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 Ejecutivo

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

1. Introducción

Si bien puede parecer una arena futurista y distante, la ciberseguridad es un campo en que toda empresa debe adentrarse para subsistir prósperamente. De acuerdo con Forbes [1], el año pasado se registraron 80,000 millones de intentos de ciberataques a empresas y organizaciones. La cantidad de ataques no constituye la preocupación principal, sino la elevada suma a la que llega la pérdida anual que registran las empresas: 3.5 millones de dólares (de acuerdo a un estudio realizado por el Instituto Ponemon [2]), repartidos entre los daños por robo de información y daños a la infraestructura. Estos datos son más que suficientes para plantear la importancia de tener disponibles herramientas efectivas para la mitigación de estas amenazas.

Para que un mecanismo sea eficaz debe ser evaluado constantemente para constatar que sea actual (lo cual representa un enorme reto en este mundo en el que la tecnología cibernética se desarrolla vertiginosamente para bien y para mal) y que funcione correctamente. Es por esto que el objetivo de este trabajo es la valuación del servicio Kaspersky Endpoint Security Cloud, que ofrece antivirus, una herramienta indispensable para las empresas que, a través de sus colaboradores, inciden en una cantidad enorme de oportunidades de incursión para un agresor cibernético [3].

Para llevar a cabo la evaluación de efectividad en identificación y neutralización de ataques por parte de este antivirus, se hará uso de una máquina virtual, que ofrece un ambiente aislado, controlado, y por lo tanto seguro para simular amenazas provenientes de distintos virus que al mismo tiempo, se buscan analizar y estudiar, de manera que estemos más familiarizados con el funcionamiento de los artefactos utilizados para agredir cibernéticamente y así estar mejor preparados para enfrentarlos.

2. Desarrollo

Creamos un entorno de pruebas para experimentar de manera segura con malware. Se instaló y configuró VirtualBox para la creación de máquinas virtuales. Se instaló Windows 11 Enterprise Evaluation 22H2 en estas máquinas virtuales, replicando el proceso tres veces para generar instancias aisladas y ejecutar malware de manera segura.

Además, se implementó Pfsense para establecer una red interna y prevenir la propagación lateral de amenazas a otros dispositivos. Se creó una máquina virtual con Pfsense, configurando adaptadores de red y asignando direcciones IP a las interfaces.

En cuanto a la seguridad, se instaló y configuró Kaspersky Endpoint Security. Hicimos también una cuenta en Kaspersky Endpoint Security Cloud, la creación y configuración de la empresa, la invitación de usuarios, y la configuración de perfiles de seguridad, incluyendo la protección contra amenazas web y en la red.

Luego instalamos el agente de Kaspersky en las máquinas virtuales para proporcionar protección contra malware y permitir la detección y respuesta en caso de amenazas.

Una vez que el entorno estuvo configurado y la seguridad implementada, procedimos a introducir diferentes amenazas como el malware MyDoom, Satana, DOUBLEFANTASY, EICAR y Vipasana, lo que nos permitió evaluar la capacidad de Kaspersky para detectar y neutralizar estos ataques en tiempo real. El análisis detallado de cómo Kaspersky respondió a cada amenaza a través de la generación de reportes nos proporcionó información importante sobre la eficacia y adaptabilidad de la herramienta de seguridad. Esto nos permitió no solo comprender su rendimiento general, sino también identificar posibles áreas de mejora y fortaleza en la protección contra diversas formas de malware.

3. Resultados

El primer código malicioso que se analizó fue el de Eicar, que es un código diseñado específicamente para probar la efectividad de los antivirus. Aunque no ejecuta ninguna acción en el dispositivo, su detección por los antivirus es una prueba de su funcionalidad. Es utilizado como un archivo de prueba inofensivo pero reconocido como amenaza por los programas antivirus. Al realizar la prueba si fue detectado y eliminado. No se identificaron procesos adicionales ni conexiones a Internet relevantes.

Luego se analizó MyDoom, que es un gusano una forma de malware autónomo que puede propagarse sin intervención del usuario. Este gusano abre dos puertas traseras en los dispositivos infectados, permitiendo el acceso remoto. Emplea técnicas como correos electrónicos engañosos. En la prueba MyDoom se originó desde el proceso de Explorer.EXE y ejecutó un script malicioso. Se identificaron archivos relevantes en donde gracias a las extensiones de los archivos se puede inferir que posiblemente se utilicen técnicas de web spoofing en los archivos adjuntos de los correos spam para propagar el malware. Se detectó, bloqueó y eliminó un archivo malicioso durante el análisis.

Satana es un troyano que encripta archivos y daña el Registro de Arranque Principal (MBR), impidiendo el inicio normal de Windows. Este comportamiento lo convierte en un ransomware, exigiendo un rescate a través de una dirección de correo. Satana utiliza métodos de infección comunes, como correos de phishing, y se centra en la destrucción de datos en lugar de la negociación para su recuperación. Satana utilizó el proceso winlogon.exe y se logró identificar un proceso hijo sospechoso y archivos relacionados con ransomware en el sistema. Se bloqueó y eliminó un archivo malicioso durante el análisis.

DoubleFantasy, creado por Equation Group, es un troyano utilizado en ataques dirigidos a empresas y organizaciones. Su objetivo principal es recopilar información esencial del dispositivo infectado, que luego se envía a un servidor de mando y control. Los atacantes pueden decidir introducir malware adicional en el sistema según la relevancia de la información recopilada. DoubleFantasy se originó desde el proceso de Explorer.EXE y ejecutó varios procesos legítimos. Se identificaron archivos relacionados con la recopilación de información y posibles descargas de malware adicional. No se detectaron conexiones a Internet relevantes.

Y finalmente se probó Vipasana, que es un virus que encripta los datos de la víctima mediante una llave pública integrada en el malware. Se propaga a través de bots de spam que envían correos electrónicos maliciosos. Una vez infectado el sistema, utiliza un algoritmo de cifrado sofisticado, incluso sin conexión a Internet. Proporciona una dirección de correo para negociar el rescate y dificulta la recuperación de datos. La cadena de proceso identificó 7 procesos hijos, los cuales no resultaron relevantes 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. De los 64 archivos identificados, dada la hora de ejecución, se descartan 58 archivos que no son pertinentes al ransomware. 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 y la amenaza `UDS:DangerousObject.Multi.Generic` fue eliminada.

4. Evaluación Final

En cada caso, Kaspersky Endpoint Security Cloud EDR demostró su capacidad para detectar, bloquear y eliminar las amenazas durante la experimentación con los malware. La detección del código malicioso de Eicar, la neutralización del gusano MyDoom con la identificación de posibles vectores de propagación, la rápida respuesta al troyano Satana, incluso frente al virus Vipasana, que utiliza técnicas de encriptación Kaspersky logró eliminar la amenaza, lo que muestra su capacidad para abordar situaciones de ransomware. La generación de reportes sobre el origen de la amenaza, su desarrollo y los indicadores de compromiso asociados nos fue de utilidad para la comprensión de las acciones realizadas por Kaspersky además de que lo hizo de una forma rápida y muy intuitivo para darle el seguimiento.

5. Recomendaciones

5.1. Infraestructura de Red

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.

5.2. Concientización y Políticas

1. **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.

2. **Políticas de Contraseñas:** Establecer políticas de contraseñas fuertes y fomentar la actualización regular de las contraseñas.

5.3. Control de Acceso y Protección de Datos

1. **Control de Acceso:** Implementar sistemas de control de acceso para limitar el acceso a datos y sistemas solo a personas autorizadas.

2. **Respaldo de Datos:** Realizar copias de seguridad regulares de datos críticos y almacenarlas de forma segura.

5.4. Configuración de Kaspersky y pruebas de código malicioso

1. **Verificar Fuentes de Descarga:** Al descargar e instalar VirtualBox, asegúrese de hacerlo desde la página oficial para evitar versiones comprometidas.

2. **Configuración de Máquinas Virtuales:** Al crear máquinas virtuales para pruebas de seguridad, configurar en entornos aislados y utilice copias de sistemas operativos y software legítimos.

3. **Registro y Configuración de Cuenta:** Al registrar una cuenta en Kaspersky, utilice información precisa. Configurar adecuadamente la empresa y establecer roles de usuario para garantizar una gestión segura.

4. **Invitación de Usuarios:** Al invitar usuarios, asegurarse de otorgar los roles necesarios. Limitar los privilegios de acuerdo con las responsabilidades de cada usuario.

5. **Configuración de Perfiles de Seguridad:** Personalizar los perfiles de seguridad según las necesidades de su entorno. Ajustar las configuraciones de protección contra amenazas web y en la red para fortalecer la defensa.

6. **Descarga Segura:** Al trabajar con códigos maliciosos para pruebas, asegúrese de obtenerlos de fuentes confiables como repositorios de análisis de malware.

7. **Entorno Controlado:** Ejecute las pruebas de códigos maliciosos en entornos controlados, como máquinas virtuales, para evitar posibles daños al sistema principal.

8. **Análisis Detallado:** Realice un análisis detallado de los resultados de las pruebas, identificando posibles indicadores de compromiso y tomando medidas adecuadas.

6. Conclusiones

La exposición a códigos maliciosos como los analizados en este informe, como el MyDoom, Satana, DOUBLEANTASY y Vipasana, puede acarrear consecuencias graves, desde la pérdida de datos hasta el robo de información sensible. Estos ataques representan amenazas significativas que pueden comprometer la privacidad, la confidencialidad y la disponibilidad de los recursos digitales.

La importancia de utilizar herramientas de seguridad confiables, como Kaspersky Endpoint Security, se destaca en la eficacia demostrada para detectar, bloquear y neutralizar activamente tales amenazas. Kaspersky no solo brinda protección contra una amplia variedad de malware, sino que también proporciona detalles exhaustivos sobre el origen y el desarrollo de las amenazas, permitiendo una respuesta rápida y eficiente. Kasperski es útil también en la asignación de roles de los usuarios, por lo que facilita la administración de la seguridad.

En un entorno digital cada vez más interconectado, donde la información se ha convertido en un activo invaluable, la adopción de soluciones de seguridad robustas se presenta como un imperativo. La elección consciente de herramientas como Kaspersky Endpoint Security no solo resguarda la integridad de los sistemas, sino que también preserva la confianza en la utilización de tecnologías avanzadas, contribuyendo así a un entorno digital más seguro y protegido.

Referencias

[1] Staff, F., & Staff, F. (2022, August 2). México registra 80,000 millones de intentos de ciberataques en 2022. Retrieved December 1, 2023, from Forbes México website: https://www.forbes.com.mx/mexico-registra-80000-millones-de-intentos-de-ciberataques-en-2022/

[2] Telcel. (2023). Millones de USD en pérdidas sin ciberseguridad — Telcel Empresas. Retrieved December 1, 2023, from Telcel.com website: https://www.telcel.com/empresas/tendencias/notas/ciberseguridad-causa-perdidas.html

[3] Endpoint Security para Windows — Kaspersky. (2018). Retrieved December 1, 2023, from Kaspersky.com website: https://latam.kaspersky.com/small-to-medium-business-security/endpoint-windows