Vol. 19, n.° 3, pp. 131-142, 2020
Revista UIS Ingenierías
Página de la revista: revistas.uis.edu.co/index.php/revistauisingenierias

Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware

Process for the identification, classification and control of the behavior of Ransomware families

Andrés Felipe Osorio-Sierra [1a], Milton Javier Mateus-Hernández [1b], Héctor Fernando Vargas-Montoya [1c]

[1] Instituto Tecnológico Metropolitano, Medellín, Colombia. Orcid: [a] 0000-0001-8947-1228, [b] 0000-0002-7273-7429, [c] 0000-0002-0861-2883. Correo electrónico: [a] andresfelipe.best.27@gmail.com, [b] miltonmateus@itm.edu.co, [c] hectorvargas@itm.edu.co

Recibido: 10 enero, 2020. Aceptado: 30 abril, 2020. Versión final: 29 mayo, 2020.

Resumen

Desde mayo del 2017, en donde se registraron diferentes ataques de Ransomware a escala mundial que afectaron a varias empresas de Europa a causa del WannaCry, ha habido un aumento progresivo entre los años 2018 y 2019 de ataques informáticos que cifran y secuestran los datos, para luego solicitar un rescate por parte de los ciberdelincuentes. Este articulo contiene un análisis de los diferentes métodos para la detección y prevención de malware tipo Ransomware, que afectan principalmente al sistema operativo Windows. Para esto se inició con una caracterización de los diferentes tipos de ransonware, se obtuvieron diversos métodos para la detección y prevención de posibles infecciones y finalmente se crearon familias de controles de acuerdo con el comportamiento del malware, estos controles permiten la reducción de los riesgos de exposición, generando con ello, las recomendaciones pertinentes que pueden ser aplicadas en las organizaciones. En ese sentido, se entrega una introducción alrededor de los conceptos de malware y su ciclo de vida, así mismo, se establece un proceso de medición del impacto con base en la metodología internacional CVSS para la clasificación de las vulnerabilidades, se crea una metodología que permite la clasificación de malware de acuerdo a su nivel de daño, filtrando aquellas con impacto medio y alto, se caracterizaron los métodos de prevención y control, se generaron recomendaciones de controles con base en el impacto de los diferentes tipos de malware y finalmente se entregan las conclusiones.

Palabras clave: cifrado; controles; malware; ransomware.

Abstract

Since May 2017, where different ransomware attacks were registered worldwide that affected several companies in Europe due to the WannaCry, there has been a progressive increase between 2018 and 2019 of computer attacks that encrypt and hijack data, and then request a ransom from cyber criminals. This article contains an analysis of the different methods to detect and prevent ransomware-type malware, which mainly affects the Windows operating system. For this, it began with a characterization of the different types of ransonware, several methods were obtained for the detection and prevention of possible infections and finally families of controls were created according to the behavior of the malware, these controls allow reducing the risks of exposure, generating with this, the pertinent recommendations that can be applied in organizations. In that sense, an introduction to the concepts of malware and

ISSN impreso: 1657 - 4583. ISSN en línea: 2145 – 8456,
A. Osorio-Sierra, M. J. Mateus-Hernández, H. F. Vargas-Montoya, "Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware," *Rev. UIS Ing.*, vol. 19, no. 3, pp. 131-142, 2020. doi: https://doi.org/10.18273/revuin.v19n3-2020013

its life cycle is provided, in the same way, an impact measurement process is established based on the international CVSS methodology for the classification of vulnerabilities. A methodology is created that allows the classification of malware according to its damage level, medium and high impact filters were characterized, prevention and control methods were characterized, control recommendations based on the impact of different types of malware were generated, and finally the conclusions were presented .

Keywords: controls; encryption; malware; ransomware.

1. Introducción

Entender y contrarrestar los ataques informáticos, supone un esfuerzo conjunto entre las organizaciones y los proveedores, una de las amenazas que se ha incrementado en los últimos años es el malware, el cual se viene desarrollando paras múltiples sistemas y con diversos objetivos: bloquear información, robo, minado, puertas traseras, secuestro de información, entre otros. Dentro del malware más relevante se tiene el *ransomware*, este es un tipo de malware que secuestra y cifra los archivos en un sistema de almacenamiento, para luego pedir un rescate [1], generalmente a través de pagos mediante criptomonedas, sin la garantía 100% de que todos los archivos se desencripten o sean devueltos con las mismas condiciones.

Uno de los Ransomware que más daño causo fue WannaCry, que en 2017 afecto a varias empresas de Europa y Rusia [2][3][4], con un aumento progresivo de ataques en el 2018 y mediados del 2019 [5] en todo el mundo. Desde esos eventos, las organizaciones han creado diferentes estrategias corporativas y gubernamentales para frenar las incidencias de este malware y sus versiones posteriores; estableciendo procesos y procedimientos que permitan identificar, reducir y erradicar la amenaza [6], y den una respuesta inmediata ante este tipo de eventos de seguridad.

Una de las problemáticas que se presentan con los ataques exitosos de Ransonware, es que los atacantes desarrollan mutaciones de sus versiones iniciales, lo que dificulta la mitigación de ataques posteriores. El aumento de familias y variantes en el último año es exponencial [8]. Para en el caso de WannaCry, se ha estimado que las diferentes variantes de ransomware han generado pérdidas de alrededor de los 200 millones de euros [9].

En este artículo se da una introducción de los conceptos bases del malware: comportamiento, distribución y ciclo de vida, se explica la metodología usada para lograr identificación, clasificación y control del malware, seguidamente se entregan los resultados, discusiones y recomendaciones con base en la metodología definida, finalmente se dan las conclusiones respectivas.

1.1. Comportamiento base de un Ransomware

El malware comprende diferentes fases en su revisión: el análisis dinámico, análisis estático, análisis mediante comportamiento e ingeniería inversa [10]. Durante el análisis dinámico del ransomware, se observa que tienen una estructura y comportamiento similares a otros tipos de malware, como troyanos o gusanos que contienen técnicas tales como ofuscación, similitud en los payload o autoreplicación. Inicialmente el malware requiere un payload, que es el código que se caracteriza por hacer el daño en un sistema operativo; es decir, el payload es el componente principal y es el que se trata de ocultar para que no pueda ser detectado por las firmas de los antivirus [11].

Algunos malware eliminan las copias shadow de Windows para evitar que los datos cifrados se restauren a una versión anterior de Windows [12], lo que permite al atacante asegurarse que su víctima no tiene una posibilidad de recuperación inmediata, con ello, tendría la ventaja en la infección y pedirá rescate por la información cifrada.

Son varias las fases que ejecuta el malware (figura 1), iniciando con un despliegue por diferentes canales, estableciendo acorde al sistema, cual es la estrategia de infección, para luego pasar al cifrado de la información que encuentre y para finalizar el proceso, genera llaves criptográficas que son enviadas hacia un Centro de Comando y Control (C&C), centro donde opera la administración remota.

1.2. Formas de distribución

Un ransomware puede llegar a la víctiva de diferentes formas (figura 2), los vectores de ataques pueden ser consolidados en la medida que los servicios informáticos estén activos, dichos vectores pueden ejecutarse de acuerdo al comportamiento o falta de conocimiento de empleados para la identificación de archivos maliciosos [13][14][15]. Se destaca dentro de los vectores de ataque lo que esté asociado al correo electrónico, dada la importancia de este servicio en las organizaciones. Otro de los vectores frecuentes es la configuración del auto-run, presente en las memorias o conexiones USB, dada su gran uso a pesar de tener multiples servicios en la nube

en donde se pueden compartir recursos (evitando el uso de dichas memorias).

1.3. Formas de distribución

El ciclo de vida son las fases que usa el ransomware para atacar y las acciones que realiza en cada una de ellas; se deben entender las estrategias, las tácticas y las técnicas que usan para poder generar una metodología de detección y prevención, que cubra todo el ciclo de vida en sus diferentes fases. Dentro de las fases (figura 3) los atacantes deben realizar un despliegue inicial a través de diferentes mecanismos, para luego establecer cómo se haría la instalación en el sistema informático final, esta instalación depende del tipo y la familia de ransomware. Una vez instalado (a través de los posibles despliegues – ver figura 1), el malware hace una búsqueda de los archivos que va a cifrar y se crea una o varias conexiones con el sistema de control, lo cual realiza a través de las diferentes redes y sistemas, para que desde un servidor central se pueda administrar el malware en todo su sentido (robo de información, ocultamiento, nuevos accesos, cifrado, entre otros) y finalmente, el atacante establece el mecanismo de cobrar la extorsión por la información cifrada y que no pudo ser recuperada por la organización [16], [17], [18].

Se ejecutó la siguiente estrategia que permitió (figura 4), de manera técnica y procedimental, la valoración de los ransomware, en cuanto a la detección y respuesta.

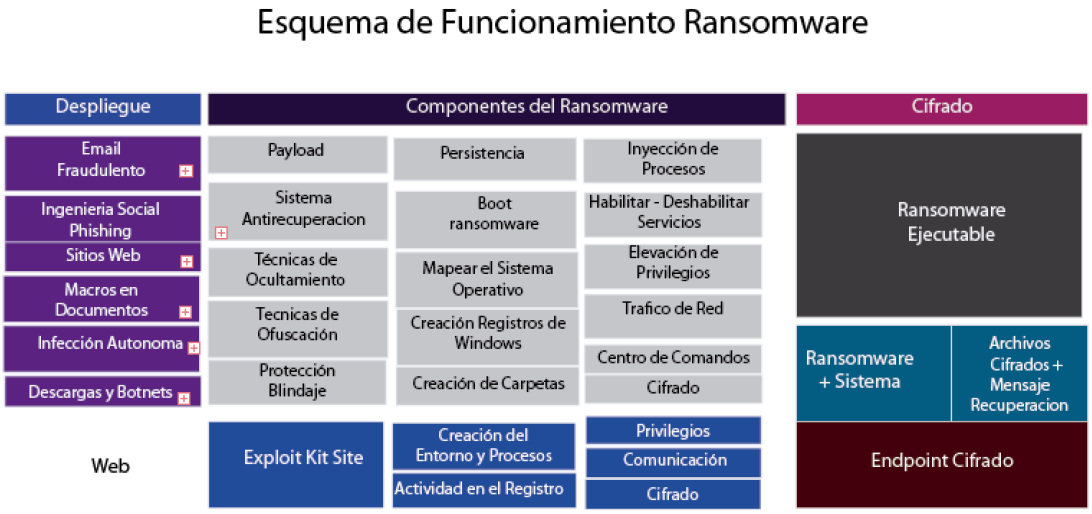

Figura 1. Fases de infección de un malware. Fuente: elaboración propia.

Figura 2. Clasificación de los vectores de ataque. Fuente: elaboración propia.

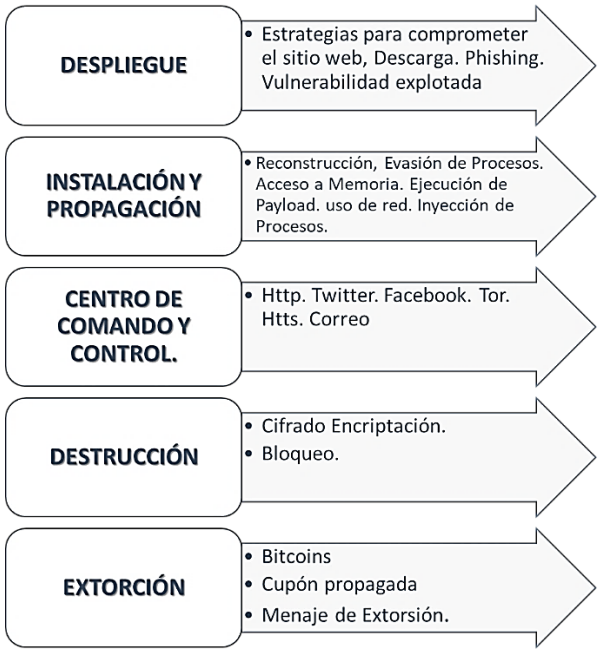

Figura 3. Ciclo de vida del malware. Fuente: elaboración propia.

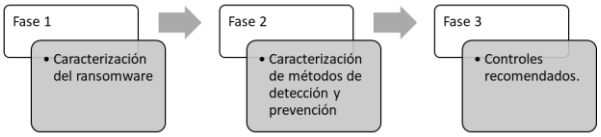

Figura 4. Metodología usada para la detección y respuesta de ransomware. Fuente: elaboración propia.

2. Metodología

Se ejecutó, de manera técnica y procedimental, la valoración de los ransomware, en cuanto a la detección y respuesta, (figura 4).

2.1. Fase 1: caracterización del Ransonware

Se identificación los diferentes ransomware, sus comportamientos en los sistemas y definir el nivel de impacto que este puede ejercer en dicho sistema. Para lo cual, se tomaron 24 familias de Ransonware (tabla 2) cuya actuación se da en los sistemas Windows, dichas familias se seleccionaron de múltiples fuentes de acuerdo con la evolución del malware [19], [20], [21], [22], esto es, aquellos malware que a través del tiempo han tenido una evolución más relevante e impactos importantes.

Se caracterizaron y validaron los comportamientos, en ese sentido, se obtuvo el código fuente y ejecutaron algunos de los malware en un ambiente controlado, que, según su operación o forma de actuar en el sistema y acorde a la cantidad de comportamientos revisados y analizados, se da un porcentaje por posible de afectación, en dónde el mayor puntaje es de 23/23 (el 100% es el caso en que un malware tenga todas las conductas).

Para poder dar un nivel de impacto estándar acorde a los resultados, se realizó una homologación del porcentaje obtenido vs. la tabla de medición de vulnerabilidades CVSSv3 [47], para lo cual, se hizo una extrapolación del porcentaje de las tablas de comportamiento con respecto a los niveles de impacto de la CVSS (tabla 1), en consecuencia, se seleccionaron aquellos considerados por encima del 39%, esto es, los que tienen una relevancia medio, alto y críticos. La escala CVSS fue seleccionada dado su nivel de madurez, su fortaleza en la medición y la asociación directa con la afectación en las plataformas de manera técnica, con ello, poder contar con un esquema de medición más estándar.

En la tabla 1 se muestra la extrapolación de los valores con los cuales se obtuvo la medición de los códigos maliciosos elegibles:

La extrapolación se realizó en consideración de la cantidad total de características que un malware puede tener (23 en total), acorde a esto, se definió los rangos acorde al porcentaje (con una aproximación) y conservando los mismos niveles de impacto. En consecuencia, se obtuvieron los malware con mayor afectación en los sistemas y con los cuales se debe establecer un plan de acción que logre mitigar los posibles riesgos que éstos generan.

2.2. Fase 2: métodos de detección y prevención

En esta fase se revisaron los diferentes métodos de seguridad asociados a la detección (D) y prevención (P) que pueden ser usados en un ransomware. Estos fueron organizados en 4 familias, considerando las siguientes: (1) Arquitectura, infraestructura y redes, (2) Servidores, estaciones y almacenamiento, (3) Aplicaciones y servicios, (4) Acciones transversales. A cada familia se le asocio la estrategia de seguridad y en cada estrategia se definió si era D o P.

Tabla 1. Extrapolación de valores para medir los malware a elegir: CVSS vs. Medición propia.

Medición CVSS			**Medición Propia**	
Puntuación	**%**	**Nivel**	**% características**	**Características seleccionadas**
0	0%	Nula	0%	<3
0,1 - 0,39	10% - 39%	Baja	10% - 39%	3-8
4,0 - 6,9	40% - 69%	Media	40% - 69%	9-15
7,0 - 8,9	70% - 89%	Alta	70% - 89%	16-20
9,0 - 10,0	90% - 100%	Crítica	90% - 100%	21 - 23

Fuente: autores a partir de las escalas de CVSS.

2.3. Controles recomendados

En consideración con el nivel de impacto de cada malware y las familias de controles, se establece una estrategia de seguridad que debería implementarse una vez se identifique. Adicionalmente, se realizó una recomendación de cómo debería ser el procedimiento para el manejo de incidentes de seguridad, una vez que el malware es identificado.

3. Resultados

3.1. Caracterización

En consideración con la metodología ya estipulada, y con el fin de construir un desarrollo para la detección y prevención para *malware* tipo *ransomware*, se realizó el proceso de ingeniería inversa a un conjunto de muestras de código fuente de diferentes *ransomware,* procedentes de los repositorios de GitHub, Gitlab y Bitbucket. Dicho proceso de ingeniería inversa permitió entender el uso, la estructura y el funcionamiento de algunas variantes de este *malware.* En la tabla 2 se encuentra el listado de malware obtenido.

Para las familias seleccionadas, se valoraron 23 comportamientos (tabla 3) que pueden ser identificados a la hora de infectarse [23][24][25][26]. Estos comportamientos pueden dar cuenta de la existencia de un malware en el sistema.

Para cada familia de ransomware, se obtuvo la información respectiva de las diferentes características en su comportamiento (figura 5), luego se analizó dicho comportamiento con respecto a los ya obtenidos (tabla 3), generando al final una consolidación (suma) y obteniendo el porcentaje con respecto al total de comportamientos que puede tener un malware (aplicación de la formula acorde a la metodología). Es claro que el cifrado de archivo y las actividades maliciosas en Windows deben ser un común en todo los malware.

Tabla 2. Listado de familias de Malware de tipo ransomware

Familia	
AIDS	OphionLocker
Archievus	TeslaCrypt
Reveton	VaultCrypt
Cryptolocker	CryptoWall 2.0
Locker	CryptoWall 3.0
CryptorBit	CryptoWall 4.0
Synolocker	Locky
CryptoBlocker	Cerber
CTB-Locker	Crysis
Onion	Dharma
CoinVault	Wannacry
CryptoWall	Petya

Fuente: elaboración propia.

El análisis realizado se centra en los criterios asociados a cada uno de los vectores del *ransomware* y las características tales como método de entrega, tipo de extensión, formato de cifrado, eliminación de copias de restauración, comunicación con centro de comandos, servicio de descifrado, pago y público objetivo [13], [27]. Dichas características fueron usadas para entender la anatomía o ciclo de vida del *ransomware*, con ello, poder consolidar y construir un esquema metodológico de detección y prevención.

Se puede apreciar (figura 5) que los CryptoWall y el Cerber son malware que tienen más del 60%, lo que indica que tienen un porcentaje muy alto de comportamiento en los sistemas, mientas que malware

como AIDS, Archievus y Reveton, su comportamiento y afectación es reducido (puede ser difíciles de detectar). También se puede apreciar que la mayoría generan notificaciones a externos, activan tráfico en la red y terminación de procesos dentro del sistema, lo que supone un punto importante a la hora de la detección.

En consideración del proceso de selección y puntuación (tabla 1, impactos por encima del nivel medio) y como resultado final, se seleccionaron 12 muestras, las cuales tuvieron un porcentaje de aplicación por encima de 39% (tabla 4).

	Posibles comportamientos																							
Familia	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	%	Estado
CTB-Locker	X	X	X	X	X	X						X			X								X	39%	Elegible
CryptoWall	X	X	X	X	X	X	X	X				X			X								X	48%	Elegible
TeslaCrypt	X	X	X		X	X	X					X			X								X	39%	Elegible
VaultCrypt	X	X	X		X	X	X					X			X								X	39%	Elegible
CryptoWall 2.0	X	X	X	X	X	X	X	X				X			X	X	X		X	X	X	X	X	74%	Elegible
CryptoWall 3.0	X	X	X	X	X	X	X	X				X			X	X	X		X	X	X	X	X	74%	Elegible
CryptoWall 4.0	X	X	X	X	X	X	X	X				X			X	X	X		X	X	X	X	X	74%	Elegible
Cerber	X	X	X	X	X	X	X	X	X			X		X	X				X				X	61%	Elegible
Crysis	X	X	X	X	X	X	X					X											X	39%	Elegible
Dharma	X	X	X	X	X	X	X					X											X	39%	Elegible
Wannacry	X	X	X	X	X	X	X					X		X				X					X	48%	Elegible
Petya	X	X	X	X	X	X	X			X		X											X	43%	Elegible
AIDS	X			X																				9%	No elegible
Archievus	X																							4%	No elegible
Reveton	X				X																			9%	No elegible
Cryptolocker	X	X		X	X							X												22%	No elegible
Locker	X	X		X	X							X												22%	No elegible
CryptorBit	X	X		X	X							X												22%	No elegible
Synolocker	X	X			X							X												17%	No elegible
CryptoBlocker	X	X	X	X	X	X						X			X									35%	No elegible
Onion	X	X			X	X	X					X			X								X	35%	No elegible
CoinVault	X	X	X		X		X					X			X								X	35%	No elegible
OphionLocker	X	X			X		X					X			X								X	30%	No elegible
Locky	X	X			X		X					X											X	26%	No elegible

Figura 5. Resultado de validación de la familia de Malware vs. el posible comportamiento vs. calificación final. Fuente: elaboración propia.

Tabla 3. Lista de posibles comportamientos que realiza un malware de tipo ransomware

1	Modificación y cifrado de archivos	**13**	Bloquea el escritorio
2	Realiza actividades en el Regedit de Windows	**14**	Reemplaza el tapiz de escritorio
3	Crea directorios para su funcionamiento	**15**	Deshabilita la restauración del sistema
4	Notificación de ransomware	**16**	Deshabilita las actualizaciones automáticas
5	Actividad en Redes	**17**	Deshabilita el servicio de Windows Security Center
6	Eliminación de Shadow Copies	**18**	Terminación de Administrador de tareas
7	Autoeliminación después de ejecución	**19**	Deshabilita la restauración de Windows
8	Geolocalización IP	**20**	Deshabilita el Windows Error Reporting
9	Búsqueda de antivirus y firewall	**21**	Deshabilita el Antivirus y el Firewall
10	Modificaciones en MBR	**22**	Apaga el equipo una vez infectado
11	Deshabilita iniciar en modo seguro	**23**	Busca todas las unidades de disco y de red
12	Terminación de procesos		

Fuente: elaboración propia.

Tabla 4. Resultado final de la selección de malware por encima del 39% en su comportamiento

CTB-Locker	CryptoWall 2.0	Crysis
CryptoWall	CryptoWall 3.0	Dharma
TeslaCrypt	CryptoWall 4.0	Wannacry
VaultCrypt	Cerber	Petya

Fuente: elaboración propia.

Ahora bien, de estas 12 muestras, en el análisis realizado, se encontró que los malware *CryptoWall*, *CryptoWall 2.0*, *CryptoWall 3.0 y CryptoWall 4.0* poseen comportamiento similar, por lo cual, solo se analizó *CryptoWall 4.0*, que fue la última versión de la sepa, quedando 9 en total.

Tabla 5. Metodología de detección y Prevención para Ransomware

Grupo o familia	Definición de grupo	Estrategia de seguridad	Tipo de control	
			Preventivo	Correctivo
Arquitectura, infraestructura y redes	Estrategias que apoyan a la reducción de riesgos en cuanto a la definición de toda la arquitectura tecnológica, e incluye las redes.	Definir la arquitectura de seguridad	x	
		Definir una segmentación de red	x	
		Firewall	x	x
		Sistemas de Detección de Intrusos	x	x
Servidores, estaciones y almacenamiento	En este grupo se encuentran las estrategias enfocadas a usuarios y sus estaciones de trabajo, servidores y el sistema de almacenamiento (local o remoto)	Honeypot File	x	
		Análisis de Comportamiento de Usuario (UBA)	x	
		Firmas mediante HASH	x	
		Software Antimalware	x	x
		Prevención de Ejecución de Datos (DEP)	x	x
		Cambiar Sistemas Operativos y protocolos obsoletos		x
		Windows File Services Resource Manager (FSRM) - Bloquear las extensiones de archivos creadas por ransomware		x
		Mostrar las extensiones de archivos ocultos	x	
		Identificación del aumento de los archivos renombrados		x
		Bloquear la reproducción automática de medios extraíbles	x	
		Deshabilitar la ejecución de archivos temporales de instalación	x	
		Configuración de Escritorio Remoto Seguro	x	x
		Deshabilitar servicio de Volume Shadow Copy	x	
		Copia y Recuperación de archivos (local o en Nube)	x	x
		Cifrado de Archivos	x	
		Prevención de Pérdida de Datos (DLP)	x	
Aplicaciones y servicios	En este grupo están incluidas todas las aplicaciones (de todos los niveles) y servicios informáticos	Predicción por aprendizaje de Maquina	x	
		Filtrado de contenido de correos o Antispam		x
		Filtrar extensiones .JS peligrosas		x
		Políticas de restricción de software (SRP)		x
		Lista blancas o negras de todas las aplicaciones	x	
		Bloquear ventanas emergentes o popups	x	
		Deshabilitar Macros	x	
Acciones transversales	Son todas las estrategias que aplican o se deben considerar en todas las tecnologías y elementos informáticos	Evaluación de Vulnerabilidades	x	
		Gestión de Parches de Seguridad	x	x
		Indicadores de compromiso (IoC)	x	
		Coincidencia de Patrones a través de firmas	x	
		Gestión de Eventos de Información de Seguridad – SIEM	x	
		Concientización	x	
		Entornos de Virtualización y Sandbox	x	

Fuente elaboración propia a partir de [28] y [29].

3.2. Métodos de detección y prevención

En la tabla 5 se observan diferentes estrategias de control que se pueden implementar en las diferentes plataformas tecnológicas, estas, fueron segmentadas por grupos o familias representativas como se indicó. Cada estrategia fue catalogada si es preventiva o correctiva frente a una posible infección por ransomware.

Para el total de métodos de prevención y detección, se tomaron en cuenta todos los comportamientos de las 23 variantes de ransomware seleccionadas (no solo sobre las 9 variantes seleccionadas), con el fin de crear un esquema metodológico más completo y amplio.

Cada grupo o familia tiene una caracterización particular, dicha agrupación tiene la siguiente descripción:

- Grupo arquitectura, infraestructura y redes: este grupo establece una serie de estrategias que se enfocan en controlar la arquitectura tecnológica, conocida también como la topología de red, en la que se pueden identificar los puntos críticos de la organización. Es recomendable contar con un diseño seguro y una segmentación en las redes mediante la creación de VLAN y Listas de control de acceso (ACL). Este método sirve para controlar el tráfico que hay entre las diferentes redes de la organización; si bien la segmentación no previene ataques de ransomware, sí ayuda a minimizar que la infección no se propague por toda la red, y su afectación se da en un determinado segmento específico de la red [30]. Así mismo, este grupo contiene la implementación de firewalls que son la primera barrera de seguridad, así como los sistemas de detección de Intrusos (IDS), que monitorean el tráfico de red en busca de actividades maliciosas, detectan y alertan al usuario del tráfico malicioso [31], [32]. Estos elementos juegan un papel importante en la seguridad de la organización como primera barrera de protección.

- Grupo servidores, estaciones y almacenamiento: en este grupo se encuentran las estrategias que pueden ser configuradas, analizando el comportamiento de los usuarios (UBA), lo que permite identificar actividades sospechosas basándose en la forma en que el usuario interactúa con los sistemas y el entorno [33]. Es recomendable implementar diversas políticas de seguridad de restricción de software (SRP), que prohíban el lanzamiento o ejecución de archivos mediante una política de grupo local o de dominio (GPO) [24].

  El software Antimalware también es fundamental en las diferentes estaciones de trabajo de los usuarios [34], [35]. La implementación de un Honeypot File, permite recopilar información sobre un ataque y su uso para la defensa, identificando al usuario que infectó el sistema [36]; los funcionarios encargados de TI, deben actualizar los sistemas operativos y protocolos obsoletos, realizando el cambio de las versiones del sistema operativo y actualizando los diferentes protocolos de seguridad a unos más robustos [37].

- Grupo aplicaciones y servicios: en este grupo están incluidas todas las aplicaciones (de todos los niveles) y servicios informáticos, en los cuales se puede ejecutar controles a través de la predicción por aprendizaje de maquina [38], [39]. Otras medidas es el filtrado del contenido de archivos ejecutables con extensión de tipo .exe, .zip, .js o url sospechosas que puedan estar en los correos electrónicos, con esto se genera una protección basada en la reputación del correo [40], [41]. Como control del usuario final, se deben implementar políticas de restricción de software (SRP) [42], por medio de lista blancas o negras de todas las aplicaciones en las diferentes estaciones de trabajo, instalación de software anti spam, bloqueadores de ventanas emergentes o popups [43], así como deshabilitar macros de los documentos de Office [44], [45].

- Grupo acciones transversales: son todas las estrategias que aplican o se deben considerar en todas las tecnologías y elementos informáticos. Una de estas estrategias, es la gestión de vulnerabilidades, que se encarga de identificar los puntos débiles y que pueden ser explotados en una organización [29]. Para mitigar estas vulnerabilidades una vez localizadas, se gestionan parches de seguridad actualizando el sistema operativo y las aplicaciones, esto ayuda a proteger contra ataques de diversos tipos de malware [37].

Si la intrusión fue materializada, se puede realizar un análisis con sus respectivos indicadores de compromiso (IoC) en un Sandbox y/o en un entorno de virtualización [46], que son un sistema automatizado de análisis de malware. Esto permite capturar el comportamiento de un archivo y lo asocia con un tipo de malware en específico. Otra estrategia es la gestión de eventos de Información de Seguridad –SIEM, que proporcionan un análisis en tiempo real de las alertas de seguridad generadas por el hardware y software de red, están dedicadas al escaneo activo y pasivo de sus redes para detectar eventos y actividades sospechosas, y predecir los ataques antes de que tengan lugar [29]. Pero sin lugar a duda la mejor estrategia para una organización es la concientización y el entrenamiento de los usuarios finales sobre los riesgos

a los cuales están expuestos, se deben generar simulaciones en ingeniería social para entrenar a los usuarios finales sobre los riesgos a que están expuestos en la organización y así puedan notificar al área de seguridad encargada [37].

Acorde al análisis realizado (tabla 4), para el total de métodos de prevención, que son los que permiten avisar o alertar sobre el posible impacto negativo que causa un ransomware, se encontró que los 40 métodos tuvieron un porcentaje de prevención del 100%, es decir, todos los métodos propuestos sirven para prevenir, esto debido a que dichos métodos, pueden de manera anticipada evitar que suceda la ejecución de un malware y representa el grueso de la muestra.

Para el total de métodos de detección que son los que realmente hacen el control de contener y proteger de manera efectiva, se encontró que de los 40 métodos solo 12 de estos pueden detectar un ransomware en una estación de trabajo, esto debido a que los métodos no tienen la capacidad de bloquear o impedir la ejecución de un ransomware, esto representa la tercera parte de la muestra con un 30%.

3.3. Recomendación de controles

En consideración que se han seleccionado 9 malware de gran impacto y existen 4 familias de controles, se establece una propuesta (tabla 6) para contrarrestar las amenazas y que pueden ser aplicados en todas las organizaciones, de forma preventiva o correctiva. Dichos controles se basan considerando las 4 familias de controles, en el mismo comportamiento de las familias de ransomware, los resultados de las pruebas controladas y las recomendaciones de varios autores. Las familias de controles permiten establecer una estrategia global en la reducción de riesgos: (1)Grupo Arquitectura, infraestructura y redes, (2) Grupo Servidores, estaciones y almacenamiento, (3) Grupo aplicaciones y servicios, y (4) Grupo acciones transversales. En ese sentido, por ejemplo, el malware TeslaCrypt en su forma de infección y actuación, no considera las funciones de red como la geolocalización, desactivar servicios de red o de actualización, por lo cual, la familia de controles 1 no aplicaría como recomendación, es el mismo caso del malware VaultCrypt.

Podemos apreciar que las familias de controles de servidores, aplicaciones y acciones transversales tienen una aplicabilidad para todos los malware, en consecuencia, se recomienda que estas actividades puedan ser escritas como un documento de línea base a ser aplicado en los diferentes sistemas Windows, con ello, una vez el sistema esta implementado, se podría eventualmente tener una reducción en el nivel de infección. De igual forma, establecer una arquitectura de seguridad y contar con políticas organizacionales, ayudarán a la mitigación de los riesgos de exposición.

Tabla 6. Propuesta de controles frente a los Malware

Id	Familia Malware	Familia de Control			
		1	2	3	4
1	CTB-Locker	x	x	x	x
2	TeslaCrypt		x	x	x
3	VaultCrypt		x	x	x
4	CryptoWall 4.0	x	x	x	x
5	Cerber	x	x	x	x
6	Crysis	x	x	x	x
7	Dharma	x	x	x	x
8	Wannacry	x	x	x	x
9	Petya	x	x	x	x

Fuente: elaboración propia.

Por otro lado, algunas estrategias que se pueden establecer desde el mismo manejo de incidentes de seguridad, es la implementación de la recomendación NIST 800-61 o la norma ISO/IEC 27035, las cuales permiten, a través de una serie de pasos y consideraciones, reducir posibles impactos a la seguridad y la información [7].

4. Conclusiones

En este trabajo hemos analizado los diferentes métodos de detección y prevención para ransomware, permitiendo a través de recomendaciones, contrarrestar el efecto negativo generando por los ciberdelincuentes y mejorando las estrategias para detener y contener un ataque. El trabajo descrito contiene 34 métodos para la prevención y detección, de los cuales 28 métodos son preventivos, 13 son correctivos y 7 cumplen las dos funciones. Dichos métodos fueron agrupados en 4 familias de controles, esto nos ayuda a sintetizar y mejorar las prácticas básicas de seguridad para proteger los archivos y datos, de igual forma, se realizó una selección de malware por su impacto con base en la escala CVSS, obteniendo de dicha selección, los ransomware con un impacto medio y superior (9 en total) y a estos se les recomendó las familias de controles.

Las organizaciones pueden definir o incluir dentro de sus líneas base de seguridad, políticas y procedimientos, los diferentes controles que ayudan a la mitigación de la infección por malware de tipo Ransonware, permitiendo un manejo adecuado de los eventos e incidentes de seguridad. Se puede observar, que muchos ransomware

tienen comportamientos similares, lo que supone una reducción de estos con los mismos controles, ahorrando esfuerzo y recursos a la hora de detectar y reducir.

Adicionalmente el ransomware, al igual que otros malware, evoluciona con el tiempo, utilizando nuevas técnicas de infección debido a los cambios en la tecnología, la falta de controles de seguridad y el comportamiento de las personas, por lo cual, esta metodología debe ser actualizada y adaptada frente a los nuevos cambios y métodos que vayan surgiendo en las nuevas plataformas o tecnologías.

Referencias

[1] "Ministerio TIC - Paraguay. Cómo recuperar ficheros afectados por WannaCry. Telefónica WannaCry File Restorer", 2019. [En línea]. Disponible en: https://www.cert.gov.py/index.php/noticias/como-recuperar-ficheros-afectados-por-wannacry-telefonica-wannacry-file-restorer

[2] "TrendMicro Corp. SMS Ransomware Tricks Russian Users", 2011. [En línea]. Disponible en: https://blog.trendmicro.com/trendlabs-security-intelligence/sms-ransomware-tricks-russian-users/.

[3] M. Á. Mendoza, "El impacto del ransomware en Latinoamérica durante 2017", 2018. [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/

[4] "Ministerio TIC de Colombia. Ransomware sigue creciendo en América Latina", 2017. [En línea]. Disponible: https://www.enticconfio.gov.co/ransomware-crece-america-latina

[5] "CBSNews. Ransomware attacks on the rise — and small towns are in the crosshairs", 2019. [En línea]. Disponible en: https://www.cbsnews.com/news/ransomware-attacks-on-the-rise-and-governments-are-in-the-crosshairs/

[6] R. Brewer, "Ransomware attacks: detection, prevention and cure", *Netw. Secur.*, no. 9, pp. 5–9, Sep. 2016, doi: 10.1016/S1353-4858(16)30086-1.

[7] "IBM Incident Response Services. Ransomware Response Guide", 2017. [En línea]. Disponible en: https://cdn2.hubspot.net/hubfs/233484/Open%20Systems%20Specialists/Content/Ransomware%20Response%20Guide.pdf?t=1507156230392

[8] J. A. Gómez-Hernández, L. Álvarez-González, P. García-Teodoro, "R-Locker: Thwarting ransomware action through a honeyfile-based approach," *Comput. Secur.*, vol. 73, pp. 389–398, 2018, doi: 10.1016/j.cose.2017.11.019

[9] "IBM News room. IBM Study: Businesses More likely to Pay Ransomware than Consumers - United States", 2016. [En línea]. Disponible en: https://www-03.ibm.com/press/us/en/pressrelease/51230.wss

[10] P. Gaviria, "Aplicación de Metodología de Malware para el Análisis de la amenaza avanzada persistente (APT)," trabajo fin de master, Universidad Nacional de la Rioja, 2016.

[11] S. Alsoghyer, I. Almomani, "Ransomware Detection System for Android Applications," *Electronics*, vol., 8, no. 8, 2019, doi: 10.3390/electronics8080868

[12] C. Hosmer, J. Bartolomie, R. Pelli. Chet Hosmer. "The Impact of Windows Command Line Investigations," en *Executing Windows Command Line Investigations*. Cambridge, MA, USA: ScienceDirect, 2016, pp. 1-9.

[13] M. U Salvi, K. Kerkar, "Ransomware: A Cyber Extortion," *Asian journal for convergence in technology (ajct)*, vol. 2, no. 3, pp. 2, 2016.

[14] A. Sanatinia, G. Noubir, "OnionBots: Subverting Privacy Infrastructure for Cyber Attacks," en *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2015, pp. 69–80, doi: 10.1109/DSN.2015.40

[15] L. Bridges, "The changing face of malware," *Netw. Secur.*, vol. 2008, no. 1, pp. 17–20, 2008, doi: 10.1016/S1353-4858(08)70010-2

[16] V. Kotov, F. Massacci, "Anatomy of Exploit Kits," en *Engineering Secure Software and Systems. ESSoS 2013*, vol 7781, pp. 181–196, doi: 10.1007/978-3-642-36563-8_13

[17] S. M. Aziz, "Ransomware in High-Risk Environments" trabajo de investigación independiente, Valparaiso University, 2016.

[18] J. Zorabedian, "Anatomy of a ransomware attack: CryptoLocker, CryptoWall, and how to stay safe (Infographic)," 2015. [En línea]. Disponible en: https://news.sophos.com/en-us/2015/03/03/anatomy-of-

a-ransomware-attack-cryptolocker-cryptowall-and-how-to-stay-safe-infographic/

[19] "Malc0de. Información de malware", 2019. [En línea]. Disponible en: http://malc0de.com/dashboard/

[20] "Github. A repository of LIVE malwares", 2019. [En línea]. Disponible en: https://github.com/ytisf/theZoo.

[21] "NoVirusThanks™ project. Malicious Domains Database", 2019. [En línea]. Disponible en: http://www.threatlog.com/

[22] "Malekal. Malware and Virus", 2019. [En línea]. Disponible en: https://www.malekal.com/

[23] "Any.Run. Interactive malware hunting service". 2019. [En línea]. Disponible en: https://any.run/

[24] "Intezer Analyze Corp. Automate your Security Operations and Incident Response with Genetic Malware Analysis", 2019. [En línea]. Disponible en: https://analyze.intezer.com/#/.

[25] Spiceworks Corp., "Prevent ransomware by using FSRM", 2016. [En línea]. Disponible en: https://community.spiceworks.com/how_to/128744-prevent-ransomware-by-using-fsrm

[26] "VMRAY. X-ray vision for malware", 2019. [En línea]. Disponible en: https://www.vmray.com/

[27] "ESET Latam. RANSOMWARE: Cómo proteger a su empresa del malware de extorsión", 2018. [En línea]. Disponible en: http://www.eset-la.com/pdf/ransomware-prevention/ransomware-como-proteger-a-su-empresa-del-malware-de-extorsion.pdf.

[28] "TrendMicro. SMS Ransomware Tricks Russian Users - TrendLabs Security Intelligence Blog", 2011. [En línea]. Disponible en: https://blog.trendmicro.com/trendlabs-security-intelligence/sms-ransomware-tricks-russian-users/

[29] M. Nicolett, A. Williams, "Improve IT Security With Vulnerability Management" Gartner Research, 2005. [En línea]. Disponible en: https://www.gartner.com/doc/480703/improve-it-security-vulnerability-management

[30] Z. Xiyang, C. Chuanqing, "Research on VLAN Technology in L3 Switch. 2009," en *IEEE Third International Symposium on Intelligent Information Technology Application*, 2009, vol. 3, pp. 722-725, doi: 10.1109/IITA.2009.498

[31] Z. Trabelsi, V. Molvizadah, "Edu-firewall device: An advanced firewall hardware device for information security education," en *13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 2016, pp. 278-279, doi: 10.1109/CCNC.2016.7444779

[32] S. Vasanthi, S. Chandrasekar, "A study on network intrusion detection and prevention system current status and challenging issues," en *IEEE 3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011)*, pp. 181-183, doi: 10.1049/ic.2011.0075

[33] C. Krasznay, B. P. Hámornik, "Analysis of Cyberattack Patterns by User Behavior Analytics," *AARMS – Academic and Applied Research in Military Science*. vol. 17, no. 3, pp. 101-114, 2018.

[34] M. Christodorescu, S. Jha, S. A. Seshia, D. Song, y R. E. Bryant, "Semantics-Aware Malware Detection," en *Semantics-Aware Malware Detection. Proceedings - IEEE Symposium on Security and Privacy*, pp. 32- 46, doi:10.1109/SP.2005.20

[35] D. Delaney, "5 Methods For Detecting Ransomware Activity". 2016. [En línea]. Disponible en: https://www.netfort.com/blog/methods-for-detecting-ransomware-activity/.

[36] C. Moore, "Detecting Ransomware with Honeypot Techniques," en *Cybersecurity and Cyberforensics Conference (CCC)*, 2016, pp. 77-81, doi: 10.1109/CCC.2016.14

[37] C. Frenz, C. Diaz, "OWASP Anti-Ransomware Guide Project – OWASP", 2018. [En línea]. Disponible en: https://www.owasp.org/index.php/OWASP_Anti-Ransomware_Guide_Project

[38] D. Nieuwenhuizen. "Based approach to ransomware detection", F-Secure Labs, 2017.

[39] H. V. Nath, B. M. Mehtre, "Static Malware Analysis Using Machine Learning Methods," en *Recent Trends in Computer Networks and Distributed Systems Security*, 2014, pp. 440-450, doi: 10.1007/978-3-642-54525-2_39

[40] "Symantec Corp. Email Gateway Security - Messaging Gateway", 2018. [En línea]. Disponible en:

https://www.symantec.com/products/messaging-gateway

[41] "Segu-Info. Cómo evitar infectarse con archivos JS adjuntos y ransomware", 2016. [En línea]. Disponible en: https://blog.segu-info.com.ar/2016/03/como-evitar-infectarse-con-archivos-js.html.

[42] "T. Buntrock. How to Block Viruses and Ransomware Using Software Restriction Policies. Windows OS Hub," 2017. [En línea]. Disponible en: http://woshub.com/how-to-block-viruses-and-ransomware-using-software-restriction-policies/.

[43] "Tripwire. 22 Ransomware Prevention Tips, The State of Security", 2016. [En línea]. Disponible en: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevention-tips/

[44] G. Krunal, P. Viral, "Survey on Ransomware: A New Era of Cyber Attack," *Int. J. Comput. Appl*., vol. 168, pp. 38-41, 2017, doi: 10.5120/ijca2017914446

[45] "Trisha Corp. OfficeMalScanner : Scan Office Documents for Macros Before Opening", 2015. [En línea]. Disponible en: https://www.trishtech.com/2015/12/officemalscanner-scan-office-documents-for-macros-before-opening/

[46] "N. Lord. What are Indicators of Compromise?", 2017. Digital Guardian. [En línea]. Disponible en: https://digitalguardian.com/blog/what-are-indicators-compromise

[47] "Firt and MITRE Corp. Common Vulnerability Scoring System Version 3.0 Calculator", 2019. [En línea]. Disponible en: https://www.first.org/cvss/calculator/3.0.