ataques de malware*. URL: <https://www.itreseller.es/seguridad/2021/03/cada-dia-se-producen-en-el-mundo-350000-ataques-de-malware>.
- Ka1d (dic. de 2021). *Basic Malware Analysis — Illusion Bot*. URL: <https://nikhilh20.medium.com/basic-malware-analysis-illusion-bot-1fa30c20e086>.
- Kaspersky (2021). *Kaspersky Security Bulletin 2021*. URL: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_eng.pdf.
- (2023a). *About Kaspersky Endpoint Security Cloud*. <https://support.kaspersky.com/Cloud/1.0/en-US/123486.htm>. Accessed: October 17, 2023.
- (jul. de 2023b). *What is WannaCry Ransomware?* URL: <https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry>.
- (s.f.[a]). *About Kaspersky*. URL: <https://latam.kaspersky.com/about>.
- (s.f.[b]). *Kaspersky Threats — dyre*. URL: <https://threats.kaspersky.com/en/threat/Trojan-Banker.Win32.Dyre/>.
- kaspersky (oct. de 2023). *¿Qué es un troyano? - definición y explicación*. URL: <https://www.kaspersky.es/resource-center/threats/trojans>.
- (s.f.). *Acerca del virus de prueba EICAR*. URL: <https://support.kaspersky.com/KESS/3.0/es-MX/147734.htm>.
- Kaspersky Machine Learning for Anomaly Detection* (s.f.). <https://mlad.kaspersky.com/technologies/>. Accessed on October 17, 2023.
- Kujawa, A. (mayo de 2017). “WannaDecrypt your files? The WannaCry solution, for some”. En: URL: <https://www.malwarebytes.com/blog/news/2017/05/wannadecrypt-your-files>.
- Labs, Cyware (2019). *What is SMB vulnerability and how it was exploited to launch the WannaCry ransomware attack?* URL: <https://cyware.com/news/what-is-smb-vulnerability-and-how-it-was-exploited-to-launch-the-wannacry-ransomware-attack-c5a97c48>.

- Microsoft (s.f.). *What is a virtual machine and how does it work — Microsoft Azure*. URL: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine>.
- MiniTool (2021). *PCs with Windows 11 Pre-Installed Will Be Available Later in 2021*. URL: <https://www.minitool.com/news/pc-with-windows-11-preinstalled.html> (visitado 21-09-2023).
- Morgan, S. (2016). *Hackerpocalypse: A Cybercrime Revelation*. URL: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>.
- Netgate (2023). *Getting Started*. <https://www.pfsense.org/getting-started/>. Accessed: October 17, 2023.
- NHS Digital (2018). *Asprox Botnet*. URL: <https://digital.nhs.uk/cyber-alerts/2018/cc-2494>.
- Norton (2018). *What is a computer virus?* URL: <https://mx.norton.com/blog/malware/what-is-a-computer-virus>.
- (2021). *Norton Cyber Safety Insights Report 2021*. URL: <https://us.norton.com/internetsecurity-emerging-threats-cybersecurity-statistics.html>.
- Red Hat (2022). *What is a virtual machine?* <https://www.redhat.com/en/topics/virtualization/what-is-a-virtual-machine>. Accessed: October 17, 2023.
- Statcounter Global Stats (2023). *Desktop Operating System Market Share Worldwide*. <https://gs.statcounter.com/os-market-share/desktop/worldwide>. Accessed: October 17, 2023.
- Stone-Gross, B. y P. Khandhar (2014). *Dyre Banking Trojan threat analysis*. URL: <https://www.secureworks.com/research/dyre-banking-trojan>.
- usa.kaspersky.com (mayo de 2023). *How to get rid of malware?* URL: <https://usa.kaspersky.com/resource-center/threats/malware-protection>.