https://repository.uaeh.edu.mx/revistas/index.php/investigium/issue/archive

Boletín Científico INVESTIGIUM de la Escuela Superior de Tizayuca

InvESTigium

ISSN: 2448-4830

Publicación semestral, Vol. 10, No. Especial (2024) 35-42

"Tercer Congreso Internacional de Investigación e Innovación en Tendencias Globales y Primer Coloquio de Posgrado en Gestión y Desarrollo de Nuevas Tecnologías"
22 –25 de octubre de 2024

Ataques de Ransomware en México, la amenaza cibernética más temida de los últimos años

Ransomware Attacks in Mexico, the most feared cyber threat in recent years

Levi Jacob Ortiz Cruz [a], *Mónica García Munguía* [b]

Abstract:

Ransomware is one of the preferred attacks by cybercriminals. This criminal modality, "consists of malware that enters a computer or a system to encrypt the data it contains, asking for a financial amount in exchange for releasing the block to have access to the files again" [1]. In this article, a systematic bibliographic review of cases of attacks carried out in the country was carried out to collect information and present the analysis of the impact that it had in recent years, being responsible for half of the attacks in Mexico, having catastrophic consequences on the victims, the attack vectors and methods used during the attack are shown to identify the types of Ransomwares and present the action protocol that victims can adopt and thereby mitigate the risk.

Keywords:

Information, computer crime, computer threat, virus

Resumen:

El Ransomware es uno de los ataques preferidos por los cibercriminales. Esta modalidad criminal, "consiste en un malware que ingresa a un equipo o a un sistema para cifrar los datos que contiene pidiendo un importe económico a cambio de liberar el bloqueo para tener acceso de nuevo a los archivos" [1]. En el presente artículo se realizó una revisión sistemática bibliográfica de casos de ataques efectuados en el país para recopilar información y presentar el análisis del impacto que tuvo en los últimos años siendo el responsable de la mitad de los ataques en México, teniendo consecuencias catastróficas en las victimas., Se muestran los vectores de ataque y métodos utilizados durante el ataque para identificar los tipos de Ransomware y presentar el protocolo de actuación que pueden adoptar las víctimas y con ello mitigar el riesgo.

Palabras Clave:

Información, delito informático, amenaza informática, virus

Introducción

El Ransomware es un malware que imposibilita el uso del sistema, se exige un recate para rescatar su funcionamiento y el acceso del sistema [2].También bloquea el acceso a los archivos del sistema ya infectado, y pueden ser todo tipo de archivos, como documentos personales hasta los que resultan esenciales para la continuidad de una empresa.

Después de iniciar este ataque, los ciberdelincuentes se ponen en contacto con las empresas o personas vulneradas, solicitan sus exigencias y les aseguran desbloquear el equipo o descifrar los archivos una vez que hayan pagado el rescate, que suelen pedir en alguna otra criptomoneda, [3]. Normalmente se cifran los archivos con una clave única, la cual solamente el desarrollador de este tipo de malware conoce y se pide el pago en criptomonedas [4]. Este ataque permite a un pirata informático confinar el acceso a la información

[a] Autor de Correspondencia, Universidad Autónoma del Estado de Hidalgo | México, https://orcid.org/0000-0002-0507-3933, Email: monicagm@uaeh.edu.mx

[b] Universidad Autónoma del Estado de Hidalgo | México, https://orcid.org/0009-0001-1920-0868, Email: or359763@uaeh.edu.mx

Fecha de recepción: 30/08/2024, Fecha de aceptación: 24/09/2024, Fecha de publicación: 13/12/2024

DOI: https://doi.org/10.29057/est.v10iEspecial.13561

trascendental de una persona u organización para luego exigir alguna forma de pago para levantar la restricción que por lo regular es el cifrado de datos en la computadora o la red, teniendo como rehenes los datos del usuario o un sistema.

La mayoría de las organizaciones no han percibido la importancia de protegerse contra un ataque de Ransomware y no solo es la implementación de políticas de seguridad, si no la comprobación o el análisis de que sean efectivas cada una de ellas, entre las estrategias deben estar consideradas la gestión de copias de seguridad y una administración de la información para su protección. La predisposición de este ataque es ir evolucionando haciéndolo más sofisticado, aprovechando las vulnerabilidades que están presentes en los sistemas operativos, logrando ejecutar funciones que deshabilitan servicios, llegando a reiniciar la máquina en modo seguro evadiendo la protección, exigiendo, mayor grado de protección y una mejor implementación de la gestión de la seguridad [5]. Las derivaciones de un ataque con éxito son además de realizar el pago, la pérdida de productividad, cierre de un negocio, mala reputación de los clientes, molestias y, potencialmente, la pérdida permanente de datos [4]. México es uno de los países más comprometidos por lo que se vuelve un desafío protegerse ya que existe un promedio de 1,607 ciberataques que se registran semanalmente en el inicio de 2023. En la primera mitad de 2022, el país fue víctima de 85 mil millones de intentos de ciberataque, lo que significa un incremento del 40% en comparación el año anterior, ya que el primer semestre de 2023 tuvo una tendencia de 14 mil millones de intentos de ciberataques, lo que ubico a México en el segundo lugar en América Latina y el Caribe en términos de ciberataques, solo detrás de Brasil y seguido por Venezuela, Colombia y Chile [6]. Por lo anterior se requiere de una capacitación y concientización de estas amenazas a las que enfrentan las organizaciones y el personal de las mismas en el país ya que el 96% de las organizaciones en América Latina indicaron su preocupación como una amenaza latente, 21% manifestó haber sufrido un ataque de Ransomware en los últimos dos años del cual solo el 77% recupero su información gracias a las políticas de respaldos, y, el 4% aseguro que efectuó el pago para su rescate, pero 84% de las organizaciones encuestadas negó estar dispuesta a negociar el pago por el rescate de sus datos [7].

De las variantes más activas de Ransomware en 2023 fueron

• SiegedSec: se caracteriza por asediar a la víctima y opera con una extorsión ejerciendo presión para que realice el pago por el rescate de la información amenazando con su venta en foros de la Dark Web y Telegram. Inicio en el 2022 y puede ser cualquier blanco ya que sus víctimas son empresas de tecnología, contabilidad, finanzas entre otras.

• Nokoyawa: De origen ruso, utiliza un cifrado de curva elíptica, añadiendo su propia extensión de archivo homónima (NOKOYAWA).

• ALPHV: conocido también como Blackcat; opera a través del Ransomware-as-a-Service (RaaS, por sus siglas en inglés) debido a que sus ataques no se hacen aleatoriamente o por campañas de tipo spam, sus objetivos son determinados mediante los asociados con los que cuenta, es decir, que reúnen esfuerzos para realizar ataques a objetivos ya perfilados. El año pasado publicó información confidencial de la exfiltración de datos de una de las empresas más grandes de México a través de su canal de Telegram, de igual forma el sector público fue afectado.

• Stormous y su alianza con GhostSec: surge en la mitad del 2023, es de origen árabe, realiza ataques hacia Estados Unidos y debido al conflicto Rusia-Ucrania, sus objetivos se modificaron y se asocian con el grupo de hacktivistas GhostSec para atacar no solo a Estados Unidos, sino también a países de América Latina y entre ellos al gobierno de Cuba.

• Vice Society: sus ataques fueron hacia industrias de la educación y atención médica y últimamente está afectando al sector de la manufactura. Dispone de un generador de Ransomware personalizado, eligiendo métodos de cifrado más robustos, lo que indica que el grupo se prepara para llevar a cabo su propia operación de Ransomware como servicio (RaaS).

• ReEvil Ransomware: su modo de operación se centra en el phishing o enlaces maliciosos, es un modelo de tipo RaaS y proviene de Rusia. Se centro en sectores como la energia, la agricultura, los servicios financieros entre otros. Los países afectados fueron México, Estados Unidos, Chile, España.

• Darkside: Este grupo de Ransomware es el responsable del ataque a la empresa de oleoductos Colonial Pipeline. Opera con un modelo RaaS y sus objetivos se centran en todo tipo de empresas, aunque aseguran no atacar hospitales, instituciones educativas o al sector público.

• Maze: Se distribuye a través de enlaces maliciosos, kits de exploits, archivos adjuntos o ataques de fuerza bruta. Este grupo se encarga de publicar en su página a sus víctimas y parte de la información que robaron. Sigue un modelo RaaS en conjunto de una red de afiliados. En 2020 el este grupo anuncio su disolución [7].

Los ataques de este software malicioso están en tendencia apoyados por los métodos de ingeniería social lo que significa que deben complementarse los métodos de defensa perimetral con sistemas adicionales, [8]. En el año 2022, los dispositivos móviles se convirtieron en el objetivo de muchos ataques por Ransomware, es decir también cuentan con cepas que los afectan entre las más

peligrosas y más recientes está MalLocker, aquí el escenario que se presenta es que no cifra los archivos de la víctima, sino que bloquea el acceso total al teléfono, una vez instalado solo aparecerá en la pantalla una nota por su rescate, muy parecida a un mensaje de la ley local, comentando que el usuario cometió un delito y tiene que pagar una multa [9]. Con todo lo anteriormente es necesario realizar el análisis con la finalidad de conocer su evolución y el impacto de estos ataques y definir las causas que dan origen a las vulnerabilidades de los sistemas de información para proponer las medidas preventivas y de actuación si es que ocurrió el ataque.

El Ransomware de acuerdo a su modo de operación se puede clasificar en dos tipos (AO Kaspersky Lab, 2024).

Ransomware de bloqueo: Este impide el funcionamiento correcto del dispositivo infectado, lo que dificulta su manipulación.

Ransomware de cifrado: Cifra la mayoría de archivos con distintas extensiones, afectando la información personal del usuario infectado.

En la mayoría de los ataques de Ransomware, los delincuentes siguen estas ocho etapas como se muestra en la figura 1 y se detallan a continuación:

Figura 1. Fases de un ataque de Ransomware [10]

Reconocimiento: utilizando ingeniería social, análisis de red e inteligencia de fuentes abiertas (OSINT)

Compromiso inicial: las personas son la vulnerabilidad clave de una organización ya que son las que ejecutaran un código o abren un enlace malicioso comprometiendo el sistema o la red.

Persistencia: se dará acceso continuo a la red vulnerada a un grupo de Ransomware o por propia cuenta de quien inicio el ataque a través de una puerta trasera, puntos de acceso o cambios en la configuración.

Recopilación de información: se busca información crítica y poder extorsionar para un rescate con éxito, también pueden filtrar datos.

Escalamiento de privilegios: se accede como administrador del dominio utilizando escalamiento vertical de privilegios aprovechando errores de configuración en el servidor y tener acceso a cuentas con altos privilegios.

Desplazamiento lateral: el atacante se desplaza por la red para ampliar el alcance y cifrar sistemas completos o filtrar datos sensibles, es decir comprometer activos críticos.

Ejecución (antes del lanzamiento del ataque): el atacante mide el impacto del ataque dejando sin la posibilidad de recuperación y es la última oportunidad de filtrar datos sensibles o críticos para utilizarlos cómo técnicas de doble extorsión o en otros casos hasta de triple extorsión.

Impacto final (el resultado): Se notifica a las víctimas de lo sucedido es decir el cifrado de la red y sus datos pidiendo el pago para el rescate.

Método

El tipo de la investigación es una revisión sistemática bibliográfica, debido a que se realizó una valoración de los casos relevantes de ataques de Ransomware en México, se recopiló información de fuentes públicas entre ellas páginas especializadas, foros, redes sociales, reportes de medios, blogs de ciberseguridad y bases de datos abiertas para obtener detalles sobre incidentes de Ransomware, convirtiéndolo en un estudio de tipo descriptivo ya que identificó indicadores y características propias de cada caso que permitieron definir un protocolo de actuación para que los usuarios no sean víctimas de este tipo de ataque. Se requería recopilar información que no superara los últimos 5 años ya que en la tecnología se avanza constantemente como en el caso de aplicaciones móviles, sistemas operativos, etc., y algunos ya están obsoletos y las recomendaciones están dirigidas a equipos y sistemas que operan en la actualidad.

Se realizó un levantamiento de información sobre casos relevantes de ataques de Ransomware en México con casos de gran impacto en todos los sectores como gobierno, empresa y sistema financiero, con ello se identifican los vectores de ataque y la metodología que utilizaron los atacantes para lograr afectar a las víctimas. Se determino como casos relevantes los que sufrieron ya sea empresa o institución en relación con las pérdidas económicas y el tiempo de recuperación ante el incidente.

Análisis de datos

En 2023, el sector bancario mexicano recibió ciberataques sin precedentes. Los delincuentes cada día encuentran nuevas formas de encontrar vulnerabilidades a la par que las entidades financieras hacen esfuerzos por reforzar su seguridad digital. El Banco de México (Banxico) reportó ataques a tres bancos y una sociedad cooperativa de ahorro y préstamo, con un saldo de 67.6 millones de pesos en pérdidas debido a estas incursiones maliciosas, estos fueron dirigidos dejando en evidencia la vulnerabilidad incluso de las instituciones más robustas. El ataque ejecutado en febrero del mismo año aprovechando una vulneración a cajeros automáticos tendiendo pérdidas de 11.83 millones de pesos. En marzo fue el segundo incidente, un código malicioso afectó el servicio de transferencias electrónicas de un banco, con un saldo negativo de 55.71 millones de pesos. Este fue el monto más elevado de los ataques del año, destacando la gravedad del asunto.

El malware Prometi tuvo como víctima a uno de los bancos mexicanos, se especializa en la minería ilícita de

criptomonedas. Este troyano aprovecha la potencia de procesamiento de las computadoras infectadas para minar Monero (XMR), una criptomoneda popular entre los ciberdelincuentes y se propaga a través de campañas de phishing y explotación de vulnerabilidades, creando puertas traseras que permiten a los atacantes tomar control remoto del sistema infectado. Y en el mes de julio del 2023 se reportó otro ataque que, a una sociedad cooperativa de ahorro y préstamo, utilizando Ransomware, afectó diversos servicios, incluyendo la banca por internet, sucursales, transferencias electrónicas y cajeros automáticos. El monto total afectado por este ataque sigue pendiente de determinación [5]. El 8 de noviembre de 2019 Pemex fue vulnerado por un ciberdelincuente y logro robar documentos e información considerable por la cual exigía un rescate de 565 bitcoins o alrededor de 96.8 millones de pesos. El pago se tenía que efectuar en 48 horas o toda la información seria publicada en la Deep Web. La consecuencia de este ataque se caracterizó por la falla de terminales de almacenamiento y distribución, los empresarios no podían realizar pedidos y los trabajadores no podían acceder al sistema de logística. De acuerdo a las cifras oficiales que dio a conocer Pemex, el Ransomware afecto al 5% de los equipos de cómputo lo que equivale a diez mil dispositivos. A pesar de las advertencias por los ciberdelincuentes, Pemex se negó a pagar por el rescate lo que le valió a la empresa la filtración de sus datos a través del portal Dopple Leaks en la Deep Web [11]. El 30 de octubre de 2023 el Aeropuerto Internacional de Querétaro informó que tuvo un incidente sobre un ciberataque. La confirmación se dio después de que el grupo de Ransomware LockBit agregara en su foro de la Dark Web al AIQ. En su anuncio sobre el aeropuerto fijó como fecha límite el 27 de noviembre de 2023 para publicar todos los datos disponibles. El AIQ como respuesta, mencionó que toda la información con la que cuenta el grupo cibercriminal es de dominio público. El aeropuerto ya no actualizo más el tema y menciono que el incidente se derivó de que el personal de la organización interactuó con un archivo que contenía software malicioso [12]. La actividad del Ransomware logró crecer hasta un 300%, el grupo de Ransomware LockBit es uno de los responsables de la mayoría de ataques a los sectores gubernamentales y de manufactura.

El modelo de Ransomware como servicio (RaaS) ha facilitado la forma de atacar a las empresas. Durante el 2023 los ataques de Ransomware se convirtieron en esquemas de extorsión en los que se roban datos y se hace una amenaza de la divulgación de estos si es que no se paga un rescate.

Las estadísticas del 2023 para México se destacan en la figura 2:

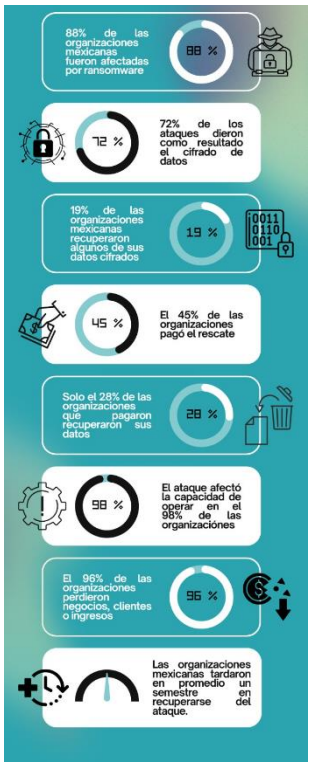

Figura 2. Estadísticas de ataque de Ransomware en México en 2023. (Imagen de elaboración propia).

La revisión documental sobre el Ransomware ayudo a conocer las diferentes cepas y variantes de este malware y se analizó sobre los casos sucedidos en México para identificar los más relevantes y de mayor impacto y obtener la información suficiente para realizar la propuesta de todo el conjunto de acciones que le permitan a los usuarios y a las organizaciones prevenir un ataque de esta naturaleza.

De acuerdo con el análisis de la unidad de investigación de [13], el país ocupa el número 14 a nivel mundial en este tipo de ataques de sus variantes de Ransomware, siendo los más atacados gobierno e industria y el que más afecto en el país es LockBit con 17 ataques documentados de ahí le la lista mostrada en la Tabla 1:

Tabla 1. Ataques por tipo en México

Ataque de Ransomware	Número
Alphv/BlackCat	9
Blackbyte	2
Cloak	1
Cl0p	16
Hunters	1
Losttrust	1
Medusa	1
Noescape	6

Play	2
Ragnarlocker	1
Ragroup	3
Rhysida	1
Royal	2
8Base	4
Lockbit	17

Muestra el número de ataques de Ransomware en México durante los últimos 5 años y cuáles son los más peligrosos [14]

Como se menciona, el principal atacante de los sistemas en México es LockBit, que es un software malicioso que está diseñado para bloquear el acceso a los sistemas informáticos y para después exigir un rescate en criptomonedas y recuperar el acceso y se encarga de buscar objetivos de gran valor y cifra todos los sistemas que sean accesibles en la misma red. Como se trata de un ciberataque auto pilotado los atacantes de LockBit amenazan a las empresas con interrumpir sus operaciones, extorsionar para así tener un beneficio financiero y finalmente robar datos y hacerlos públicos como imposición si no efectúan el pago por el rescate, [15].

Este grupo de Ransomware conocido en parte por su truco de tatuajes y como servicio (RaaS), fue una de las variantes de mayor impacto en el primer semestre del año 2022. El administrador del grupo, que se cree que utiliza "LockBitSupp" lanzo una actualización de la versión 2.0 a la versión 3.0, que incluía un blog de fuga de datos actualizado, un programa de recompensas por errores y una nueva funcionalidad en el Ransomware. Su éxito se basa en varias estrategias que han logrado mantenerse por delante de otras variantes. Esto ha incluido un fuerte enfoque en la seguridad operativa (OPSEC) y el desarrollo continuo de métodos técnicos, extorsión y técnicas de negociación. La versión actualizado logro 367 infracciones, [16].

En los inicios del año 2024 se dieron varios ataques en el país por lo que la ciberseguridad y el cibercrimen es un tema que se debe abordar por parte de las autoridades y empresas antes que ocurra un incidente dirigido. Los incidentes que suman a las estadísticas negativas del país se deben a una ausencia de acciones y la no preocupación de los interesados en proteger a las empresas, ya sea gobierno y dueños de la información que no tienen los herramientas y estrategias para prevenir o contener sea el caso de un Ransomware. Cada administración pública debe de tener estrategias de acciones, leyes y capacitación para encarar esta tarea que de no ser atendida cada día será más compleja de resolver.

Como se mencionó con anterioridad durante los primeros meses de 2024, se registró un considerable aumento de 66.8% en el número de víctimas reportadas en comparación con el mismo período del año anterior. Por lo que se supone que la cantidad de grupos de Ransomware activos ha experimentado un notable aumento, pasando de 19 grupos distintos en el primer trimestre de 2023 a 76 en el mismo período de 2024. En cuanto a México, se han documentado 73 ataques de Ransomware en el período comprendido entre 2021 y 2024, reafirmando que LockBit es el responsable de 29 de ellos.

Para que el negocio de Ransomware siga teniendo éxito es gracias a que las empresas no atienden vulnerabilidades por diferentes razones [14].

Resultados

Las organizaciones (gobierno, empresas) deben centrar sus esfuerzos en la preparación para contener un ataque de Ransomware, y con ello garantizar que se tomarán las medidas que ayuden a su protección, independientemente de su industria de negocio, deben establecer políticas internas en combinación con la implementación de tecnologías que les permitan protegerse, además de involucrar eficazmente a todos los empleados de las empresas, con un programa de capacitación y concientización frente a las amenazas cibernéticas tanto físicas como lógicas [17] :

- Mantener los sistemas actualizados: Garantizan que los sistemas ante una vulnerabilidad estén ya con parches de seguridad y que es lo que aprovecha el ciberdelincuente para realizar un ataque exitoso.
- Copias de seguridad: Realizar un plan para el respaldo de los datos importantes con una planeación que además incluya los sitios de almacenamiento considerando que deben ser fuera de la red principal.
- Utilizar un software de seguridad: antivirus y antimalware actualizado.
- Implementar medidas de seguridad adicionales: Utilizar firewalls, sistemas de detección de intrusiones y programas de seguridad de endpoint. Este tipo de herramientas ofrecen una capa más de protección ante los ataques de Ransomware.
  Para la gestión del sistema se recomienda además de las anteriores
- Actualizaciones de los complementos y navegadores.
- Control de acceso a usuarios.
- Lista blanca de aplicaciones.
- Administración de conexiones inalámbricas.
- Uso de extensiones para el bloqueo de anuncios en los navegadores.
- Deshabilitar procesos de Windows que no se utilizan.
- Deshabilitar conexiones de protocolo de escritorio remoto.
- Bloqueo de tráfico a puertos asociados
- Si se requiere el acceso remoto, auditar el acceso, verificar contraseñas seguras y tengan implementado un doble factor de autenticación.
- Configuraciones para evitar que archivos ejecutables como .exe, .rar, .pdf, exe, .zip, se ejecuten.
- Implementar herramientas de ciberseguridad para evitar que se ejecute Ransomware.
- Utilizar protección web y de correo electrónico para bloquear el acceso a sitios web maliciosos
- Análisis de todos los correos electrónicos con sus archivos adjuntos, descargas y configurar los

servidores de correo electrónico para bloquear aquellos que contengan archivos sospechosos como ejecutables .exe, .vbs o .scr.
- Implementar herramientas anti Ransomware gratuitas o de licencia con los principales proveedores de seguridad informática.

En la parte de Administración de redes se recomienda
- Contar con un firewall habilitado y configurado correctamente de acuerdo a las necesidades de la empresa.
- Bloquear direcciones IP Tor maliciosas conocidas.
- Implementar una Zona Desmilitarizada
- Virtualizar los servicios para salvaguardar los recursos [18].

Cuando ocurre un ataque los daños pueden van desde la responsabilidad civil de la empresa por la divulgación de información confidencial propia o ajena, hasta daños patrimoniales causados a los sistemas informáticos o por una interrupción del negocio, para ello también es importante considerar los seguros de Cyber Risk, donde se puede brindar cobertura para los riesgos, es fundamental analizar los alcances de los riesgos cubiertos y sus exclusiones indicado que no van a cubrir, [19].

Existen métodos de prevención que resultan ser eficaces, como crear una copia de seguridad y mantenerla actualizada además de no hacer clic en enlaces y archivos adjuntos de correo electrónico que no sean de confianza (Banco Santander, 2024).

El uso de los Honeypot como un señuelo para detectar la actividad de Ransomware seleccionando , el servicio de filtrado de archivos de la característica Microsoft File Server Resource Manager y EventSentry para manipular los registros de seguridad de Windows, esta propuesta es limitada ya que no hay forma de influir en el malware para que acceda a los archivos que están monitoreados, por lo que la estrategia debe estar acompañada por las ya mencionadas como el envío de alertas por correo electrónico a los usuarios, acompañadas de la concientización del usuario y desconectar el equipo de la red [8].

Utilizan herramientas forenses donde capturan tráfico de un sistema infectado para identificar las claves de cifrado simétricas que utiliza el software malicioso, analizaron muestras de Ransomware híbrido NotPetya, Bad Rabbit y Phobos [20]. Una vez que se detectan las claves, crean manualmente una línea de tiempo mostrando el periodo en que permanecen las clases de cifrado en la memoria para después intentar descifrar los archivos cifrados por el Ransomware utilizando las claves encontradas. Con esta técnica se pudo confirmar que era posible identificar las claves de cifrado utilizadas además de describir cómo se utilizaron estas claves encontradas para descifrar con éxito los archivos que se habían cifrado durante la ejecución del Ransomware.

Hay que recordar que los efectos de este ataque son permanente y difícil de recuperarse a un estado igual al que estaba el equipo antes del ataque, incluso después de la eliminación, sin la ayuda del autor del ataque, por lo que lo hace uno de los ataques más peligrosos en el mundo cibernético y todas las estrategias presentadas son válidas siempre y cuando se tenga al equipo capacitado para la realización.

Conclusiones

A lo largo de los últimos años, el país ha sido testigo de un aumento alarmante en la incidencia de este tipo de ataques, con repercusiones que van más allá de las fronteras digitales para impactar la economía, la infraestructura y la seguridad nacional. Además de estas recomendaciones, es importante hacer del conocimiento de todos los empleados y grupos de interés la importancia sobre un ataque cibernético acompañado de la concientización. Se debe enfatizar en la importancia de no abrir archivos adjuntos o hacer clic en enlaces sospechosos. Estar prevenidos y preparados es fundamental para reducir el riesgo de ser víctima de Ransomware y minimizar el impacto en caso de un ataque.

En el tema de prevención se sugiere la monitorización y vigilancia a nivel de red, analizar todos los datos que entran a través del perímetro, los que salen de la compañía y el tráfico entre equipos dentro de la red propia, a esta actividad se le denomina NSM (Network Security Monitoring) [20].

Usar un honeypot para engañar al software de rescate y descubrirlo es un método más rápido para detectar ataques de Ransomware.

Para este año 2024 y los próximos años se enfatiza la necesidad crítica de lograr un equilibrio entre la ciberseguridad y la ciber resiliencia. Mientras los especialistas en tecnología de la información y seguridad se preparan para el año entrante, es crucial dar prioridad a la capacidad de visualizar, proteger y gestionar de manera constante toda la superficie de ataque.

Bien se sabe que las infecciones de Ransomware no se pueden prevenir, los usuarios pueden reducir este riesgo de una manera óptima con estrategias de ciberseguridad y mejorando la concientización sobre las ciber amenazas al igual que las buenas prácticas de la seguridad.

Para México se destaca la creciente sofisticación de los actores maliciosos debido a la falta de preparación de las organizaciones para hacer frente a estas amenazas, además de la falta de conciencia sobre la importancia de la ciberseguridad, combinada con la escasez de recursos y una regulación efectiva, ha creado un entorno propicio para la propagación del Ransomware y otros tipos de ataques. Dentro de los impactos devastadores esta la interrupción de servicios críticos hasta la pérdida de datos sensibles pasando por la extorsión financiera y los resultados pueden ser desastrosos y de largo alcance. Para mantener la continuidad de las operaciones es importante considerar en sus estrategias de un alto estándar de Operaciones de Seguridad (OPSEC), que son medidas destinadas a frustrar la identificación o interrupción de la actividad en curso y en el país queda mucho por hacer para mitigar eficazmente la amenaza y proteger los sistemas y datos críticos., considerando un enfoque integral que involucre a todos los actores relevantes, desde el gobierno y las empresas hasta la sociedad en su conjunto. Solo mediante la colaboración y el compromiso continuo se protegerán mejor los sistemas y datos de los devastadores efectos del Ransomware y

garantizar un futuro digital seguro y próspero para México y sus ciudadanos.

Como se mencionó LockBit es un grupo que tiene un gran dominio en ransomware ya que cuenta con conocimiento de OPSEC, ya que es sus actualizaciones no se descarta que estén competidores, investigadores de inteligencia de amenazas cibernéticas (CTI), agentes encargados de hacer cumplir la ley y periodistas se infiltraran en el grupo y filtraran información confidencial, además que conto con programa de recompensas por errores que ofrecía pagos de hasta 1 millón de dólares por el descubrimiento de vulnerabilidades en el malware del grupo.

Con el aumento y la caída de las variantes de Ransomware a lo largo de los años se manifiestan lo complejo que es, además que se fusionan grupos para distribuir el troyano a ciertos objetivos y evidenciar a sus víctimas en la red Tor o blogs.

Cuando los datos están cifrados, las organizaciones que no tienen copias de seguridad deberán comprar claves de descifrado para su continuidad. Para aquellas organizaciones con buenas copias de seguridad, no hay necesidad de pagar cuando existe un robo. Muchos de los planes de acción anti-ransomware lanzados en todo el mundo incluyen medidas para mejorar los niveles básicos de ciberseguridad en todas las industrias, como la implementación de autenticación multifactor (MFA), la limpieza de la gestión del acceso privilegiado, el cierre de puertos externos, la aplicación de parches más rápidos a las aplicaciones y más.

Ante un malware que evoluciona rápidamente y los antivirus a veces no pueden detectar estas amenazas, [2] se propone tres métodos de detección y se basan en clasificar y analizar el tráfico de red para extraer comportamientos anómalos y así detectar el Ransomware combinado con técnicas de aprendizaje automático sin dejar a un lado el uso de técnicas de memoria volátil (forense) para identificar las claves de cifrado utilizadas en el ataque.

Las mejoras en la ciberseguridad son proyectos a largo plazo. Sin embargo, con el tiempo, será más difícil para los actores del Ransomware tener éxito.

Referencias

[1] García-Córdoba, J, & Herrero-Pérez, L. (2020). La ciberdefensa en los sistemas de información sanitarios militares. Sanidad Militar, 76(3), 140-142. Epub 08 de marzo de 2021.https://dx.doi.org/10.4321/s1887-85712020000300001

[2] Banco Santander, S.A. (2024). bancosantander. Obtenido de https://www.bancosantander.es/glosario/ransomware#:~:text=El%20ransomware%2C%20en%20inform%C3%A1tica%2C%20es,%2C%20bloqueando%20la%20pantalla%2C%20etc.

[3] Seguin, P., & Latto, N. (2021). Gen Digital Inc. Obtenido de Avast: https://www.avast.com/es-es/c-what-is-ransomware

[4] Ross Brewer. (2016). Ransomware attacks: detection, prevention and cure, Network Security, Volume 2016, Issue 9, Pages 5-9, ISSN 1353-4858, https://doi.org/10.1016/S1353-4858(16)30086-1. (https://www.sciencedirect.com/science/article/pii/S1353485816300861)

[5] Ávila Niño, F. Y. (2021). Evolución e Impacto del Ransomware en América Latina desde el año 2015. México, México: Universidad Nacional Abierta Y A Distancia – UNAD.

[6] González Cuautle, D. (2023). ESET. Obtenido de https://www.welivesecurity.com/es/cibercrimen/5-grupos-ransomware-activos-america-latina-2023/

[7] Cumbicus-Pineda, Oscar M. & Preciado, Pablo & Neyra, Lisset. (2022). Técnicas de machine Learning para la detección de Ransomware: Revisión sistemática de literatura. Machine Learning Techniques for Ransomware Detection: Systematic Literature Review. 7. 32-60. 10.5281/zenodo.7373655.

[8] Moore, C. (2016). Detección de ransomware con técnicas honeypot. En 2016 Conferencia de Ciberseguridad y Ciberanálisis Forense (CCC) (pp. 77-81). IEEE.

[9] Ivanov, A., Emm, D., Sinitsyn, F., & Pontiroli, S. (2016). SecureList por Kaspersky. Obtenido de AO Kaspersky Lab: https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/

[10]Petersen, B. (2023). Proofpoint. Obtenido de https://www.proofpoint.com/es/blog/email-and-cloud-threats/eight-stages-of-the-ransomware-attack-chain

[11] Efrain, M. (2020). Energy and Commerce. Obtenido de https://energyandcommerce.com.mx/hackers-filtran-informacion-robada-a-pemex/

[12] Tecnología Por Palabras SL. (2020). Microsofters. Obtenido de https://microsofters.com/microsoft/mallocker-el-ransomware-para-android-mas-peligroso/

[13] Silikn. (2023). Silink. Obtenido de https://www.silikn.com/2023/10/ransomware-en-la-mira-como-evitar-ser.html

[14] Ruiz, V. (2024). Silikn. Obtenido de https://www.silikn.com/2024/05/estadisticas-de-cibercrimen-que-el.html

[15] AO Kaspersky Lab. (2024). latam Kaspersky. Obtenido de https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware

[16] Intel471 . (2023). Intel471 . Obtenido de https://intel471.com/blog/a-ransomware-forecast-for-2023

[17] Ramírez Duque, A. (2022). Tendencias en Ciberseguridad en Latinoamérica. Revista Empresarial & Laboral. https://revistaempresarial.com/tecnologia/seguridad-informatica/tendencias-en-ciberseguridad-en-latinoamerica/

[18] Zhuma, Mera lscr, Emilio, Brito Casanova, Orlando Jesús, Tubay Vergara, José, & Oviedo Bayas, Byron. (2021). Análisis dinámico de malware en ambiente de red virtualizado. Conrado, 17(78), 113-120. Epub 02 de febrero de 2021. Recuperado en 02 de mayo de 2024, de http://scielo.sld.cu/pdf/rc/v17n78/1990-8644-rc-17-78-113.pdf.

[19] Sobrino, W. (2018). Los seguros de 'cyber risk' (A propósito del ciberataque mundial de fecha 12 de mayo de 2017). Revista Ibero-Latinoamericana De Seguros, 26(47). https://doi.org/10.11144/Javeriana.ris47.

[20] Simon R. Davies, Richard Macfarlane, William J. Buchanan. (2020). Evaluation of live forensic techniques in ransomware attack mitigation, Forensic Science International: Digital Investigation, Volume 33, ISSN

2666-2817, https://doi.org/10.1016/j.fsidi.2020.300979. (https://www.sciencedirect.com/science/article/pii/S2666281720300858)

[21] Brisa, S. (2015). SecurityArtWork. Obtenido de Genesis Framework: https://www.securityartwork.es/2015/06/22/squert/

..