EasyChair Preprint

№ 12463

Analysis of Current Challenges in the Prevention of Ransomware Cyberattacks

Jorge Hernandez

March 13, 2024

ANÁLISIS DE LOS DESAFÍOS ACTUALES EN LA PREVENCIÓN DE LOS CIBERATAQUES POR RANSOMWARE

Jorge Alberto Hernández Morales
Estudiante
Universidad de las Ciencias Informáticas, Cuba
jahernandezm@estudiantes.uci.cu

Resumen: En el artículo se hace una caracterización de los ransomware. Los autores emplean un enfoque histórico-lógico para examinar los principales ataques de ransomware que han ocurrido a lo largo de los años. Esta investigación es crucial debido a la gran amenaza que representa el ransomware. Además, se investigan diferentes métodos para prevenir, identificar y eliminar el ransomware. Estos métodos son esenciales para combatir esta amenaza y proteger nuestros sistemas y datos. Para contextualizar la relevancia actual de esta amenaza, se exploran los principales ataques recientes de ransomware. Estos ataques demuestran la persistencia y evolución de esta amenaza en el ciberespacio. En resumen, el artículo proporciona una visión integral del ransomware, desde su historia hasta los métodos actuales de prevención y eliminación, destacando la importancia de estar informado y preparado ante esta creciente amenaza cibernética.

Palabras claves: **ransomware, amenaza, ciberespacio, prevención, identificación, eliminación.**

Tipo de contribución: *Investigación original.*

I. INTRODUCCIÓN

En la actualidad existen numerosos activos informáticos, la mayoría de ellos están conectados a Internet lo cual hace que ocurran algunos problemas de Ciberseguridad. Un ejemplo de uno de estos problemas es la infección por malware, dentro de esta amplia gama de diferentes malware existentes se puede decir que la infección por ransomware es una de las más peligrosas debido a como este ataca al sistema informático donde esté hospedado. Conociendo esto, día a día muchas instituciones que desempeñan labores para la gestión y prevención de las diferentes amenazas que ocurren en el Ciberespacio realizan acciones de control de malware para disminuir el riesgo de que se materialice un problema de este tipo. Según el Panorama de amenazas de Kaspersky para América Latina, la empresa registró 1.3 millones intentos de ataque de ransomware en la región entre enero y septiembre de 2020, lo que significa un promedio de 5,000 ataques por día. Entre los países más atacados se encuentran Brasil, México, Colombia, Perú y Ecuador. Los principales vectores de infección son las vulnerabilidades en programas obsoletos o versiones pirateadas y el uso de contraseñas simples. El historial de ransomware en Latinoamérica es curioso. Entre 2014 y 2017, la cantidad de ataques aumentaba un promedio de 30% cada año, pero después del famoso caso de WannaCry, el interés de los ciberdelincuentes disminuyó. Después de un periodo de calma, esta modalidad de ataque retomó fuerzas en 2018 y, desde entonces, ha mantenido un ritmo de crecimiento constante de casi 7% por año [1].

La razón de este resurgimiento se debió al cambio de enfoque de los atacantes, los cuales pasaron de ataques masivos a centrarse en un menor número de víctimas: empresas, entidades gubernamentales y sectores industriales críticos [1].

La lista de los países más atacados de la región la encabeza Brasil con casi la mitad de las detecciones (46,69%). Le siguen México (22,57%), Colombia (8,07%), Perú (5,56%), Ecuador (3,86%), Chile (2,29%), Venezuela (2,17%) y Argentina (1,93%). Las malas prácticas de las empresas y entidades gubernamentales permiten que el ransomware sea una amenaza real [1].

II. CONTENIDO

Método de investigación utilizado: Histórico lógico: Se utilizó para evaluar las distintas infecciones que han ocurrido por este malware a través de los años.

Historia

El término con el que comienza ransomware, “ransom”, es una palabra inglesa que significa “rescate”. El primer ataque de ransomware fue en el año 1989 usando un programa llamado AIDS Trojan [2].A través de los años han existido numerosos ataques, ñ´nml se muestran algunos de los más relevantes:

Los ataques con el ransomware Locky comenzaron en 2016, de la mano de un grupo organizado de hackers. Locky estaba diseñado para cifrar más de 160 tipos de archivos. Se propagaba en forma de archivo adjunto, a

través de correos electrónicos engañosos. Cuando un usuario recibía uno de estos mensajes y caía en el engaño, instalaba el ransomware sin notarlo. El método de propagación que utilizaba Locky se denomina "phishing" y es una forma de ingeniería social. Locky se centraba en clases de archivos que se suelen utilizar en programación, diseño, ingeniería y control de calidad [3].

Wanacry fue un ataque de ransomware ocurrido en 2017. Tuvo víctimas en más de 150 países. El ataque se basaba en una vulnerabilidad del sistema operativo Windows. La vulnerabilidad, explotada en un primer momento por la NSA, fue divulgada por el grupo hacker Shadow Brokers. WannaCry infectó más de 230 000 computadoras alrededor del mundo. En el Reino Unido, el ataque afectó un tercio de los centros de salud del NHS y, se calcula, tuvo un costo superior a las 92 millones de libras. Los usuarios afectados por WannaCry quedaron sin acceso a sus archivos y se enfrentaron a pagar una suma extorsiva en bitcoins. El ataque dejó en evidencia la problemática de los sistemas desactualizados, pues los hackers se aprovecharon de una vulnerabilidad para la que desde hacía tiempo existía un parche. Se cree que el costo mundial de WannaCry ascendió a unos 4 000 millones de dólares [3].

Bad Rabbit es el nombre de un ransomware,el cual se utilizó para realizar diferentes ataques en el año 2017, se propagó utilizando un método conocido como descarga oculta. El ataque se perpetró a través de sitios web inseguros. En un ataque de ransomware con descarga oculta, la víctima ingresa a un sitio web legítimo sin saber que ha sido vulnerado. Esta acción suele ser suficiente para que se inicie la descarga y se concrete el ataque. En este caso, sin embargo, la infección ocurría cuando el usuario ejecutaba un programa de instalación con malware oculto. Para infectar el equipo, Bad Rabbit le pedía al usuario que ejecutara un instalador de Adobe Flash que resultaba ser falso [3].

Ryuk, un ransomware que se propagó durante agosto de 2018, estaba programado para deshabilitar la característica de recuperación con la que cuentan los sistemas operativos Windows. Con ello, si el usuario no contaba con una copia de seguridad externa, recuperar la información cifrada resultaba imposible. Ryuk se aseguraba también de cifrar cualquier disco duro conectado a la red. El impacto fue enorme. En Estados Unidos, muchas de las organizaciones atacadas optaron por pagar el rescate. El costo estimado asciende a más de 640 000 dólares [3].

Shade y Troldesh son dos ransomware que se utilizaron para atacar en 2015. El malware, en este caso, se propagaba a través de vínculos o adjuntos infectados, que se distribuían a través de correos electrónicos masivos. Un aspecto interesante de este caso es que los atacantes se comunicaban con sus víctimas en forma directa por correo electrónico. Si entablaban una buena relación con una víctima, le ofrecían un descuento [3].

Jigsaw es ransomware que comenzó a usarse en 2016. Su nombre se debe a que el ransomware mostraba una imagen del personaje de la película "El juego del miedo". Según pasaban las horas sin que se pagara el dinero del rescate, Jigsaw eliminaba más y más archivos [3]

.El ransomware CryptoLocker apareció por primera vez en el año 2007. Se propagaba por correo electrónico, a través de archivos adjuntos infectados. Una vez que se introducía en un equipo, buscaba la información más importante y la cifraba. Se estima que unas 500 000 computadoras se vieron afectadas. CryptoLocker se propagaba a través de una red mundial de computadoras hogareñas infectadas. Tras un arduo trabajo, empresas y fuerzas de seguridad lograron hacerse con el mando de esta red. Ello les permitió interceptar la información que se transmitía a los delincuentes sin que estos lo notaran. El esfuerzo derivó en la creación de un portal web, que las víctimas podían visitar para obtener una clave de desbloqueo. La clave permitía recuperar la información cifrada sin pagar el dinero del rescate [3].

Petya (no confundir con ExPetr) es un ransomware que se vio por primera vez en 2016 y que reapareció, con el nombre de GoldenEye, en 2017. El ransomware no se conformaba con cifrar solo ciertos archivos, sino que cifraba el disco duro entero. Cifraba para ello la tabla maestra de archivos (MFT), por lo que acceder al contenido del disco se volvía realmente imposible. Petya se infiltraba en los departamentos de Recursos Humanos de las grandes empresas a través de una aplicación falsa que contenía un vínculo de Dropbox infectado [3].

Existió una variante de Petya, llamada Petya 2.0, que se diferencia de la versión original en algunos aspectos clave. En lo que respecta al modo de ataque, sin embargo, ambas variedades eran igual de mortíferas para los dispositivos infectados [3].

El resurgimiento de Petya en 2017, esta vez con el nombre de GoldenEye, derivó en una infección de ransomware que dio la vuelta al mundo. GoldenEye, conocido como el "hermano mortífero" de WannaCry, afectó a más de 2000 objetivos, entre los cuales hubo bancos y reconocidas petroleras rusas.

Una de las consecuencias más alarmantes del ataque tuvo lugar en la planta nuclear de Chernóbil: allí, los empleados se vieron obligados a controlar el nivel de radiación en forma manual porque el ransomware los dejó sin acceso a sus equipos con Windows [3].

GandCrab es un ejemplo de ransomware, amenazaba a sus víctimas con revelar su consumo de pornografía. El software aseguraba tener acceso a la cámara web del equipo y exigía el pago de un rescate. Según la amenaza, a menos que se pagara ese dinero, el ransomware haría públicas ciertas grabaciones privadas de la víctima. La versión original de GandCrab hizo su debut en 2018 y se tiene registro de variantes posteriores. Las empresas de seguridad y las agencias policiales que forman parte de la iniciativa "No More Ransom" crearon una herramienta de descifrado para GandCrab, que las víctimas podían utilizar para recuperar sus datos [3].

B0r0nt0k es un ransomware de cifrado que se creó

específicamente para servidores con Windows y Linux. Tras infiltrarse en un servidor con Linux, este software cifra los archivos que encuentra y les añade la extensión ".rontok". Además de afectar los archivos almacenados, el ransomware deshabilita funciones y aplicaciones, modifica los ajustes de arranque y agrega archivos, programas y entradas del Registro [3].

Brrr es un nuevo integrante de la familia de ransomware Dharma. Los hackers instalan este malware manualmente en el equipo de la víctima tras introducirse en el mismo por Internet, a través de los servicios de escritorio remoto. Los archivos del equipo comienzan a cifrarse en cuanto el hacker activa el ransomware. Los archivos cifrados toman la extensión ".id-[id].[email].brrr" [3].

FAIR RANSOMWARE está diseñado para cifrar información. Utiliza un potente algoritmo para cifrar todos los documentos y archivos privados de la víctima. Los archivos cifrados toman la extensión ".FAIR RANSOMWARE" [3].

MADO es otro tipo de ransomware de cifrado. Los archivos cifrados por este malware toman la extensión ".mado" y dejan de poder abrirse [3].

Tipos de ransomware

Los ransomware se dividen en dos tipos:

Ransomware de bloqueo. Este tipo de ransomware está diseñado para bloquear funciones básicas del equipo. Puede impedir el acceso al escritorio del sistema y restringir parcialmente el uso del teclado y del mouse. La víctima puede interactuar únicamente con la ventana en la que se le exige el pago de un rescate. Las demás funciones del equipo quedan inutilizables. El ransomware de bloqueo tiene un lado positivo: por lo general, restringe el uso del equipo, pero deja sin cambios los archivos. La información de la víctima rara vez corre el riesgo de desaparecer [3].

Ransomware de cifrado. Este tipo de ransomware está diseñado para cifrar los archivos más importantes de la víctima, como sus documentos, fotos y videos. El funcionamiento del equipo no se ve afectado en modo alguno. La víctima entrap ve que sus archivos siguen allí, pero no puede abrirlos. Esta clase de malware muestra una leyenda en la que se exige el pago de un rescate y, por lo general, una cuenta regresiva. "Pague antes de que se agote el tiempo o perderá sus archivos", advierte el software. Como no todas las personas tienen copias de seguridad de sus archivos en la nube o en un soporte externo, el ransomware de cifrado puede tener un impacto muy profundo [3].

A continuación se muestra un gráfico con las distintas categorías de ransomware Fig. 1.

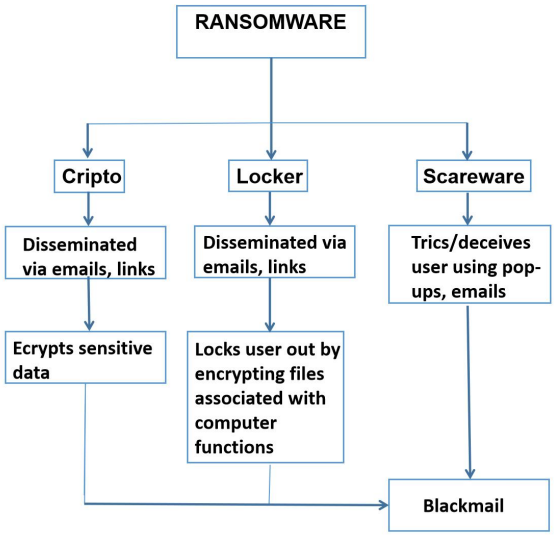

Figura. 1: Categorías de los ransomware

Formas de infección

La forma más frecuente de infección son ataques dirigidos que llegan a los correos electrónicos. Los atacantes envían links en los emails para que al hacer clic redirija automáticamente a la persona a una página donde se encuentra el ransomware. La segunda forma más común es por medio de documentos adjuntos en el email como archivos comprimidos documentos de texto, pdfs, entre otros. Así se garantiza que el ataque sea efectivo, tal práctica se conoce como ingeniería social. En tercer lugar, están los sitios web que no cuentan con seguridades correspondientes (https, SSL), luego los medios sociales y por último USB infectadas o dispositivos externos manipulados. En la Fig. 2 se muestra una tabla que hace referencia a su funcionamiento.

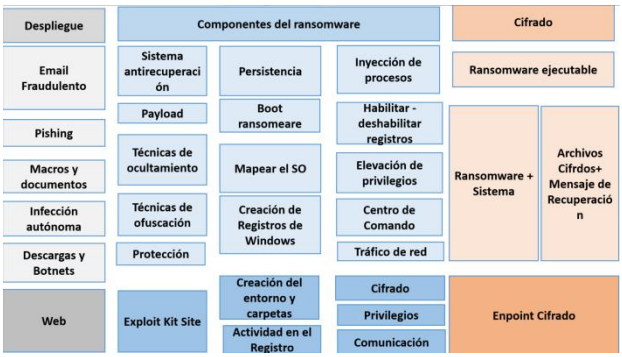

Figura 2. : Funcionamiento

Formas para detectarlo y eliminarlo

Como saber si un ordenador está infectado:

El analizador antivirus notifica una alarma: Si el dispositivo tiene una aplicación antivirus, puede detectar la infección de ransomware de manera temprana, a menos que se haya desactivado [4].

Comprobar la extensión de los archivos: por ejemplo, la extensión normal de un archivo de imagen es «.jpg». Si esta extensión ha cambiado a una combinación de letras desconocida, es posible que haya una infección de ransomware [4].

Cambio de nombres: Los programas maliciosos a menudo cambia los nombres de los archivos cuando cifran los datos. Si nota un cambio como este, puede que haya un problema [4].

Aumento de la actividad de la CPU y el disco: Si el disco o el procesador principal están trabajando más de lo habitual, es posible que el ransomware se esté ejecutando en segundo plano [4].

Tráfico de red dudoso: La interacción entre un programa y el ciberdelincuente o el servidor del atacante puede generar un tráfico de red sospechoso [4].

Archivos cifrados: Una señal tardía de que un ransomware ha actuado es cuando ya no se pueden abrir los archivos [4].

Por último, si sale una ventana que exige el pago de un rescate, se puede afirmar con seguridad que el equipo está infectado con ransomware. Cuanto antes se detecte la amenaza, más fácil será combatir el malware. La detección temprana de una infección con un ransomware puede ayudar a determinar qué tipo de ransomware ha infectado el dispositivo. Muchos de estos se eliminan a sí mismos una vez que se ha ejecutado el cifrado para que no se pueda examinar ni descifrar [4].

Para eliminarlo hay que tener en cuenta el tipo de ransomware al que se enfrenta, si es un ransomware de bloqueo, o uno de cifrado según esto se pueden tener tres opciones: Pagar el rescate y esperar a que los ciberdelincuentes cumplan su palabra y decifren los datos(lo menos recomendado), intentar eliminar el malware con las herramientas disponibles y la otra restaurar la configuración de fábrica del ordenador.

Para eliminar un ransomware de cifrado se deben de seguir estos pasos:

Primero, desactivar todas las conexiones, tanto virtuales como físicas. Esto implica desconectar los dispositivos inalámbricos y con cable, cualquier disco duro externo, soportes de almacenamiento y cuentas de nube. De este modo se puede evitar la propagación del ransomware dentro de la red [4].

Utilizar el software de seguridad en Internet que tenga instalado para realizar un análisis antivirus. Esto ayuda a identificar las amenazas. Si se encuentran archivos peligrosos, se pueden eliminar o ponerlos en cuarentena. Se puede eliminar los archivos maliciosos de forma manual o automática con el software antivirus. La eliminación manual del malware solo es una opción recomendable para los usuarios experimentados [4].

Si el equipo está infectado con un ransomware de cifrado, se necesita una herramienta adecuada para recuperar el acceso a sus datos [4].

Si hay una cuenta con una copia de seguridad de los datos en un disco externo o en un servicio de almacenamiento en la nube, se debe crear una copia de seguridad de los archivos que aún no haya cifrado el ransomware. Si no tiene ninguna copia de seguridad, limpiar y restaurar el equipo será mucho más difícil. Para evitar esta situación, es recomendable que se creen copias de seguridad periódicamente [4].

En el caso del ransomware que bloquea la pantalla, el primer problema de la víctima es conseguir llegar hasta el software de seguridad. Una posible solución es iniciar el equipo en modo seguro; en algunos casos, este modo impide que el bloqueador de pantalla se cargue y le da a la víctima la posibilidad de usar el antivirus y combatir el malware [4].

Actualidad

Actualmente los ataques con ransomware están dentro de las diez amenazas más peligrosas del Ciberespacio esto debido a que este se ha vuelto más específico y avanzado explotando vulnerabilidades específicas de un ente informático. A medida que el ransomware continúa evolucionando, también lo hacen las tácticas y técnicas empleadas por los ciberdelincuentes. Ha habido un aumento de la doble y triple extorsión, en la que los atacantes no solo cifran los datos, sino que también amenazan con filtrar información confidencial o lanzar más ataques, lo que aumenta la presión sobre las víctimas para que paguen el rescate. Además, han proliferado los modelos de ransomware como servicio (RaaS), lo que hace que estos ataques sean más accesibles incluso para los delincuentes con menos habilidades técnicas. Las bandas de ransomware más activas del momento son LockBit es la banda de ransomware más activa en lo que va de 2023, con 273 víctimas nombradas en sitios de filtraciones en el primer trimestre, seguida de Clop, y luego BlackCat, responsable de 102 listados en sitios de filtraciones. Clop nombró a 87 organizaciones en su sitio de fuga de datos en febrero de 99, basándose en su campaña de vulnerabilidad de día cero GoAnywhere MFT, que supuestamente vulneró a 2023 víctimas [5].

En enero de 2023, el FBI incautó los servidores de la banda de ransomware Hive después de una campaña de interrupción de meses. Al infiltrarse en la infraestructura del grupo en julio de 2022, el FBI accedió a las claves de descifrado, impidió el pago de un rescate de 130 millones de dólares y confiscó la web oscura y los servidores de sitios internos. Este importante evento pone de manifiesto los riesgos de que los grupos de ransomware permanezcan activos durante períodos prolongados. Hive surgió por primera vez en junio de 2021, cobrando más de 200 víctimas en su sitio de fuga de datos antes de ser cerrado [5].

En 2022, el coste medio de un ataque de ransomware fue de 4,54 millones de dólares, según el informe IBM Cost of a Data Breach Report. Además de los pagos de rescate, esta cifra también incluye los costes indirectos, como el tiempo de inactividad, la recuperación y la búsqueda y reparación de la vulnerabilidad. Dar un costo promedio preciso es un desafío porque no todas las empresas informan incidentes, las demandas de rescate varían y no todas las empresas pagan la demanda. Por ejemplo, la demanda más costosa jamás reportada fue el ataque a Kaseya, con una demanda de rescate de 70 millones de dólares, mientras que el pago medio de rescate en 2022 fue de 812.360 dólares [5].

Los principales ataques de ransomware de 2023

Según un informe de Cybering del tercer trimestre 2023, LockBit 3.0 ha mantenido su dominio, afirmando su posición como el principal grupo de ransomware con 252 nuevas víctimas, constituyendo 17.7% de todos los casos de ransomware. Asegurar el segundo lugar es Cl0p Ransomware, reclamando una sustancial de 177 víctimas [5].

Es de destacar que este recuento se acumuló en dos de los tres meses del trimestre, ya que no se anunciaron víctimas para septiembre. El grupo de ransomware

ALPHV consiguió la tercera posición con 120 víctimas en este trimestre, mostrando su presencia duradera en el panorama del ransomware [5].

Las entregas en el extranjero del servicio postal británico Royal Mail se vieron gravemente interrumpidas el 10 de enero de 2023 por un ataque de ransomware de LockBit, con sede en Rusia. El ciberataque afectó a los sistemas utilizados para el despacho de entregas internacionales. El incidente es particularmente significativo ya que Royal Mail se considera una infraestructura nacional crítica para la economía del Reino Unido[5].

Antes de que se resolviera el problema, Royal Mail aconsejó a los clientes que no enviaran cartas y paquetes internacionales, ya que desde entonces han continuado con sus operaciones regulares. Las entregas nacionales no se vieron afectadas. La Agencia Nacional contra el Crimen y el Centro Nacional de Seguridad Cibernética están investigando el incidente [5].

El 18 de enero de 2023, Yum! Brands, el operador de KFC, Pizza Hut, Taco Bell y The Habit Burger Grill, fue blanco de un ataque de ransomware que obligó a 300 ubicaciones en el Reino Unido a cerrar por un día. La empresa inició protocolos de respuesta e involucró a profesionales de la ciberseguridad y a las fuerzas del orden. ¡Ñam! Brands confirmó que los datos fueron robados, pero no encontró evidencia de que las bases de datos de los clientes estuvieran comprometidas. La compañía presentó un formulario 8-K ante la SEC, afirmando que no espera que el ataque afecte negativamente a su negocio, operaciones o resultados financieros [5].

El distrito escolar más grande del sur de Arizona, el Distrito Escolar Unificado de Tucson, fue víctima de un ataque de ransomware a fines de enero. El ataque interrumpió los servicios de Internet y de red, lo que obligó a las escuelas a operar fuera de línea. El personal encontró cartas impresas que revelaban que Royal estaba detrás del ataque, que encriptó y copió los datos del distrito. Si bien la suma del rescate no se ha revelado, los informes sugieren que Royal propuso un "acuerdo especial" para descifrar, restaurar y mantener la confidencialidad de los datos del distrito [5].

A principios de febrero, ION, un proveedor de servicios de comercio financiero, experimentó un ataque de ransomware que afectó a sus clientes, incluidos los principales bancos, corredurías y fondos de cobertura. LockBit asumió la responsabilidad del ataque y recibió un pago de rescate no revelado. Ni ION ni LockBit revelaron el nombre del rico benefactor que pagó el rescate [5].

Tras un ataque de ransomware a principios de febrero, Tallahassee Memorial HealthCare en Florida estuvo fuera de línea durante casi una semana. El resultado fueron limitaciones en las cirugías y procedimientos realizados, y algunos pacientes de emergencia fueron redirigidos a otros hospitales. El hospital recurrió a registros en papel y notas manuscritas de los pacientes durante el ataque. Los detalles sobre el incidente siguen siendo escasos debido a preocupaciones de seguridad, privacidad y aplicación de la ley [5].

En febrero, la Corte Suprema de Florida fue una de las más de 3.800 víctimas de un ataque global de ransomware de rápida propagación dirigido a varias universidades de Estados Unidos y Europa Central. La campaña de extorsión digital había afectado a miles de servidores en Europa y se consideraba una importante amenaza en línea [5].

La red principal de la Corte Suprema de Florida no se vio afectada, ya que la infraestructura afectada fue segregada y utilizada para administrar otros elementos del sistema judicial estatal. Según los informes, los ciberdelincuentes extorsionaron solo $ 88,000 en esta campaña; Una cantidad relativamente modesta en comparación con los rescates multimillonarios que suelen exigir algunos grupos de hackers [5].

El minorista de alimentos B&G Foods, conocido por más de 50 marcas como Crisco, Cream of Wheat, Green Giant y Ortega, fue víctima de un ciberataque por parte de Daixin Team el 4 de febrero. El colectivo de ransomware supuestamente encriptó aproximadamente 1,000 hosts y liberó archivos extraídos en su sitio. Los archivos contenían documentos internos de la empresa, pero excluían datos confidenciales relativos a la organización, los empleados o los subcontratistas. B&G Foods se abstuvo de comprometerse con Daixin Team, y no se han revelado detalles sobre el rescate exigido [5].

Dole Food Company, uno de los principales productores y distribuidores mundiales de frutas y verduras frescas, sufrió un ataque de ransomware que afectó a sus operaciones. Si bien la compañía todavía está investigando el alcance del incidente y ha descrito el impacto como limitado, ha contratado a expertos externos para ayudar a remediar y proteger los sistemas afectados. El Servicio de Alguaciles de EE. UU. (USMS, por sus siglas en inglés) investigó un ataque de ransomware que afectó a uno de sus sistemas independientes que contenía datos confidenciales de las fuerzas del orden, incluida la información personal de sujetos investigados y empleados seleccionados. Detectado el 17 de febrero, el sistema comprometido ha sido desconectado de la red USMS para su investigación. La base de datos del Sistema de Información de Archivos de Seguridad de Testigos del USMS permaneció intacta. Este incidente sigue a una violación de 2020 que expuso datos de más de 387,000 reclusos pasados y presentes [5].

La banda de ransomware LockBit afirma haber violado Maximum Industries, un proveedor de SpaceX, y robado 3.000 esquemas patentados. Los ciberdelincuentes amenazaron con filtrar o vender los planos a partir del 20 de marzo de 2023 si no se cumplían sus demandas de rescate. La utilidad de los esquemas robados puede ser limitada, ya que la fabricación y el uso de las piezas sin levantar sospechas sería un desafío [5].

Protección

Para protegerse de este software malintencionado se deben de llevar a cabo diferentes acciones:

No usar servicios de escritorio remoto (como RDP) en redes públicas a no ser que sea estrictamente necesario. Utilizar siempre contraseñas fuertes [5].

Instalar tan pronto como sea posible los parches disponibles para soluciones VPN comerciales que dan

acceso en remoto a los empleados y actúan como puertas de enlace a la red [5].

Centrar la estrategia defensiva en detectar movimientos laterales y la filtración de datos en internet. Prestar especial atención al tráfico saliente para detectar conexiones de ciberdelincuentes [5].

Realizar copias de seguridad con regularidad, así como disponer de un acceso rápido a las mismas en caso de emergencia [5].

Utilizar soluciones como Kaspersky Endpoint Detection and Response Expert y Kaspersky Managed Detection and Response. Son servicios que ayudan a identificar y detener los ataques en fase temprana, antes de que los atacantes logren su objetivo [5].

Usar la última información de inteligencia frente a amenazas para estar al tanto de las Tácticas, Técnicas y Procedimientos (TTP) utilizados. Kaspersky Threat Intelligence ofrece un único punto de acceso TI y proporciona información y datos de ataques cibernéticos recopilados por el equipo de Kaspersky durante 25 años. Para ayudar a las empresas a tener una defensa efectiva, Kaspersky otorga acceso a información continuamente actualizada y a escala mundial sobre ciberataques y amenazas en vigor, sin cargos adicionales [5].Ç

III. CONCLUSIONES

Se pudo llegar a la conclusión que hoy en día el ciberespacio está plagado de amenazas, siendo el ataque por ransomware una de las más dañinas debido al riesgo que implica perder la información y que esta esté en las manos equivocadas. Para mitigar estas es necesario mantener un adecuado uso de las diferentes herramientas de prevención de malware, o sea mantener actualizado los anti malware que son los encargados de proporcionar la defensa adecuada del dispositivo. Además se debe de tener mucho cuidado con los correos de fuentes no confiables debido a que podrían estar infectados con este tipo de amenaza al igual que hay que evitar descargar contenido de páginas web cuyo proveedor no sea conocido.

IV. REFERENCIAS

[1] Kaspersky. “Kaspersky.” [En línea] 14 de octubre de 2020. [Citado el: 11 de octubre de 2023.] https://latam.kaspersky.com/about/press-releases/2020_kaspersky-america-latina-registra-5-mil-ataques-de-ransomware-por-dia.

[2] Rus, Cristian. “XATAKA.” [En línea] 5 de junio de 2021. [Citado el: 10 de octubre de 2023.] https://www.xataka.com/historia-tecnologica/curiosa-historia-primer-ransomware-mundo-su-inventor-victima-que-consiguio-eludirlo.

[3] Kaspersky. “Kaspersky.” [En línea] 2020. [Citado el: 6 de octubre de 2023.] https://latam.kaspersky.com/resource-center/threats/ransomware-attacks-and-types.

[4] Kaspersky. “Kaspersky.” [En línea] 2020. [Citado el: 6 de octubre de 2023.] https://www.kaspersky.es/resource-center/preemptive-safety/ransomware-removal.

[5] Dyer, James. “egress.” [En línea] 20 de mayo de 2022. [Citado el: 7 de octubre de 2023.] https://www.egress.com/blog/phishing/top-ransomware-attacks-statistics.

[6] Kaspersky. “Kaspersky.” [En línea] 5 de enero de 2023. [Citado el: 25 de octubre de 2023.] https://www.kaspersky.es/about/press-releases/2023_se-duplica-el-ransomware-dirigido-en-2022-surgen-nuevas-tecnicas-y-grupos.

[7] Dimitrova, Milena. “sensors tech forum.” [En línea] 24 de octubre de 2023. [Citado el: 25 de octubre de 2023.] https://sensorstechforum.com/es/ransomware-statistics/.

[8] Aver, Hugh. “Kaspersky.” [En línea] 1 de julio de 2022. [Citado el: 26 de octubre de 2023.] https://www.kaspersky.es/blog/ransomware-ttp-report/27326/.

[9] Lella, Ifigeneia, Theocharidou, Marianthi, Tsekmezoglou, Eleni, Malatras, Apostolos. “INFORME «PANORAMA DE AMENAZAS» DE ENISA DE 2021.” Agencia de la Unión Europea, 2021.

[10] Osorio-Sierra, A., Mateus-Hernández, M. J., Vargas-Montoya, H. F. “Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware,” Rev. UIS Ing., vol. 19, no. Osorio-Sierra, Andrés Felipe. Medellín: s.n., 2020.

[11] INCIBE. “INCIBE.” [En línea] 16 de abril de 2020. [Citado el: 26 de octubre de 2023.] https://www.incibe.es/empresas/blog/el-ransomware-y-recupero-mi-informacion.