CÓMO SABER SI LO **ESPÍAN** POR SU CÁMARA WEB | UN VISTAZO AL RELOJ MÁS **ECONÓMICO** DE APPLE | ROBOTS POLICÍAS QUE PUEDEN **MATAR**

ENTER.CO

Por qué se está perdiendo la guerra contra el ransomware

Edición 279

DICIEMBRE 2022

ISSN 2215-9134

Por Javier Méndez
Twitter: @javiermendezz

Ransomware: una guerra que se está perdiendo

Imagen: Freepik

Colombia está en la mira de los ciberdelincuentes, que han atacado con ransomware varias entidades y empresas privadas en el último año. Keralty, la dueña de Sanitas y Colsanitas, es la víctima más reciente. Pero el fenómeno es global, y es un delito muy difícil de combatir. Le explicamos por qué.

A finales de noviembre, las redes de la empresa Keralty sufrieron un ciberataque del que todavía no se han recuperado por completo. Esa compañía, cuyas subsidiarias Sanitas y Colsanitas ofrecen servicios de salud para cerca de 5,4 millones de personas en Colombia, fue atacada con ransomware, un tipo de malware que encripta la información de una organización hasta que se paga un rescate en criptomonedas.

Las operaciones de esa empresa sufrieron grandes traumatismos. Procesos como pedir una cita médica, pagar la mensualidad del servicio prepago o comprar vales, que habitualmente se realizan en línea, dejaron de estar disponibles en los sitios web de la EPS y de Colsanitas, que desde hace varias semanas muestran una

página en donde se avisa que siguen en un plan de contingencia. Los servicios de salud, sin embargo, se están prestando sin inconvenientes.

Keralty no ha dicho qué tipo de incidente sufrió, pero el portal de seguridad Bleeping Computer reveló que se trata de ransomware. Según el mismo sitio, el ataque fue realizado por una organización delincuencial llamada RansomHouse, que utiliza el ransomware White Rabbit, una variante que apareció a finales del año pasado.

El de Keralty es solo el último de varios ciberataques que se han producido en Colombia contra grandes entidades privadas y estatales. Meses atrás, el Invima, el Dane y el Ejército de Colombia también fueron atacados.

Lo que se está viviendo en Colombia muestra que los ciberdelincuentes se están enfocando en ataques dirigidos contra entidades y empresas del país. Pero este es un fenómeno que se está presentando a nivel mundial. Las alertas que diversas empresas de seguridad informática han venido lanzando desde hace años se volvieron realidad: el ransomware se ha convertido en la principal ciberamenaza hoy en día.

Ese delito se desbordó en los últimos tres años, cuando las empresas y entidades estatales se volcaron hacia Internet por cuenta de la pandemia del covid-19. Ese virus obligó a las organizaciones a acelerar su transformación digital. Pero eso también las volvió más vulnerables a los ciberdelincuentes (ver artículo 'Las principales modalidades de ataque').

Las acciones de los criminales se han vuelto cada vez más irresponsables. Por ejemplo, varias clínicas fueron atacadas con ransomware en varios países durante los peores momentos de la pandemia del covid-19. Y este mes, mientras Keralty trataba de restablecer sus redes, fue atacado un hospital en las afueras de París, el André-Mignot, lo que lo obligó a suspender parcialmente sus operaciones y a trasladar a otras clínicas a pacientes de sus unidades neonatal y de cuidados intensivos.

Entre el 2021 y el 2022, en Estados Unidos se han producido acciones que han afectado a muchas personas, debido a que se enfocaron en la infraestructura crítica de ese país.

Una de ellas fue la que realizó una banda rusa contra Colonial Pipeline, uno de los principales oleoductos estadounidenses, que tuvo que detener sus operaciones durante varios días a mediados del año pasado; esto hizo que se agotara el combustible en varias zonas del país porque la gente se volcó a tanquear sus vehículos ante el temor de que se produjera un desabastecimiento.

Poco después, la banda rusa REvil atacó a la empresa Sol Oriens, un contratista especializado en armas nucleares en Estados Unidos. Para los delincuentes, no hay límites a la hora de escoger a sus víctimas.

Ataques dirigidos

Un informe de la firma de soluciones de seguridad Eset, titulado 'Ransomware: a Look at the Criminal Art of Malicious Code, Pressure and Manipulation', menciona varias tendencias que han transformado ese delito en los últimos años, y que han aumentado su impacto negativo (ese informe está disponible aquí: bit.ly/3YvfQoI).

La primera tendencia es que, en vez de atacar grandes números de personas de forma aleatoria, para pedir sumas de rescate modestas, los delincuentes

Imagen: Michael Geiger / Unsplash

Imagen: TheDigitalArtist / Pixabay

ahora se están concentrando en ataques dirigidos hacia entidades y empresas a las que les pueden pedir sumas más grandes de dinero. Eso es lo que se está viendo en Colombia.

La segunda tendencia es algo que Eset llama 'doble extorsión', y que se inició en el 2019: ahora no solo se encriptan los datos de las organizaciones, sino que adicionalmente se sustrae información valiosa y se amenaza con hacerla pública o con venderla a otros grupos criminales. Así, piden un rescate para desencriptar los datos, y una segunda suma para no publicar la información robada.

Incluso, hay grupos que agregan un tercer factor de extorsión: si la organización víctima se niega a pagar, los delincuentes les informan a sus socios y clientes que se ha accedido a sus datos confidenciales y les piden dinero para no divulgar esa información, o les sugieren que presionen a la organización que fue atacada.

Otra tendencia en este negocio macabro es el Ransomware as a Service (RaaS). Un artículo de la firma de seguridad informática Kaspersky explica que el Raas es un modelo en el que los desarrolladores del malware le 'arriendan' el ransomware y su infraestructura de control a otros criminales.

Según Kaspersky, entre las herramientas que se ofrecen como parte de este servicio están el ransomware compilado o su código fuente, las herramientas para personalizar el ransomware (por ejemplo, para apuntarle al sistema operativo de la víctima o para escribir la nota de extorsión), la infraestructura para controlar el ransomware, el soporte técnico y las instrucciones. Incluso, dice esa firma, "desde finales del 2019, muchos desarrolladores de ransomware también han incluido el robo de datos como parte del servicio para amenazar a las víctimas con su publicación si no se paga el rescate".

Por qué es tan difícil combatir el ransomware

El ransomware se está tornando cada vez más difundido y destructivo, y no hay indicios de que eso vaya a cambiar a corto o mediano plazo. Por ahora, es una guerra que se está perdiendo. ¿Pero por qué es tan difícil combatirlo? Hay varias razones. Quizás el principal problema es que es muy difícil capturar a los delincuentes.

Un análisis del diario The New York Times dice sobre ese tema: "Rusia es, según los expertos, el país en donde se originan la mayoría de los ataques. Otros tres países, China, Irán y Corea del Norte, también son jugadores serios, y lo que tienen en común es que todos son

autocracias cuyos aparatos de seguridad sin duda saben quiénes son los hackers y podrían acabar con ellos. Entonces, la presunción es que los criminales están protegidos, ya sea a través de sobornos, o haciendo trabajos gratuitos para el gobierno, o ambos".

El mismo diario explica que esas bandas se cuidan mucho de no atacar a los países que las alojan. Por ejemplo, un estudio realizado por la firma de seguridad Trustwave SpiderLabs reveló que el código del ransomware usado por la banda rusa REvil tiene instrucciones que evitan que el malware ataque computadores cuyo lenguaje predeterminado es el ruso, lo mismo que otros idiomas de las antiguas repúblicas soviéticas.

Entonces, el problema no es identificar a los autores de los delitos, ya que las agencias de seguridad occidentales saben quiénes son, sino que ellos están alojados en países con dictaduras que no tienen tratados de extradición con países occidentales, y que no van a colaborar con sus gobiernos.

Algunos delincuentes sí han sido capturados, pero lo que ha hecho el gobierno estadounidense es esperar a que los criminales viajen a países amigos para atraparlos allá. Esa fue la suerte que corrieron los hackers rusos Aleksei Burkov, capturado en Israel en el 2019, y Yevgeniy Nikulin, capturado en la República Checa en el 2018. Los dos fueron extraditados a Estados Unidos y el año pasado recibieron penas de prisión de 9 y 7 años, respectivamente. Es un triunfo de las autoridades, pero uno que llega tarde: esas condenas se produjeron cinco años después de que los delitos habían sido cometidos.

El problema del ransomware tiene tan preocupados a los estadounidenses que el presidente Joe Biden incluyó el tema en la agenda de una reunión que tuvo con Vladimir Putin a mediados del 2021. Biden le pidió al presidente ruso que desarticulara las bandas que operan desde su país. No sucedió nada.

De hecho, apenas dos semanas después de los diálogos, se produjo uno de los ataques más devastadores del 2021, cuando la banda rusa REvil introdujo un ransomware en la red del proveedor estadounidense de servicios de administración

Imagen: Freepik

remota Kaseya, y así terminó afectando a 1.500 clientes de esa compañía. Ahora que Rusia se ha convertido en un paria mundial por cuenta de la invasión a Ucrania, la posibilidad de que ese delito se combata en ese país se aleja todavía más.

Las criptomonedas son otro factor que ha contribuido al auge de ese delito. Como los rescates se pagan con criptomonedas como el bitcoin, ahora es más difícil rastrear y recuperar el dinero que se paga. Por eso, algunos expertos opinan que los gobiernos deberían crear leyes que permitan tener más control sobre el mercado de las criptomonedas, y además deberían exigir que las empresas que han sido atacadas informen a las autoridades, en vez de pagar, como muchas están haciendo.


Imagen: Worldspectrum / Pexels

¿Por qué muchas compañías pagan?

Otro factor que está contribuyendo a fortalecer ese delito es que la mayoría de las empresas están pagando las extorsiones, pese a que es la primera recomendación que se hace: no pagar, ya que hacerlo es lo que motiva a los delincuentes a seguir con sus acciones. Además, nada garantiza que los criminales les devuelvan el acceso a sus datos a las víctimas.

Pero se ha pagado incluso en casos que han tenido gran notoriedad en los medios. Por ejemplo, el presidente de Colonial Pipeline, el oleoducto que mencionamos antes, reveló en una declaración ante el Congreso de Estados Unidos que les pagó 5 millones de dólares a unos delincuentes rusos para poder restablecer sus operaciones; el pago se realizó un día después del ataque.

Por los mismos días, JBS, la mayor procesadora de carne del mundo, le pagó 11 millones de dólares en bitcoins a la banda rusa REvil. Y esa cifra palidece frente a la que pagó el año pasado CNA Financial Corp., una de las principales aseguradoras estadounidenses: le entregó 40 millones de dólares a los delincuentes, según Bloomberg.

Esto ha llevado a que el delito florezca, pero también les ha dado alas a los criminales para pedir rescates más altos. REvil pidió 70 millones de dólares el año pasado tras el ataque a Kaseya, un incidente que impactó compañías en todo el mundo.

Un informe publicado este año por CyberEdge (cyber-edge.com/cdr), con base en entrevistas con directores de tecnología de 17 países, reveló que 63 por ciento de las empresas que habían sido víctimas de ransomware en el 2021 terminaron pagándole a los delincuentes.

Esas organizaciones decidieron pagar principalmente por tres razones. Primero, influyó la amenaza de los delincuentes de filtrar datos confidenciales de la compañía; les preocupaba, por ejemplo, ver expuesta su propiedad intelectual o datos sensibles que pusieran en una situación embarazosa a la organización.

Segundo, costaba menos pagarles a los delincuentes que

iniciar el proceso de recuperación de los datos; tener las operaciones de la empresa detenidas puede ser muy costoso, y a veces expone a una compañía a otros daños, como demandas de sus clientes.

Tercero, las empresas tenían confianza en que los delincuentes les iban a devolver el acceso a sus datos. Sin embargo, el mismo informe dice que solo 72 por ciento de esas organizaciones que pagaron pudieron recuperar sus datos con éxito.

De hecho, la imposibilidad de saber si los datos se van a recuperar después de pagar es una de las pesadillas que enfrentan las víctimas de este delito. Y muchas nunca recuperan su información.

Eset menciona algunas de las razones por las cuales una empresa podría no recuperar su información aunque haya pagado el rescate: algunos datos se pueden dañar durante el proceso de encriptación y eso los hará irrecuperables; el delincuente nunca entrega las llaves de descifrado; o la empresa inicialmente 'limpió' el malware con un software de seguridad.

Sobre este último punto, Eset explica que las compañías que han sido atacadas deben tener en cuenta que si eliminan el ransomware con un software de seguridad, después no servirá que paguen el rescate: "Eliminar el ransomware activo con un software de seguridad no equivale a recuperar los datos. Y eliminar el ransomware y luego decidir pagar significa que los datos podrían no ser recuperables, incluso con la cooperación de los delincuentes, porque el mecanismo de descifrado a menudo es parte del malware. En otras palabras, si decide pagar, proceda con cautela", dice Eset.


Imagen: Freepik

A los que pagan los atacan de nuevo

Hay un problema adicional: la mayoría de las empresas que están pagando son atacadas de nuevo.

La firma de seguridad informática Cybereason publicó este año el informe 'Ransomware: The True Cost to Business', en el cual reveló que 80 por ciento de las organizaciones que les pagaron a los delincuentes sufrieron un segundo ataque de ransomware, el cual en la mayoría de los casos se produjo menos de un mes después del primero. Pese a ello, el 40 por ciento de las empresas consultadas pagó ese segundo rescate, y varias compañías fueron atacadas una tercera y una cuarta vez. Y cada nueva extorsión exigió una suma de dinero más alta.

De otro lado, el 60 por ciento de las compañías le dijeron a Cybereason que los delincuentes habían penetrado en sus redes entre uno y seis meses antes de que se descubriera la intrusión, lo cual les dio tiempo de sobra para robar información valiosa y tomar el control de la red.

Sam Curry, líder de tecnología de Cybereason, le explicó a la publicación SecurityWeek que estas extorsiones continuas tienen que ver con la forma como funciona el Ransomware como Servicio (RaaS). "Por el nombre que les damos a esos grupos, es tentador pensar que son bandas itinerantes. Pero eso es engañoso. 'Carteles de ransomware' sería un mejor nombre para ellos que 'bandas de ransomware'.

Imagen: Freepik

Hay una red de afiliados que recolecta víctimas de manera automatizada y las vende a los equipos de ransomware que realizan el trabajo sucio de penetración en la red, detonación y extorsión".

Curry cree que "los afiliados en muchos casos le venden 'la víctima' a otra pandilla o cartel. O simplemente el mismo cartel vuelve por más dinero. ¿Por qué no hacerlo si la víctima no cambia sus prácticas de seguridad? El crimen organizado no le da la espalda al dinero y, como en el mundo real, a veces eso termina convirtiéndose en un modelo de extorsión a cambio de 'protección' con un pago continuo".

Los backups también pueden estar infectados

Otras razones por las cuales las empresas pagan, según Eset, es que a veces no tienen backups o no los pueden restablecer. Y esto último podría pasar porque la copia de seguridad también está infectada con el ransomware.

Eset dice que se debe tener en cuenta que algunos ataques de ransomware se ejecutan durante un período prolongado de tiempo (a veces los criminales penetran en una red varios meses antes de dar la cara), y "por eso puede pasar que el ransomware también vaya incluido en una copia de seguridad, lo que compromete el potencial para una recuperación sin problemas. Por eso, el backup no es una defensa de 'configurar y olvidar'; debe ser monitoreado y administrado, y el proceso de recuperación necesita ser probado regularmente".

Es tan grande la impotencia que están sintiendo las empresas que algunas han optado por protegerse con seguros. Una de las firmas que ofrece esos ciberseguros es AIG, una de las mayores aseguradoras del mundo. Un artículo de CNN sobre los seguros de AIG dice: "Dependiendo del tamaño de la empresa y lo que deba cubrirse (equipos de seguridad, abogados, posibles demandas, reembolsos por pérdidas comerciales o incluso pagos de rescate), los planes pueden costar desde un par de cientos de dólares hasta varios millones".

Por todo lo que hemos mencionado se puede ver lo complicado que es combatir el ransomware y lidiar con sus consecuencias cuando una compañía ya ha sido atacada. El ransomware seguirá siendo pan de cada día, y esto hace que sea muy importante tener presentes las recomendaciones de prevención que constantemente dan las compañías especializadas en seguridad informática (ver artículo 'Consejos para protegerse').

Principales modalidades de ataque

El informe 'Ransomware: a Look at the Criminal Art of Malicious Code, Pressure and Manipulation', de la compañía de soluciones de seguridad Eset, concluye que, en la medida en que muchos empleados empezaron a trabajar desde sus casas por cuenta de la pandemia, los accesos remotos RDP se convirtieron en una de las principales puertas de entrada de los ataques de ransomware (el PDF de ese informe de Eset se puede descargar de esta dirección: bit.ly/3YvfQoI).

Eset explica que con la llegada de la pandemia, muchos empleados empezaron a acceder a los sistemas internos de las compañías a través del Remote Desktop Protocol (RDP). Un endpoint RDP es un dispositivo Windows de una empresa que ejecuta el software de RDP para que se pueda acceder a él a través de Internet. Así, el usuario puede entrar desde su casa a esos dispositivos, tal como si estuviera sentado en su oficina. Para acceder necesita introducir una contraseña e, idealmente, la empresa debería tener un doble sistema de autenticación. El problema, dice Eset, es que hay muchos dispositivos RDP que están mal configurados.

"Para los delincuentes es sencillo encontrar sistemas accesibles desde el exterior y luego abusar de ellos. Los sistemas que ejecutan RDP pueden identificarse mediante motores de búsqueda especializados como Shodan, que buscan constantemente en Internet dispositivos conectados y recopilan información sobre ellos. Para un atacante, todas esas máquinas son blancos potenciales para ser explorados", dice Eset, que agrega que las bandas con buenos recursos también pueden pagar en la Dark Web para comprar el acceso a sistemas RDP comprometidos.

Según Eset, muchos sistemas RDP tienen configuraciones débiles, y es fácil para los atacantes afianzarse en ellos. "Además, las herramientas y técnicas para escalar privilegios y obtener derechos de administrador en sistemas RDP comprometidos son ampliamente conocidas y están disponibles".

Si un sistema RDP solo requiere un nombre de usuario y una contraseña para acceder a él remotamente, el atacante puede usar técnicas de fuerza bruta para tratar de obtener las credenciales (son intentos repetidos de adivinar una contraseña, que se hacen a gran velocidad mediante programas automatizados). Si el equipo RDP no está configurado para limitar el número de intentos, ese ataque puede funcionar.

"Obtener acceso no autorizado desde Internet a dispositivos que ejecutan RDP puede requerir un mayor esfuerzo inicial que el ransomware basado en correo electrónico, pero el vector RDP ofrece a los delincuentes beneficios significativos, como poder usar de forma indebida ese acceso legítimo y el potencial de evadir las protecciones de endpoints" (en contraste, dice Eset, cualquier organización con un programa maduro de seguridad detectará y bloqueará un ransomware incrustado en un archivo adjunto en un correo electrónico entrante)".

Otra ventaja de los ataques vía RDP es que le ofrecen al


Imagen: Freepik


Imagen: Freepik

delincuente la capacidad de comprometer rápidamente múltiples sistemas, o incluso toda una red.

"Una vez tiene acceso al sistema RDP comprometido, el atacante puede hacer mucho más que encriptar archivos en la máquina y pedir dinero, especialmente si ese equipo puede servir como un punto de acceso a toda una red de dispositivos para encriptar, o puede servir para robar datos de misión crítica. Al obtener acceso remoto, el atacante querrá obtener más información sobre la máquina comprometida, evaluando su potencial de abuso, incluido el mapeo de conexiones a otros sistemas. Y si el acceso no fue obtenido con las credenciales de administrador, se pueden usar varias técnicas para escalar los privilegios al nivel de administrador", dice Eset.

Otros tipos de ataques

Aunque los dispositivos RDP son uno de los principales blancos hoy en día, especialmente entre las bandas más sofisticadas, Eset aclara que las técnicas antiguas no se han dejado atrás.

Muchos criminales todavía usan archivos anexos en el correo electrónico –que los usuarios abren de forma desprevenida– para introducir el malware que sirve como primer escalón en un ataque.

De otro lado, también son cada día más comunes los ataques a través de la cadena de suministro de software. Eset explica que antes, cuando la gente instalaba el software mediante discos, el malware a veces se introducía en discos de producción o en los discos de prueba que solían distribuirse con revistas de tecnología. Ahora que el software de usa en la nube, los delincuentes se han concentrado en esos proveedores de aplicaciones.

Un ataque realizado hace varios años, por ejemplo, llegó a través de un software de contabilidad legítimo. "Los atacantes penetraron en los servidores de actualización de la compañía de software y agregaron su propio código a los archivos de actualización legítimos. Cuando los usuarios del software de contabilidad hicieron clic para instalar actualizaciones del programa, también estaban instalando una puerta trasera de malware" dice Eset.

Algo similar pasó el año pasado con Kaseya: el ransomware terminó en las redes de miles de empresas luego de que los atacantes plantaron malware en los servidores de esa empresa, que ofrece un software de administración remota de dispositivos tecnológicos.

Otra forma en que los delincuentes entran en las redes de las organizaciones es explotando vulnerabilidades en los sistemas operativos y las aplicaciones. Y ni siquiera tienen que ser vulnerabilidades recién descubiertas, que el fabricante del software no conoce (conocidas como zero-day o de día cero), sino que en muchos casos aprovechan vulnerabilidades ampliamente conocidas, para las que ya había parches, pero que muchas compañías no han instalado.

Consejos para protegerse

En Internet hay muchas guías con recomendaciones para prevenir ataques con ransomware. Algunos de los consejos más comunes son los siguientes:

- Copias de seguridad. Realice copias de seguridad de sus sistemas con frecuencia, y verifique con regularidad que esos backups funcionan bien. Ante una infección con ransomware, es clave contar con las copias de seguridad para poder restaurar los datos que los delincuentes han encriptado.

- Guárdelos aparte. Los backups se deben almacenar en un dispositivo separado, al que no se pueda acceder a través de la red de computadores (por ejemplo, en un disco externo), ya que el ransomware también ataca las copias de seguridad.

- Software al día. Los computadores deben mantener actualizados y con parches el sistema operativo y las aplicaciones. Las vulnerabilidades no corregidas en el software son uno de los principales blancos de los delincuentes.

- Capacite a sus empleados. En una encuesta realizada por CyberEdge con directores de tecnología de 17 países, muchas organizaciones que sufrieron ataques de ransomware dijeron que la falta de personal técnico bien capacitado influyó en que fueran víctimas de esos ataques, lo mismo que la falta de concientización de los empleados en la importancia de los temas de seguridad. Por eso, es clave que las empresas tengan sesiones de entrenamiento para sus empleados de forma regular y obligatoria en temas de seguridad informática.

- Use software de protección. Todos los dispositivos deben estar protegidos con software de seguridad. Y en las empresas los antivirus no son suficientes. Para contrarrestar las vulnerabilidades de día cero, los botnets y los ataques vía RDP, se requiere software más avanzado; por ejemplo, soluciones de protección de punto final de múltiples capas, capaces de detectar y bloquear amenazas entrantes en el correo electrónico, los enlaces, en accesos RDP y otros protocolos de red.

- Cautela con los attachments. Una de las formas como se inician los ataques con ransomware es a través de software maligno que llega en archivos anexos en el correo electrónico. Ese malware puede provenir incluso de remitentes conocidos, así que uno debe ser cauto y no abrir attachments sospechosos.

- Proteja los accesos RDP. Los accesos vía RDP se convirtieron en uno de los principales vectores de ataque, en la medida en que más personas empezaron a trabajar de forma remota (ver nota 'Las principales modalidades de ataque'). Por eso, se deben configurar bien los dispositivos RDP, usar autenticación de dos pasos para el acceso y limitar el número de intentos de la contraseña (para evitar ataques de fuerza bruta).

- El inventario es clave. Eset recuerda que no se puede defender un sistema si no se es consciente de su existencia. Por eso, para defenderse de ataques vía RDP, es muy importante hacer un inventario de los activos de una organización en Internet. Muchas entidades son atacadas a través de un activo conectado a Internet que el departamento de TI no sabía que existía (por ejemplo, el portátil personal de algún empleado).

Fuentes: Eset, CyberEdge, Cisa.gov y Kaspersky.

Imagen: Freepik