



Instituto Tecnológico y de Estudios Superiores de Monterrey  
Escuela de Ingeniería y Ciencias

Ingeniería en Ciencias de Datos y Matemáticas

Aplicación de criptografía y seguridad (MA2005B.301)

# Kaspersky Endpoint Security Cloud Reporte Técnico

## **Equipo:**

Karla Andrea Palma Villanueva (A01754270)

Daniela Márquez Campos (A00833345)

Julio Eugenio Guevara Galván (A01704733)

Adrian Pineda Sánchez (A00834710)

David Fernando Armendáriz Torres (A01570813)

Kevin Antonio González Díaz (A01338316)

## **Docentes:**

Alberto F. Martínez y Oscar Labrada

## **Socio Formador:**

IPC Services

Monterrey, Nuevo León, México. 1 de diciembre 2023

# Índice

<b>1. Introducción</b>	<b>3</b>
<b>2. Desarrollo</b>	<b>4</b>
2.1. Entorno de Pruebas . . . . .	4
2.1.1. Instalación de VirtualBox . . . . .	4
2.1.2. Instalación de Windows . . . . .	4
2.2. Instalación de Pfsense . . . . .	5
2.3. Kaspersky Security Endpoint . . . . .	5
2.3.1. Creación y Configuración de una cuenta . . . . .	6
2.3.2. Creación y Configuración de la empresa . . . . .	7
2.3.3. Invitación de Usuarios y configuración de equipos y roles . . . . .	10
2.3.4. Configuración de los perfiles de Seguridad . . . . .	11
2.3.5. Instalación del agente de Karspersky en dispositivos y usuarios . . . . .	13
2.4. Códigos maliciosos . . . . .	13
2.4.1. Eicar . . . . .	13
2.4.2. MyDoom . . . . .	13
2.4.3. Satana . . . . .	14
2.4.4. DOUBLEFANTASY . . . . .	16
2.4.5. Vipasana . . . . .	16
<b>3. Resultados</b>	<b>18</b>
3.1. EICAR . . . . .	18
3.1.1. Origen de la Amenaza . . . . .	18
3.1.2. Desarrollo de la Amenaza . . . . .	18
3.1.3. Indicadores de Compromiso . . . . .	19
3.2. MyDoom . . . . .	20
3.2.1. Origen de la Amenaza . . . . .	20
3.2.2. Desarrollo de la Amenaza . . . . .	20
3.2.3. Indicadores de Compromiso . . . . .	21

3.3. Satana . . . . .	22
3.3.1. Origen de la Amenaza . . . . .	22
3.3.2. Desarrollo de la Amenaza . . . . .	22
3.3.3. Indicadores de Compromiso . . . . .	23
3.4. DOUBLEANTASY . . . . .	24
3.4.1. Origen de la Amenaza . . . . .	24
3.4.2. Desarrollo de la Amenaza . . . . .	25
3.4.3. Indicadores de Compromiso . . . . .	25
3.5. Vipasana . . . . .	26
3.5.1. Origen de la Amenaza . . . . .	26
3.5.2. Desarrollo de la Amenaza . . . . .	27
3.5.3. Indicadores de Compromiso . . . . .	28
<b>4. Recomendaciones</b>	<b>29</b>
<b>5. Conclusiones</b>	<b>30</b>
<b>Referencias</b>	<b>31</b>

# 1. Introducción

La ciberseguridad constituye una carrera constante y vertiginosa por desarrollar métodos que permitan la ejecución de ataques cibernéticos y paralelamente, por perfeccionar y renovar las estrategias con las que se enfrentan dichas agresiones. En ambos lados del espectro se trabaja por el avance en la efectividad de las herramientas que se emplean respectivamente. En el caso de la prevención, una de estas herramientas es Kaspersky Endpoint Security Cloud. El primer paso para poder perfeccionar algo es evaluarlo, por lo que con vista en la importancia de este proceso, se plantea como objetivo la valoración de los servicios provistos por la antes mencionada en materia de EDR por medio del uso controlado de amenazas cibernéticas conocidas que simultáneamente se estudiarán, en aras de obtener un entendimiento de las mismas, dado que todo peligro debe conocerse para poder enfrentarse. La ejecución controlada que se mencionaba se realizará gracias al uso de máquinas virtuales, las cuales permitirán un ambiente hermético y seguro por medio del cual se podrá evaluar la capacidad de la herramienta de Kaspersky para detectar los virus y anular los potenciales perjuicios causados por éstos. Como otro foco de atención de lo realizado, se analizarán las cadenas de desarrollo generadas por el servicio Cloud Based Endpoint Security de Kaspersky en su detección y detención o mitigación de malware para obtener un mejor entendimiento del comportamiento e implicaciones de este.

## 2. Desarrollo

### 2.1. Entorno de Pruebas

#### 2.1.1. Instalación de VirtualBox

Para poder realizar la experimentación con *malwares* de forma segura, se realizó la creación de un laboratorio de pruebas con máquinas virtuales a partir del *software Oracle VM VirtualBox*, el cual es un entorno para la ejecución de este tipo de máquinas. Esta herramienta se descargó a través de la liga <https://www.virtualbox.org/wiki/Downloads>. El respectivo archivo .zip fue extraído y se ejecutaron las acciones pertinentes para iniciar el funcionamiento del programa.

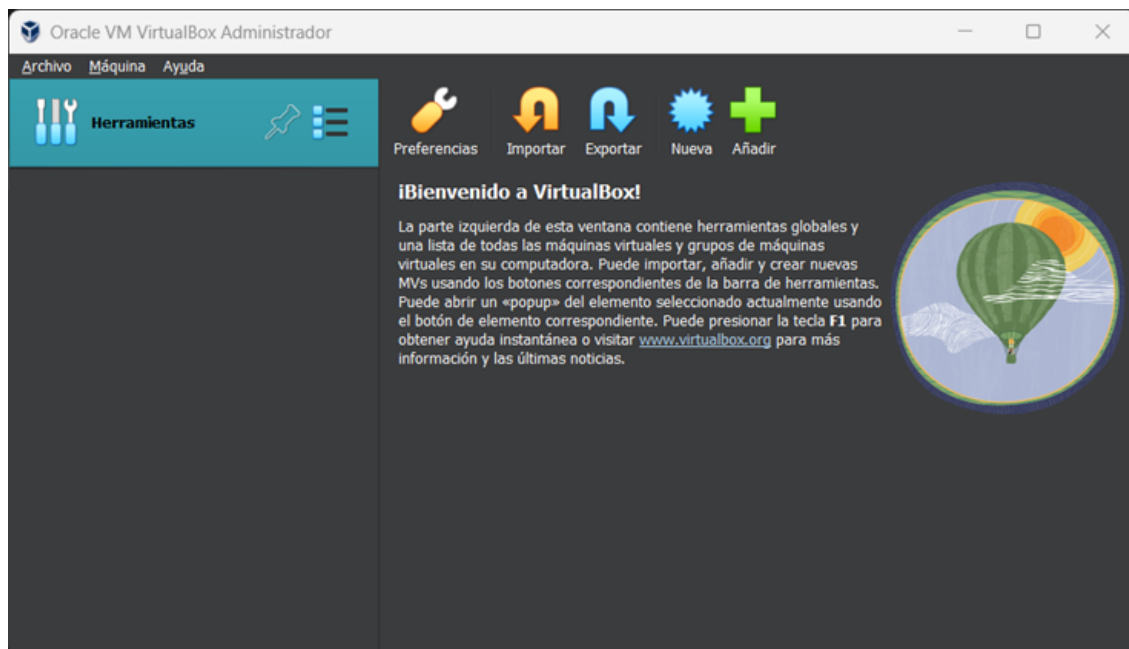


Figura 1: Captura de pantalla de la aplicación inicializada

#### 2.1.2. Instalación de Windows

La imagen de Windows para VirtualBox se instaló siguiendo estos pasos:

Después de descomprimir el archivo descargado de <https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/>, se eligió la opción “Importar servicio virtualizado” en en *VirtualBox*. Luego, se hace clic en “Continuar” y se configura con los valores

predeterminados.

Es importante destacar que esta imagen no cuenta con una contraseña y se ajustó la asignación de memoria a 6 GB. La imagen instalada es Windows 11 Enterprise Evaluation 22H2.

Este proceso se repitió 3 veces para generar múltiples instancias de las maquina virtuales, el motivo de este curso de acción es el de ejecutar aquellos malware mas riesgosos, en este caso los dos ransomwares, de manera aislada para evitar peridad de información o interferencia en las cadenas de desarrollo de los otros virus.

## **2.2. Instalación de Pfsense**

Con la intención de implementar una red interna para prevenir propagación lateral a otros dispositivos en la misma red, se instalo y configuró el software Pfsense como se indica a continuación.

De primera forma se creó una máquina virtual llamada "pfSenseTest" con la imagen ISO "pfSense-CE-2.6.0-RELEASE-amd64.iso", configurada como BSD con FreeBSD de 64 bits, 1024 MB de memoria y un disco duro virtual de 6 GB. Luego, se configuró el adaptador de red 1 en modo NAT. Después, se inició la máquina virtual y se procedió con la instalación estándar del pfSense. Una vez completada la instalación, se eliminó la imagen ISO del almacenamiento de la máquina virtual. Posteriormente, se apagó la máquina virtual y se creó una red de prueba llamada RedPruebaInternaTest con el adaptador 2 configurado como Red Interna. Al reiniciar la máquina virtual y acceder a la terminal, se utilizó el comando `ifconfig` para identificar la dirección IP asignada a la interfaz de red del pfSense.

## **2.3. Kaspersky Security Endpoint**

Kaspersky Endpoint Security for Windows representa una solución de vanguardia diseñada para contrarrestar las amenazas persistentes que afectan a los entornos empresariales basados en sistemas operativos Windows. La prevalencia de este sistema operativo lo convierte en un objetivo constante para los ciberdelincuentes, a pesar de las medidas de seguridad integradas que ofrece [6].

Esta aplicación ha recibido reconocimiento por ser una de las más probadas y galardonadas en su categoría, gracias a su capacidad para proteger cada dispositivo Windows y los datos sensibles que albergan. Emplea un enfoque multicapa que combina tecnologías avanzadas con funciones proactivas como controles de dispositivos, aplicaciones y web, gestión de vulnerabilidades y cifrado de datos. Estas características se integran en un agente de endpoints con archivos EDR, respaldado por un conjunto completo de herramientas de administración de sistemas [6].

Las ventajas clave de esta solución son evidentes: protege los activos más críticos de las empresas, garantiza la eficiencia y simplicidad en su implementación y gestión a través de una consola unificada con políticas centralizadas. Además, su efectividad ha sido rigurosamente probada en evaluaciones independientes, validando su fiabilidad. Kaspersky Endpoint Security for Windows se destaca por su estrategia de desarrollo interno, enfocada en proporcionar integración e innovación reales, adaptándose a las infraestructuras preexistentes de las empresas [6].

### 2.3.1. Creación y Configuración de una cuenta

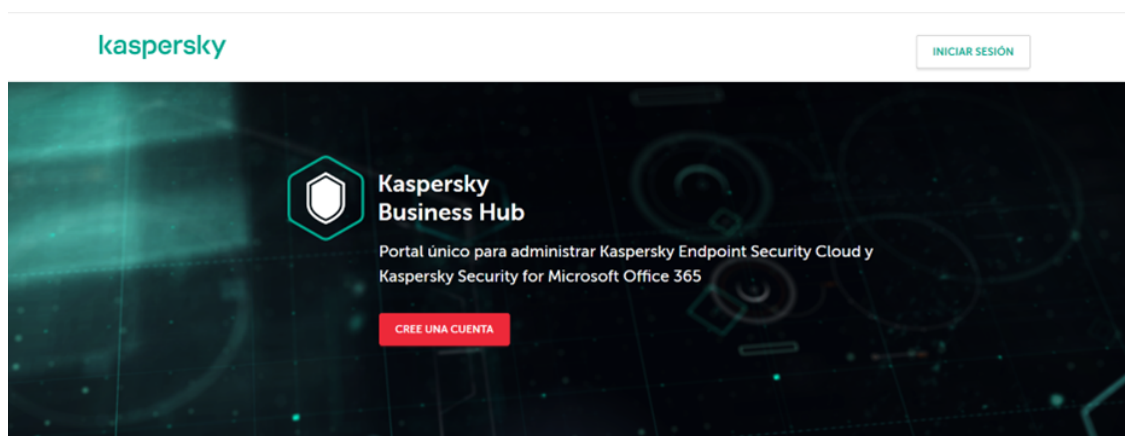


Figura 2: Pagina de inicio creación de cuenta Kaspersky Endpoint Security Cloud

Para crear una cuenta en Kaspersky, se accede al sitio web oficial de la plataforma en Kaspersky Endpoint Security. Se busca la sección de registro o creación de cuenta, donde

generalmente se encuentra un botón específico para crear una cuenta nueva.

Una única cuenta para acceder a las soluciones empresariales de Kaspersky

Iniciar sesión

Cree una única cuenta para acceder a las soluciones empresariales de Kaspersky

Introduzca su dirección de correo electrónico actual. Le enviaremos un enlace para activar su cuenta a esa dirección.

Dirección de correo electrónico

Cree e introduzca una contraseña segura para su nueva cuenta. La contraseña debe cumplir con los siguientes requisitos de seguridad:

- Como mínimo 8 caracteres
- Letras mayúsculas y minúsculas
- Número
- Todos los símbolos son válidos

Contraseña

Vuelva a escribir la contraseña

- Las contraseñas coinciden

☐ Entiendo y acepto que mis datos se gestionen y transmitan (incluso a otros países) conforme se describe en la [Política de privacidad](#). Confirmando que he leído y entendido en su totalidad la [Política de privacidad](#).

Para continuar, debe confirmar que acepta la Política de privacidad

Crear cuenta

Figura 3: Llenado de datos para cuenta Kaspersky Endpoint Security Cloud

Una vez allí, se rellena el formulario de registro con datos básicos como nombre, dirección de correo electrónico y contraseña, asegurándose de proporcionar información precisa y válida. Posteriormente, es posible que se te pida verificar tu dirección de correo electrónico mediante un enlace de confirmación que será enviado a la dirección proporcionada. Se deben seguir las instrucciones incluidas en el correo electrónico para completar el proceso de verificación de la cuenta.

### 2.3.2. Creación y Configuración de la empresa

A través de la creación de la primera cuenta de usuario en Kaspersky Endpoint Security Cloud, se prosigue con la creación de la empresa en el entorno, iniciando con el paso 1, que será la utilización del software, en la cual seleccionaremos: **Kaspersky Endpoint Security Cloud** y proseguiremos con los pasos posteriores de la configuración de la empresa.



#### Paso 01: Seleccione una solución de software

Seleccione la solución de software que desea utilizar.

#### Soluciones de software excelentes administradas desde una única consola

Estas soluciones son la manera más fácil de proteger su negocio sin sacrificar recursos de TI, tiempo ni presupuesto. Están listas para usar y cuentan con la configuración de protección recomendada por los expertos de Kaspersky previamente configurada.

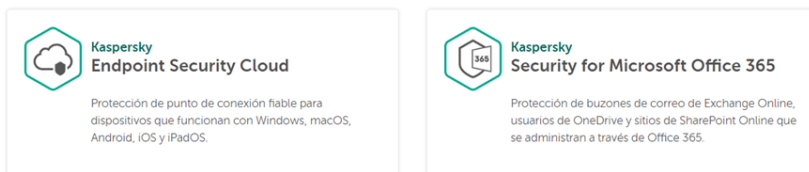


Figura 4: Paso 1 Selección del software Kaspersky Endpoint Security Cloud

El paso 2 simplemente consiste en el llenado y firmado de las condiciones de uso en torno a las políticas de Kaspersky Endpoint Security Cloud.

#### Paso 02: Condiciones de uso de Kaspersky Endpoint Security Cloud

Lea con atención y acepte los términos y condiciones de los documentos legales en la ventana de abajo: [Contrato](#) y [Contrato de procesamiento de datos](#).

De lo contrario, no podrá utilizar Kaspersky Endpoint Security Cloud.

vigor cuando hace clic en el botón "Acepto" o marca la casilla que indica su aceptación de estos términos.

Si hay un acuerdo independiente entre Kaspersky y Usted, o entre Usted y el socio autorizado correspondiente de Kaspersky ("Socio"), y dicho acuerdo ("Acuerdo independiente") entre Kaspersky o un Socio y Usted entra en conflicto con cualquier disposición de este Contrato, tendrá prioridad dicho Acuerdo independiente.

**SECCIÓN A: TÉRMINOS GENERALES**

**1. Descripción general del producto**

Kaspersky Endpoint Security Cloud es una solución de software para la administración centralizada y la protección de equipos y dispositivos móviles que controle el Usuario.

En concreto, el uso de Kaspersky Endpoint Security Cloud permite al Usuario:

- instalar y actualizar el software de punto final de Kaspersky ("Software administrado") de forma centralizada en los equipos y dispositivos móviles de la empresa que estén conectados a Kaspersky Endpoint Security Cloud ("Dispositivos administrados");
- administrar la configuración de Dispositivos administrados y la protección de los dispositivos mediante perfiles de

☐ Confirmando que he leído, entendido y acepto en su totalidad los términos y las condiciones del [Contrato de Kaspersky Endpoint Security Cloud](#)

☐ Confirmando que he leído, entendido y acepto en su totalidad los términos y las condiciones del [Contrato de procesamiento de datos de Kaspersky Endpoint Security Cloud](#) ([Descargar](#))

Figura 5: Llenado de datos para cuenta Kaspersky Endpoint Security Cloud

Finalmente terminamos con la configuración de la empresa en torno a llenar el formulario con la información requerida, como detalles de la empresa, la dirección de correo electrónico de contacto, así como desde el inicio se ingreso el nombre de usuario y la contraseña para la cuenta de administrador desde el paso 1 (la persona que crea y configura este entorno de trabajo).

### Paso 03: Información del espacio de trabajo

Rellene todos los campos obligatorios para que podamos optimizar su experiencia con nuestra solución de software.

#### Crear una empresa

Introduzca la información sobre la nueva empresa que desea administrar

Nombre de su empresa\*

Tecnologico

País\*

México

Número de dispositivos\*

40

Descripción adicional de la empresa

Puede resultar útil si tiene más de un espacio de trabajo en Kaspersky Business Hub.



ATRÁS

SIGUIENTE

Figura 6: Llenado de datos para cuenta Kaspersky Endpoint Security Cloud

Al terminar estos 3 pasos, deberíamos visualizar un entorno similar al siguiente, en donde se despliega el nombre de la empresa y características de la configuración establecida en torno al número de miembros, equipos máximo, etc. Donde podremos dirigirnos al hipervínculo de **ir al espacio de trabajo**, para terminar de configurar nuestro entorno en la invitación de usuarios.

Figura 7: Llenado de datos para cuenta Kaspersky Endpoint Security Cloud

### 2.3.3. Invitación de Usuarios y configuración de equipos y roles

Posterior a ello, direccionalaremos hacia la pestaña en la parte izquierda en la sección de **Usuarios**, en dicha sección encontraremos el entorno para la creación de nuestros equipos de trabajo donde a través de la creación de un equipo, podemos iniciar la invitación vía e-mail en el botón de **Añadir usuarios a grupo** de los usuarios, así poder designar o modificar sus roles y por ende sus privilegios en el espacio de trabajo de Kaspersky.

Mostrar usuarios: Todos (6) ❗ [Crítico \(0\)](#) ⚠️ [Advertencia \(0\)](#) ✅ [Aceptar \(1\)](#) ❓ [Todavía no hay datos \(5\)](#) 🔍 Buscar

<span>👤 Añadir usuarios a grupo</span> <span>✎ Modificar</span> <span>🔄 Mover al grupo</span> <span>✉ Enviar instrucciones</span> <span>✖ Eliminar</span>						
<input type="checkbox"/>	Estado	Usuario/grupo	Número de dispositivos	Comentario	Derechos de acceso	Perfil de seguridad
<input type="checkbox"/>	❓	<a href="#">A00833345</a> A00833345@tec.mx	-		<span style="background-color: red; color: white;">Admin</span>	David
<input type="checkbox"/>	❓	<a href="#">A00834710</a> A00834710@tec.mx	-		<span style="background-color: red; color: white;">Admin</span>	David
<input type="checkbox"/>	❓	<a href="#">A01338316</a> A01338316@tec.mx	-		<span style="background-color: red; color: white;">Admin</span>	David
<input type="checkbox"/>	✅	<a href="#">A01570813</a> A01570813@tec.mx	4		<span style="background-color: red; color: white;">Admin</span>	David

Figura 8: Grupo de trabajo en el espacio de trabajo de Karspersky

Posterior a ese paso, y después de seleccionar el botón de añadir usuarios, podemos observar una ventana similar a la siguiente donde se introducirán todos los usuarios pertenecientes al grupo y que dándoles permisos de administrador en la configuración anterior podrán editar el entorno de karspersky con los mismos privilegios que el **administrador** principal creador del espacio de trabajo.



Figura 9: Invitación de usuarios vía e-mail

#### 2.3.4. Configuración de los perfiles de Seguridad

En la consola de Karspersky en el entorno de la pestaña **administración de seguridad**, en la sección de **perfiles de seguridad**, proseguimos a la configuración del o los perfiles pertenecientes a los dispositivos donde se estarán ejecutando la cadena de procesos y la evaluación de códigos maliciosos, en este entorno en la sección de **Configuración de Seguridad** podremos encontrar un catalogo de las múltiples acciones que podremos realizar en la configuración y protección de nuestro entorno, por ejemplo la protección contra archivos, correos maliciosos, sitios web, y redes, estas dos ultimas pertenecientes a las secciones **Protección frente a amenazas web** y **Protección frente a amenazas en la red**.

## Configuración del perfil de seguridad "David"

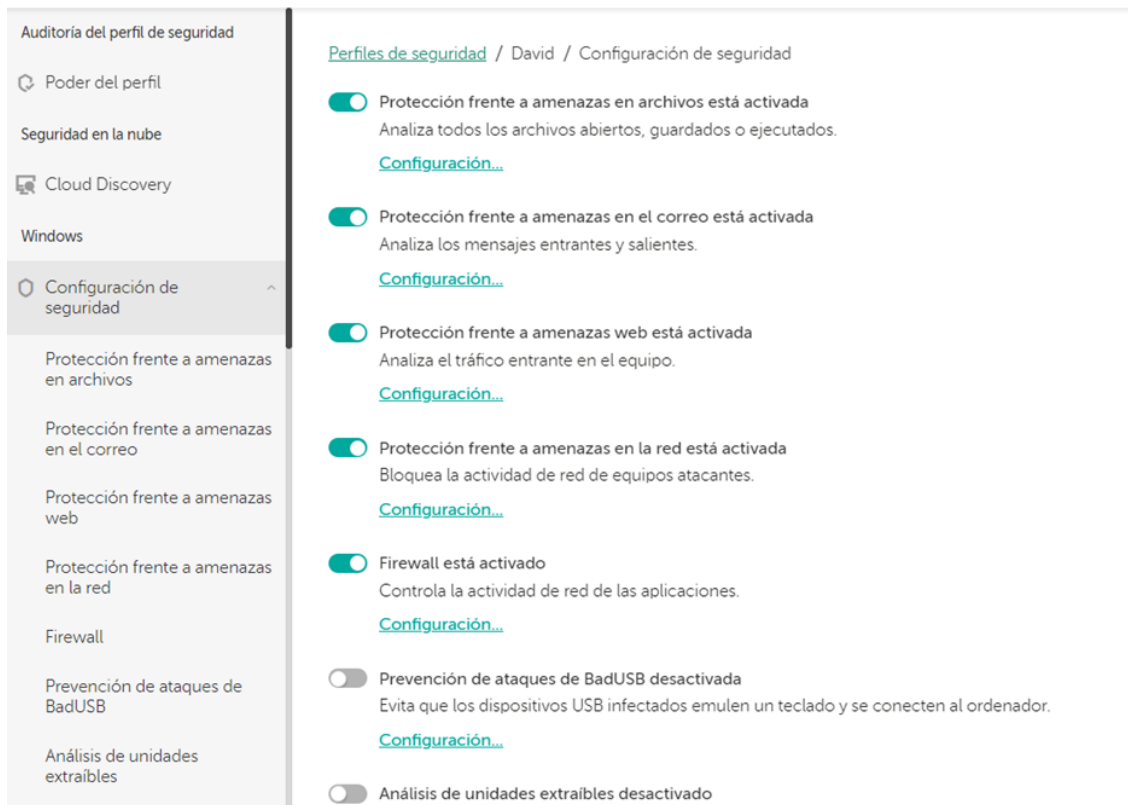


Figura 10: Configuración de Seguridad en el entorno de Perfil de Seguridad

En estas secciones podremos modificar y seleccionar las direcciones de sitios web como los repositorios de las direcciones web donde encontraremos los condigos maliciosos, e integrar tanto para el perfil **Predeterminado** o en este caso uno especifico como lo es **David**.



Figura 11: Sección de Protección frente amenazas web

### 2.3.5. Instalación del agente de Kaspersky en dispositivos y usuarios

Después de la finalización de la configuración de los perfiles de seguridad y en el entorno donde no se disponga de algún antivirus, procedemos a obtener el paquete de instalación desde la **consola de Kaspersky para Windows**, disponible en la sección de **Paquetes de distribución**. También es posible instalarlo mediante el enlace recibido por correo, el cual invita a unirse al espacio de trabajo.

La instalación puede ser predeterminada para todos los usuarios o seleccionando los usuarios donde esto se ejecutara para la instalación, esto permite visualizar todas las amenazas registradas y su cadena de procesos en cada dispositivo utilizado a través de la sección de **Endpoint Detection and Response** dentro de la **Administración de seguridad**.

La instalación se realizó en cada una de las instancias de las maquinas virtuales.

## 2.4. Códigos maliciosos

De acuerdo con la propia Kaspersky, “el código malicioso está diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos” (Kaspersky, s. f.). Con el objetivo de poner a prueba el antivirus, se bajaron desde el repositorio de GitHub de un proyecto para el análisis de malware llamado theZoo, y fueron los siguientes:

### 2.4.1. Eicar

Eicar: código diseñado para poner a prueba antivirus, ya que si bien no ejecuta ninguna acción en el dispositivo, suele ser detectado como amenaza. Fuente: Sitio oficial de EICAR <https://www.eicar.org/download-anti-malware-testfile/>

### 2.4.2. MyDoom

MyDoom: un gusano (un *malware* autónomo, que después de haber alcanzado un sistema, tiene la capacidad de iniciar su propagación de inmediato, sin necesidad de interactuar con

el usuario), que abre dos *backdoors* en el dispositivo, permitiendo el acceso remoto a los ordenadores infectados. Causó pérdidas de 59,000 millones de dólares, empleando técnicas muy efectivas de *social engineering* para impulsar su proliferación.[7] Fuente: Repositorio Github theZoo <https://github.com/ytisf/theZoo>

## Modus Operandi

- **Propagación a través del correo electrónico:** Mydoom se propagaba enviando correos electrónicos infectados a direcciones de correo electrónico obtenidas de los archivos locales de la víctima. Los correos electrónicos incluían un archivo adjunto malicioso que, al abrirse, ejecutaba el código del gusano en el sistema de la víctima.
- **Ingeniería social:** El gusano se disfrazaba como un mensaje legítimo o urgente, a menudo con asuntos llamativos o engañosos para incitar a los usuarios a abrir el archivo adjunto.
- **Ataques DDoS:** Mydoom estaba programado para lanzar ataques de denegación de servicio distribuido (DDoS) contra sitios web específicos en fechas predeterminadas. Estos ataques podían abrumar los servidores y causar interrupciones masivas.
- **Puerta trasera:** Una vez infectado un sistema, Mydoom abría una puerta trasera que permitía a los atacantes controlar de forma remota el equipo infectado. Esto podía utilizarse para llevar a cabo otros ataques o para robar información.
- **Suplantación de direcciones IP:** El gusano intentaba ocultar su origen al suplantar direcciones IP, dificultando su rastreo y mitigación.

### 2.4.3. Satana

Satana: un troyano que encripta los archivos y daña el Registro de Arranque Principal (MBR, por sus siglas en inglés), impidiendo de esta manera el inicio normal de Windows. Gracias a esto, se produce un *ransomware*, en el cual, el medio de contacto es una dirección de correo que se añade al principio de los nombres de los archivos encriptados.[10] Repositorio

## Modus Operandi

- **Infección inicial:** Satana suele infiltrarse en los sistemas a través de vectores de ataque comunes, como correos electrónicos de phishing, kits de explotación, puertas traseras o vulnerabilidades de software no parcheadas. Puede usar exploits para obtener acceso inicial al sistema objetivo.
- **Encriptación de archivos:** Una vez dentro, Satana emplea algoritmos de cifrado fuertes como AES (Advanced Encryption Standard) para encriptar los archivos del sistema. Esto se realiza para bloquear el acceso a los datos y evitar que el usuario acceda a su contenido sin la clave de descifrado.
- **Alteración del MBR o tabla de particiones:** Además de la encriptación de archivos, Satana modifica el Registro Maestro de Arranque (MBR) o la tabla de particiones del disco duro. Esto puede hacer que el sistema sea inarrancable o mostrar mensajes maliciosos al iniciar el sistema operativo, aumentando el impacto y la dificultad de recuperación.
- **Ausencia de instrucciones para el rescate:** A diferencia de otros ransomware, Satana no siempre proporciona instrucciones claras sobre cómo contactar al atacante o realizar el pago del rescate. Esta ausencia de instrucciones dificulta que las víctimas se comuniquen con los atacantes y posiblemente recuperen los datos, lo que lleva a una situación más desafiante.
- **Escaso enfoque en la negociación:** Satana tiende a enfocarse más en la destrucción y el bloqueo permanente de datos, en lugar de ofrecer una ruta de negociación para recuperar la información. Esto hace que la recuperación sea más difícil, incluso si las víctimas están dispuestas a pagar un rescate.



#### 2.4.4. DOUBLEFANTASY

DOUBLEFANTASY: fue creado por *Equation Group* un sofisticado actor de amenaza. Es un troyano que se emplea en ataques específicamente dirigidos a empresas y organizaciones. Su propósito es recopilar información esencial del dispositivo, la cual se transfiere al servidor de mando y control (C&C). Al recibir esta información, los atacantes determinan si el sistema infectado es relevante para sus objetivos y, si así lo desean, pueden introducir *malware* adicional en el sistema, particularmente ataques como GRAYFISH o EQUATIONDRUG, también desarrollados por *Equation Group*. [8] Repositorio Github theZoo <https://github.com/ytisf/theZoo>.

##### Modus Operandi

- **Objetivo y funcionamiento inicial:** Este código dañino tiene como objetivo principal recopilar información básica del equipo infectado. Esta información se envía a un servidor de mando y control (C&C). Los atacantes utilizan esta información para identificar si el sistema infectado es de interés para sus objetivos. [9]
- **Identificación y posible carga adicional:** Una vez que los atacantes analizan la información recopilada del sistema infectado, determinan si desean llevar a cabo acciones adicionales. Esto podría incluir cargar *malware* adicional en el sistema infectado si consideran que puede ser beneficioso para sus objetivos. [9]

#### 2.4.5. Vipasana

Vipasana: un virus innovador que encripta los datos de la víctima mediante una llave pública que el mismo *malware* ya tiene integrada, por lo que no necesita de conexión a internet para realizar este proceso. Con esto, se abre la posibilidad de realizar un *ransomware*. Repositorio Github theZoo <https://github.com/ytisf/theZoo>

- **Propagación y métodos de infección:** Vipasana se propaga a través de bots de spam que envían correos electrónicos maliciosos a cuentas de correo. Estos correos pueden contener enlaces o archivos adjuntos maliciosos disfrazados como documentos importantes o enlaces a sitios web relevantes, que al ser activados infectan el sistema. [11]

- **Funcionamiento de la encriptación:** Una vez que Vipasana infecta el sistema, utiliza un algoritmo de cifrado sofisticado (AES) para bloquear los archivos, incluso cuando el dispositivo está offline. Cambia el nombre de los archivos cifrados agregando una extensión complicada y muestra una nota de rescate en forma de fondo de pantalla.[11]
- **Contacto con los atacantes:** La nota de rescate proporciona una dirección de correo electrónico (vipasana@aol.com) a la que las víctimas deben escribir para obtener instrucciones sobre cómo pagar el rescate. El tamaño del rescate no se revela hasta que las víctimas contactan a los atacantes, quienes exigen una comunicación en una semana.[11]

### 3. Resultados

A continuación se presenta un análisis de las cadenas de desarrollo generado por el servicio EDR sobre las 5 piezas de malware seleccionadas.

#### 3.1. EICAR



##### 3.1.1. Origen de la Amenaza

Origen de la amenaza detectada con Kaspersky Endpoint Security Cloud EDR:

Parámetro de Inicio	Tipo	PID del Sistema 3	Crítico	Nivel de Integridad
C:\Windows\Explorer.EXE	Proceso	5036	No	Media

Usuario	Fecha	Hora
WINDEV2310EVAL\User	11/29/2023	15:19

Process C:\Windows\explorer.exe				...	
System PID	5036	Critical process	No		
MD5	<a href="#">c8a00f2fd7f7a580a8638e8a08270dd3</a>	Startup parameters	C:\Windows\Explorer.EXE		
Integrity level	Medium integrity	User alias	WINDEV2310EVAL\User		
Privileged user	Yes	Timestamp	11/29/2023 3:13 pm		

##### 3.1.2. Desarrollo de la Amenaza

Del diagrama desplegado se identifican 4 *child processes*, los cuales corresponden a la ejecución legítima de las aplicaciones de VirtualBox, Microsoft Edge y OneDrive.

- C:\Windows\System32\VBoxTray.exe
- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe (2 instancias)
- C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe

Parámetro	Número	Tipo	Comprobación de fiabilidad	Hora de Detección
File Drop	2	Varios	No Confiable	11/29/2023 15:19

Se identificaron dos archivos, el primero corresponde a la ubicación del archivo de prueba malware mientras que el segundo indica la presencia de un flujo alternativo de datos que contiene información respecto a la zona de seguridad del archivo descargado de internet.

File drop <sup>(2)</sup>	...
C:\Users\User\Desktop\eicar_com\eicar.com:Zone.Identifier	...
C:\Users\User\Desktop\eicar_com	...

No se detectaron conexiones a internet.

### 3.1.3. Indicadores de Compromiso

Se detectó un archivo malicioso bloqueado.

Ruta	Amenaza	Tipo	Acción	Hora de Detección
C:\Users\User\Desktop\ eicar_com\eicar.com	EICAR-Test-File	Archivo	Eliminado	11/29/2023 15:19
MD5		SHA-256		
44d88612fea8a8f36de82e1278abb02f		275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f		

Action	Deleted	Date and time	11/29/2023 3:20 pm
Threat	EICAR-Test-File	Object name	C:\Users\User\Desktop\eicar_com\eicar.com
Scan mode	On disinfect	Object type	File
MD5	<a href="#">44d88612fea8a8f36de82e1278abb02f</a>	SHA-256	<a href="#">275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f</a>
Creation date	11/29/2023 3:19 pm	Modification date	11/29/2023 3:19 pm

## 3.2. MyDoom



### 3.2.1. Origen de la Amenaza

Origen de la amenaza detectada con Kaspersky Endpoint Security Cloud EDR:

Parámetro de Inicio	Tipo	PID del Sistema 3	Crítico	Nivel de Integridad
C:\Windows\Explorer.EXE	Proceso	5076	No	Media

Usuario	Fecha	Hora
WINDEV2310EVAL\User	11/29/2023	13:07

System PID	5076	Critical process	No
MD5	<a href="#">c8a00f2fd7f7a580a8638e8a08270dd3</a>	Startup parameters	C:\Windows\Explorer.EXE
Integrity level	Medium integrity	User alias	WINDEV2310EVAL\User
Privileged user	Yes	Timestamp	11/29/2023 1:07 pm

### 3.2.2. Desarrollo de la Amenaza

La cadena de proceso identificó 7 procesos hijos, no obstante, discriminando con base en la hora de ejecución del malware (13:29) y la legitimidad de los procesos de ejecución de VirtualBox, Microsoft Edge y OneDrive, solo se identifica uno de interés a dos instancias: C:\Users\User\Desktop\W32.MyDoom.A\f-mydoom.exe. Dicho proceso corresponde a la ejecución de un script de esta variante de MyDoom.

Parámetro	Número	Tipo	Comprobación de fiabilidad	Hora de Detección
File Drop	140	Varios	No Confiable	11/29/2023 13:10-13:19

De los 140 archivos identificados, dada la hora de ejecución, se descartan 61 archivos que no son pertinentes al worm. Algunos de los archivos relevantes, son los siguientes:

- C:\Users\User\Desktop\W32.MyDoom.A\
  - W32.Mydoom\_files\search-go.gif
  - W32.Mydoom\_files\nav\_bar.gif
  - W32.Mydoom\_files\nav\_privacy.gif
  - W32.Mydoom\_files\main\_menu.js
  - W32.Mydoom\_files\secure.css
  - W32.Mydoom2.htm
  - Netcraft www\_sco\_com is a weapon of mass destruction\_files

Se pueden observar extensiones de archivos, .js, .css, y .htm entre otras las cuales son comúnmente asociadas al desarrollo de sitios web. También, algunos archivos poseen nombres asociados a componentes de una página web “nav\_bar”, “main\_menu”. Con base en esto se infiere que posiblemente se utilicen técnicas de web spoofing en los archivos adjuntos de los correos spam para propagar el malware. Adicionalmente, se identifican algunos archivos los cuales hacen referencia al objetivo, “www.sco.com” de los ataques DDoS que MyDoom efectúa

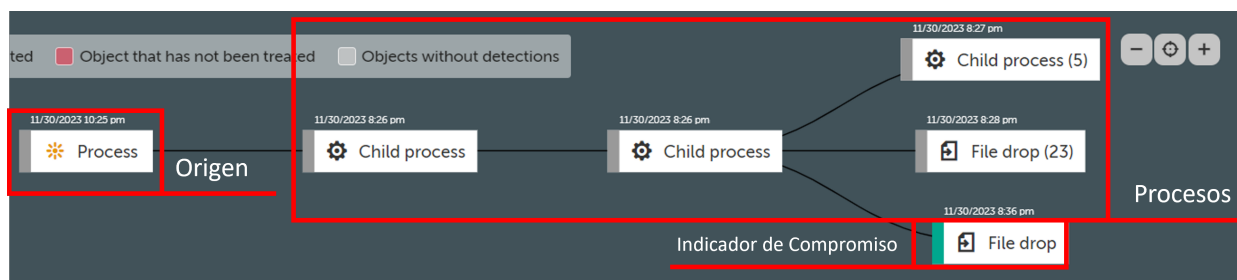
La conexión identificada corresponde a una ubicación en California, USA, no obstante dado que la hora de la conexión precede a la ejecución y descifrado del malware, no se considera relevante para el análisis del comportamiento del malware.

### **3.2.3. Indicadores de Compromiso**

Se detectó un archivo malicioso bloqueado.

Ruta	Amenaza	Tipo	Acción	Hora de Detección
C:\Users\User\Desktop\W32.MyDoom.A\strip-girl-2.0bdcom_patches.exe	Email-Worm.Win32.Mydoom.a	Archivo	Eliminado	11/29/2023 13:29
MD5		SHA-256		
53df39092394741514bc050f3d6a06a9		fff0ccf5feaf5d46b295f770ad398b6d572909b00e2b8bcd1b1c286c70cd9151		

### 3.3. Satana



#### 3.3.1. Origen de la Amenaza

Origen de la amenaza detectada con Kaspersky Endpoint Security Cloud EDR: El origen

Parámetro de Inicio	Tipo	PID del Sistema 3	Crítico	Nivel de Integridad
winlogon.exe	Proceso	820	No	Integridad del Sistema

Usuario	Fecha	Hora
WINDEV2310EVAL\User	11/30/2023	22:25

de la amenaza corresponde a un proceso privilegiado del sistema operativo de Microsoft Windows el cual se sospecha, dada su naturaleza y proximidad, haya sido *targeteado* por Satana para disfrazar sus acciones como un proceso legítimo y ayudarse en su labor de encriptar el MBR. Adicionalmente, se observan técnicas antiforenses, el timestamp del origen fue modificado para desplegar un valor incorrecto, es decir uno mucho posterior a la ejecución del malware o su registro en el sistema.

#### 3.3.2. Desarrollo de la Amenaza

El EDR identificó un total de 7 procesos hijos, de los cuales solo 1 fue sospechoso. Este proceso corresponde a la ejecución de userinit.exe fuera no al momento del inicio del sistema.

Se teoriza que se hayan explotado los privilegios de este proceso y el anterior, winlogon.exe, para establecer persistencia post-reinicio en el sistema.

Parámetro	Número	Tipo	Comprobación de fiabilidad	Nivel de Integridad
userinit.exe	1	Children Process	No	Media

Parámetro	Número	Tipo	Comprobación de fiabilidad	Hora de Detección
File Drop	23	Varios	No Confiable	11/29/2023 13:10-13:19

De los 23 archivos detectados, con base en la hora de ejecución del malware, solo 8 de ellos son pertinentes para el análisis. Algunos de estos archivos se encuentran en la siguiente dirección.

- C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\Ransomware  
.Satana.lnk
- C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\68  
3a09da219918258c58a7f61f7dc4161a3a7a377cf82a31b840baabfb9a4a96.bin.lnk
- C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\  
unpacked.mem.lnk
- C:\Users\User\Desktop\Ransomware.Satana\unpacked.mem

### 3.3.3. Indicadores de Compromiso

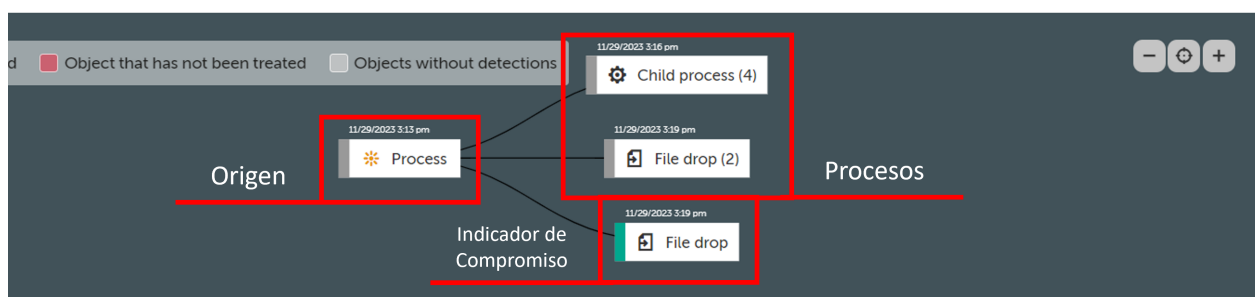
Se detectó un archivo malicioso bloqueado.

Ruta	Amenaza	Tipo	Acción	Hora de Detección
C:\Users\User\Desktop\Ransomware.Satana\683a09da219918258c58a7f61f7dc4161a3a7a377cf82a31b840baabfb9a4a96.bin	Trojan-Ransom .Win32.Satan.f	Archivo	Eliminado	11/30/2023 20:36
MD5		SHA-256		
46bfd4f1d581d7c0121d2b19a005d3df		683a09da219918258c58a7f61f7dc4161a3a7a377cf82a31b840baabfb9a4a96		



Action	Deleted	Date and time	11/30/2023 8:36 pm
Threat	Trojan-Ransom.Win32.Satan.g	Object name	C:\Users\User\Desktop\Ransomware.Satana\unpacked.me m
Scan mode	On disinfect	Object type	File
MD5	<a href="#">108756f41d114eb93e136ba2feb838d0</a>	SHA-256	<a href="#">b38b4c1dcf6d6ecd1bbfc236b43c37c18044c2f42f11e5088384f4bd0751929c</a>
Creation date	11/30/2023 8:36 pm	Modification date	11/30/2023 8:36 pm

### 3.4. DOUBLEANTASY




#### 3.4.1. Origen de la Amenaza

Origen de la amenaza detectada con Kaspersky Endpoint Security Cloud EDR:

Parámetro de Inicio	Tipo	PID del Sistema 3	Crítico	Nivel de Integridad
C:\Windows\Explorer.EXE	Proceso	5036	No	Media


Usuario	Fecha	Hora
WINDEV2310EVAL\User	29/11/2023	15:22



Process

C:\Windows\explorer.exe

...

System PID	5036	Critical process	No
MD5	 <a href="#">c8a00f2fd7f7a580a8638e8a08270dd3</a>	Startup parameters	C:\Windows\Explorer.EXE
Integrity level	Medium integrity	User alias	WINDEV2310EVAL\User
Privileged user	Yes	Timestamp	11/29/2023 3:13 pm

### 3.4.2. Desarrollo de la Amenaza

La cadena de desarrollo identifica 4 procesos hijos los cuales corresponden a funciones legítimas de la ejecución de VirtualBox, Microsoft Edge y OneDrive.

- C:\Windows\System32\VBxTray.exe
- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe (2 instancias)
- C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe

Parámetro	Número	Tipo	Comprobación de fiabilidad	Hora de Detección
File Drop	7	Varios	No Confiable	11/29/2023 15:19-15:22

Se identificaron siete archivos; de los mismos, después de realizar una revisión de para corroborar la coordinación de los horarios y la neutralización de la amenaza por Kaspersky, los más relevantes corresponden a un archivo con extensión .db, el cual corresponde a un archivo de almacenamiento de bases de datos, lo cual sugiere que el *malware* estaba recopilando información sustancial del dispositivo para enviarla al servidor de mando y control, para posteriormente identificar si el dispositivo en el cual se encuentra es el deaseado. De ser el caso de descargan dos malwares adicionales del mismo grupo, GRAYFISH y EQUATIONDRUG utilizados en el robo de información.

C:\\$Recycle.Bin\S-1-5-21-3100713454-2124896179-2687965256-1000\SI TORRQ4	...
C:\Users\User\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x000000000000002b.db	...
C:\Users\User\Desktop\EquationGroup.DoubleFantasy	...
C:\Users\User\Desktop\EquationGroup.DoubleFantasy\DoubleFantasy_2A12630FF976BA0994143CA93FECDD17F.Zone.Identifier	...

No se detectaron conexiones a internet.

### 3.4.3. Indicadores de Compromiso

Se detectó un archivo malicioso bloqueado.

Ruta	Amenaza	Tipo	Acción	Hora de Detección
C:\Users\User\Desktop\EquationGroup.DoubleFantasy\DoubleFantasy_2A12630FF976BA0994143CA93FECDD17F	Trojan.Win32.DoubleFantasy.gen	Archivo	Eliminado	11/29/2023 15:22
MD5		SHA-256		
2a12630ff976ba0994143ca93fecdd17f		1e55abb94951cedc548fd8d67bd1b50476808f1d0ae72f9842181761ff92f83f		

Action	Deleted	Date and time	11/29/2023 3:22 pm
Threat	Trojan.Win32.DoubleFantasy.gen	Object name	C:\Users\User\Desktop\EquationGroup.DoubleFantasy\DoubleFantasy_2A12630FF976BA0994143CA93FECDD17F
Scan mode	On disinfect	Object type	File
MD5	<a href="#">2a12630ff976ba0994143ca93fecdd17f</a>	SHA-256	<a href="#">1e55abb94951cedc548fd8d67bd1b50476808f1d0ae72f9842181761ff92f83f</a>
Creation date	11/29/2023 3:22 pm	Modification date	11/29/2023 3:22 pm

### 3.5. Vipasana



#### 3.5.1. Origen de la Amenaza

Origen de la amenaza detectada con Kaspersky Endpoint Security Cloud EDR:

Parámetro de Inicio	Tipo	PID del Sistema 3	Crítico	Nivel de Integridad
C:\Windows\Explorer.EXE	Proceso	4928	No	Media

Usuario	Fecha	Hora
WINDEV2310EVAL\User	29/11/2023	14:08

Acción	Eliminado	Fecha y hora	29/11/2023 14:24
Amenaza	UDS: DangerousObject.Multi.Generic	Nombre de objeto	C:\Users\User\Desktop\Ransomware.Vipasana\c0cf40b8830d666a24bdd4febd6162e95aa30ed968fa3675e26ad97b2e88e03a
Modo de análisis	Durante desinfección	Tipo de objeto	Archivo
MD5	<a href="#">a890e2f924dea3cb3e46a95431ffae39</a>	SHA-256	<a href="#">c0cf40b8830d666a24bdd4febd6162e95aa30ed968fa3675e26ad97b2e88e03a</a>
Fecha de creación	29/11/2023 14:24	Fecha de modificación	29/11/2023 14:24

### 3.5.2. Desarrollo de la Amenaza

La cadena de proceso identificó 7 procesos hijos, los cuales, resultan no relevante, puesto que se manifestaron mucho antes de la hora de ejecución del malware (14:24) y la legitimidad de los procesos de ejecución de VirtualBox, Microsoft Edge y OneDrive.

Parámetro	Número	Tipo	Comprobación de fiabilidad	Hora de Detección
File Drop	64	Varios	No Confiable	29/11/2023 14:14-14:24

De los 64 archivos identificados, dada la hora de ejecución, se descartan 58 archivos que no son pertinentes al ransomware. Algunos de los archivos relevantes, son los siguientes:

- C:\Users\User\Desktop\
  - Ransomware.Vipasana
  - Ransomware.Vipasana\ea9778d20a2f9b1f8b00ddd24b6bcee81af381ed02cfe0a3c9ab3111cda5f573:Zone.Identifier
  - Ransomware.Vipasana\ea9778d20a2f9b1f8b00ddd24b6bcee81af381ed02cfe0a3c9ab3111cda5f573

No se detectaron conexiones a internet, lo cual era de esperar ya que el malware en cuestión viene con una llave para encriptación ya incorporada.

### 3.5.3. Indicadores de Compromiso

Ruta	Amenaza	Tipo	Acción	Hora de Detección
C:\Users\User\Desktop\Ransomware.Vipasana\0442cfabb3212644c4b894a7e4a7e84c00fd23489cc4f96490f9988e6074b6ab	UDS: DangerousObject. Multi.Generic	Archivo	Eliminado	11/29/2023 14:24
MD5		SHA-256		
2aea3b217e6a3d08ef684594192cafc8		0442cfabb3212644c4b894a7e4a7e84c00fd23489cc4f96490f9988e6074b6ab		

## 4. Recomendaciones

1. **Firewall:** Implementar un firewall para controlar el tráfico de red y bloquear accesos no autorizados.
2. **Antivirus y Antimalware:** Instalar software antivirus y antimalware actualizado en todos los dispositivos para detectar y eliminar amenazas.
3. **Actualizaciones de Software:** Es crucial mantener actualizado cualquier sistema operativo, ya sea Windows, Mac OS X, Linux u otros. Los desarrolladores emiten parches de seguridad para corregir vulnerabilidades, garantizando así la protección del sistema.
4. **Concientización del Personal:** Capacitar a los empleados en seguridad informática y concientizarlos sobre prácticas seguras.
  - a) Cerrar el sitio web cuando el navegador indique que no es un sitio seguro.
  - b) No abrir enlaces sospechosos o correos de contactos desconocidos.
  - c) Analizar antes de descargar cualquier archivo de internet.
  - d) Tener cuidado con las redes WiFi abiertas.
  - e) No compartir contraseñas con otras personas.
5. **Políticas de Contraseñas:** Establecer políticas de contraseñas fuertes y fomentar la actualización regular de las contraseñas.
6. **Verificar Fuentes de Descarga:** Al descargar e instalar VirtualBox, asegúrese de hacerlo desde la página oficial para evitar versiones comprometidas.
7. **Control de Acceso:** Implementar sistemas de control de acceso para limitar el acceso a datos y sistemas solo a personas autorizadas como técnicas de autenticación multifactor. Kasperski es útil también en la asignación de roles de los usuarios, por lo que facilita la administración de la seguridad.
8. **Respaldo de Datos:** Realizar copias de seguridad regulares de datos críticos y almacenarlas de forma segura.

## 5. Conclusiones

Al evaluar el rendimiento de Kaspersky Endpoint Security Cloud en el contexto de la ciberseguridad pudimos notar su eficacia en la detección y neutralización de amenazas cibernéticas. La implementación de un entorno de pruebas utilizando VirtualBox y máquinas virtuales nos permitió realizar un análisis controlado de la herramienta frente a diferentes tipos de malware. Algunas ventajas del uso de Kaspersky Endpoint Security son sus controles de dispositivos, aplicaciones y web, gestión de vulnerabilidades y cifrado de datos. La creación y configuración de una cuenta, así como la invitación de usuarios y la asignación de roles, facilitaron la administración de la seguridad.

Después de ponerla a prueba frente a diferentes códigos maliciosos, como EICAR, MyDoom, Satana, DOUBLEFANTASY y Vipasana, pudimos notar su capacidad para identificar y bloquear archivos maliciosos, proporcionando detalles sobre el origen de la amenaza, el desarrollo de la misma y los indicadores de compromiso asociados, por lo que podemos decir que demostró una respuesta eficiente ante este tipo de amenazas, ya que no sólo cumplió el objetivo, sino que lo hace de una forma rápida y sencilla para el usuario que la está utilizando. Por lo que podemos concluir que la herramienta Kaspersky es muy útil y puede ser una buena opción en el ámbito de la ciberseguridad.

## Referencias

- [1] ¿Qué es el código malicioso? (2023, April 19). latam.kaspersky.com.  
<https://latam.kaspersky.com/resource-center/definitions/malicious-code>
- [2] Acerca del virus de prueba EICAR. (n.d.). <https://support.kaspersky.com/KESS/3.0/es-MX/147734.htm>
- [3] Titova, V. (2020, July 3). Satana: el ransomware del infierno. Kaspersky. Retrieved November 30, 2023, from <https://latam.kaspersky.com/blog/satana-ransomware/7362/>
- [4] CCN-CERT - Publicados cinco nuevos Informes de Código Dañino. 2015, October 22). <https://www.ccn-cert.cni.es/es/comunicacion-eventos/comunicados-ccn-cert/3094-publicados-cinco-nuevos-informes-de-codigo-danino.html>
- [5] A close look at ransomware by the example of Vipasana – I. (2016, October 7). <https://www.boxcryptor.com/en/blog/post/a-close-look-at-ransomware-vipasana-part-i/>
- [6] Endpoint Security para Windows — Kaspersky. (2018). Kaspersky.com. <https://latam.kaspersky.com/small-to-medium-business-security/endpoint-windows>
- [7] Los 10 virus más letales de la historia (para los ordenadores). (2021). Retrieved from <https://informatix.es/10-virus-mas-letales-de-la-historia/>
- [8] Staff, A. (2015, February 17). How Kaspersky May Have Discovered NSA Malware. Colocation America. <https://www.colocationamerica.com/blog/kaspersky-uncovers-equation-group>
- [9] CCN-CERT - Publicados cinco nuevos Informes de Código Dañino. (2015, October 22). Ccn-Cert.cni.es. <https://www.ccn-cert.cni.es/es/comunicacion-eventos/comunicados-ccn-cert/3094-publicados-cinco-nuevos-informes-de-codigo-danino.html>
- [10] Titova, V. (2016, July 11). Satana: el ransomware del infierno. Kaspersky.com; Kaspersky. <https://latam.kaspersky.com/blog/satana-ransomware/7362/>



- [11] Majauskas, G. (2016). Vipasana ransomware. Retrieved from <https://www.2-viruses.com/remove-vipasana-ransomware>