REVISTA Más TIC	Vol. 1, No. 2	diciembre 2024 – mayo 2025 pp. 96-113 ISSN L 3072-9696

Implementación de git y cifrado en documentos XML como estrategia de mitigación contra ransomware

Implementation of git and encryption in XML documents as a mitigation strategy against ransomware

Luis Isaac Trigás Cerezo
Universidad Tecnológica de Panamá, Panamá
luis.trigas@utp.ac.pa
https://orcid.org/0009-0009-1721-4578

Miguel Vargas Lombardo
Universidad Tecnológica de Panamá, Panamá.
miguel.vargas@utp.ac.pa
https://orcid.org/0000-0002-2074-2939

Recibido: 31-10-2024, Aceptado: 1-1-2025

DOI: https://doi.org/10.48204/3072-9696.7414

Resumen

La tecnología ha avanzado significativamente en poco tiempo, lo que ha provocado que los ataques cibernéticos, como el ransomware, se vuelvan más complejos y letales. Muchos expertos en seguridad informática investigan formas de contrarrestar estos ciberataques, en especial el ransomware.

Los resultados más frecuentes de las investigaciones sobre ransomware se centran en evitar la introducción de vectores maliciosos en los sistemas, utilizando tecnologías como el machine learning y la inteligencia artificial. Sin embargo, una debilidad de este enfoque es que, si la defensa se vulnera, el sistema queda completamente expuesto, permitiendo el acceso y control de todos los archivos.

El presente artículo se enfoca en la premisa de proteger documentos importantes ante un ataque de ransomware, haciendo uso del principio de Git (sistema de control de versiones). La investigación propone tener versiones o copias de documentos

importantes protegidas a nivel de permisos de edición y acceso. Para ello, se contempla la implementación de este concepto como un componente o extensión para Microsoft Word, que generaría automáticamente una nueva copia de los últimos cambios al finalizar el trabajo en un documento. También se evalúa el impacto en el rendimiento del computador durante la ejecución del complemento. Como valor adicional, se analiza la implementación del cifrado SHA-256 en los documentos como una capa extra de seguridad.

Palabras claves: ciberataque, control de versiones, cifrado, seguridad informática

Abstract

Technology has made significant advances in a short time, which in turn makes cyberattacks such as ransomware more complex and lethal. Many stakeholders in the computer security sector are investigating ways to counter cyberattacks and especially ransomware. The most frequent results regarding ransomware attacks usually focus on avoiding the introduction of malicious vectors into the systems, using machine learning and artificial intelligence. A weakness of this approach is that when the defense is breached, the system is completely exposed, and therefore, access and control of all files are lost.

The approach or premise that this article investigates is to protect important documents against a ransomware attack by using the principle of Git (a version control system). The research aims to have versions or copies of important documents protected at the level of editing and access permissions. The research also considers implementing this concept as a component or extension for Microsoft Word, so that when a document is finished, a new copy of the latest changes is automatically generated. The impact on performance during the execution of the plugin on a computer is also evaluated. As an additional value to the research, the implementation of SHA-256 encryption on documents is contemplated and analyzed as an additional layer of security.

Keywords: cyberattack, version control, encryption, computer security

Introducción

El ransomware es una amenaza cibernética cada vez más prevalente que implica el cifrado malicioso de archivos de una víctima, seguido de una demanda de rescate para restaurar el acceso a los datos. Este tipo de programa maligno representa un riesgo significativo para individuos, empresas e instituciones gubernamentales, ya que puede paralizar sistemas completos y provocar pérdidas financieras sustanciales. El ransomware generalmente se distribuye a través de correos electrónicos de *phishing*, descargas maliciosas y vulnerabilidades de software no parcheadas, propagándose rápidamente a través de redes y dispositivos conectados (Alcántara & Melgar, 2016).

Dada la gravedad y la frecuencia de los ataques de ransomware, es crucial implementar estrategias efectivas de mitigación para proteger los datos y minimizar el impacto de un ataque. Las medidas preventivas incluyen la educación y capacitación de los usuarios para reconocer intentos de *phishing*, el uso de software antivirus y de seguridad actualizado, y la aplicación regular de parches de seguridad. Además, es esencial realizar copias de seguridad regulares y almacenarlas de manera segura, fuera de la red principal, para asegurar que los datos puedan ser recuperados sin necesidad de pagar el rescate (Al-Dwairi et al., 2022).

Otra estrategia clave es la implementación de sistemas de control de versiones como Git, que permite mantener un historial detallado de los cambios en los archivos y facilita la recuperación de versiones anteriores en caso de compromiso. Estas medidas, combinadas con una política robusta de ciberseguridad y una respuesta rápida a incidentes, pueden ayudar a mitigar los efectos devastadores de los ataques de ransomware y proteger la integridad y disponibilidad de los datos críticos.

En el mundo actual, la tecnología es un pilar fundamental en el funcionamiento de todo tipo de actividades. La podemos ver en los sectores financieros, deportivos, literarios, de comercio, alimenticio, logísticos, automotriz e incluso en el ámbito particular, ya que al alcance de todos hay un equipo computacional con el que se puede realizar todo tipo de funciones.

La tecnología hace que se compilen datos que son transformados en información, donde la información es un activo vital para cada organización o persona, que se custodia de manera confidencial para su uso propio. A raíz de esto, y como todo se ha volcado al uso de la tecnología, también surgen quienes buscan aprovecharse para realizar crímenes, tomando como uno de los objetivos la información que pueden obtener de otros.

El cibercrimen está comprendido por los ciberataques y sus autores. Un ciberataque es un ataque electrónico dirigido a equipos de cómputo o redes informáticas donde están conectados varios equipos electrónicos en un intento de robar, alterar o destruir cualquier componente vital o crítico, como archivos e información presente en él (Biju, 2019).

Existen varios tipos de ciberataques (Bouam et al., 2021):

- Denegación de servicio (DoS) y de modo Distribuido (DDoS): Es un tipo de ciberataque que tiene como objetivo inundar o superar la capacidad de respuesta con falsas peticiones a los servidores o servicios en línea que brindan algún tipo de funcionalidad, como sitios web, aplicaciones, programas o videojuegos, afectando la disponibilidad o el acceso al uso de estos, lo que ocasiona pérdidas económicas y de operatividad a los usuarios. Es difícil tratar con este tipo de ataque, ya que se necesita mantener una infraestructura grande para manejar una gran cantidad de peticiones, y a su vez, identificar o prevenir la llegada de un ataque de este tipo se puede confundir con un alto tráfico de usuarios reales del servicio o programa.
- Man-in-the-middle (Mitm): El Mitm hace referencia a cuando el atacante utiliza varios métodos de intercepción de comunicaciones entre dos puntos. Por

ejemplo: la comunicación entre un equipo de cómputo y un servidor donde el equipo de cómputo está solicitando un documento. El atacante puede interrumpir esa conexión y redirigirla a un equipo propio para luego regresarla a su destino final. Al realizar esto, puede examinar y obtener toda la información que suceda en esa conexión sin ser detectado.

- Ataques de Phishing: Estos ataques hacen uso de ingeniería social. La ingeniería social es una técnica utilizada por los atacantes para engañar a usuarios. Estos engaños, donde se imita o se hace pasar por otra persona, pueden hacer que el usuario ingrese a un sitio web malicioso u otorgue información confidencial que para el atacante es útil para obtener credenciales y poder irrumpir en el equipo de cómputo.
- Drive-by-download: Este ataque ocurre cuando un usuario se infecta con un software malicioso simplemente visitando un sitio web. El usuario no necesita hacer clic en ningún lugar para infectarse. Aquí, los atacantes suelen utilizar un sitio web legítimo e inyectar un objeto malicioso dentro de las páginas web, lo que hace que se instale en los equipos un software malicioso cuya finalidad es obtener información confidencial o inhabilitar al mismo.
- Ataques de Password: Son ataques orientados a obtener las contraseñas para poder acceder a sitios web, intranets o equipos de cómputo. Se utilizan métodos como ataques de fuerza bruta, que consiste en colocar una serie de posibles contraseñas para lograr acceder al objetivo, o herramientas de *cracking* para lograr descifrar contraseñas protegidas por métodos de *Hash* u otros.
- Inyección de SQL: SQL hace referencia a un lenguaje de cómputo utilizado en Bases de Datos para obtener información dentro de la misma, y es utilizado por sitios webs y programas para su debido funcionamiento por medio de “Consultas”. El ataque de Inyección de SQL busca aprovechar vulnerabilidades para alterar las “Consultas” realizadas por los diferentes softwares para obtener información confidencial.

- Ataque de Programa maligno: Este ataque es donde un software se instala en un equipo de cómputo sin el consentimiento del usuario. Esto es lo que ahora llamamos virus, *spyware* o ransomware, etc. Se adjunta un código malicioso al código legítimo, luego es propagado y ejecutado por ellos mismos. Se pueden clasificar el diferente programa maligno (CheckPoint, 2024; CSIRT, 2022):
- Virus: Un software malicioso que se adjunta a cualquier programa informático, se replica y modifica códigos cuando se ejecuta.
- Gusanos: Se propagan a través de computadoras o redes a través de adjuntos de correo electrónico.
- Troyanos: Uno de los *programas malignos* más peligrosos que tiene una función maliciosa. Se esconde en un programa útil y no se replica como los virus.
- Ransomware: Un tipo de software malicioso que bloquea los datos del usuario y lo amenaza a menos que se pague el rescate. Es muy difícil prevenir este ataque a pesar de que el código es simple.
- Spyware: Un tipo de *programa maligno* que inspecciona la actividad del usuario sin su aprobación y la informa al agresor.

Recientemente se puede observar un incremento en el uso del ataque de ransomware, y mayor aún durante la pandemia de COVID-19 en el 2020. A medida que el paradigma del lugar de trabajo se trasladaba al hogar, resultaba en controles de seguridad más débiles. Los atacantes atrajeron a las personas a través de programas temáticos de COVID-19 y correos electrónicos de *phishing*. Por ejemplo, muchas campañas de *phishing* se encargaron de incitar a los usuarios a hacer clic en enlaces específicos para obtener información confidencial, información relacionada con una vacuna de COVID-19, escasez de mascarillas, etc. Los atacantes hicieron buen uso de falsos informes de COVID-19 e información actualizada como gancho para lanzar ataques de *phishing* más exitosos.

El ransomware ha sido el ataque por excelencia de parte de los atacantes, ya que otorga el poder de extorsionar a los afectados solicitando un pago normalmente en criptomonedas como Bitcoin (Beaman et al., 2021).

El ransomware se puede dividir en dos tipos básicos (Richardson, 2017):

- Ransomware de bloqueos: Esta versión bloquea la computadora u otros dispositivos, impidiendo que las víctimas los utilicen. Los datos almacenados en el dispositivo normalmente no se modifican. Como resultado, si se elimina el *programa maligno*, los datos están intactos. Incluso si el *programa maligno* no se puede eliminar fácilmente, los datos a menudo se pueden recuperar moviendo el dispositivo de almacenamiento, generalmente un disco duro, a otra computadora que funcione. Esto hace que el ransomware de bloqueo sea mucho menos eficaz.
- Crypto ransomware: Esta cifra los datos, por lo que incluso si el *programa maligno* se elimina del dispositivo o el medio de almacenamiento se mueve a otro dispositivo, no se podrá acceder a los datos. Normalmente, este ataque no se dirige a archivos críticos del sistema, lo que permite que el dispositivo siga funcionando a pesar de estar infectado. Esto es debido a que sea posible colocar un mensaje o señalización para que se pueda realizar un pago como parte de la extorsión.
- El ransomware debe comunicarse con un servidor para obtener una clave de cifrado e informar sus resultados. Esto requiere un servidor alojado por una empresa que ignora la actividad ilegal y garantiza el anonimato de los atacantes. Estas empresas de *hosting* se llaman "Alojamiento BulletProof". La mayoría están ubicadas en China o Rusia. Los atacantes también utilizan un proxy o servicios VPN para disfrazar aún más el origen de estos ataques.
- Los afectados, que pueden ser organizaciones, empresas o usuarios individuales, se enfrentan a la decisión de pagar o no cuando carecen de copias de seguridad adecuadas para recuperarse de los ataques. Como tal, la decisión se reduce a dos preguntas: ¿Valen tanto los datos como para pagar la extorsión?

¿Se podrá confiar en que descifren los datos luego de pagar al atacante? (Richardson, 2017).

Materiales y métodos

En nuestra investigación, hemos encontrado, luego de haber revisado un grupo importante de documentos, cómo prevenir o mitigar el efecto ransomware en los sistemas informáticos (Veritas, s.f.):

Copias de seguridad: Si se realiza una copia de seguridad de los datos, no es necesario pagar un rescate para recuperarlos, aunque se aconseja que las copias de seguridad estén actualizadas. Algunos ransomware intentan cifrar los sistemas de copias de seguridad conectados localmente. Esto se mitiga cumpliendo con la norma 3-2-1 de almacenamiento, la cual consiste en tener 3 copias, donde 2 de ellas estén en formato distinto y una en un lugar remoto a donde no esté el equipo.

El bloqueo de los enlaces y archivos adjuntos de correo electrónico de origen malicioso: Los ataques de *phishing* son la forma más común de propagación de ransomware, por lo que evitar hacer clic en enlaces o abrir archivos adjuntos en correos electrónicos no deseados contribuye en gran medida a prevenir el ransomware. Sin embargo, los delincuentes también han comenzado a utilizar publicidad comprometida (*publicidad maliciosa*) para difundir ransomware. Estos pueden apuntar a sitios webs confiables. Los bloqueadores de anuncios pueden proteger contra la publicidad maliciosa.

Actualizar (*Patch*) y bloquear: El sistema operativo, los navegadores y el software de seguridad siempre deben estar actualizados. Del mismo modo, los complementos de terceros, como Java y Flash, deben mantenerse actualizados. Los sistemas empresariales disponen de un sistema de gestión de accesos tanto de usuarios como de equipos por medio de la red para reducir la posibilidad de una infección.

Desconexión y aislamiento: Al primer signo de infección, la máquina infectada se apaga inmediatamente (o desenchufa) para minimizar el daño a los archivos. Si está

conectada a una red, los administradores cierran inmediatamente la red para minimizar la propagación del ransomware.

Todos estos puntos deben estar regidos bajo el mandato o supervisión de políticas y controles de seguridad, y protocolos de gestión de riesgos e incidencias. Se recomienda a toda organización o persona individual hacer uso de procedimientos, políticas o controles de seguridad para poder proteger diversos formatos de datos e infraestructuras importantes.

Se considera un control de seguridad cualquier tipo de protección o contramedida utilizada para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad de la propiedad física, la información, los sistemas informáticos u otros activos.

Resultados

Controles de seguridad ante el ransomware

Hay varios tipos de controles de seguridad que se pueden implementar para proteger hardware, software, redes y datos de acciones y eventos que podrían causar pérdidas o daños (IBM, s.f.):

- Los controles de seguridad física: Incluyen medidas como establecer barreras en los perímetros de los centros de datos, cerraduras, guardias, tarjetas de control de acceso, sistemas de control de acceso biométrico, cámaras de vigilancia y sensores de detección de intrusiones.
- Los controles de seguridad digital: Incluyen elementos como nombres de usuario y contraseñas, autenticación de dos factores, software antivirus y *firewalls*.
- Los controles de ciberseguridad: Incluyen cualquier elemento diseñado específicamente para evitar ataques a los datos, incluidos la mitigación de DDoS y sistemas de prevención de intrusiones.
- Los controles de seguridad en la nube: Incluyen las medidas que se toman en colaboración con un proveedor de servicios en la nube para garantizar la protección necesaria para los datos y las cargas de trabajo. Si su organización ejecuta cargas de trabajo en la nube, debe cumplir con los requisitos de seguridad

de sus políticas corporativas o comerciales, además de las regulaciones de la industria.

Luego de haber revisado los controles y conocer la complejidad de los ataques de ransomware, se presenta en la siguiente sección la actualidad del ransomware.

La actualidad del ransomware (Un caso de Estudio)

En la actualidad existen diversas investigaciones innovadoras para mitigar y responder ante un ataque de ransomware. Para destacar uno de esos, está descrito en un artículo publicado para *Future Internet* llamado: “Ransomware-Resilient Self-Healing XML Documents” (Al-Dwairi et al., 2022).

El artículo propone la implementación de una metodología de control de versiones que, por lo general, se utiliza en la administración de código de programación. Esta metodología funciona guardando copias de cada archivo de código cada vez que ha tenido alguna alteración o modificación por parte de un programador. Esto permite que, en el caso de que un cambio no haya sido el correcto o provoque problemas en el código, pueda ser revertido a un punto anterior de manera controlada.

Se propone la aplicación de esta metodología de control de versiones a documentos XML (documentos de Microsoft Word, Microsoft Excel, PDF, etc.), es decir, generar copias en base a las modificaciones que se van realizando al documento. Adicional al control de versiones, se propone la protección de las copias bajo cifrado o protección a nivel de gestión de usuarios para evitar que en el evento de un ataque de ransomware, este no pueda afectar a estos archivos.

Aparte de la propuesta descrita, varias empresas encargadas de ofrecer soluciones de seguridad, dispositivos de red basados en seguridad, han comenzado a integrar Inteligencia Artificial para que sea la encargada de monitorear, aprender y accionar ante los procesos que ocurran dentro de un equipo computacional o una red. La protección contra el ransomware es fundamental en la era digital actual, donde las amenazas cibernéticas están en constante evolución y pueden causar graves daños a individuos y organizaciones. Para salvaguardarse contra este tipo de ataques, es crucial implementar una combinación de medidas preventivas y de respuesta.

Además, mantener el software y los sistemas operativos actualizados con los últimos parches de seguridad puede cerrar las vulnerabilidades conocidas que los ciberdelincuentes podrían aprovechar. La implementación de *firewalls* y software antivirus robustos también puede ayudar a detectar y bloquear posibles amenazas.

Discusión

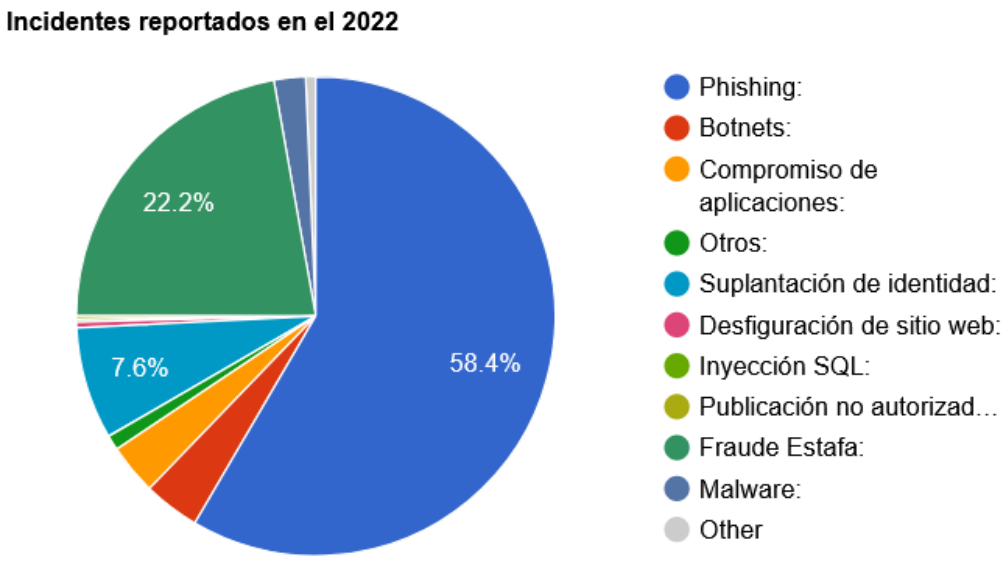
La solución o técnicas brindadas por el articulo generan dudas como ¿Entorpece la funcionalidad normal de un equipo informático? ¿Realmente quedan protegidos los documentos? ¿Qué tan complejo es implementar lo propuesto? Pero inicialmente ¿Las empresas e instituciones de Panamá aplican medidas ante el ransomware?

Panamá ha realizado esfuerzos concertados para mejorar su ciberseguridad. En 2011, se estableció el CSIRT Panamá (Equipo de Respuesta a Incidentes de Seguridad Informática) bajo la Autoridad Nacional para la Innovación Gubernamental (AIG) para prevenir, identificar y resolver incidentes de seguridad cibernética, y para aumentar la concienciación sobre ciberseguridad en el país (Presidencia de Panamá, 2012).

Los ataques recibidos por empresas y entidades públicas son cada vez más frecuentes. Según Fortinet en su informe “Global de Amenazas de FortiGuard Labs” semestral del 2022, el país tuvo un total de 1,400 millones de intentos de ciberataques en ese año, siendo la amenaza principal el ransomware (Fortinet, 2022). Los eventos registrados o reportados al CSIRT han sido en total 3,820 incidentes (CSIRT, s.f.). Ver Figura 1.

Figura 1

Incidentes reportados hacia el CSIRT (CSIRT).



Cada empresa panameña y entidad pública recibe ciberataques en un promedio de 1,300 veces por semana, siendo los principales objetivos las entidades del gobierno, la banca y empresas de finanzas. CheckPoint comenta sobre un considerable aumento en ciberataques de un 124% a empresas panameñas en relación con el año anterior. Detallando que para julio de 2021 los ciberataques en Panamá representaban un promedio de 581 a cada organización por semana y en julio de 2022 se reportan 1,300 (Seguras, 2022).

En la actualidad la situación de Panamá ha mejorado. CheckPoint publicó “Cyber Security Report 2024” donde marca pautas sobre el estado actual de la ciberseguridad a nivel global. En este reporte, Panamá muestra la obtención de un porcentaje de riesgo de 41.3%, en comparación a 43.1% del 2023 y 47.8% del 2022, siendo una mejora del 1.8% y 6.5% respectivamente en la probabilidad de sufrir algún riesgo informático, teniendo un puntaje similar a países de otras latitudes como Italia (41.5%) (CheckPoint, 2024). En cuanto a la legislación, Panamá ha tomado pasos para alinear su marco legal con los estándares internacionales, incluyendo la modificación del Código Penal y la aprobación del Convenio de Budapest sobre delitos cibernéticos.

Además de la creación de la Ley 81 para la protección de datos personales. En conjunción, la educación y formación en ciberseguridad también son prioridades,

con becas y capacitaciones ofrecidas en colaboración con instituciones internacionales para reducir la escasez de profesionales en este campo. Una herramienta que puede aplicar una empresa o institución en su departamento de tecnología, específicamente en el desarrollo de software, es un sistema basado en GIT. Tiene como objetivo principal el proteger el código que se genera de la programación, pero puede tener una aplicación más diversa.

La implementación de GIT en las empresas e instituciones que tengan códigos fuentes de sus sistemas debe ser casi obligatoria para poder resguardar la integridad de estos. Incorporar GIT no supone un consumo notable tanto en la puesta en marcha como en la funcionalidad del día a día; las funcionalidades que encontramos en GIT se muestran a continuación:

- Control de Versiones Distribuido
  - Repositorios Locales Completos: Cada desarrollador tiene una copia completa del historial del proyecto, lo que permite trabajar sin conexión y realizar operaciones de manera rápida y eficiente.
  - Colaboración: Al permitir que múltiples desarrolladores trabajen en diferentes partes del proyecto simultáneamente, Git facilita la colaboración sin interferencias.
- Seguimiento Detallado de Cambios
  - Historial Completo: Git mantiene un registro detallado de todos los cambios, permitiendo a los desarrolladores ver qué cambios se hicieron, quién los hizo y cuándo.
  - Reversión de Cambios: Es fácil revertir a versiones anteriores del proyecto en caso de errores o problemas.
- Seguridad e Integridad
  - Hashes: Git utiliza *hashes* SHA-1 para identificar de manera única cada cambio realizado, asegurando que el historial no pueda ser alterado sin ser detectado.
- Flexibilidad y Compatibilidad
  - Multiplataforma: Git es compatible con diversos sistemas operativos, incluyendo Windows, macOS y Linux.

Con lo plasmado sobre las funcionalidades de GIT, la propuesta de la cual se centra la discusión hace uso de un sistema GIT para resguardar archivos y no código fuente, lo cual resulta ser novedoso en la forma en que es aplicado. Teniendo en cuenta las preguntas formuladas en esta sección como: ¿Entorpece la funcionalidad normal de un equipo informático? ¿Realmente quedan protegidos los documentos? ¿Qué tan complejo es implementar lo propuesto?

En la propuesta se comenta sobre la creación de un *plug-in* para el aplicativo Word a modo de "prueba de concepto". Una vez con el *plug-in* instalado en el equipo, cuando se finaliza la edición de un documento en Word, el *plug-in* procede a generar un *snapshot* del archivo y a dicho *snapshot* le aplica medidas de seguridad, como los permisos de edición, para que no pueda ser alterado en un posible ataque. Todo esto se realiza en segundo plano sin que se interrumpa al usuario durante el proceso.

El artículo menciona la noción de una limitante: el proceso que se ejecuta en segundo plano y realiza las verificaciones de los permisos de edición de los archivos necesita tener privilegios elevados (Administrador) y que los usuarios que estén utilizando el equipo de cómputo no tengan rango de administrador. Esto plantea el otorgarle permiso de Administrador en el equipo de cómputo al proceso, que puede llegar a ser vulnerable en un hipotético ataque de cadena de suministro. Este tipo de ataque de ciberseguridad se basa en que los atacantes comprometen un componente que forma parte o se integra a los sistemas de software que implementan en las empresas. Estos ataques pueden ser particularmente devastadores porque explotan la confianza que las organizaciones tienen en sus proveedores y en los productos que utilizan.

Pasando al punto sobre la integridad y confidencialidad de los archivos, la propuesta no contempla la posibilidad de cifrar los archivos. Esto significa que, durante un ataque donde se pueda vulnerar la funcionalidad de la propuesta, la información de los archivos queda expuesta para la utilidad del atacante. Si bien los ataques de ransomware se caracterizan por su *modus operandi* de cifrar los archivos de la víctima y pedir un rescate económico, también puede ocurrir que el atacante genere

copias de los archivos para uso propio. Por lo que se podría considerar la implementación adicional de cifrado de los archivos por medio de algoritmos convencionales y robustos como SHA-256 (Fauziah et al., 2019).

Agregar esta funcionalidad adicional a la propuesta podría añadir más carga al procesador del equipo de cómputo en el tiempo de ejecución durante el guardado de un archivo de Word. Esto podría notarse si el equipo de cómputo tiene prestaciones no recomendadas o son bajas para los requisitos mínimos de la propuesta. Esto es debido a que el consumo de poder computacional al momento de cifrar archivos es elevado si el equipo no tiene una unidad especializada para cifrar.

Haciendo un pequeño ejercicio, según la propuesta se menciona que el tiempo tomado por el procesador al realizar la ejecución del proceso no excede los 120 ms (milisegundos) para un archivo de 1 MB (MegaByte). Se hizo el ejercicio indicado en la Figura 2, añadiendo el cifrado del archivo, lo que sumaría unos 12 ms, lo cual no representa un impacto significativo para el uso normal del equipo de cómputo.

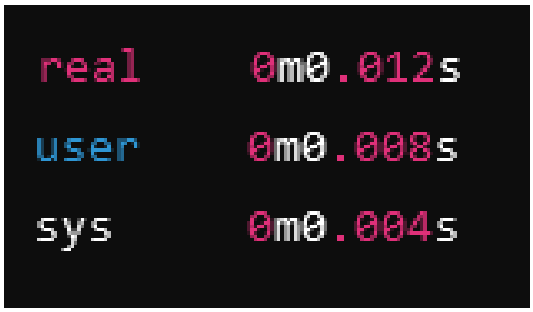
Utilizando los siguientes comandos:

- dd if=/dev/zero of=testfile bs=1M count=1
  (Crea un archivo de 1MB de tamaño).

- time openssl enc -aes-256-cbc -salt -in testfile -out testfile.enc -pass pass:mysecurepassword
  (Cifra el archivo recién creado por el comando anterior

Figura 2

Resultados sobre el cifrado de un archivo de 1MB



Respecto al cifrado, la implementación a nivel de rendimiento no añadiría al consumo y ejecución siempre y cuando se maneje en archivos pequeños ya que a medida que aumenta el tamaño, el consumo aumenta.

Conclusiones

La propuesta discutida en este documento muestra la aplicación de una metodología que normalmente se utiliza en el área de la programación al entorno de uso cotidiano para los usuarios de equipos de cómputo. Esta metodología ofrece protección a los documentos que son tratados por ella ante ataques de ransomware y de la pérdida de la integridad del archivo. Esto muestra que tiene un impacto mínimo o casi imperceptible para el equipo de cómputo y para el usuario.

Adicionalmente, en este documento se planteó la posibilidad de añadir el cifrado de los documentos utilizando una técnica de cifrado como SHA-256 durante la ejecución de la metodología, para tener un grado mayor de protección. Esto con la premisa de que, si bien no se adultera el archivo durante un ataque de ransomware, también se pueden extraer archivos que quedan expuestos ante los atacantes. Al cifrarlos, los atacantes no podrán tener acceso al contenido del archivo. Adicionalmente al planteamiento de agregación del cifrado de archivos, se realizó una pequeña prueba de tiempo para determinar si afectaba a la usabilidad de los usuarios y equipos de cómputo, con un resultado de afectación imperceptible.

Referencias bibliográficas

Al-Dwairi, M., Shatnawi, A. S., Al-Khaleel, O., & Al-Duwairi, B. (2022). *Ransomware-Resilient Self-Healing XML Documents*. Future Internet, *14*(4), 118. https://doi.org/10.3390/fi14040118

Alcántara, M., & Melgar, A. (2016). Risk Management in Information Security: A Systematic Review. Journal of Advances in Information Technology, *7*(1), 1-13. https://www.semanticscholar.org/paper/Risk-Management-in-Information-Security%3A-A-Review-Alcantara-Melgar/eecec6f2c2822abd7077238cb636734f182de218

Beaman, C., Barkworth, J., Akande, T., Hakak, S., & Khan, H. A. (2021). The Impact of the COVID-19 Pandemic on Ransomware Attacks. 2021 International Conference on Information Networking (ICOIN), 638-643. https://doi.org/10.1109/ICOIN51403.2021.9392211

Biju, J. M. (2019). Types of Cyber Attacks and Their Prevention Methods. International Journal of Advanced Engineering and Management, *4*(2), 1-5. https://www.ijamr.com/index.php/ijamr/article/view/100088

Bouam, M., Bouillaguet, C., Delaplace, C., & Noûs, C. (2021). A Survey on Cyber-Attacks and Their Impact on Modern Society. Journal of Cybersecurity and Digital Forensics, *4*(2), 1-15. https://www.jcdf.eu/index.php/jcdf/article/view/123

CheckPoint. (2024). *Cyber Security Report 2024*. Recuperado de https://www.checkpoint.com/downloads/downloads-reports/2024-cyber-security-report.pdf

CSIRT. (2022). *Ransomware: una amenaza para la seguridad de la información*. Recuperado de https://csirt.gob.cl/vulnerabilidades/ransomware-una-amenaza-para-la-seguridad-de-la-informacion/

CSIRT. (s.f.). *Incidentes reportados hacia el CSIRT*. [Gráfico].

Fauziah, R., Rachmawanto, E. H., Setiadi, D., & Sari, C. A. (2019). An Overview of SHA-256 and Its Implementation in Digital Signature. Journal of Physics:

Conference Series, *1374*(1). https://doi.org/10.1088/1742-6596/1374/1/012015

Fortinet. (2022). *Global Threat Landscape Report 2022*. Recuperado de https://www.fortinet.com/content/dam/fortinet/assets/reports/report/2022-fortiguard-labs-global-threat-landscape-report.pdf

IBM. (s.f.). *What are security controls?* Recuperado de https://es.wiktionary.org/wiki/complet%C3%A1

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. SAGE Publications.

Presidencia de Panamá. (2012). *Decreto Ejecutivo No. 403 de 2012*. https://www.gacetaoficial.gob.pa/pdfTemp/27043_A/Gaceta Oficial.pdf

Richardson, R. (2017). Ransomware: A Comprehensive Guide to Prevention, Detection, and Recovery. SAGE Publications.

Seguras, J. (2022). *Ciberataques en Panamá se incrementan 124%*. La Prensa. https://www.prensa.com/economia/ciberataques-en-panama-se-incrementan-124-en-un-ano/

Veritas. (s.f.). *Ransomware Prevention and Protection*. https://www.veritas.com/services/ransomware-protection