ALMACENAMIENTO SINCRÓNICO VERSIONADO COMO CAPA DE SEGURIDAD ADICIONAL FRENTE AL CRYPTOVIRUS RANSOMWARE

SYNCHRONOUS VERSIONED STORAGE AS AN ADDED SECURITY LAYER AGAINST OF CRYPTO-RANSOMWARE

AUTOR
HOLZEN A. MARTÍNEZ-GARCÍA
Doctor en Sistemas Computacionales
*Instituto Tecnológico Superior Progreso
Profesor de Tiempo Completo
Departamento de Ingeniería en Sistemas Computacionales
hmartinez@itsprogreso.edu.mx
MÉXICO

AUTOR
MELQUIZEDEC MOO MEDINA
Maestro en Tecnologías de Información
*Instituto Tecnológico Superior Progreso
Profesor de Tiempo Completo
Departamento de Ingeniería en Sistemas Computacionales
mmoo@itsprogreso.edu.mx
MÉXICO

AUTOR
GANDHI S. HERNÁNDEZ-CHAN
Doctor en Ciencia y Tecnología Informática
**Universidad Tecnológica Metropolitana
Profesor de Tiempo Completo
División de Tecnologías de la Información y Comunicación
gandhi.hernandez@utmetropolitana.edu.mx
MÉXICO

***INSTITUCIÓN**
Instituto Tecnológico Superior Progreso
ITSProgreso
Institución de Educación Superior Tecnológica
Victor M. Cervera Pacheco S/N x 62
Progreso, Yucatán.
difusion@itsprogreso.edu.mx
MÉXICO

****INSTITUCIÓN**
Universidad Tecnológica Metropolitana
UTM
Universidad Pública Tecnológica
Circuito Colonias Sur No. 404 Santa Rosa, Mérida, Yucatán.
utm@utmetropolitana.edu.mx
MÉXICO

INFORMACIÓN DE LA INVESTIGACIÓN O DEL PROYECTO: El proyecto que da soporte al presente trabajo de investigación se titula "Cloud Storage para neutralizar los efectos del ransomware en datos sensibles", el cual fue promovido por el Programa para el Desarrollo Profesional Docente (PRODEP), y registrado en el Instituto Tecnológico Superior Progreso con clave de registro 007/2015. Cabe resaltar que, adicionalmente, este proyecto obtuvo financiamiento económico proveniente de la Convocatoria de Apoyo a Proyectos de Investigación Científica, Aplicada, Desarrollo Tecnológico e Innovación 2015, convocatoria del Tecnológico Nacional de México, a fin de presentar los resultados finales en diciembre de 2016.

RECEPCIÓN: 9 de Enero de 2017 **ACEPTACIÓN:** 28 de Abril de 2017

TEMÁTICA: Seguridad Informática

TIPO DE ARTÍCULO: Artículo de Investigación Científica e Innovación

Forma de citar: Martínez-García, H., Moo, M., Hernández-Chan, G. (2017). Almacenamiento sincrónico versionado como capa de seguridad adicional frente al Cryptovirus Ransomware. En R, Llamosa Villalba (Ed.). Revista Gerencia Tecnológica Informática, 16(44), 65-76. ISSN 1657-8236.

RESUMEN ANALÍTICO

El presente trabajo aborda el problema de cifrado de datos de manera no autorizada a causa del ransomware criptográfico, un tipo de malware con alta efectividad en su cometido. Los cibercriminales utilizan este tipo de malware para obtener un beneficio económico ilegalmente, lo que ha provocado pérdidas económicas considerables alrededor del mundo. Si bien existen los métodos tradicionales de protección para evitar una infección con este tipo de malware, el estudio realizado se basa en la premisa de que la infección es inminente y propone un esquema de almacenamiento con tecnología de nube, combinando el control de versiones y el respaldo sincrónico, para poder recuperar los datos e información afectados en caso de un ataque eventual por ransomware criptográfico. Se trata, en resumen, de un estudio experimental que involucró trabajo de campo y de desarrollo, innovando los conceptos ya existentes para darle un nuevo uso distinto a su área de aplicación, y así solucionar una problemática de alto impacto en la actualidad mediante un esquema genérico, económico y escalable a cualquier magnitud y tamaño de infraestructura.

PALABRAS CLAVES: Almacenamiento Sincrónico Versionado/Integridad y Disponibilidad/Software malicioso/Ransomware.

ANALYTICAL SUMMARY

This work aim the problem of data encryption in an unauthorized way because of the crypto-ransomware, a type of malware with high effectiveness in its task. Cybercriminals use this type of malware to obtain a ilegal economic benefit, which has caused sizeable economic losses around the world. Although traditional protection methods exist to avoid infection with this type of malware, the study is based on the premise that the infection is imminent, and proposes a storage scheme with cloud technology, combining version control and synchronous backup, in order to recover the data and information affected in case of an eventual attack by crypto-ransomware. This is, in summary, an experimental study involving field work and development, innovating existing concepts to give it a new use different from its area of application, and thus solve a problem of high impact today through a scheme Generic, economical and scalable to any magnitude and size of infrastructure.

KEYWORDS: Synchronous Versioned Storage/Integrity and Availability/Malware/Ransomware

INTRODUCCIÓN

Hoy en día, es innegable que las tecnologías de la información y comunicación han revolucionado al mundo. Muchos procesos diarios de la sociedad son apoyados por algún tipo de dispositivo tecnológico, de tal manera que mientras más avanza la historia de la humanidad, las personas vuelcan su vida en la tecnología de una manera cada vez mayor.

Con la finalidad de aprovechar las bondades que la tecnología ofrece, las empresas también la han adoptado en sus procesos de negocio y comunicación. Los procesos naturales de la sociedad han evolucionado, y con este fenómeno, también han aparecido personas que ven la tecnología como una excelente plataforma para cometer acciones ilícitas, con el fin de obtener un beneficio incluso a costa de los demás [1].

El presente estudio realizado tiene como contexto un mundo globalizado, donde la importancia de mantener los datos es cada vez mayor en proporción con el avance tecnológico. Sánchez [2] toma como referencia la norma ISO 27001:2013 cuando afirma que la información es un activo que, como otros activos comerciales importantes, tiene un alto valor para la organización y, en consecuencia, necesita ser protegido adecuadamente.

Los cibercriminales han adoptado técnicas variadas para lucrar con este principio. Una de las más actuales y peligrosas es la infección de dispositivos con ransomware criptográfico. El crecimiento de este malware ha sido exponencial, de tal manera que en 2013 la magnitud se estimó en un aumento del 500% en proporción comparada con los ataques lanzados en 2012 [3]. Esta cifra incrementó en los años posteriores, lo que permite proyectar que la amenaza seguirá vigente en el futuro.

De acuerdo con los reportes de seguridad en 2016, el ransomware criptográfico creció un 35% durante el año 2015. Considerado como un tipo extremadamente rentable de ataque, se espera que el ransomware continúe iludiendo a los usuarios de PC y se expanda a cualquier dispositivo conectado a la red que pueda mantenerse como rehén para obtener lucro [4].

Si bien ya existen soluciones en el mercado que ayudan en la detección de ransomware en algunas de sus variantes, la presente investigación tiene como premisa la inminente infección de algún tipo de ransomware criptográfico en el sistema a proteger. Pretende apoyar a los administradores de TI e infraestructura computacional ofreciendo una capa de seguridad extra basada en control de versiones y respaldo sincrónico para complementar la seguridad en la integridad y disponibilidad de los datos. Aunque existen algunos estudios acerca del ransomware, estos informes se centran principalmente en los avances en ataques ransomware y sus niveles de sofisticación, en lugar de proporcionar algunas ideas sobre técnicas de defensa efectiva que deban adoptarse contra esta amenaza [5].

La propuesta se basa en el uso de un sistema de almacenamiento que implemente el modelo de computación en nube local, en combinación del respaldo sincrónico y el control de versiones en una entidad diferente al equipo hipotéticamente atacado por una cepa de ransomware criptográfico. Esto permite eventualmente la recuperación de los datos con la restauración de históricos almacenados. El modelo se presenta de una manera simple y genérica, que puede ser escalable y adaptable para cualquier tamaño de infraestructura, e incluso con la posibilidad de ser replicada por particulares que deseen añadir una capa de seguridad y proteger su información.

A continuación se presenta la hipótesis de investigación.

Hipótesis de investigación (H_1): La implementación de un sistema de almacenamiento sincrónico versionado en nube local permite la recuperación efectiva de datos ante un ataque del tipo ransomware.

1. MARCO REFERENCIAL

1.1 DEFINICIÓN DEL RANSOMWARE

El ransomware es un tipo de malware que utiliza técnicas y algoritmos de cifrado para secuestrar un bien informático virtual, tal como los datos, o funcionalidades del sistema operativo. Esto lo hace generalmente con el fin de extorsionar al usuario o dueño del bien y obtener algún beneficio económico.

De acuerdo a Ruiz [6], este tipo de malware mantiene cautivo el dispositivo exigiendo un rescate.

El modus operandi de este tipo de software malicioso se basa en cifrar archivos del disco o bloquear el acceso al sistema completa o parcialmente hasta que el usuario paga al creador del malware, por lo general con monedas digitales como el bitcoin.

El ransomware se define como la extorsión digital mediante el uso de un malware que infecta un sistema informático, el cual puede ser atacado desde diferentes vectores, los cuales pueden ser desde exploits de navegador, descarga e instalación de aplicaciones freeware, adjuntos de correo electrónico, anuncios que ofrecen dinero en efectivo e incentivos para invitar a víctimas potenciales a caer en el engaño [7].

1.2 ORÍGENES DEL RANSOMWARE

De acuerdo a Gazet [8] el ransomware tiene sus inicios en 1989, cuando se propagó por primera vez un malware de este tipo en aquella época. La forma de propagación se dio mediante el envío masivo de discos flexibles de 3 ½ pulgadas a través del correo postal. Estos discos se presentaban como portadores de información privilegiada que ayudaría a encontrar una cura contra el Síndrome de Inmuno Deficiencia Adquirida. Al ingresarlos al equipo informático, el troyano se activaba e internamente colocaba un contador que esperaba el reinicio del anfitrión para ir en aumento. Cuando el equipo anfitrión tenía su reinicio número 90, el malware cifraba los nombres de los archivos, lo que dejaba inutilizable el equipo anfitrión y las aplicaciones.

Las víctimas podían ver el archivo de licencia, el cual solicitaba dos tipos de pago de rescate diferentes, ya sea por 365 aplicaciones funcionales o por el disco duro completo. El pago debía hacerse vía cheque bancario con unos datos específicos a la compañía "Pc Cyborg Corporation". Por eso este malware fue conocido como "AIDS info disk" o "PC Cyborg Trojan". El cifrado resultó ser débil: un algoritmo de cifrado mono alfabético. Sin embargo, el primer antecedente de ransomware había surgido.

A partir de ese momento, los investigadores en seguridad tomaron interés en este campo, y a pesar de que surgían nuevas variantes de este malware, los cambios tecnológicos y las regulaciones en los sistemas de pago hacían que la efectividad de este ataque mermase. Durante algunos años se mantuvo bajo el índice de ataques con este comportamiento. Sin embargo, el uso de cifrado cada vez más complejo y los sistemas de moneda digitales harían que resurgiese el uso de ransomware.

1.3 CLASIFICACIÓN DEL RANSOMWARE

El ransomware se cataloga en dos tipos de acuerdo a su forma de extorsionar a la víctima. Estas dos variantes son: ransomware-crypto (o ransomware criptográfico) y rasomware-locker [7].

El ransomware-locker se centra en el sistema operativo o sus funcionalidades, lo que ha permitido a usuarios con conocimientos técnicos en computación la posibilidad de rescatar los datos y reinstalar la funcionalidad de la parte afectada. El impacto y efectividad de este ransomware es menor en comparativa con el criptográfico, por lo cual cada vez es menor la tasa de ataques de este tipo.

Un ransomware es clasificado como criptográfico cuando su comportamiento está orientado a cifrar los datos almacenados para dejarlos inservibles e ilegibles para un ser humano y de esta manera exigir un rescate económico, por lo general en moneda digital. Esto obliga al usuario final a pagar hasta obtener la clave de descifrado. Por lo general, no se afectan los archivos del sistema operativo ni sus funcionalidades, a fin de que el usuario pueda abrir y comprobar que los archivos se encuentran cifrados e ilegibles. Las imágenes, los videos, archivos de texto, y archivos con extensiones comunes son los objetivos de esta categoría.

El ransomware criptográfico representa la infección por ransomware más esparcida en la actualidad. El éxito y la efectividad de este ataque se consolidan en gran porcentaje gracias a la ingeniería social. Aunque esta técnica no es única, es un hecho que explota ciertas características propias del ser humano manipulándolo psicológicamente o mediante el engaño para instarlo a hacer (o dejar de hacer) alguna operación sensible y que permite al ciberdelincuente proseguir con el ataque [9]. Las técnicas de ingeniería social pueden ser variadas, pero no necesariamente exclusivas entre sí [10].

En la actualidad, los niveles de afectación del ransomware son cada vez mayores. De acuerdo al Internet Crime Complaint Center, entre abril de 2014 y junio de 2015 el FBI recibió 992 reportes relacionados a CryptoWall y otras variantes de ransomware cuyas víctimas tuvieron pérdidas económicas que llegaron a los 18 millones de dólares [11].

CryptoWall y sus cepas derivadas han estado en uso activamente desde abril de 2014, para infectar víctimas que incurren en gastos no solo por el rescate que piden los cibercriminales detrás, sino también por otros costos asociados. A este rescate, que oscila entre 200 y 10 mil dólares, se suman la pérdida de productividad, la mitigación del riesgo en la red, los servicios de Tecnologías de Información, tasas legales, y más [12].

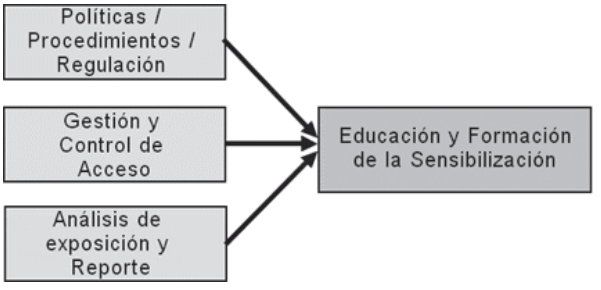
Tal como señala el informe del IC3, estos fraudes financieros afectan tanto a individuos como a compañías del sector empresarial.

1.4 ESTUDIOS RELEVANTES

A continuación se lista una serie de trabajos consultados para este proyecto de investigación, los cuales tienen relación directa con la problemática descrita, que sin embargo tienen un enfoque diferente al propuesto en estas líneas.

Luo y Liao [13] proponen un framework basado en cuatro etapas para prevenir la infección por ransomware en las organizaciones. Para estos autores, la clave es disuadir proactivamente los ataques de ransomware a través de la conciencia en la gestión integral, en las tecnologías de información y en el nivel de usuario final. Esta propuesta se encuentra representada en la Figura 1.

FIGURA 1. Framework preventivo propuesto por Luo y Liao.



Fuente: Elaboración propia basada en [13]

Otro trabajo interesante que se relaciona es el de Gazet [8], en el cual se hace una comparativa de varias muestras de ransomware, su comportamiento, tipo de cifrado y la forma de extorsión al usuario, entre otros datos. Se trata de un trabajo informativo y documental para comprender este fenómeno y la importancia de tener un esquema de protección adecuado.

O'Gorman y McDonald [14] también ofrecen datos relevantes en cuanto a infección por ransomware se refiere. Estos autores proporcionan un panorama geográfico de distribución del ransomware, y recomiendan algunas estrategias de mitigación, principalmente en la actualización instantánea de sistemas para evitar que alguna muestra aproveche un bug conocido de versiones viejas de software.

Bhardwaj et al. [7] ofrecen un panorama distinto a los anteriores, consistente en un servicio en nube para la mitigación del ransomware, al cual se nombra MDaaS

(Malware Detection as a Service). Ellos realizaron y registraron las pruebas con este servicio propuesto, mezclando muestras de malware de todas las familias, entre ellas el ransomware. El esquema propuesto se presenta en la Figura 2.

FIGURA 2. Propuesta de análisis de malware en nube.

Fuente: Elaboración propia basada en [7]

Los resultados de este sistema, en palabras de sus autores, son satisfactorios con distintos tipos de malware. Para ellos, la detección del malware mediante sistemas de análisis en nube, son líneas de investigación que deben seguir su curso para fortalecer esta área. Sin embargo, concluyen que el estado actual de esta propuesta es ineficiente contra el ransomware, afirmando que este tipo de malware tiene cierta ventaja sobre los sistemas de detección, proyectando que otros usuarios seguirán siendo afectados con la infección y extorsión digital.

2. METODOLOGÍA

De acuerdo a Moreno [15] el tipo de estudio que se realizó según su propósito fundamental es de desarrollo, dado que se centra en derivar de la teoría existente elementos para innovar y adaptar materiales en el campo en que se desenvuelve, en este caso la seguridad de la información. Por sus fuentes su naturaleza es de campo, ya que se recurrió al contacto directo con los hechos o fenómenos que se encuentran en estudio, pues se provocaron fenómenos para medirlos; y por su forma y momento cae en la categoría experimental, pues el investigador manipuló la variable independiente para conocer los efectos que ésta produce en la variable dependiente que es del interés del estudio.

La metodología incluyó dos fases primordiales para esta investigación de tipo experimental. Como primera fase se realizó un estudio de caso con dos mediciones, por lo que se realizó un pre experimento con tratamiento múltiple, preprueba y posprueba.

Esquema del diseño:

$$\mathbf{G\ O\ X_1\ O\ X_2\ O}$$ donde:

G = Grupo de sujetos, en este caso un equipo de cómputo con sistema operativo virtualizado que contiene una serie de archivos íntegros en diferentes formatos (extensiones, tales como xlsx, pdf, pptx, docx, entre otros) sincronizados con el servicio de almacenamiento en la nube Dropbox. Este equipo es operado por una persona.

O = Medición o prueba, la cual consistió en verificar que los archivos y datos objetivo sean legibles y utilizables, para luego registrar los resultados.

X_1 = Tratamiento primario, que consistió en aplicar al equipo de cómputo un ransomware open source, configurado para atacar los datos objetivo.

X_2 = Tratamiento secundario, consiste en aplicar el control de versiones que incluye Dropbox en los archivos objetivo que han sido cifrados.

Seguidamente después de confirmar que el sistema de Dropbox fue efectivo en la recuperación de archivos, se procedió a la fase dos, que consistió en analizar el éxito de la arquitectura para replicarla en un entorno local y distribuido. Se desarrolló la arquitectura de red con características de respaldo sincrónico y control de versiones, un software denominado centinela para los nodos finales en la red y se aplicó un experimento verdadero tratamiento múltiple con preprueba, posprueba y grupo de control.

Diseño del experimento:

$$\mathbf{RG_1\ O\ X_1\ O\ X_2\ O}$$
$$\mathbf{RG_2\ O\ --\ O\ --\ O}$$ donde:

RG_1 = Grupo de interés. Consiste en una red de computadoras con archivos íntegros dentro de la arquitectura de red con el servidor de almacenamiento que contiene las características observadas en el preexperimento anterior, las cuales son respaldo de datos sincrónico y control de versiones. Cada computadora tiene un cliente que sincroniza los datos del equipo

con el servidor de almacenamiento y respaldo, además de un software monitor de los mismos. Es importante recalcar que no se les instaló antivirus alguno, pues el propósito era infectar con ransomware criptográfico y probar la recuperación deseada. La R previa significa aleatoriedad que se refleja en el grupo de personas que operó dichos equipos de cómputo.

RG_2 = Grupo de control. Consiste en una segunda red de computadoras con archivos íntegros dentro de una red con arquitectura tradicional que no incluye respaldo de datos sincrónicos. El servidor no contiene las características observadas en el preexperimento anterior ni los equipos de cómputo software de monitoreo de archivos alguno. Tampoco tienen antivirus alguno.

X_1 = Tratamiento primario, el cual consiste en infectar los datos objetivo con ransomware.

X_2 = Tratamiento secundario, que consiste en aplicar el control de versiones mediante imagen de sistema del servidor.

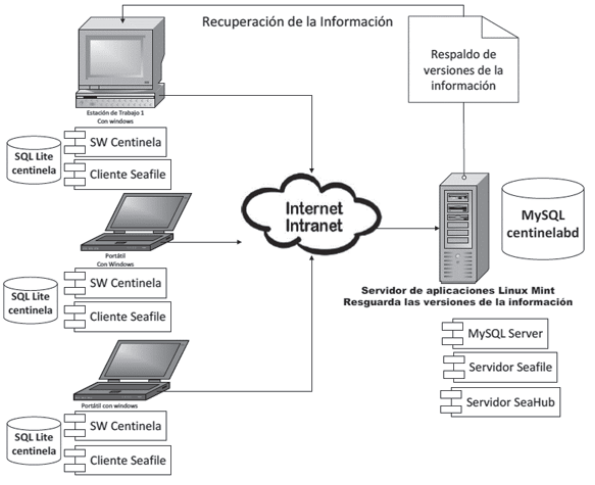
O_1 = Medición u observación. Verifica que los archivos sean íntegros en el tiempo de la observación y se registran los resultados.

El ransomware criptográfico utilizado para esta prueba fue Hidden Tear, cuyo análisis se ha hecho en estudios previos [16]. Este ransomware originalmente fue distribuido como código abierto y para fines meramente educativos. Fue liberado en el portal Github en agosto de 2015 por el experto en seguridad informática Utku Sen. El autor ha escrito el código de fuente abierta en GitHub para que todos los interesados puedan comprender la anatomía de un ataque ransomware.

Hidden Tear utiliza el bloque de cifrado AES para cifrar los datos, tiene un muy pequeño cargador de tan sólo 12 KB, y cuenta con capacidades de evasión antivirus. Actores de delitos informáticos, por desgracia, utilizan este kit para construir ransomware en el mundo real.

En la fase uno se constató el hecho de que con un sistema de almacenamiento sincrónico versionado en internet hace posible la recuperación de los datos cifrados por ransomware criptográfico. Sin embargo, el sistema utilizado no proveía una recuperación eficiente cuando hay una cantidad indefinida de archivos. La cantidad de archivos cifrados es directamente proporcional al tiempo de restauración, al poder ser restaurados únicamente de manera individual. Esto dio paso a la segunda fase, con la utilización de la arquitectura propuesta para el grupo experimental de 13 alumnos, y al mismo tiempo se tuvo un grupo de control de 13 estudiantes que pasaron por el mismo proceso sin la arquitectura propuesta. Esta arquitectura puede observarse en la Figura 3.

FIGURA 3. Arquitectura propuesta con nube local privada y software centinela.



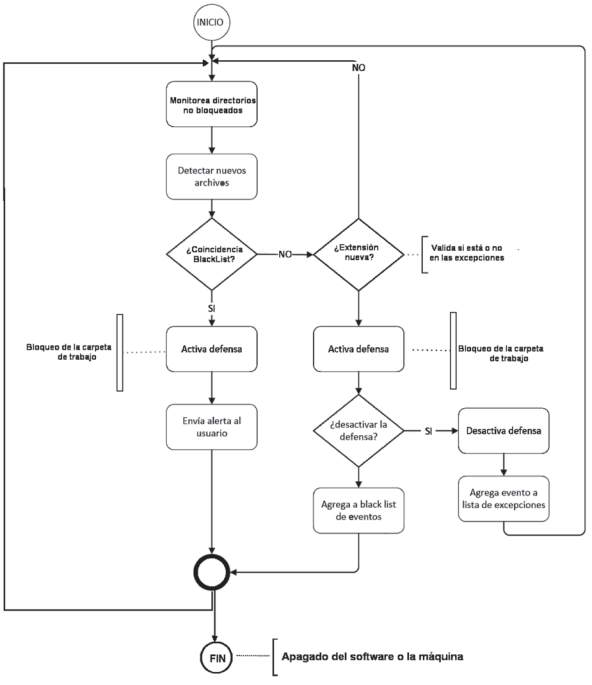
Esta arquitectura consta de un servidor de aplicaciones con el sistema operativo con el kernel Linux. Para efectos de este proyecto de investigación se optó por el sistema Linux Mint, en su versión 17.3 de 64 bits. La elección de un sistema operativo diferente al instalado en los clientes es parte importante para que se minimice al máximo el riesgo de ser infectado por ransomware, en caso que este se propagara en la red como un gusano, ya que si por alguna razón llegara al servidor, se reducen las probabilidades de verse afectado.

El sistema informático propuesto tiene diversos servicios instalados, los cuales pueden observarse en la Figura 3. El software Seafile Server es el que se encarga del almacenamiento y control de versiones en esta nube privada, con apoyo del módulo Seahub, que se ocupa de la interfaz web para interacción con el usuario. En la capa del cliente se tiene instalado el servidor Seafile, y el Software Centinela, desarrollo propio que surgió como producto de esta investigación.

El software centinela está diseñado para ser un monitor de carpetas configuradas previamente por el usuario. Está desarrollado en C# .NET y se vincula al servidor central de la arquitectura propuesta para bloquear las carpetas monitoreadas en caso de sospecha de ransomware criptográfico. Utiliza una base de datos SQLite de manera local que puede ser actualizada desde un servidor, que para efectos de esta prueba es el mismo que contiene el software de gestión de archivos.

Este centinela está diseñado para proteger de manera individual cada computadora cliente. Su función básica consiste en proporcionar alertas de los cambios realizados en el directorio de trabajo y evitar que el ransomware tenga éxito. Su funcionamiento es descrito brevemente en la Figura 4.

FIGURA 4. Flujo de trabajo de software centinela.



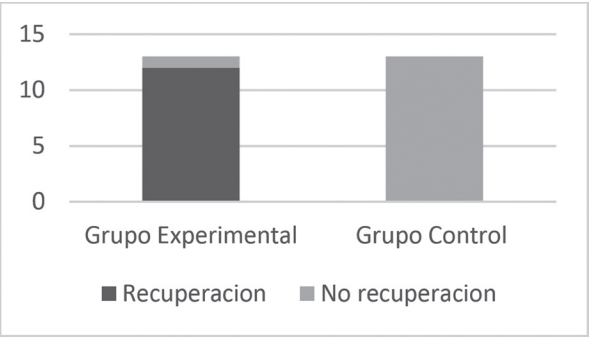
Los pasos a seguir en el experimento fueron los siguientes:

a) Interconectar al grupo experimental a la arquitectura de red propuesta.
b) Instalar el software centinela en las máquinas de los integrantes del grupo experimental.
c) Verificar que el grupo de control se encontrara fuera de la arquitectura de red propuesta.
d) Infectar ambos grupos con el ransomware Hidden Tear.
e) Verificar que los archivos han sido cifrados en ambos grupos.
f) Solicitar a los participantes tratar de recuperar los archivos cifrados sin usar el sistema de almacenamiento.
g) Solicitar a los participantes tratar de recuperar los archivos cifrados a través del sistema de almacenamiento.
h) Registrar resultados obtenidos.

3. RESULTADOS

A excepción de un caso particular en el cual se tuvo problemas persistentes con la red, todos los demás clientes del grupo experimental realizaron la prueba tal y como se había previsto, desde la infección con ransomware hasta la recuperación en un clic desde la interfaz web del servidor de almacenamiento sincrónico. La gráfica de estos resultados se presenta en la Figura 5.

FIGURA 5. Comparación de resultados entre grupos experimental y de control.



Si bien en el grupo experimental se suscitó un caso con problema de comunicación con la red, se contabilizó el elemento como válido ya que las comunicaciones forman parte del sistema. Esta decisión se tomó para no sesgar el estudio y mantenerlo lo más íntegro y confiable posible. Más tarde se comprobó que se produjo un problema interno de hardware con la tarjeta de red, al parecer corrupción de drivers, lo cual derivó en interrupciones y cortes de comunicación en el equipo en cuestión.

Para obtener algunos otros datos, se procedió a elaborar una tabla cruzada, en la cual se puede observar que todos los casos de recuperación efectiva se dieron cuando se utilizó el sistema de almacenamiento propuesto, con una efectividad del 92.3%, solamente un fallo que representa el 7.7% del total y que se dio precisamente por el error de comunicación en el sistema. Los datos obtenidos de la tabla son descritos en la Tabla 1.

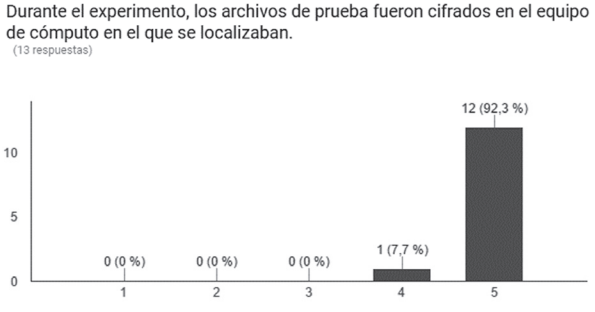
TABLA 1. Cruce de resultados Recuperación x Sistema de Almacenamiento propuesto.

			Sistema de Almacenamiento		Total
			No utilizado	Utilizado	
Recuperación	No efectiva	Recuento	13	1	14
		% dentro de Sistema de Almacenamiento	100.0%	7.7%	53.8%
	Efectiva	Recuento	0	12	12
		% dentro de Sistema de Almacenamiento	0.0%	92.3%	46.2%
Total		Recuento	13	13	26

Terminada la fase experimental, se realizó un test de Likert al grupo experimental de la prueba, para conocer sus actitudes frente a la propuesta. La escala fue del 1 al 5, donde 1 representa en total desacuerdo, y 5 en total acuerdo, con el valor 3 como ni acuerdo ni desacuerdo. Los resultados obtenidos se desglosan a continuación.

En primer lugar, se validó que los participantes hayan visto lo mismo que los observadores, por lo que se les preguntó acerca del cifrado de datos durante la prueba. En este punto, lo esperado era que ellos contestaran si se logró o no el cometido esperado. Los resultados se observan en la Figura 6.

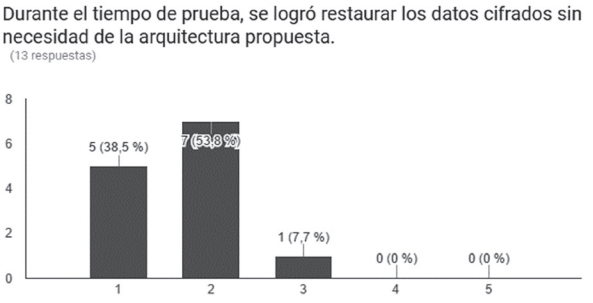
FIGURA 6. Actitud de los participantes grupo experimental frente al cifrado.



Es posible observar que el total de los alumnos del grupo experimental pudo constatar que los archivos de la carpeta objetivo fueron cifrados en una cantidad considerable. Si bien el software centinela alertó de las modificaciones que se realizaron en ese momento, el cifrado fue tan rápido que logró corromper una cantidad de archivos considerables antes de bloquear la carpeta para evitar la modificación de todos los archivos que contenía.

En este punto es pertinente mencionar que el software centinela, al encontrarse en fase prototipo, no garantiza un 100% de protección de datos, sino que identifica cuando se intente alterar una carpeta monitoreada y la bloquea enseguida. Este bloqueo implica de 5 a 15 segundos en su proceso, y se ejecuta en un hilo distinto al del ransomware criptográfico, lo que en las pruebas realizadas permitió al malware la modificación y cifrado de algunos archivos de prueba. El software centinela mitiga el ataque por el momento bloqueando la carpeta para evitar infectar más archivos, pero no revierte el cifrado realizado a los archivos que resultaron afectados por Hidden Tear. Estos archivos se recuperarían más adelante con la parte complementaria del sistema, desde el servidor.

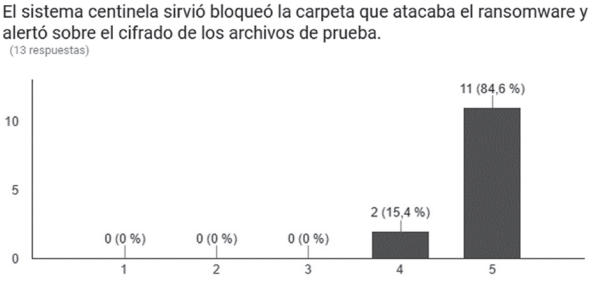
FIGURA 7. Actitud de los participantes frente al intento de recuperación primario.



En la Figura 7 se visualiza la percepción de los alumnos en cuanto a la recuperación de datos sin incluir la recuperación desde el sistema de almacenamiento propuesto. Esto es, intentar recuperar los datos sin acceder al servidor con Seafile instalado y verificar el histórico. El 92.3% de los participantes experimentales indicaron que no fue posible. Solamente el 7.7% no estaba de acuerdo ni en desacuerdo. Estos resultados coinciden con la observación realizada, ya que un alumno tuvo problemas en la red y se desconectó, sin completar con éxito la prueba.

La desconexión se contabilizó como fallo y no como entrada inválida, ya que se tomó en cuenta que en un entorno real se pudo haber trabajado sobre los datos y de la manera en la que no subió al servidor la versión corrupta de los mismos, los cambios generados de una operación en producción también se habrían perdido.

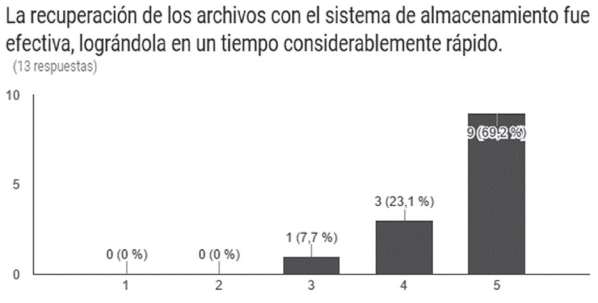
FIGURA 8. Actitud de los participantes respecto a la efectividad del software centinela.



Es de notarse en la Figura 8 que los participantes experimentales lograron observar los avisos del software centinela, y comprobaron que la carpeta donde se encontraban los archivos se bloquearon. Por lo tanto, el ransomware no fue capaz de completar el cifrado de todos los archivos monitoreados. Al ser un servicio en tiempo real, las advertencias también lo son, lo que permite mitigar el impacto local del ransomware.

Finalmente, se quiso contrastar la observación de datos de los participantes con respecto a la recuperación efectiva de datos. La Figura 9 muestra los datos obtenidos del test aplicado, lo que coincide armónicamente con la observación externa realizada. La persona que no está ni de acuerdo ni en desacuerdo representa el 7.7%, mismo porcentaje del equipo experimental que tuvo problemas con la red y no obtuvo por ende la recuperación de datos proyectada.

FIGURA 9. Actitud de los participantes respecto a la efectividad y eficiencia de la propuesta.



4. DISCUSIÓN

Para poder aceptar la hipótesis de investigación, se realizó la prueba de hipótesis con los datos obtenidos por los observadores. Se eligió la prueba del chi cuadrado por su afinidad con el tipo de investigación y la dicotomía en las variables evaluadas. Como en este caso el interés fue comprobar la relación existente entre las dos variables medidas, se usó la prueba de independencia.

El estadístico de contraste utilizado se define en la ecuación 1:

$$x^2 = \sum_{i=1}^{r} \sum_{j=1}^{k} \frac{(n_{ij} - e_{ij})^2}{e_{ij}} \quad (1)$$

La fórmula anterior se aplicó de la manera tradicional con (k-1) (r-1) grados de libertad y donde se genera el cálculo basado en la ecuación 2:

$$e_{ij} = n_i \cdot n_j / n. \quad (2)$$

Al sustituir los valores, se obtuvo que:

$$x^2 = \frac{(12-6)^2}{6} + \frac{(0-6)^2}{6} + \frac{(12-6)^2}{6} + \frac{(1-7)^2}{7} + \frac{(12-6)^2}{6} + \frac{(13-7)^2}{7} \quad (3)$$

Lo que concluye en un valor final del estadístico de contraste de 22.2857143, tal como se muestra en la Tabla 2. Como los grados de libertad se definen (k-1) (r-1) = (2-1) (2-1) = 1, se localizó el valor en la tabla de distribución correspondiente con una confiabilidad del 95%., para finalmente contrastar las cifras. El resultado final del percentil se resume en la ecuación 4:

$$x^2_{.95}(1) = 3.8415. \quad (4)$$

TABLA 2. Resultados obtenidos en pruebas de hipótesis.

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	22.2857143	1	0.0000023		
Corrección de continuidad	18.7261905	1	0.0000151		
Razón de verosimilitud	28.8387315	1	0.0000001		
Prueba exacta de Fisher				0.0000027	0.0000013
Asociación lineal por lineal	21.4285714	1	0.0000037		
N de casos válidos	26				

Como el valor del estadístico es superior al valor crítico, se rechazó la premisa de independencia entre las variables, y se aceptó la relación de dependencia de la recuperación de datos con el uso del sistema de almacenamiento propuesto. Con esto, es posible afirmar que el uso del sistema de almacenamiento sincrónico versionado es una ventaja que permite recuperar los datos secuestrados por ransomware criptográfico sin la necesidad de efectuar pago alguno exigido por los ciberdelincuentes, lo que deriva en poner en marcha el proceso de negocio o personal de manera inmediata.

5. PRUEBAS CON OTRAS CEPAS

Todo lo anterior resultó efectivo teniendo como contexto el ransomware Hidden Tear, el cual se provee con el código fuente para hacer las modificaciones pertinentes. Derivado de ese hecho, se produjo la necesidad de validar los resultados obtenidos y compararlos con los registrados a frente a otras muestras de ransomware criptográficos y de mayor reconocimiento.

Se procedió por tanto a recolectar y probar la propuesta con muestras de ransomware criptográfico reales, las cuales pueden encontrarse en el repositorio de malware llamado "The Zoo" [17]. Por seguridad, todos los códigos maliciosos contienen password para su ejecución. El password es "infected" para lograr la correcta ejecución de las cepas descargadas. A continuación, en la Tabla 3 se presenta los resultados obtenidos con cuatro distintas cepas.

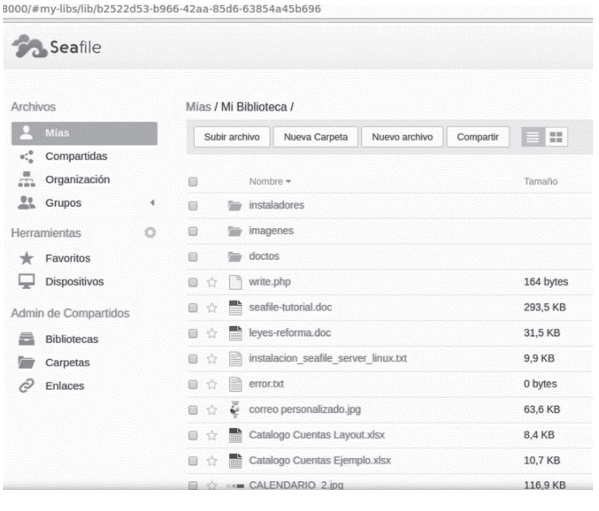
Tabla 3. Resultados frente a cepas reconocidas.

	Cepa			
	Ransomware. Locky	**CryptoLocker (Enero_2014)**	**Ransomware. WannaCry**	**Ransomware. Petwrap**
Cambia las extensiones de archivos	Si	Si	Si	Si
Borra las copias shadow	Si	No	Si	Si
Es recuperable con la arquitectura propuesta	Si	Si	Si	Si

Es posible observar que la cepa CryptoLocker no logró el cifrado de las copias ocultas de Windows, lo que permite otra vía de recuperación de los archivos secuestrados. Sin embargo, la ventaja de la propuesta radica en que la recuperación con la arquitectura propuesta se realiza con un simple click a una fecha anterior.

Los archivos en el servidor son restaurados a una versión anterior, revirtiendo los efectos de las cepas testeadas. La Figura 10 muestra el entorno de Seafile con los archivos restaurados.

FIGURA 10. Seafile con los archivos versionados.



El software centinela monitoreó adecuadamente la carpeta local que se configuró para protección. Los elementos monitoreados, al ser transformados por las cepas y cambiados en extensión, son detectados e inmediatamente se bloquea el directorio para evitar propagar el cifrado.

La Figura 11 y Figura 12 se refieren a las alertas al usuario mediante avisos en pantalla, para que proceda a desconectar el equipo de la red, limpiar el equipo y recuperar los archivos mediante la sincronización con el servidor versionado, previa recuperación de imagen antes de la corrupción de datos.

FIGURA 11. Aviso de corrupción de datos y posible infección

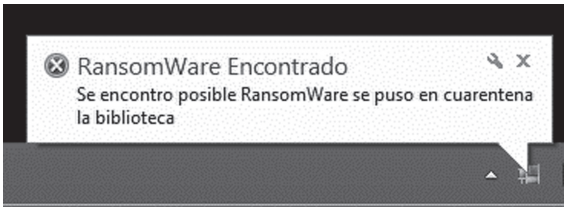
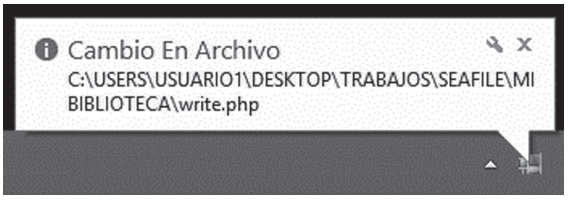


Figura 12. Aviso de cambio en archivo.



El comportamiento fue similar en los cuatro casos, logrando la recuperación efectiva de los archivos monitoreados y configurados con el control de versiones en un servidor externo.

Es importante mencionar que se trabajó en un entorno controlado y una red aislada, además de tener los sistemas operativos anfitriones actualizados, debido a la posibilidad de que estas cepas se propaguen en la red aprovechando vulnerabilidades como parte de su comportamiento propio.

6. CONCLUSIONES

Con la implementación de la arquitectura propuesta, se logró diseñar un sistema genérico de almacenamiento, el cual constó de un servidor con sistema operativo Linux Mint, el cual incorporaba el software de almacenamiento de datos en nube llamado Seafile. Este software, como se ha mencionado, actúa de forma similar a los sistemas de almacenamiento en nube como Dropbox, OneDrive de Microsoft o GDrive de Google. Como estos sistemas homólogos, la actualización es síncrona y también incluye control de versiones, lo que permitió recuperar imágenes de datos a disposición del usuario, desde la interfaz web que provee el sistema.

Adicionalmente durante el transcurso de la investigación, surgió el desarrollo e implementación del software centinela, el cual permite monitorear las carpetas de los sistemas cliente que se conectan al servidor, y generar un bloqueo de las mismas en caso de un ataque de ransomware o cualquier modificación no autorizada en los datos monitoreados.

Con los datos obtenidos y la comprobación de hipótesis planteada, es posible afirmar que el sistema propuesto cumple satisfactoriamente con lo proyectado, pues fue capaz de revertir la corrupción de datos ocasionados por infección de ransomware criptográfico, restaurándolos a condiciones óptimas, lo cual deriva en una alternativa de mitigación y recuperación de datos actualizados frente a amenazas de ransomware criptográfico.

Esta propuesta se pensó para hacerle frente al ransomware criptográfico, que como ya se ha planteado, los casos de ataque aumentan y las víctimas se multiplican alrededor del mundo. Sin embargo, puede ser utilizado como un medio también de recuperación en caso de corrupción de datos por daño físico. En el caso de las organizaciones establecidas y consolidadas, esto no debería suponer un problema dada la infraestructura y los niveles de implementación de seguridad que deberían tener.

Sumado a sus capas de protección que incluyan firewalls, sistemas detectores de intrusos, soluciones antivirus y demás tecnología de protección, no está de más incluir la propuesta de este trabajo como una capa más dentro de su esquema de seguridad. Si bien los sistemas que ya se tengan implementados están enfocados en no dejar penetrar el ransomware criptográfico a la red de la organización, la plusvalía de esta propuesta es que se tiene una alternativa de recuperación de datos actualizados en caso de que el ransomware criptográfico penetre los sistemas antes descritos.

En el caso de las organizaciones medianas o los usuarios personales que no cuenten con el presupuesto para tecnologías de soluciones a nivel de varias capas, tienen al alcance esta propuesta que sería suficiente para añadir mayor seguridad a sus datos frente al ransomware criptográfico. Al utilizar un sistema operativo basado en Linux, puede implementarse incluso en tarjetas de desarrollo o computadores con sistemas embebidos baratos, tal como la Raspberry pi. Estas tarjetas tienen soporte para instalar un sistema operativo Linux y el servidor Seafile, con la responsabilidad del usuario de configurar y sustentar el total del almacenamiento físico de datos, ya sea mediante discos rígidos o dispositivos que se puedan conectar al servidor instalado.

7. TRABAJOS FUTUROS

El proyecto de investigación realizado concluyó satisfactoriamente, con el logro del objetivo primordial de comprobar el uso de un sistema de almacenamiento sincrónico versionado como herramienta para mitigar y neutralizar las afectaciones por ransomware criptográfico. Sin embargo, de este mismo proyecto se pueden derivar otros estudios para analizarlos con amplitud y detenimiento. Por ejemplo, al ser una arquitectura genérica se puede combinar con algunas otras capas de seguridad extra y probar el comportamiento y la eficiencia del sistema informático. Otra vertiente es que el servidor puede estar en un entorno de nube local, tal como se ha demostrado en el presente trabajo de investigación, o implementar el servidor en un hosting dedicado en internet.

También surge la línea de investigación del software centinela, el cual detecta cualquier afectación en las carpetas contenidas mediante las modificaciones de extensiones en los archivos. Este mismo software centinela puede ser estudiado y optimizado para experimentar y proteger ante otras amenazas diferentes al ransomware, intrusiones de archivos por otro tipo de malware o ciberdelincuentes, entre otros estudios.

Por otra parte, Seafile server fue un elemento clave en la solución propuesta, lo que abre el camino para desarrollar una investigación de desarrollo de software propio para control de versiones históricas.

8. AGRADECIMIENTOS

Los autores agradecen al Tecnológico Nacional de México por financiar el proyecto de investigación "Cloud Storage para neutralizar los efectos del ransomware en datos sensibles" del cual forma parte este estudio. A los participantes de las diversas pruebas, profesores y alumnos, y al Instituto Tecnológico Superior Progreso por las facilidades otorgadas en los recursos de tiempo y espacio.

9. REFERENCIAS

[1] F. Portantier, Seguridad informática, 1a ed. Buenos Aires: Fox Andina, 2012.
[2] S. Sánchez, "Importancia de implementar el SGSI en una empresa certificada BASC", Bogotá, D.C.: Universidad Militar Nueva Granada, 2014.
[3] "Internet Security Threat Report 2014", Symantec, 19, 2014.
[4] "Informe de Amenazas a la Seguridad de Internet", Symantec, 21, 2016.
[5] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, y E. Kirda, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks", presentado en International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2015, pp. 3–24.
[6] E. Ruiz, "Técnicas criptográficas utilizadas en malware", Trabajo fin de grado, Universidad Politécnica de Madrid, Madrid, 2015.
[7] A. Bhardwaj, V. Avasthi, H. Sastry, y G. V. B. Subrahmanyam, "Ransomware Digital Extortion: A Rising New Age Threat", Indian Journal of Science and Technology, vol. 9, núm. 14, Abril 2016.
[8] A. Gazet, "Comparative analysis of various ransomware virii", J Comput Virol, vol. 6, núm. 1, pp. 77–90, 2010.
[9] J. Mieres, "Ataques informáticos: Debilidades de seguridad comúnmente explotadas", ene-2009.
[10] Y. Zhou y X. Jiang, "Dissecting Android Malware: Characterization and Evolution", en 2012 IEEE Symposium on Security and Privacy, 2012, pp. 95–109.
[11] Internet Crime Complaint Center, "Public Service Announcement: Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes", 23-jun-2015. [En línea]. Disponible en: https://www.ic3.gov/media/2015/150623.aspx [Consultado: 13-dic-2016].
[12] S. Pagnotta, "CryptoWall, el ransomware más activo: reportan pérdidas por 18 millones de dólares", We Live Security en Español, 24-jun-2015. [En línea]. Disponible en: http://www.welivesecurity.com/la-es/2015/06/24/cryptowall-ransomware-activo-millones-dolares/. [Consultado: 26-dic-2015].
[13] X. Luo y Q. Liao, "Awareness Education as the Key to Ransomware Prevention", Information Systems Security, vol. 16, núm. 4, pp. 195–202, 2007.
[14] G. O'Gorman y G. McDonald, "Ransomware: A Growing Menace", Symantec Security Response, 2012.
[15] M. G. Moreno, Introducción a la Metodología de la investigación educativa 2, 2a reimpresión., vol. 2. México, D.F.: Editorial Progreso, 2000.
[16] H. A. Martínez García y L. B. Chuc Us, "Hidden Tear: Análisis del primer Ransomware Open Source.", en Avances y perspectivas de la innovación, investigación y vinculación, Mérida Yucatán, México, 2015, vol. 1, pp. 31–54.
[17] Y. Nativ, theZoo: A repository of LIVE malwares for your own joy and pleasure. 2017. Disponible en: https://github.com/ytisf/theZoo.