2023

White paper series
Edición 10

Retos y Estrategias:

Las consideraciones de los ataques de ransomware en las Américas

OEA | Más derechos para más gente

aws

Créditos

Luis Almagro
Secretario General de la Organización de Estados Americanos (OEA)

Equipo técnico de la OEA
Luis Fernando Lima Oliveira
Alison August Treppel
Kerry-Ann Barrett
Mariana Jaramillo

Equipo técnico de AWS
Abby Daniell
Melanie Kaplan
Camilo Gonzalez
Arturo Cabañas
Jordana Siegel

Editor
Jeimy Cano

Tabla de Contenido

Definiciones 01

Introducción 02

Secuestro de datos: ¿Qué ocurre en una organización? 04

Materialización del ransomware: Dos lados una misma ecuación 06

Recomendaciones/Mejores Prácticas frente al secuestro y extorsión con datos: *Ideas convencionales* 08

Caso de estudio – Guacamaya y Conti: *Amenazas presentes en la región* 10

Conclusiones 13

Appendix 14

Listado de recursos en internet disponibles para enfrentar el ransomware 14

Estadísticas relevantes sobre el ransomware a nivel global 14

Anatomía de un ransomware: Nivel de explotabilidad y etapas clave 16

Referencias 18

Definiciones

Botnet (El vocablo botnet procede de "robot network")
Es una red de equipos infectados (vía un código malicioso) que se controlan a distancia y a los que se puede obligar a enviar spam, propagar malware o llevar a cabo un ataque DDoS, y todo sin la autorización del dueño del dispositivo[1].

Carga útil (Payload)
Parte de un malware (código malicioso) que realiza la acción adversa o dañina en el sistema objetivo después de haber realizado una intrusión exitosa.

Ciberhigiene
Es la adopción de una mentalidad y unos hábitos de uso diario centrados en la seguridad que ayuden a las personas y las organizaciones a mitigar posibles infracciones en línea[2].

Cifrado de datos
Cualquier procedimiento utilizado en criptografía para convertir texto plano en texto cifrado con el fin de impedir que cualquier persona, salvo el destinatario previsto, pueda leer esos datos[3].

Copia de resguardo
Una copia de los archivos y programas realizada para facilitar la recuperación, en caso necesario[4].

DDos
Una técnica de bloqueo de servicio que utiliza numerosos equipos para realizar el ataque[5].

Doxing
Acción o proceso de buscar y publicar en Internet información privada o identificable sobre una persona concreta, normalmente con malas intenciones[6].

Enlace malicioso
Un enlace malicioso es un vínculo que dirige a un sitio fraudulento. Por lo general, consiste en una conexión que parece dirigir a una web legítima, pero, en realidad, se trata de una web falsa[7].

Exfiltración de información o fuga de información
Es la copia, transferencia o recuperación de datos o información de forma ilícita de un servidor que termina en manos de un tercero no autorizado.

Malware
Programa que se inserta en un sistema, normalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistema operativo de la víctima, o de causar disrupciones de cualquier otro tipo a la víctima[8].

Ransomware
Tipo de malware que en general secuestra y cifra los archivos en un sistema de almacenamiento, para luego pedir un rescate, habitualmente a través de pagos mediante criptomonedas, sin la garantía de que todos los archivos puedan ser descifrados o sean devueltos con las mismas condiciones.

1 https://www.avast.com/es-es/c-botnet
2 https://www.kaspersky.es/resource-center/preemptive-safety/cyber-hygiene-habits
3 https://csrc.nist.gov/glossary/term/encryption
4 https://csrc.nist.gov/glossary/term/backup
5 https://csrc.nist.gov/glossary/term/ddos
6 Tavella, F. (2021). Ransomware Conti: principales características y cómo operan sus afiliados. ESET. https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/
7 https://www.mundopc.es/links-maliciosos-como-detectar-una-url-fraudulenta-484.html
8 https://csrc.nist.gov/glossary/term/malware

Introducción

Noticias recientes en diferentes informes, tanto de proveedores de tecnologías de seguridad de la información como de autoridades policiales, reportan que el ***"ransomware"***[9] se ha convertido en uno de los riesgos y amenazas de mayor relevancia para la seguridad global, no sólo por su versatilidad y capacidad de acción, sino también por su expansión e impacto financiero y de reputación a nivel organizacional (Interpol, 2020). En este contexto, esta amenaza digital conocida como ransomware se configura como un punto de reflexión relevante para los sectores públicos y privados.

Cuando una organización es afectada por un ransomware, se presenta la pregunta clave ***"¿cómo responder y mitigar un evento de seguridad de ransomware?"***[10], una pregunta que genera, tanto en el sector público como en el privado, tensiones de diferentes magnitudes e implicaciones de atribución de responsabilidad al interior de una organización, y consideraciones como revelar detractores de la inversión en ciberseguridad, así como un sinnúmero de implicaciones colaterales que comúnmente cumplen con el propósito del adversario: generar confusión, confrontación y juego de responsabilidades que le permitan mayor tiempo de acción y posicionamiento frente al momento para conseguir motivar un pago como extensión y con su fin último. Por lo tanto, los sectores público y privado quieren mitigar el impacto en los datos y la reputación, a través de un evento de ransomware el cual puede presentar incertidumbre sobre cómo manejar y si responder al rescate o no.

Cuando una organización en sus niveles ejecutivos se informa de la materialización de un *ransomware* comúnmente se entabla el comprender qué tipo de información es la que está comprometida en primer lugar, posterior a solicitar las explicaciones técnicas de cómo este evento de seguridad impacta las operaciones y las implicaciones jurídicas potenciales que esto conlleva, así como si la información está sujeta a una protección legal particular. Con estos datos, usualmente las organizaciones tratan de establecer con todos los involucrados internamente una vista general de lo que ha pasado y definir una postura base para actuar en consecuencia con el ransomware.

Hay situaciones en los que estos eventos de seguridad pueden severamente afectar organizaciones, por ejemplo, la extorsión con datos es una modalidad de cibercrimen que está basada en la inteligencia, el engaño y la distracción desarrollada por el adversario, que se conecta con un patrón de comportamiento basado en las necesidades y expectativas de los individuos. En este sentido, al identificar aquello que puede ser de interés para el usuario objetivo (por ejemplo, una expectativa de un ascenso, la entrega de una bonificación, el pago de una multa, un llamado de una institución policial, entre otras), y enlazarlo con la dinámica del contexto actual (el específico que está viviendo la persona con sus expectativas), los adversarios logran mimetizar sus acciones en un tejido social concreto con el fin de abordar a sus posibles víctimas sin que ellas lo noten.

9 Definición página 1

10 Las buenas prácticas internacionales desarrolladas a la fecha sugieren no pagar. Ver The European Union Agency for Cybersecurity (ENISA) Landscape for ransomware attacks - https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

La falta de comprensión de los controles de seguridad para los servicios técnicos contribuye al éxito de los usuarios no autorizados. Si adicionalmente a lo anterior, se identifica una baja higiene informática, comúnmente referida como *ciberhigiene*, que las personas tienen en el contexto digital, la confianza ingenua en los medios y tecnologías disponibles, así como el aumento de productos y servicios digitales que se despliegan con limitadas medidas de seguridad y control, los agresores tienen el escenario ideal para movilizarse a fin de lograr sus acciones y planes con poco margen de acción.

La siguiente publicación busca proporcionar recomendaciones y reflexiones basadas en buenas prácticas internacionales para los tomadores de decisiones de organizaciones del sector público y privado, alrededor de la realidad de un ataque de *ransomware* y sus implicaciones, para ilustrar el proceso que ocurre durante la materialización de este evento y así, brindar espacios para examinar el cómo abordar este reto, qué margen de acción se puede lograr y cómo encontrar algunos patrones que adviertan sobre el avance de este tipo de amenazas en una organización.

Secuestro de datos: ¿Qué ocurre en una organización?

El secuestro de datos priva a la persona o a las organizaciones de uno de sus activos más importantes como son los datos y la información representa en la actualidad una afrenta directa que pone en peligro los derechos y prerrogativas de las organizaciones y los seres humanos en su libre actuación en la dinámica social. El secuestro de datos, y su posterior extorsión por parte de terceros, configura una acción delictiva que en su momento deberá ser abordada por diferentes jurisdicciones y acciones legislativas para ser incorporada en los ordenamientos jurídicos nacionales e internacionales (Grimes, 2022).

Cuando una organización se ve afectada por un evento de ransomware, surgen dilemas que se generan y usualmente son pocas las maniobras jurídicas que se pueden activar para tratar de contener los posibles efectos adversos en su contra (Leo et al., 2022).

Por un lado, una organización puede utilizar políticas en materia de ciberseguridad, que de acuerdo con sus alcances y exclusiones podrá apoyar a las entidades para manejar este reto. Por otro lado, puede negociarse con el agresor que ha capturado los datos, con la claridad de que, aun teniendo la forma de restaurar la información, es probable que no pueda hacerlo. No obstante, es importante recalcar que mejores prácticas y recomendaciones internacionales, no recomiendan negociar con el agresor.[11] La alternativa de pagar no es una opción recomendada por las mejores prácticas en el tratamiento del ransomware (y es abiertamente ilegal en diferentes jurisdicciones nacionales e internacionales). Cualquiera de las acciones convencionales que se tome tendrá como resultado hacer más resistente la organización frente a la materialización de un ransomware, sin perjuicio que en algún momento el adversario podrá tener éxito. Adicionalmente este tipo de acciones estarán ajustadas al ordenamiento legal (con excepción del pago de la extorsión) lo que les dará tranquilidad a los ejecutivos en sus marcos de cumplimiento y reporte a los entes de control.

Finalmente, informar e involucrar a las autoridades competentes[12] durante una investigación puede contribuir a proporcionar información acerca del actor de la amenaza para utilizar diferentes estrategias que permitan encontrar al agresor, desactivar el mecanismo de cifrado, usar los canales diplomáticos,[13] si son del caso y así, ajustarse a los cánones establecidos por la constitución y la ley son algunas de las maneras en las que se puede optar por abordar un secuestro de datos.

11 https://www.nomoreransom.org/en/ransomware-qa.html
12 Supervisores de un sector particular, Autoridades de policía o fuerzas del orden.
13 Cuando los datos que se han sido comprometidos se encuentran o se trasladan a otros países y jurisdicciones, y se hace necesario usar los canales diplomáticos para coordinar acción policiales y judiciales para adelantar las acciones de recuperación o eliminación de la información.

El *ransomware* saca de la zona cómoda a los profesionales de seguridad de la información, a los abogados corporativos y a los tomadores de decisiones, habida cuenta que si la información o los datos comprometidos están sujetos a condiciones particulares de protección y debido cuidado deberán establecer con claridad la manera de responder a la situación a los diferentes grupos de interés afectados. En consecuencia, la organización afectada estará sujeta a una encrucijada donde será evaluada frente a sus prácticas de seguridad, privacidad y control, y cómo estas se han venido desarrollando y aplicando, por otro lado, las tensiones jurídicas, con sus respectivas sanciones (generalmente económicas), que pueden terminar impactando la reputación en su sector.

Abordar un ataque de ransomware es una temática que va más allá del fenómeno tecnológico que la materializa, es habilitar una examinación sistémica de la problemática que conecta las prácticas de seguridad, las relaciones institucionales, los marcos jurídicos, los aseguradores, las vulnerabilidades tecnológicas y sobremanera, los comportamientos humanos (Sittig & Singh, 2016).

> El *ransomware* saca de la zona de confort de los profesionales de seguridad de la información, al área jurídica de las instituciones y a los tomadores de decisiones. Para ser resiliente, es importante que cada organización cuente con un plan proactivo para responder a la situación, por ejemplo, siguiendo el proceso de preparación de NIST.[14]

14 Ransomware | NIST

Materialización del ransomware: Dos lados una misma ecuación

Las acciones que proceden luego de un secuestro de datos tienen algún tipo de motivación (no siempre económica) y lleva a un contacto directo o indirecto con los grupos de interés de la víctima, con el fin de iniciar un juego de presiones y tensiones que buscan doblegar la voluntad de la parte impactada. Para ello, las pruebas de supervivencia, las llamadas amenazantes y las manifestaciones visibles que generan incertidumbre (fotos, símbolos, o pertenencias), son piezas fundamentales para crear la necesidad y las acciones necesarias que lleven al cumplimiento del objetivo del agresor.

En el mundo digital, el *ransomware* tiene al menos dos vistas en la actualidad. Secuestro de información o datos (generalmente sensibles) por los cuales hay que pagar un rescate (con la amenaza de que no hacerlo se procederá a su destrucción o desaparición), o acceso a información sensible o comprometedora que podrá ser expuesta (con posible afectación de la reputación) sino hay un pago al delincuente digital (Baykara & Sekin, 2018). En ambos casos, los delincuentes buscarán relevar pruebas a sus víctimas de que la amenaza de cualquiera de estas acciones es real y seria, para lo que se lleva a cabo acciones para intimidar y generar presión, incluyendo cuentas regresivas visibles, mensajes de voz modificados para intimidar a las organizaciones o las personas, y medios de contacto basados en cuentas de correo anónimas o descartables. Al analizar la materialización de un evento como el *ransomware* habrá que evaluar los dos lados de la ecuación: a la organización (o la persona), así como al atacante.

Por el lado de la persona o la organización el análisis sobre la posible materialización y alcance de los daños por cuenta de un ransomware, puede incluir los siguientes aspectos:

- Nivel de aseguramiento de las prácticas de seguridad y control
- Nivel de afinamiento y uso de las tecnologías de seguridad y control disponibles
- Pruebas y lecciones aprendidas de la evaluación y seguimiento a los planes de recuperación y continuidad de negocio
- Análisis de comportamientos de navegación y uso de internet
- Nivel de desarrollo de cultura de seguridad de la información (incluida la ciber higiene personal)
- Análisis prospectivos de riesgos latentes y emergentes relevante a la industria de la organización en el contexto de las operaciones y estrategias de esta
- Definición del apetito al riesgo[15] empresarial (o personal) (Herrera Silva, Barona López, Valdivieso Caraguay & Hernández-Álvarez, 2019)

15 La cuota de riesgo que una organización está dispuesta a aceptar y soportar en la consecución de su misión/visión. Fuente: Quinn et al. (2021). Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. NIST. NISTIR 8286A. https://doi.org/10.6028/NIST.IR.8286A

Cualquier deficiencia o resultado que no corresponda a lo esperado en cada uno de estos elementos previamente mencionados, será asociado con una limitada capacidad de gestión de riesgo tanto de la organización como de la persona frente al debido cuidado que se debe tener en la protección de la información o los datos a cargo o de su propiedad, al igual como se podría deducir como negligencia la cual podría ser comprobada vía ejercicios de auditoría o verificación independiente.

Desde la perspectiva del agresor el análisis de las capacidades y soportes con los que cuenta para lograr sus objetivos puede incluir, entre otros aspectos, los siguientes:

- Nivel de especialización y habilidad para desarrollar inteligencia
- Motivaciones específicas que llevan a la acción
- Uso de herramientas conocidas o especializadas
- Conexiones con otros grupos criminales
- Pagos basados en criptomonedas, o monetizaciones de otras formas
- Patrones de actuación previos
- Antecedentes disponibles a nivel nacional o internacional (Cano, 2020)

Cualquier información que se considere, basado en el listado anterior, ofrecerá orientaciones y pistas para seguir el rastro del atacante. Cada uno de éstos ayudará a darle forma al rompecabezas que implica conectar las diferentes acciones del agresor, con el fin de encontrar patrones consistentes que den claridad para reconstruir su acción criminal y así, lograr en el mejor de los casos su ubicación y captura. Esto no siempre se logra, y, por lo tanto, cuanta más información confiable y relevante se pueda obtener mejores mapas se podrán delinear sobre un territorio de naturaleza incierta que plantea el adversario (El-Kosairy & Azer, 2018).

En el mundo digital, el *ransomware* tiene al menos dos vistas en la actualidad. *Secuestro de información o datos* (generalmente sensibles) por los cuales se exige un rescate (con la amenaza de que no hacerlo se procederá a su destrucción o desaparición), o *acceso a información sensible o comprometedora* que podrá ser expuesta (con posible afectación de la reputación) sino hay un pago al delincuente digital.

Recomendaciones/Mejores Prácticas frente a un ataque de ransomware: *Ideas convencionales*

Cuando una organización sufre de la materialización de un *ransomware* debe considerar las dos partes de la ecuación, y no sólo concentrarse en el daño que esto genera al interior con las consecuencias naturales que esto trae desde el punto de responsabilidades individuales y colectivas, pero también considerar el posible impacto a los individuos dentro de la organización.

Hay varias agencias que proporcionan información para equipar mejor a las organizaciones para manejar estos incidentes. En este sentido, se plantean algunas acciones convencionales que las organizaciones o personas pueden aplicar cuando se ha concretado el secuestro y la extorsión con datos. Por ejemplo, en el caso de Estados Unidos, el Buró Federal de Investigaciones (FBI por su sigla en inglés) alienta a las organizaciones a reportar incidentes de rescate a la policía. El Centro de Quejas de Delitos en Internet (IC3 por sus siglas en inglés) acepta denuncias de delitos en Internet en línea, ya sea de la víctima real o de un tercero al denunciante y trabajará con ellos para determinar el mejor curso de acción en el futuro. En este caso la siguiente información es indispensable para proceder:

1. Cualquier información relevante que se considere necesaria para respaldar la queja
2. Encabezado(s) de correo electrónico
3. Información de transacciones financieras (información de la cuenta, fecha y monto de la transacción, detalles del destinatario)
4. Nombre del sujeto, dirección, teléfono, correo electrónico, sitio web y dirección IP
5. Detalles específicos sobre cómo ha sido afectado la víctima
6. Nombre, dirección, teléfono y correo electrónico de la víctima

Las siguientes recomendaciones se proporcionan basado en las buenas prácticas internacionales disponibles a la fecha[16] :

• Contratar o buscar servicios especializados para restaurar los datos que se han comprometido. Este tipo de servicios son costosos e implican usos de herramientas particulares que tratan de encontrar patrones y establecer vías alternas para tener acceso a los datos, lo que no siempre se logra.

• Contactar a los proveedores de herramientas de seguridad y control, o sus contactos para establecer alternativas que permitan encontrar maneras de recuperar la información o parte de ella. Esta acción, generalmente suele generar logros discretos y existen centros de investigación asociados que pueden aportar al respecto.

• Usar los respaldos de información con los que cuenta la organización o la persona, los cuales generalmente no responden a una práctica sistemática y validada. Esta estrategia suele funcionar de forma parcial dado que la actualización de la información respaldada define el nivel alcance y maniobra que la organización o la persona puede tener. El uso de esta información como forma de recuperación podrá generar deficiencias y diferencias al ser usada, pues depende de la confiabilidad de los medios de almacenamiento utilizados, la tecnología de apoyo que tienen para hacer los respaldos y la estrategia que se utilice: respaldo diario, incremental o total, o el uso del almacenamiento en la nube.

• Desarrollar y actualizar el plan de continuidad de negocio, que considere la información sujeta a protección legal (como primera prioridad, por ejemplo, bases de datos con información personal) para mantener el debido cuidado y cumplimiento regulatorio frente los supervisores de su sector a nivel nacional e internacional.

• Mantener los datos cifrados (codificados en tránsito y mientras no se usen) en los medios de almacenamiento establecidos por la organización/persona (para casos de doble extorsión: exfiltración y cifrado).

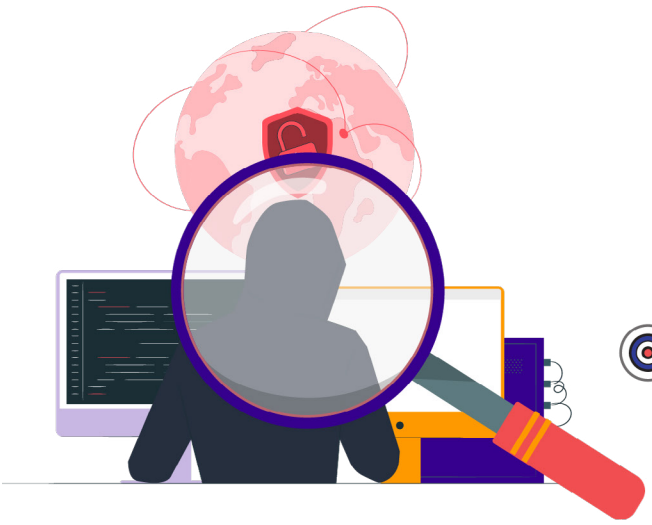
• Aplicar los parches o ajustes críticos, liberados por los proveedores, a los programas o sistemas operativos disponibles para la organización/individuo.

• Asegurar entrenamiento y simulación periódicas a los individuos frente a las estrategias utilizadas por los atacantes para concretar engaños y motivar acciones que habiliten la materialización de un ransomware.

• Motivar el reporte de las personas sobre comportamientos sospechosos de los dispositivos que utiliza (por ejemplo, inhabilitación de servicios, reinicio, alertas del sistema antivirus, entre otros).

16 U.S. Cybersecurity & Infrastructure Security Agency - https://www.cisa.gov/stopransomware/ransomware-guide
The European Union Agency for Cybersecurity (ENISA) Landscape for ransomware attacks - https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
Australian Cyber Security Centre (ACSC) - Ransomware Attacks Emergency Response Guide - https://www.cyber.gov.au/sites/default/files/2021-07/11515_ACSC_Emergency-Response-Guide_Accessible_08.12.20.pdf

Caso de estudio – Guacamaya y Conti: *Amenazas presentes en la región*



Considerando los análisis previos realizados alrededor del *ransomware* es importante reconocer y analizar a los posibles adversarios que se encuentran detrás de estas acciones. En este sentido, se desarrolla a continuación una breve caracterización de dos casos de estudio y los impactos de sus acciones en la región.

GUACAMAYA

De acuerdo con Vicens (2022) Guacamaya se trata de un grupo de activistas centroamericano cuyo objetivo principal es infiltrarse en empresas mineras y petroleras, policías y diversas agencias reguladoras latinoamericanas con el fin de revelar la injusticia en general, delitos penales contra la población, el territorio local y el planeta. Critica abiertamente el "imperialismo norteamericano" y su agresión a los pueblos de América.

Este grupo hacktivista tiene como objetivos gobiernos, entidades estatales, militares y extractivas con el fin motivar presuntamente mayor transparencia de la información sobre iniciativas de los Estados o de las instituciones mencionadas y así darle a la ciudadanía detalles que no se advierten directamente.

El modo de operación de este grupo es identificar vulnerabilidades comunes o típicas en las infraestructuras de las instituciones objetivo como son fallas en actualización o en configuración del sistema operativo o aplicaciones específicas, las cuales son explotadas para tener acceso privilegiado a la información residente en dispositivos tecnológicos y luego revelar la información y publicarla en diferentes medios de acceso público. Adicionalmente cuentan con un portal[17] donde llevan un registro de sus acciones y sus declaraciones.

Dentro de sus acciones más destacadas se encuentran ataques al sector público en Chile, México, Perú, El Salvador y Colombia, donde debido a este ataque de ransomware se revelo información sensible de gobiernos, instituciones militares y empresas del sector extractivo.

17 https://enlacehacktivista.org

CONTI

A diferencia del grupo Guacamaya, CONTI es una organización de crimen organizado transnacional que presuntamente tiene su origen en Rusia. Se les detectó por primera vez en 2020 y se cree que es el sucesor del grupo de ransomware Ryuk. Según Chainalysis (2022) este grupo de ransomware fue el de mayor recaudación en 2021, con unos ingresos estimados de al menos 180 millones de dólares.

De acuerdo con Tavella (2021), CONTI suele utilizar la modalidad doble extorsión, también conocida como *doxing*, que consiste en exfiltrar información confidencial de sus víctimas previo al cifrado para luego extorsionarlas amenazándolas con publicar información exfiltrada a menos que paguen el monto de dinero exigido. De esta forma aumentan la presión, ya que no solo se trata de recuperar los archivos cifrados, sino también de evitar una posible brecha de información que podría perjudicar a la víctima de diversas maneras.

CONTI tiene un modus operandi que sigue las siguientes actividades:

- Compañas de phishing con documentos adjuntos maliciosos;
- Reclutar personal interno de la empresa afectada para concretar y expandir su actividad ilícita;
- Explotación de vulnerabilidades conocidas sobre equipos expuestos en internet;
- Ataques sobre equipos con el servicio "Remote Desktop Protocol – RDP" (Protocolo de escritorio remoto)[18].

El grupo criminal CONTI funciona como cualquier empresa del mundo. Tiene múltiples departamentos, desde recursos humanos y administradores hasta codificadores e investigadores. Tiene políticas sobre cómo sus hackers deben procesar su código, y como contraparte, las mejores prácticas para mantener a los miembros del grupo ocultos de las fuerzas del orden (Burguess, 2022).

CONTI ha estado involucrado en numerosos ataques de alto perfil, incluyendo aquellos contra la ciudad de Tulsa, las escuelas públicas del condado de Broward y Advantech en los Estados Unidos de América. Sin embargo, no fue hasta que atacaron el Servicio Ejecutivo de Salud (Health Service Executive (HSE)) y el Departamento de Salud (Department of Health (DoH)) de Irlanda, dejando fuera de servicio los sistemas informáticos del país durante semanas, cuando ganaron notoriedad (Abrams, 2022).

Recientemente CONTI ha estado actuando en Latinoamérica donde su acción más reciente y revelada a través de los medios internacionales fue el ataque ejecutado el 12 de abril de 2022 contra las bases de datos del Ministerio de Hacienda de Costa Rica y otras instituciones públicas del país, que llevó a la declaratoria del "Estado de Emergencia Nacional en todo el sector público del Estado de Costarricense" de acuerdo con lo establecido en el decreto No. 43542-MP-MICITT de 8 de mayo de 2022.

Como se puede observar tanto Guacamaya como CONTI establecen amenazas concretas para la estabilidad de la región habida cuenta que sus estrategias y métodos, si bien son diferentes para alcanzar sus objetivos, se fundan en una limitada aplicación y aseguramiento de buenas prácticas y estándares en ciberseguridad/seguridad a nivel empresarial y estatal, lo que demanda desarrollar y crear capacidades conjuntas para fortalecer una postura vigilante que permita no solo responder, sino disuadir, demorar o confundir a estos adversarios.

18 Protocolo que permite a que un usuario remoto tenga pleno acceso a su dispositivo, de forma que podrá mover el ratón y usar el teclado como si estuviese delante del equipo.

Un resumen de la caracterización de estos dos grupos se puede ver a continuación:

Características	Guacamaya	Conti
Fundamento de su acción	Hacktivista	Crimen organizado
Procedencia	Aparentemente Centroamérica	Aparentemente de Rusia
Técnicas utilizadas	Explotación de vulnerabilidades en equipos: falla en la actualización o en configuración del sistema operativo o aplicaciones específicas.	Phishing con documentos adjuntos maliciosos, explotación de vulnerabilidades conocidas, ataque a equipos con exposición del protocolo de escritorio remoto, descifrar contraseñas.
Sector foco	Inteligencia militar, entidades estatales, seguridad nacional, empresas mineras y extractivas.	Entidades del Estado o empresas claves que afecten a los ciudadanos y la dinámica de un país.
Organización	Grupo organizado y centralizado alrededor de una causa común: presuntamente bienestar social e intereses nacionales.	Grupo de operación descentralizado a nivel global con fines económicos y extorsivos.
Objetivo	Mayor transparencia de la información que manejan los gobiernos y las empresas extractivas.	Incertidumbre, inestabilidad, caos y ganancias económicas.
Filosofía	Hacking como forma de resistencia.	Hacking como forma de desestabilización política y generación de ingresos.
Resultado esperado	Exfiltra datos sensibles.	Contiene, exfiltra y cifra datos para garantizar el pago.

Tabla 1. Caracterización de Guacamaya y Conti

Conclusiones

Ransomware es una modalidad de crimen organizado que es fruto de la transformación digital de la criminalidad desde hace más de 10 a 15 años, cuando se iniciaba con el tema de las botnets (ver en definiciones). Poder tener control de un equipo sin que la víctima tenga conocimiento de ellos es uno de las expresiones y motivaciones más relevantes que experimentan los atacantes para concretar acciones delictivas basadas en el posible anonimato o falta de rastreabilidad que esto puede llevar (Kardile, 2017).

Los aspectos actuales de la criminalidad digital como son: i) el máximo anonimato con la mínima evidencia, ii) la máxima ambigüedad jurídica con el mínimo conocimiento tecnológico disponible y iii) la máxima efectividad de su acciones con el mínimo esfuerzo, establecen una economía del cibercrimen que habilitan el desarrollo de capacidades técnicas, sociales y de inteligencia lo suficientemente sofisticadas para aumentar el nivel de incierto en las personas, las organizaciones y los países, y así motivar acciones ilegales lucrativas que pueden pasar por debajo de los radares de las autoridades oficiales (Interpol, 2020).

Antes que una persona u organización sea una víctima de un ransomware deberá considerar sus estrategias de acción para establecer con claridad y visión holística la respuesta más apropiada para limitar a la medida posible los efectos adversos de esta condición, para lo cual se hace necesario aplicar las buenas prácticas y mantener un ejercicio permanente de ejercicios y simulaciones que generen una “memoria procedimental y práctica” para actuar de forma coordinada que limite la agenda del adversario: generar confusión, inestabilidad e incierto en la víctima.

Appendice

Listado de recursos en internet disponibles para enfrentar el ransomware

Dado la evolución acelerada del ransomware a nivel internacional se detalla a continuación un conjunto de algunos recursos disponibles en internet que pueden servir de apoyo y orientación para consulta y revisión por parte de los tomadores de decisión para actuar de forma coordinada y focalizada en medio de las tensiones que este evento genera.

- Allianz Global Corporate & Specialty (AGCS) (2021). Ransomware trends: Risks and Resilience - https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2021.html

- Cybereason (2022). Ransomware. The True Cost to Business 2022. A Global Study on Ransomware Business Impact - https://www.cybereason.com/ransomware-the-true-cost-to-business-2022

- Institute for Security and Technology (2022). Blueprint for Ransomware. Defense. An Action Plan for Ransomware Mitigation, Response, and Recovery for Small- and Medium-sized Enterprises - https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf

- ThreatPost (2021). 2021: The Evolution of Ransomware - https://media.threatpost.com/wp-content/uploads/sites/103/2021/04/19080601/0354039421fd7c82eb4e1b4a7c90f98e.pdf

- NIST (2020). Data Integrity: Recovering from Ransomware and Other Destructive Events. NIST Special Publication 1800-11 - https://www.nist.gov/news-events/news/2020/09/data-integrity-recovering-ransomware-and-other-destructive-events-nist

Estadísticas relevantes sobre el ransomware a nivel global

Múltiples informes a nivel internacional demuestran los retos e implicaciones de la extorsión con datos, indicando la necesidad de avanzar y concretar estrategias que permitan identificarlo y tratarlo de la forma más adecuada para limitar los daños que su materialización pueda causar. En este sentido, Gartner[19] en sus riesgos emergentes para el 2022 (Cohn, 2022), establece en primer lugar la aparición de nuevos modelos de *ransomware* como la tendencia de mayor importancia para mantener en el radar corporativo, habida cuenta que su evolución permanente y la habilidad de los atacantes para transformar sus prácticas extorsivas advierten de novedosas alternativas y adaptaciones de esta temática.

De otra parte, el sitio web *Cybersecurity Ventures* (2021) en su reporte más reciente sobre la extorsión con datos, presenta una estadística, la cual establece que un ataque de ransomware se materializará en un negocio, consumidor o dispositivo cada dos segundo para 2031, lo que implica una aceleración frente a los 11 segundos calculados en 2021. Este dato supone un ejercicio de alerta y vigilancia permanente que, en correlación con lo establecido por Gartner, requiere un tratamiento diferencial y particular dado la alta probabilidad de éxito que se puede tener por cuenta de esta amenaza.

19 Consultora y de investigación de las tecnologías de la información con sede en Stamford, Connecticut, Estados Unidos.

Otros reportes recientes (Coverware, 2022) indican marcados vectores de ataque utilizados por los cibercriminales como son el phishing, la vulnerabilidades en el software (algunas conocidas o no parchadas, como puede ser la asociada con WannaCry[20]) y el uso del protocolo de escritorio remoto (protocolo técnico de conexión remota (en inglés *Remote Desktop Protocol* (RDP)) , los cuales configuran la estrategia base para concretar el acceso no autorizado requerido para plantar el código malicioso y proceder con su ejecución. Es importante destacar que el atacante requiere de la acción de la víctima para iniciar el proceso, por tanto, en la medida que se haga más resistente al engaño, más tiempo deberá invertir el adversario para lograr su fin.

Cuando una organización ha sido víctima de ransomware sus efectos directos se configuran en al menos cinco temáticas: (SpyCloud, 2022)

- Exposición de datos propietarios o sensibles
- Daño en la reputación
- Alto esfuerzo en la recuperación y restauración de las operaciones
- Pérdida de clientes o de su satisfacción por las fallas operacionales
- Interrupción de los servicios/infraestructura crítica

Cualquiera sea la afectación que se tenga las organizaciones quedan expuestas y afectadas en la confianza del cliente, creando una espiral de pérdida de credibilidad y control que terminará afectando la dinámica de la entidad y sus iniciativas digitales en el mediano y largo plazo.

Recientemente en Latinoamérica y el Caribe se ha reportado una importante actividad de exfiltración[21] y extorsión[22] con datos en la región por cuenta de dos grupos particulares denominados “Guacamaya” y “Conti” que, si bien tienen intencionalidades y métodos distintos, ambos han creado inestabilidad y pérdidas financieras en muchos países de la región. Sus acciones dirigidas contra entidades del gobierno, entidades de la defensa nacional, infraestructuras críticas y empresas de sector minero energético dan cuenta de una marcada agenda agresiva que busca no sólo llamar la atención, sino también concretar lucrativos negocios de extorsión para aumentar sus capacidades y ganancias económicas.

> Un ataque de ransomware se materializará en un negocio, consumidor o dispositivo cada dos segundo para 2031, en contraste con los 11 segundos calculados en 2021.

20 Se aprovecha una vulnerabilidad en la implementación del protocolo Server Message Block (SMB) de Microsoft. Server Message Block (SMB) es un protocolo de red que permite compartir archivos, impresoras, etcétera, entre nodos de una red de computadoras que usan el sistema operativo Microsoft Windows. Fuente: https://www.avast.com/es-es/c-eternalblue

21 Ver sección de definiciones.

22 Secuestro de datos o información por la cual se pide un rescate generalmente con pago en criptomonedas.

Anatomía de un ransomware: Nivel de explotabilidad y etapas clave

Desde el punto de vista práctico, la extorsión con datos exige comprender el nivel de explotabilidad que tiene la organización objetivo frente a esta amenaza. Esto es conocer e identificar: (Stallings, 2019)

- **Vector de ataque:** proximidad del atacante al componente vulnerable
- **Complejidad del ataque:** nivel de dificultad requerido para que un atacante explote una vulnerabilidad una vez identificado el componente objetivo
- **Privilegios requeridos:** acceso que necesita un atacante para explotar una vulnerabilidad
- **Interacción con el usuario:** indicativo si un usuario distinto del atacante debe participar para que el ataque tenga éxito

En ese sentido, para que la extorsión con datos tenga éxito es necesario que participe la persona de forma directa, es decir, que un individuo tome una acción concreta en su computador o dispositivo, como puede ser un clic sobre un enlace malicioso (ver sección definiciones), con el fin de tener un pivote base donde iniciar las tres etapas claves para materializar dicha amenaza (Figura No.1)

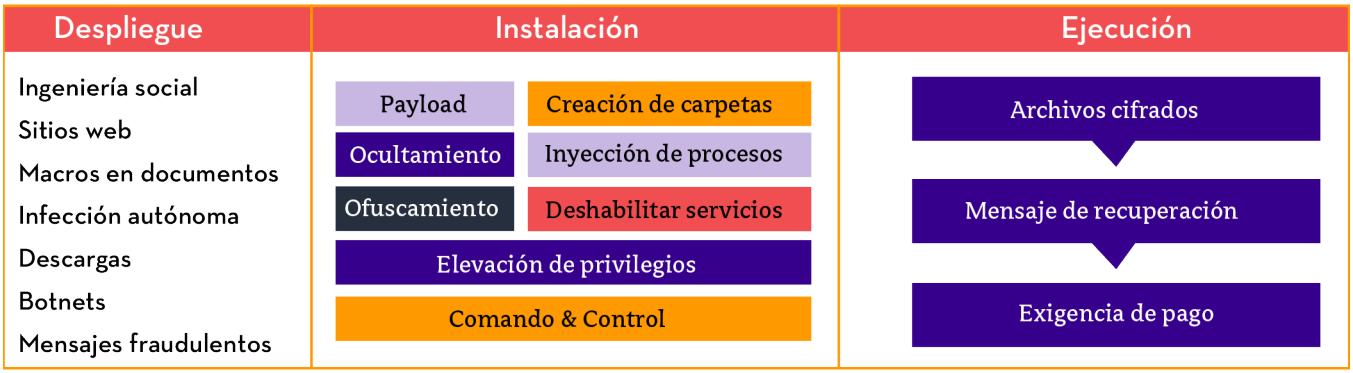


Figura 1. Anatomía de un ransomware (Elaboración propia con ideas de Osorio et al., 2020)

El primer momento es el *despliegue*, aquel proceso que se concreta a través del esfuerzo planeado y diseñado por el atacante que inicia con la inteligencia sobre la información de individuos o comunidad objetiva para concretar los intereses y temas que son relevantes en la dinámica social de las posibles víctimas. Seguidamente se desarrolla el engaño creíble y confiable que permite a las personas acceder a un sitio web, descargar documento y acceder a mensajes fraudulentos sin ser notados. Finalmente, la distracción, que es el aprovechamiento de la pérdida de atención por parte de las personas para efectuar la acción que inicia la descarga o el acceso del código malicioso al equipo móvil, portátil o de escritorio.

Una vez se ha concretado la descarga del malware, se inicia la *instalación* del *ransomware*. Se activa la "carga útil" (o *payload* en inglés) que dispara una serie de eventos de forma oculta en el dispositivo, como son la creación de carpetas, ocultamiento y ofuscación del código malicioso, la elevación de privilegios en el sistema objetivo, la inyección de procesos que se mimetizan con el proceso estándar del sistema operativo, se inhabilitan servicios de monitoreo y protección, para finalmente preparar el sistema comprometido a fin de tener comando y control de forma total.

Terminada esta etapa, donde el dispositivo ha quedado preparado para el control y manejo por parte del adversario, por lo general ocurren dos actividades al tiempo. Inicia la exfiltración de los datos sensibles que ha logrado obtener el adversario y posteriormente, el cifrado[23] de la misma en el dispositivo, el cual se desarrolla con algoritmos que se ejecutan en paralelo para lograr la máxima eficiencia en el proceso. Concluido este proceso, se genera el mensaje de alerta sobre la nueva condición de la máquina y la exigencia del pago para recuperar la información que se ha comprometido.

La literatura establece al menos cuatro (4) tipos de extorsiones que los atacantes pueden desarrollar una vez tienen comprometidos los datos: (MunichRe, 2022)

- **Extorsión sencilla:** solicitud de pago para devolver los datos cifrados
- **Doble extorsión:** robo y amenaza de publicación de datos
- **Triple extorsión:** amenaza de lanzar un ataque de denegación de servicio distribuido contra la víctima en caso de incumplir un pago
- **Cuádruple extorsión:** ataque a los proveedores, cadena de suministro y clientes de la víctima para expandir, y promover la presión por el pago

Al ser este tipo de actividad ilícita un negocio altamente rentable que genera en promedio un billón de dólares al año (Chainalysis, 2022), las ganancias económicas de esta extorsión se fundan en tres aspectos fundamentales: (Falco & Rosenbach, 2022, p.24)

1. Aprovechamiento de la venta de datos robados a terceros interesados
2. Amenaza a las organizaciones con lanzar un ciberataque o filtrar información sensible
3. Rescate en el que se prohíbe el acceso de una organización a sus datos hasta que se pague por la extorsión

Cualquiera sea el tipo de extorsión que se concrete, la institución tendrá presiones y exigencias que la llevarán a rendir cuentas por las consecuencias que se generen en sus grupos de interés y al mismo tiempo, el reconocimiento de las condiciones y capacidades que tiene el adversario para lograr la materialización de esta amenaza y lograr sus propósitos: extorsión y/o exfiltración.

Las ganancias económicas del ransomware se fundan en tres aspectos fundamentales:
- Aprovechamiento de la venta de datos robados a terceros interesados;
- Amenaza a las organizaciones con lanzar un ciberataque o filtrar información sensible;
- Rescate en el que se prohíbe el acceso de una organización a sus datos hasta que se pague por la extorsión.

18 Codificación de la información realizado por el adversario para impedir que su propietario tenga acceso a ella.

Referencias

Abrams, L. (2022). Conti ransomware finally shuts down data leak, negotiation sites. *Bleepingcomputer*. https://www.bleepingcomputer.com/news/security/conti-ransomware-finally-shuts-down-data-leak-negotiation-sites/

Baykara, M. & Sekin, B. (2018). A novel approach to ransomware: Designing a safe zone system. *2018 6th International Symposium on Digital Forensic and Security* (ISDFS), Antalya. 1-5. Doi: 10.1109/ISDFS.2018.8355317

Burgess, M. (2022). The Workaday Life of the World's Most Dangerous Ransomware Gang. *Wired*. https://www.wired.co.uk/article/conti-leaks-ransomware-work-life

Cano, J. (2020). Modelo SOCIA. Una reflexión conceptual y práctica desde la perspectiva del adversario. *Actas X Congreso Iberoamericano de Seguridad Informática 2020*. Universidad Politécnica de Madrid - Universidad del Rosario. Enero. Doi: 10.12804/si9789587844337.09

Chainalysis (2022). The 2022 crypto crime report. https://go.chainalysis.com/2022-Crypto-Crime-Report.html

Cohn, L. (2022). The Cutting Edge: 2Q22 Cool New Data Points. *Gartner Business Quarterly. Second Quarter*. 5-8. https://www.gartner.com/en/insights/gartner-business-quarterly

Coverware (2022). Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022. https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

El-Kosairy, A. & Azer, M. A. (2018). Intrusion and ransomware detection system. *2018 1st International Conference on Computer Applications & Information Security* (ICCAIS), Riyadh. 1-7, Doi: 10.1109/CAIS.2018.8471688

Falco, G. & Rosenbach, E. (2022). *Confronting cyber risk. An Embedded Endurance Strategy for Cybersecurity*. New York, NY. USA: Oxford University Press.

Herrera Silva, J. A.; Barona López, L. I.; Valdivieso Caraguay, A. L. & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. *Remote Sens*. 11(10). 1-20. Doi: 10.3390/rs11101168

Interpol (2020). Cybercrimen: Covid-19 Impact. August. De: https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

Kardile, A. (2017). Crypto ransomware analysis and detection using process monitor. *Master Thesis*. University of Texas, Arlington. De: http://hdl.handle.net/10106/27184

MunichRe (2022). Global Cyber Risk and Insurance Survey 2022. *Global Report*. https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html

Osorio, A., Mateus, M. & Vargas, H. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías*. 13(3). 131-142. doi: 10.18273/revuin.v19n3-2020013

Richard, L. (2022). "LA LUCHA POR UN TERRITORIO ES LA LUCHA DE TODAS". Forbidden Stories. https://forbiddenstories.org/es/la-lucha-por-un-territorio-es-la-lucha-de-todas/

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill

Sittig, D. F., & Singh, H. (2016). A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied clinical informatics*, 7(2), 624–632. Doi: 10.4338/ACI-2016-04-SOA-0064

SpyCloud (2022). Ransomware defense report. https://spycloud.com/resource/ransomware-defense-report-2022

Stallings, W. (2019). *Effective cybersecurity. A guide to using best practices and standards*. USA: Addisson Wesley.

Tavella, F. (2021). Ransomware Conti: principales características y cómo operan sus afiliados. *ESET*. https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/

Vicens, A. (2022). Hacking group focused on Central America dumps 10 terabytes of military emails, files. *CyberScoop*. https://www.cyberscoop.com/central-american-hacking-group-releases-emails/

Grimes, R. (2022). *Ransomware Protection Playbook*. Hoboken, NJ. USA: John Wiley & Sons.

Leo, P., Isik, O. & Muhly, F. (2022). The Ransomware Dilemma. *Sloan Management Review*. https://sloanreview.mit.edu/article/the-ransomware-dilemma/

2023

White paper series
Edición 10

Retos y Estrategias:

Las consideraciones de los ataques de ransomware en las Américas

OEA | Más derechos para más gente

aws