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 Ejecutivo

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 **2**

1.1. Problema . . . 2

1.2. Justificación . . . 3

1.3. Objetivo . . . 3

2. ANTECEDENTES **4**

2.1. Máquina virtual . . . 4

2.2. Sistema operativo . . . 4

2.3. Malware . . . 4

2.4. Virus informático . . . 4

2.5. Troyano . . . 5

2.6. Ransomware . . . 5

3. DESARROLLO **6**

3.1. Herramientas . . . 6

3.2. Kaspersky Endpoint Security Cloud . . . 6

3.3. EICAR . . . 7

3.4. WannaCry . . . 7

3.5. IllusionBot . . . 9

3.6. AsproxOld . . . 9

3.7. DyreOriginal . . . 10

4. RESULTADOS **11**

4.1. EICAR . . . 11

4.2. WannaCry . . . 11

4.3. IllusionBot . . . 12

4.4. AsproxOld . . . 12

4.5. Dyre Original . . . 13

4.6. Recomendaciones de seguridad . . . 14

5. CONCLUSIONES **17**

REFERENCIAS **18**

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 cibernéticas, 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 cibernéticos. 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 propósito de estas pruebas desde el punto de vista ejecutivo es analizar y mitigar las amenazas cibernéticas que pueden afectar a un usuario final. Estas pruebas permiten comprender cómo la herramienta se comporta frente a códigos maliciosos reales, lo que es esencial para garantizar la seguridad de la información y la integridad de los sistemas. Al estudiar el funcionamiento de estos códigos maliciosos, podemos identificar vulnerabilidades en los sistemas y fortalecer las defensas cibernéticas. Además, estas pruebas brindan información crítica para la toma de decisiones a nivel ejecutivo en cuanto a la inversión en herramientas de seguridad cibernética.

El alcance de las pruebas abarcó la simulación de situaciones realistas de ataques cibernéticos 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 cibernéticas. 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 cibernéticas 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 cibernéticas 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

En el proceso de evaluación de la seguridad cibernética, utilizamos una serie de herramientas clave que garantizaron un ambiente controlado y representativo de un entorno de usuario promedio. A continuación, se describen las herramientas más relevantes:

- **VirtualBox:** VirtualBox es una herramienta de virtualización que permite crear máquinas virtuales (VM) para ejecutar sistemas operativos y aplicaciones aislados del sistema anfitrión. Esta herramienta fue fundamental para crear un entorno virtual de pruebas, lo que nos permitió experimentar con diferentes configuraciones de software y sistemas operativos sin afectar nuestro entorno de producción. La instalación y configuración de VirtualBox fueron simples y se realizaron siguiendo los pasos recomendados en el sitio web oficial de Oracle (Red Hat 2022).

- **Sistema Operativo Windows 11:** Para emular el entorno de un usuario promedio en una computadora de escritorio, se utilizó una máquina virtual con el sistema operativo Windows 11. Dado que Windows es el sistema operativo más común en computadoras de escritorio, con una participación de mercado del 68 % (Statcounter Global Stats 2023), la elección de Windows 11 como sistema operativo virtual fue adecuada. La instalación de Windows 11 en la máquina virtual se realizó siguiendo las instrucciones del sitio web oficial de Microsoft (MiniTool 2021).

- **pfSense:** pfSense es un software de código abierto que proporciona funcionalidades de firewall y enrutamiento para crear un entorno de red seguro. Utilizamos pfSense para emular la conexión a Internet, lo que permitió que la máquina virtual de Windows se conectara a través de un router virtual y simular así una conexión a Internet segura. La configuración de pfSense se realizó siguiendo los pasos recomendados en el sitio web de pfSense (Netgate 2023).

3.2. Kaspersky Endpoint Security Cloud

Para llevar a cabo un análisis exhaustivo de códigos maliciosos y comportamientos anómalos, utilizamos Kaspersky Endpoint Security Cloud (KESC). Esta herramienta desempeñó un papel fundamental en la protección de dispositivos y la detección de amenazas. A continuación, destacamos las características clave de Kaspersky Endpoint Security Cloud:

- **Inteligencia Artificial (IA):** KESC utiliza modelos de aprendizaje supervisado (machine learning) para la detección de anomalías. Esto implica el análisis de datos de actividad en dispositivos supervisados para entrenar modelos capaces de predecir valores en ventanas de tiempo futuras. La detección de anomalías se basa en la comparación de valores observados con valores predichos, identificando discrepancias significativas como anomalías (*Kaspersky Machine Learning for Anomaly Detection* s.f.).

- **Base de Datos de Firmas de Código Malicioso:** Kaspersky cuenta con una extensa base de datos de firmas de código malicioso que permite la identificación y eliminación efectiva de amenazas conocidas

y previamente documentadas (Kaspersky 2023a).

- **Análisis Heurístico Avanzado:** Además de las firmas de código malicioso, KESC utiliza un análisis heurístico avanzado para detectar comportamientos inusuales y patrones desconocidos en tiempo real. Esto proporciona una defensa sólida contra amenazas conocidas y nuevas (usa.kaspersky.com 2023).

La instalación de Kaspersky Endpoint Security Cloud se realizó después de registrarse en el sitio web oficial de Kaspersky y descargar el instalador desde la consola de administración. El agente de seguridad se instaló en la máquina virtual de Windows, y se configuraron las políticas de seguridad desde la consola de administración en línea. Esta configuración permitió la supervisión de la seguridad de los dispositivos y la detección de amenazas. Se realizaron actualizaciones periódicas para mantener la protección actualizada (Kaspersky 2023a).

3.3. EICAR

Es un programa que fue creado por el Instituto Europeo de Investigación de Antivirus de Ordenadores, es utilizado para probar la efectividad de los programas de antimalware y la detección de malware. En sí mismo no es un malware, si no es una cadena de caracteres que está diseñado para parecerse a un malware, pero en realidad no tiene ninguna funcionalidad maliciosa. Se utiliza como un estándar para evaluar las funcionalidades de los programas de antivirus y su capacidad para detectar posibles amenazas. Algunas de las aplicaciones para las que se utiliza 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.

3.4. WannaCry

Es un ransomware, el cual se detectó por primera vez en el 2017. Se caracteriza por cifrar todos los archivos del usuario en el equipo infectado y prácticamente los deja inaccesibles. La particularidad de este malware es que pide un pago en Bitcoins para poder dar la llave de descifrado que es necesaria para recuperar los archivos. Cabe destacar que este malware es muy peligroso debido a su capacidad de escanear a los equipos en la red local y por un mecanismo de propagación automática puede llegar a infectar más equipos que estén dentro de la red. (Kaspersky 2023b).

El orden de lo que hace este ransomware en un equipo son:

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.

En el caso de que se cuente con un equipo sin una herramienta de protección o que, por otro lado, la herramienta se encuentre desactualizada, algunas de las posibles consecuencias que puede tener en una empresa son las siguientes:

- 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)

3.5. IllusionBot

Es un malware el cual se detectó por primera vez en abril del 2006, hace pasar por un bot de comercio, pero en realidad es un programa que roba información personal y puede dañar el equipo en donde se encuentre. Fue diseñado para operar de una manera sigilosa y perjudicial en sistemas informáticos. Además de que este malware usualmente se propaga por correos electrónicos, descargas de archivos adjuntos infectados y por explotación de vulnerabilidades de sistemas operativos. (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)

3.6. AsproxOld

Este malware fue detectado por primera vez en 2008, es más conocido bajo el nombre de 'Asprox' o W32/Asprox, es un malware que ha perdurado a lo largo de los años, está diseñado para robar información y la propagación de otros tipos de malware. Es un troyano; es decir, que se hace pasar por archivos legítimos para infiltrarse en el equipo. Usualmente, suele llegar al equipo mediante emails de phishing e inyecciones SQL a través de páginas web.

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)

3.7. DyreOriginal

Es un troyano que está diseñado para el robo de información financiera, como credenciales bancarias, tarjetas de crédito y detalles de la cuenta. Fue descubierto por primera vez en junio del 2014. Una particularidad de este malware es que no utiliza inyecciones web para modificar el contenido del navegador, lo que hace es que modifica el tráfico de su interés a sus propios servidores. Este malware se puede a llegar a propagar a través de otro malware llamado Upatre, el cual usualmente llega a los equipos por correos 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.

4. RESULTADOS

4.1. EICAR

El objetivo principal de esta evaluación fue determinar si Kaspersky puede detectar y neutralizar amenazas basadas en el archivo EICAR de manera eficiente. Se puede observar en la figura 1 que la herramienta lo detectó exitosamente y bloqueó los procesos del programa, en este caso al no tratarse de un 'malware' como tal, no tuvo consecuencias significativas en la máquina virtual desprotegida. No obstante, se puede ver en la figura 1 que la herramienta no desarrolló una cadena de desarrollo, por lo que no, nos es posible determinar lo que hace este programa con la herramienta de Kaspersky.

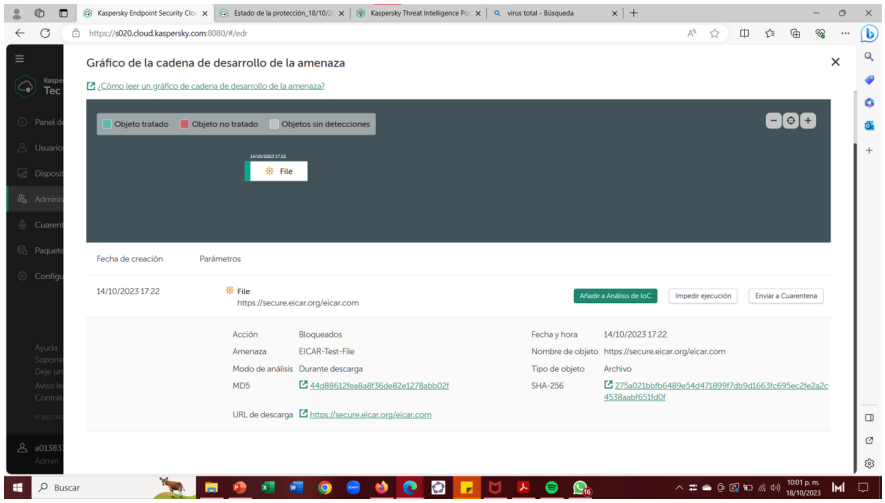

Figura 1: Captura del reporte de la consola de Kaspersky del código malicioso con terminación .com de la prueba EICAR

4.2. WannaCry

En el caso del ataque del malware llamado WannaCry, este resultó en la encriptación de una serie de archivos críticos en el entorno de la máquina virtual de Windows, utilizando la extensión .wncry y dejando los archivos como no utilizables, pidiendo a cambio una cuota de rescate de 300 dólares en bitcoin (tal como lo indicó la literatura). Afortunadamente, la rápida respuesta del software antivirus de Kaspersky logró contener el brote antes de que WannaCry pudiera propagarse como un gusano y expandirse a otras redes. Esta pronta acción limitó la capacidad del malware para propagarse aún más y evitar potenciales daños a gran escala. Sin embargo, la rápida respuesta también ha significado que una cadena de desarrollo completa sobre la ejecución del malware y su potencial de adaptación no ha sido completamente analizada, dejando preguntas sobre sus posibles capacidades de evasión y comportamientos futuros en entornos similares, en la Figura 2. De igual manera, hay que mencionar que en este caso la intervención del antivirus no fue del todo oportuna, puesto que, la eliminación del archivo ejecutable que hacía la labor de encriptar es un error si se desea revertir esta acción, puesto que, de acuerdo con Kujawa 2017 existen herramientas que pueden desencriptar de regreso los archivos afectados si no se borra ese ejecutable y si no se reinicia el equipo infectado.

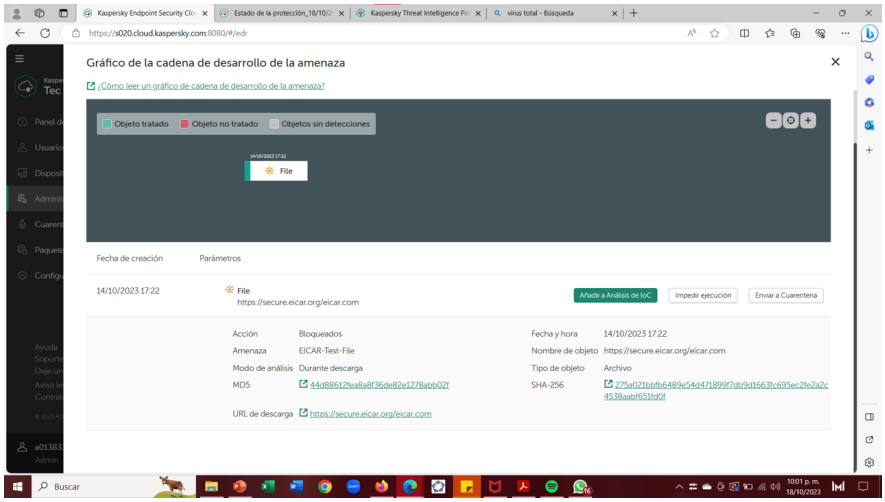

Figura 2: Captura del reporte de la consola de Kaspersky del código malicioso de WannaCry

4.3. IllusionBot

Una vez que se descomprimió la carpeta que contenía el malware, se corrió el ejecutable y se dejó por un par de minutos el equipo, el comportamiento del malware empezó a evolucionar teniendo varios procesos simultáneos. Los cuales se pudieron observar en el administrador de tareas de Windows. Sin embargo, una vez que se encendió la herramienta de Kaspersky, fue capaz de detectarla exitosamente y mató los procesos de este malware. Si bien la herramienta fue capaz de detectar y eliminar código malicioso, no desarrolló una cadena de desarrollo tal y como se puede observar en la Figura 3.

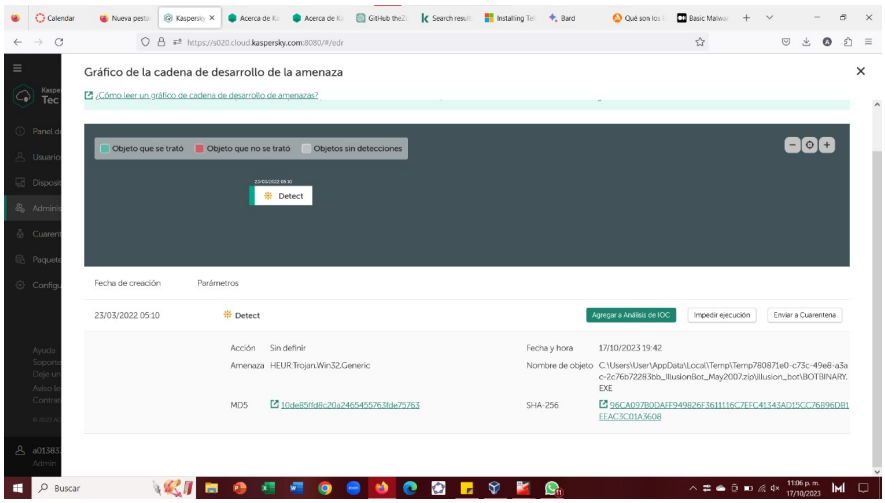

Figura 3: Captura del reporte de la consola de Kaspersky del código malicioso de IllusionBot

4.4. AsproxOld

El malware AsproxOld adoptó una táctica insidiosa al enviar un mensaje en formato .txt al escritorio de la máquina virtual, simulando un aparente error en la impresión de un boleto de avión, con la intención de

engañar al usuario mediante un posible intento de phishing. Mientras tanto, en segundo plano, este malware ejecutó un código malicioso en el administrador de tareas. Afortunadamente, la pronta intervención del agente antivirus de Kaspersky permitió una rápida supresión de la amenaza antes de que pudiera desarrollar una cadena completa de eventos. Aunque se contuvo la amenaza en cuestión, la ausencia de una cadena de desarrollo de la amenaza con detalles sobre lo acontecido, dejó interrogantes sobre las posibles intenciones y capacidades adicionales de este malware, como se puede ver en la Figura 4.

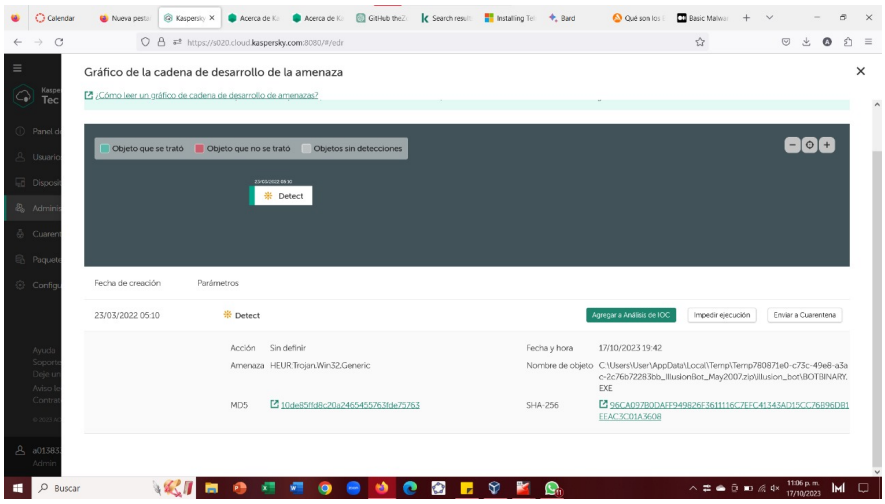

Figura 4: Captura del reporte de la consola de Kaspersky del código malicioso de AsproxOld

4.5. Dyre Original

La intervención en la VM del malware Dyre desplegó una serie de intentos de ejecutar múltiples comandos en la terminal de la Windows de la máquina virtual. Estos comandos incluían la identificación del entorno como virtual, lo que provocó ajustes en su comportamiento. Además, el malware abrió el navegador Edge para realizar búsquedas de archivos en la web y determinó la ubicación de la aplicación OneDrive con el objetivo de buscar posibles respaldos en el sistema. A pesar de estos esfuerzos, la oportuna intervención del antivirus de Kaspersky logró detener la ejecución del malware después de varios minutos. Sin embargo, este tiempo fue suficiente para generar una cadena de desarrollo de la amenaza detallada, lo que destaca la efectividad del software antimalware en términos de detección y respuesta proactiva a amenazas emergentes de este tipo, como se puede ver en la Figura 5.

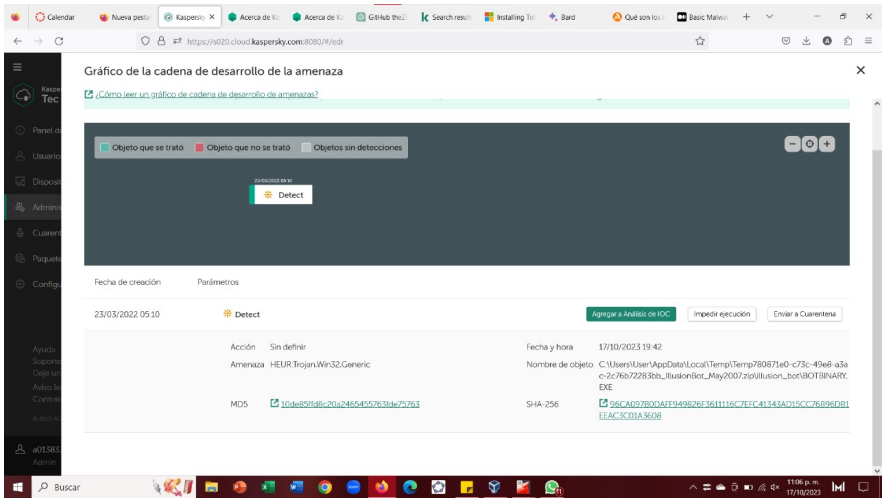

Figura 5: Captura del reporte de la consola de Kaspersky del código malicioso de Dyre Original

El análisis de múltiples casos de malware mediante la herramienta de Kaspersky y el sitio web de `virustotal.com` ha permitido resumir la información en una tabla comparativa (ver Cuadro 1). Se destaca que EICAR es el malware más detectado, posiblemente debido a su uso como una prueba estándar de antivirus. A pesar de tener un menor número de detecciones, se ha observado que el malware IlusionBot y DyreOriginal representan serias amenazas, dada su habilidad para eludir detecciones y comprometer sistemas de manera sigilosa. Además, se ha notado que un número similar de proveedores son capaces de detectar estos diferentes tipos de malware, lo que sugiere una mejora generalizada en los sistemas de detección para abordar la diversa gama de amenazas que existen 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 1: Comparativa de registros de ataques de malware en distintas bases de datos de ciberseguridad

4.6. Recomendaciones de seguridad

Los ciberdelincuentes emplean una amplia variedad de técnicas para robar datos, extorsionar a individuos y empresas, y comprometer la integridad de sistemas informáticos. Para protegerse contra estas amenazas, es fundamental implementar sólidas prácticas de seguridad cibernética. A continuación, presentamos 15 recomendaciones detalladas que pueden ayudar tanto a usuarios individuales como a empresas a fortalecer sus defensas contra el malware y otros ataques cibernéticos. Estas medidas no solo protegerán su información confidencial, sino que también pueden salvaguardar su reputación y su capacidad para llevar a cabo operaciones

comerciales sin problemas en un mundo cada vez más interconectado y digital.

- Mantener el software actualizado: Es crucial mantener el sistema operativo y todas las aplicaciones actualizados. Las actualizaciones a menudo corrigen vulnerabilidades que los ciberdelincuentes podrían explotar.
- Utilizar software antivirus confiable: Se debe instalar y mantener actualizado un software antivirus confiable con una base de datos de firmas actualizada.
- Educación sobre seguridad: Tanto en usuarios individuales como en empresas, es esencial capacitar al personal en las mejores prácticas de seguridad cibernética, como la identificación de correos electrónicos de phishing y enlaces sospechosos.
- Implementar firewalls: El uso de firewalls a nivel de red y en dispositivos individuales ayuda a filtrar y controlar el tráfico, lo que protege contra amenazas en línea.
- Autenticación de dos factores (2FA): Activar la autenticación de dos factores siempre que sea posible proporciona una capa adicional de seguridad al requerir una segunda forma de autenticación además de la contraseña.
- Ejecutar copias de seguridad regulares: Realizar copias de seguridad de datos con regularidad en un dispositivo o servidor que no esté directamente conectado a la red es fundamental para restaurar datos en caso de un ataque de ransomware.
- Cautela con los correos electrónicos y descargas: Se debe tener precaución al abrir correos electrónicos de remitentes desconocidos o con adjuntos sospechosos y evitar la descarga de archivos o clic en enlaces de fuentes no verificadas.
- Monitorear la actividad inusual: Tanto usuarios como empresas deben estar atentos a la actividad inusual en sus redes y sistemas, ya que los comportamientos sospechosos pueden indicar una posible infección.
- Seguridad en navegación web: Utilizar extensiones de navegadores y herramientas de seguridad para evitar la ejecución de scripts maliciosos y bloquear sitios web peligrosos.
- Segmentación de redes: En entornos empresariales, se debe implementar la segmentación de redes para aislar sistemas críticos y reducir la propagación de malware en caso de una infección.
- Política de contraseñas sólida: Establecer políticas de contraseñas sólidas que requieran contraseñas complejas y cambios regulares.
- Respuesta a incidentes: Tanto usuarios como empresas deben contar con planes de respuesta a incidentes que incluyan pasos claros para identificar, contener y mitigar amenazas.
- Cifrado de datos: Utilizar el cifrado de datos para proteger información sensible y confidencial, especialmente en dispositivos móviles y portátiles.

- Auditorías de seguridad regulares: Realizar auditorías de seguridad de manera regular para identificar y corregir vulnerabilidades en el entorno de TI.
- Colaboración con expertos en seguridad: En caso de un ataque cibernético, especialmente en entornos empresariales, buscar la ayuda de expertos en seguridad cibernética o empresas de respuesta a incidentes para contener y mitigar el impacto.

De igual manera, para el malware WannaCry, 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).

5. CONCLUSIONES

En la era digital en la que vivimos, la amenaza de los códigos maliciosos se cierne constantemente sobre individuos y organizaciones por igual. A través de un análisis profundo de ejemplos notorios como WannaCry, IllusionBot, AsproxOld y Dyre Original, se revela la magnitud de este peligro cibernético. Estos códigos maliciosos no son simples anomalías en el mundo digital; son armas sofisticadas que se aprovechan de las vulnerabilidades sistémicas, convirtiéndolas en amenazas reales para la ciberseguridad. Un patrón emergente es claro: la explotación de vulnerabilidades en sistemas cibernéticos es la puerta de entrada para estos códigos maliciosos. Ya sea explotando una vulnerabilidad en el protocolo SMB de Windows, como lo hizo WannaCry, o infiltrándose a través de vectores como el phishing, estos códigos encuentran fisuras en las defensas digitales y las explotan sin piedad. La ciberseguridad es, por tanto, una preocupación constante y una responsabilidad compartida.

Las consecuencias de una infección por códigos maliciosos pueden ser devastadoras. El robo de datos personales y financieros puede llevar a la pérdida de identidad y a la ruina financiera. La interrupción de operaciones comerciales puede resultar en pérdidas financieras significativas y daños a la reputación. Las ramificaciones legales y regulatorias también pueden ser un resultado no deseado. La prevención y la preparación son esenciales en la lucha contra estas amenazas. La defensa proactiva, que incluye la aplicación de políticas de seguridad cibernética sólidas y el uso de herramientas de seguridad actualizadas, es fundamental. La educación en seguridad cibernética y la conciencia sobre el phishing son prácticas esenciales que todos deben adoptar. La respuesta rápida a incidentes y la supervisión continua son elementos vitales en la ciberseguridad.

REFERENCIAS

Bigelow, Stephen J. (abr. de 2023). "Operating System (OS)". En: *WhatIs.com*. URL: https://www.techtarget.com/whatis/definition/operating-system-OS.

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.

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.

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.

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.

usa.kaspersky.com (mayo de 2023). *How to get rid of malware?* URL: https://usa.kaspersky.com/resource-center/threats/malware-protection.