



RANSOMWARE:

Una mirada al arte criminal detrás del código malicioso, la presión y la manipulación

CONTENIDO

OBJETIVOS.	2
RANSOMWARE: LA PEOR AMENAZA CIBERNÉTICA	2
EL RANSOMWARE ES UN GRAN NEGOCIO	3
CÓMO LO LOGRA EL RANSOMWARE PSICOLÓGICAMENTE	3
CÓMO LO LOGRA EL RANSOMWARE TÉCNICAMENTE	4
ATAQUES DE RANSOMWARE VÍA RDP	5
Movimiento lateral y estrategia de “vivir de la tierra”	8
Cómo defenderse contra ataques de ransomware mediante RDP	9
Apartado breve: Protocolo SMB, en segundo lugar tras el RDP	11
Cómo proteger el RDP del ransomware	11
ATAQUES DE RANSOMWARE POR CORREO ELECTRÓNICO	13
ATAQUES DE RANSOMWARE POR CADENA DE SUMINISTRO	15
ATAQUES DE RANSOMWARE MEDIANTE LA EXPLOTACIÓN DE VULNERABILIDADES	16
NUBES Y SEGMENTOS	17
LOS PARCHES Y EL BACKUP COMO DEFENSAS CONTRA EL RANSOMWARE	18
CÓMO RESPONDER A UN ATAQUE DE RANSOMWARE	19
DETECCIÓN Y RESPUESTA PARA ENDPOINTS	20
DOS PALABRAS SOBRE EL PAGO DEL RESCATE	21
EL FUTURO DEL RANSOMWARE	22
CONCLUSIÓN	23

V 2.0

Author: Ondrej Kubovič

Agradecimientos: Esta actualización se basa en la contribución fundamental realizada por Stephen Cobb en 2018 y los esfuerzos actuales (2021) aportados por mis colegas de ESET: Rene Holt, James Shepperd, Nick FitzGerald, Hana Matušková y Klára Kobáková.

Author original: Stephen Cobb

Agradecimientos: Agradecimientos: Este white paper le debe mucho al trabajo de mis colegas de ESET James Rodewald, Ben Reed y Fer O’Neil, y a mi talentoso equipo: Aryeh Goretsky, Bruce P. Burrell y Cameron Camp.

Agosto de 2021

OBJETIVOS

Los objetivos de este documento son demostrar lo peligroso que se ha vuelto el ransomware, describir las últimas técnicas utilizadas por las bandas de ransomware, y sugerir qué puede hacer su organización para reducir la exposición a estos ataques y minimizar el daño que ocasionan. Se analizan tres vectores de ataque de ransomware en el siguiente orden: acceso remoto, correo electrónico y cadena de suministro.

RANSOMWARE: LA PEOR AMENAZA CIBERNÉTICA

Un ataque de ransomware se puede definir como un intento de extorsionar a una organización impidiéndole el acceso a sus datos. El ransomware es un tipo de malware (un término que abarca todas las formas de código malicioso, incluyendo los virus y gusanos informáticos).

El ransomware es probablemente una de las amenazas cibernéticas más graves a las que se enfrentan las organizaciones. ¿Por qué? Porque en los últimos años, las bandas criminales que crean este tipo de malware y lo ofrecen como servicio han estado perfeccionando un enfoque diferente con objetivos más específicos, y las métricas de estos ataques son mucho más difíciles de obtener.

Además, los ciberdelincuentes están constantemente ideando nuevos métodos para asegurarse el pago del rescate, por lo general aumentando la presión sobre la víctima. En 2019, comenzaron a usar la doble extorsión, que combina el cifrado de datos "habitual" con la extracción de datos para su divulgación. De esta manera, no solo le impiden a la víctima el acceso a sus archivos valiosos, críticos o confidenciales, sino que también amenazan con exponerlos públicamente o venderlos a otros actores maliciosos.

Para aumentar aún más sus probabilidades de éxito, algunos operadores de ransomware han adoptado la modalidad de la triple extorsión, en la cual añaden el paso adicional de contactar a partners comerciales o clientes de víctimas que no han pagado el rescate. Los ciberdelincuentes les informan a los partners o clientes de la víctima que han accedido a sus datos confidenciales como parte del ataque de ransomware, y les sugieren que presionen a la víctima para que pague de modo de evitar la divulgación de sus datos. En algunos casos, los atacantes incluso exigen el pago directamente a los partners o clientes de la víctima.

En los últimos años se ha visto una transición en los ataques de ransomware: pasaron de ser ataques masivos apuntando a un gran número de personas solicitando sumas modestas por los rescates, a ser ataques dirigidos a sectores específicos exigiendo rescates mucho mayores a grupos de víctimas más pequeños. Estas víctimas tienen bolsillos más grandes y miembros que no pueden permitirse perder el acceso a sus datos o el control sobre ellos.

Titulares de 2021 sobre organizaciones de alto perfil afectadas por ataques de ransomware:

- [Kaseya estaba corrigiendo una vulnerabilidad zero-day cuando el ransomware REvil lanzó su ataque](#)
- [El ransomware REvil ataca a un contratista estadounidense de armas nucleares](#)
- [Los servicios de salud irlandeses se ven afectados por un ataque de ransomware que demanda 20 millones de dólares](#)
- [Un ataque de ransomware fuerza el cierre temporal de una importante red de oleoductos en los Estados Unidos](#)
- [ADATA fue víctima de un ataque del ransomware Ragnar Locker](#)
- [La ciudad de Tulsa cerró sus servicios online tras un incidente de ransomware](#)

Si observamos estos ataques, notaremos que las víctimas pertenecen tanto al sector público como al privado en diversas industrias. Ningún sector empresarial está exento de convertirse en víctima del ransomware dirigido y, aunque no es la amenaza más compleja desde el punto de vista técnico, protegerse de ella es una de las preocupaciones principales de muchos equipos de seguridad.

EL RANSOMWARE ES UN GRAN NEGOCIO

Nadie sabe realmente cuánto ganan los operadores de ransomware. Un análisis reciente asegura que el monto promedio solicitado por los rescates es de aproximadamente 170.000 dólares, [según Group-IB](#). Sin embargo, los investigadores también añaden que algunos grupos más descarados piden decenas de millones de dólares: Sodinokibi (también conocido como REvil) les exigió a Acer y Quanta 50 millones de dólares a cada uno. Otras sumas incluyen:

- [Informe de ransomware de ENISA](#): 10 mil millones de euros en rescates pagados durante 2019;
- [144 millones de dólares entre 2013 y 2019](#) en rescates pagados a Ryuk, según el FBI;
- [100 millones de dólares en 2020](#) en ganancias, según Sodinokibi, que puede haber exagerado;
- [150 millones de dólares en 2020](#) pagados a Ryuk, según AdvIntel;
- [40 millones de dólares en 2021](#) pagados a Phoenix Locker por CNA Financial: el pago único más alto reportado hasta ahora;
- [17,5 millones de dólares en 2021](#) pagados a DarkSide por su ataque a Colonial Pipeline, tras el cual se retiró;
- [350 millones de dólares en 2020](#) por pagos de rescates, según una estimación de Chainalysis; y
- [70 millones de dólares en 2021](#) exigidos por Sodinokibi por un descifrador universal después de su ataque a Kaseya VSA.

CÓMO LO LOGRA EL RANSOMWARE PSICOLÓGICAMENTE

fundamental es que cifra datos importantes de la víctima y los deja fuera de su alcance. Los datos, ya sean considerados de propiedad personal, profesional o intelectual, son, en todo caso, confidenciales y valiosos.

La presión se incrementa cuando las personas u organizaciones pueden llegar a sufrir daños a la reputación, interrupciones comerciales o incluso sanciones legales y financieras. Estos riesgos empeoran con el doxing, una práctica empleada por múltiples bandas de ransomware que implica hacer un barrido por los sistemas de sus víctimas en busca de datos confidenciales y luego amenazar con divulgarlos a menos que paguen una tarifa adicional además del rescate: un tipo de doble extorsión. El grupo Maze, que comenzó a implementar el doxing en noviembre de 2019, incluso mejoró el enfoque original al crear su propio sitio clandestino para publicar datos confidenciales, lo que dificulta mucho que las víctimas logren eliminar sus datos de la web.

Una vez que ejercieron presión y, por regla general, la incrementaron, sin duda lo que sigue es la manipulación. Las víctimas a menudo ven afectadas múltiples facetas de sus puntos de contacto digitales, desde ataques de DDoS en sus sitios web hasta molestas demostraciones de la presencia de los cibercriminales en la red. Algunas de estas demostraciones provocan una conmoción, como es en el caso del [print bombing](#), en el que se ordena a varias impresoras de la red que impriman la nota con el pedido de rescate, lo que impide que la gerencia pueda controlar la comunicación interna y externa sobre el incidente. La presión también puede aplicarse de manera más directa; por ejemplo, accediendo a los datos de los clientes de una empresa y luego poniéndose en contacto con las víctimas, posiblemente incluso [haciendo llamados telefónicos inesperados](#) para seguir amenazándolas e incitándolas públicamente mientras sus departamentos de TI luchan por mitigar los impactos de un ataque.

Estas son solo algunas de las tarjetas de presentación que vienen con las campañas de ransomware actuales. En pocas palabras, el ransomware puede convertir un incidente de malware desafortunado en una guerra psicológica cuyo objetivo es obligar a las víctimas a actuar contra su propia voluntad y sus mejores intereses. Los delincuentes involucrados en secuestros físicos suelen comenzar sus campañas de presión con una ventaja pero pueden quedarse sin opciones más adelante. En cambio, los

ciberdelincuentes cuentan con una variedad aún más amplia de métodos a los que recurrir para ganar influencia y aplastar cualquier esperanza de recuperación sin problemas.

Para lograr sus objetivos maliciosos, los ciberdelincuentes utilizan una gran cantidad de enfoques que potencialmente les permiten obtener acceso remoto, monitorear las actividades de sus víctimas y luego aplicar una presión extremadamente precisa. Esto demuestra el poder que tienen sobre los datos, las redes, la continuidad del negocio y la reputación de sus víctimas. De hecho, estos ataques no provienen necesariamente de malware personalizado, exploits o-day ni campañas persistentes a largo plazo. Pueden ser tan solo el resultado de malas prácticas de seguridad por parte de los empleados, una mala configuración del protocolo RDP u otras herramientas de acceso remoto, o prácticas y procesos defectuosos, tanto dentro de su propia organización como de sus proveedores de servicios u otros eslabones de su cadena de suministro.

CÓMO LO LOGRA EL RANSOMWARE TÉCNICAMENTE

Si bien el ransomware ha estado molestando con su presencia por más de una década, en el período de intensificación digital provocado por la pandemia del COVID-19 amplió considerablemente su alcance. Surgió una clara y rápida correlación entre las cuarentenas establecidas por COVID-19 y los correos electrónicos de phishing, que en muchas ocasiones utilizaban el temor de los usuarios sobre temas de actualidad, como los impactos comerciales negativos y las oportunidades perdidas.

Otra manifestación de este fenómeno fue que los empleados comenzaron a trabajar repentinamente desde casa y a acceder (en muchas ocasiones por primera vez) a los sistemas y servicios internos corporativos a través del Protocolo de escritorio remoto (RDP). Dicho protocolo se convirtió en un vector extremadamente popular para entregar ransomware. Con los derechos de administrador que acompañan en algunos casos el uso del RDP, el ransomware se sumó a las preocupaciones de seguridad ya existentes en una red.

También podemos notar que el uso del ransomware como herramienta para llevar a cabo delitos digitales se adapta a las distintas ambiciones de los perpetradores y alcanza diferentes magnitudes. Los actores menos hábiles pueden incursionar en la codificación de scripts maliciosos imperfectos que afectarán a un número muy limitado de víctimas a través del spam. Otros pueden probar suerte propagando diversos payloads (componentes maliciosos), incluyendo el ransomware, a través de downloaders o botnets. Los actores más ambiciosos pueden adquirir un producto de ransomware totalmente personalizado e implementarlo para obtener ganancias directas, convirtiéndose en afiliados de los desarrolladores de ransomware a través del modelo de negocio que se conoce como ransomware como servicio (RaaS, por sus siglas en inglés).

Los delincuentes más avanzados que operan a través del modelo del RaaS a menudo aprovechan las vulnerabilidades de una máquina para obtener acceso a ella, luego se mueven lateralmente hasta llegar a un servidor y pasar a la red más amplia; solo más tarde deciden implementar el ransomware. Si estas bandas criminales cuentan con recursos suficientes, pueden comprar exploits zero-day o incluso desarrollar los propios, lo que les permite eludir muchos tipos de tecnologías de mitigación proactivas. Finalmente, ya sea por suerte, habilidad o inversiones significativas de recursos humanos y financieros, [los atacantes pueden llegar a realizar ataques de cadena de suministro para acceder a ecosistemas de TI completos](#). Por ejemplo, al apoderarse de plataformas populares de proveedores de servicios gestionados (MSP) y herramientas de productividad, los actores de amenazas pueden liberar ransomware en múltiples redes (y por lo tanto organizaciones) a gran escala. El aprovechamiento de los ataques de cadena de suministro para distribuir ransomware es otro temible escenario al que se enfrentan las empresas.

Considerar la variedad de enfoques en crecimiento constante y la velocidad con la que el ransomware puede evolucionar es fundamental para comprender cuál es la postura de seguridad necesaria para

evitar interrupciones comerciales. La innovación por parte del ransomware avanza rápidamente. Un ejemplo es el ransomware Sodinokibi (también conocido como REvil). Investigadores que lo [analizaron](#) demostraron que cifraba los archivos de la PC utilizando el Modo seguro, con lo que pasaba desapercibido pero requería un inicio de sesión de usuario adicional. [En un mes](#), esta nueva capacidad se mejoró cambiando la contraseña de inicio de sesión por una elegida por el atacante y configurando la PC para que se reinicie automáticamente e inicie sesión en Modo seguro, lo que la convierte en un vector viable para una campaña a gran escala.

Los dispositivos de almacenamiento conectados a la red (NAS), que se utilizan comúnmente para compartir archivos y realizar backup, también se han ganado la atención de las bandas de ransomware. En 2021, el fabricante de dispositivos NAS QNAP [alertó](#) a sus clientes de que el ransomware eChoraix estaba atacando sus dispositivos NAS, en especial aquellos con contraseñas débiles. La telemetría de ESET del cuarto trimestre de 2020 mostró que eChoraix era el ransomware más prominente dirigido a dispositivos NAS.

ATAQUES DE RANSOMWARE POR RDP

Un endpoint de RDP es un dispositivo Windows que ejecuta el software de Protocolo de escritorio remoto (RDP) para que se pueda acceder a él a través de una red, como Internet. El RDP permite acceder de manera remota a los dispositivos Windows de una organización como si sus teclados y pantallas estuvieran sobre el escritorio del usuario. Los beneficios de hacer uso del RDP pueden ser varios, desde administrar o solucionar problemas de los dispositivos de los empleados hasta brindar recursos centralizados como equipos de escritorio capaces de ejecutar grandes cargas de trabajo, aplicaciones o bases de datos.

Los sistemas corporativos a los que los empleados necesitan acceder en forma remota deben tener el protocolo RDP habilitado e, idealmente, implementar la [autenticación en dos fases](#) (2FA) para acceder a la plataforma. Luego, los empleados se conectan a dichos sistemas ejecutando el software RDP; por ejemplo en sus computadoras portátiles. Cuando se ingresa la dirección de red del sistema remoto, el software del cliente llega al puerto designado en el sistema remoto (el puerto predeterminado para RDP es 3389, aunque se puede cambiar). El sistema remoto muestra una pantalla de inicio de sesión que solicita un nombre de usuario y contraseña. La [Imagen 1](#) muestra cómo se ve en un sistema Windows.

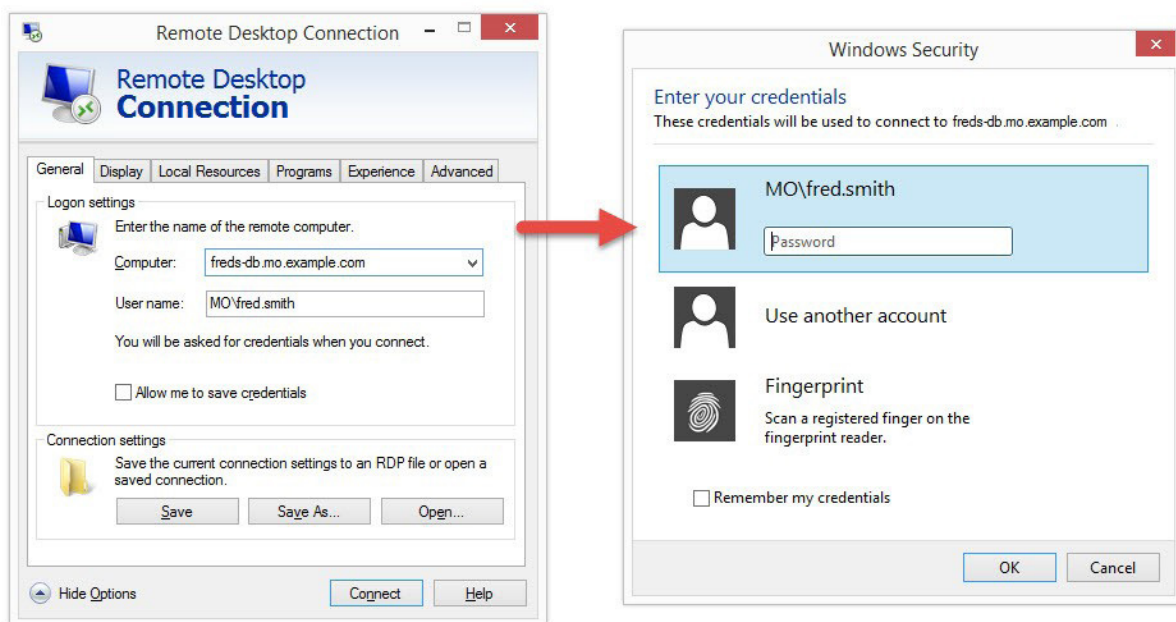


Imagen 1. // Pantalla de inicio de sesión de RDP

Las dos principales formas de utilizar el RDP por parte de las organizaciones:

1. La primera es para administrar los programas que se ejecutan en un servidor; por ejemplo, un sitio web o una base de datos en el back-end. En este escenario, la configuración más simple es tener un administrador de sistemas que abra el puerto 3389 al mundo exterior para permitir la administración remota.
2. Un segundo uso de RDP es permitir el acceso remoto a escritorios corporativos o máquinas virtuales que tienen acceso a recursos no accesibles fuera de la red corporativa. El acceso a dichos sistemas a través de RDP significa que no es necesario abrir directamente a Internet los servidores internos confidenciales. También puede ocurrir que los equipos de escritorio de la oficina tengan una potencia de procesamiento adicional imprescindible para muchos procesos, o que tengan instalado un costoso software especializado necesario para que el personal complete algunas (o en algunos casos la mayoría) de sus tareas. Una vez más, cuando esto se hace a través de Internet, por lo general se abre el puerto 3389 al mundo exterior.

Para las personas con inclinaciones criminales, encontrar sistemas accesibles desde el mundo exterior y luego aprovecharlos con fines maliciosos es sencillo porque:

- Los sistemas RDP vulnerables son fáciles de encontrar.
- Es fácil para los atacantes afianzarse en los sistemas RDP si su configuración es deficiente.
- Muchos sistemas RDP tienen configuraciones débiles.
- Las herramientas y técnicas para escalar privilegios y obtener derechos de administrador en sistemas RDP comprometidos son ampliamente conocidas y están disponibles.

Los sistemas que ejecutan RDP pueden ser identificados por motores de búsqueda especializados como [Shodan](#), que constantemente buscan en Internet dispositivos conectados y recopilan información sobre ellos. Al 15 de junio de 2021, Shodan indicó que había más de 3 millones de sistemas en Internet con el puerto 3389 abierto (es posible que sea necesario registrarse para ver las búsquedas de Shodan usando filtros). Como se puede observar en la interfaz de Shodan en la [Imagen 2](#), más de 1 millón de esos sistemas se encontraban en los Estados Unidos.

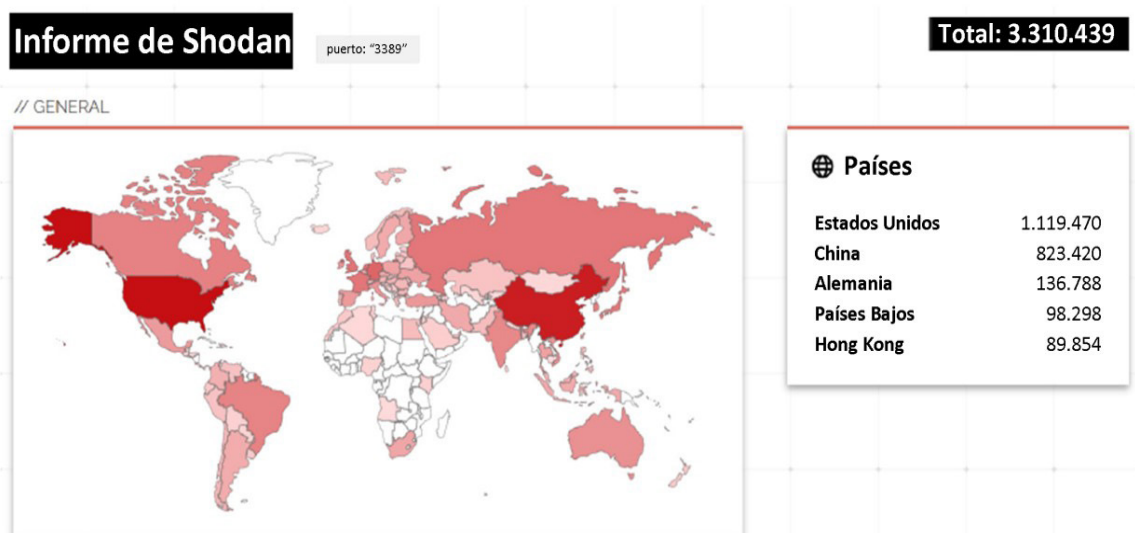


Imagen 2. // Más de 3 millones de sistemas en Internet utilizaban el puerto 3389 (Fuente: Shodan)

Tras hacer una [búsqueda diferente](#), se descubrió que más de 2,7 millones de máquinas ejecutaban explícitamente RDP. Para un atacante, todas estas máquinas son objetivos potenciales a explorar. Si bien el inicio de sesión en un sistema RDP generalmente requiere un nombre de usuario y una contraseña, estos pueden ser sorprendentemente fáciles de adivinar para los atacantes, por lo que accederán a muchos de esos equipos sin problemas.

Un atajo para los atacantes que tienen fondos suficientes es simplemente comprar accesos a sistemas RDP comprometidos. Estas credenciales están disponibles en los mercados de la Dark Web. Es importante recordar que el ransomware no es la única razón para comprar credenciales RDP robadas. Otros usos que se da a un sistema RDP comprometido incluyen el envío de spam, el alojamiento de malware, el descifrado de contraseñas, la extracción de criptomonedas y una variedad de actividades para las cuales el anonimato es deseable y la atribución no lo es, como las compras fraudulentas y el blanqueo de capitales.

Si solo se requieren el nombre de usuario y la contraseña para acceder de forma remota al dispositivo, un actor malicioso, tras haber identificado el endpoint blanco de ataque, puede realizar repetidos intentos para adivinar dichas credenciales. Cuando esto se hace a gran velocidad usando una base de datos de credenciales probables, se denomina ataque mediante fuerza bruta. En caso de que no haya ningún mecanismo que limite la cantidad de intentos erróneos, estos ataques pueden ser muy efectivos e incluso infectar toda la red.

La telemetría de ESET confirma que el RDP es uno de los vectores de ataque más populares, cuyas detecciones superaron las 71 mil millones entre enero de 2020 y junio de 2021. Si bien el aumento más notable se produjo en la primera mitad de 2020, en 2021 se registraron las cifras más altas hasta la fecha. Al comparar el primer semestre de 2020 con el primero de 2021, ESET notó que las detecciones de ataques por fuerza bruta contra el RDP fue seis veces mayor.

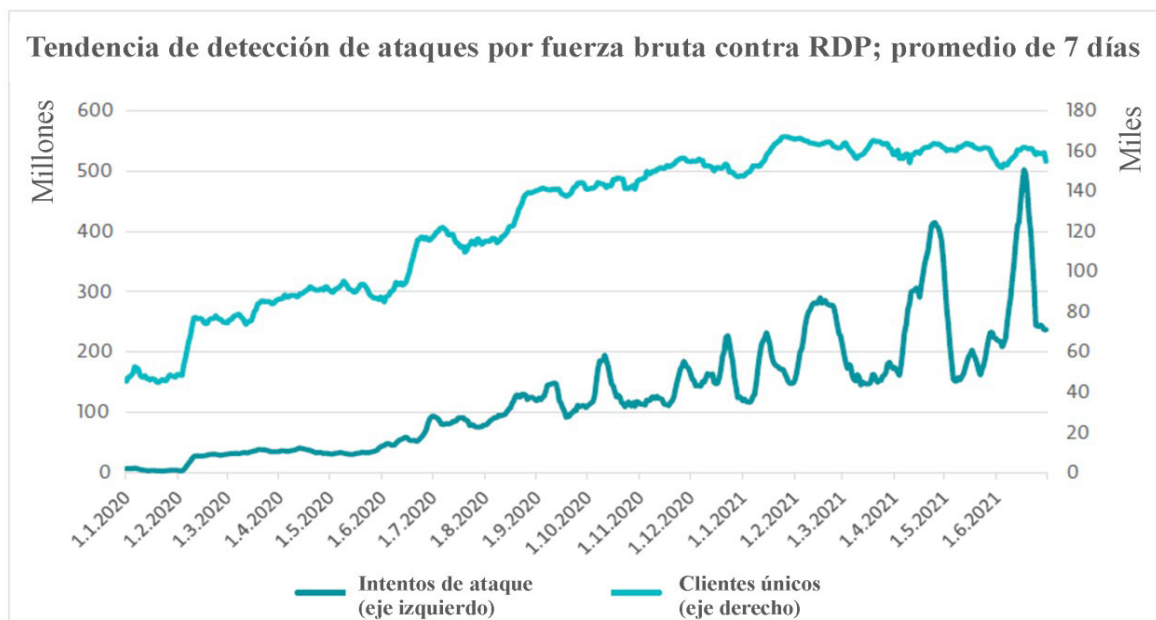


Imagen 3. // Tendencias de intenciones de conexión por RDP con clientes únicos entre enero de 2020 y junio de 2021, promedio móvil de siete días

Si bien obtener acceso no autorizado desde Internet a dispositivos que ejecutan RDP puede requerir más esfuerzo inicial que utilizar un ransomware basado en correo electrónico, el vector RDP les ofrece a los actores de amenazas beneficios importantes, como hacer un uso indebido del acceso legítimo, la posibilidad de evadir las protecciones de los endpoints y la capacidad de infectar rápidamente múltiples sistemas (o incluso la red completa) dentro de una misma organización.

“ Los ataques a través de RDP son capaces de pasar desapercibidos para muchos métodos de detección, lo que significa menos métricas y menos conciencia de la existencia de amenazas. ”

Cualquier organización que tenga un programa de seguridad de la información maduro detectará y bloqueará un ransomware embebido en un archivo adjunto de un correo electrónico entrante, por ejemplo. Estos incidentes suelen ser registrados e informados por los programas de protección para endpoints, cuyos fabricantes recopilan las estadísticas anónimas de dichos informes para determinar las tendencias de las amenazas.

Lo mismo ocurre con los intentos de engañar a los usuarios para que visiten sitios web maliciosos que propagan ransomware. Sin embargo, si un atacante con privilegios de administrador del sistema infecta un servidor y apaga el software de protección de endpoints antes de implementar su ransomware, el ataque podrá eludir las métricas típicas.

Movimiento lateral y estrategia de “living off the land”

Para el atacante de ransomware, un sistema RDP comprometido puede significar mucho más que el simple pago de un rescate por descifrar los archivos en la máquina infectada, en especial, si ese sistema puede proporcionar un punto de entrada a una red completa de dispositivos, lo que permitiría el cifrado a gran escala o el robo de datos críticos. De hecho, esto es lo que ocurrió en muchos de los casos a los que hacen referencia los titulares citados anteriormente, y las técnicas para llevar a cabo este tipo de ataque no son un secreto.

Al obtener acceso remoto, el atacante querrá conocer más sobre la máquina infectada, por lo que evaluará su potencial de abuso, incluyendo sus conexiones a otros sistemas. En caso de no haber accedido al equipo con credenciales de administrador, puede utilizar varias técnicas para escalar los privilegios al nivel de administrador. Si el sistema tiene instalada una solución de protección para endpoints que puede ser desactivada por cualquier usuario con privilegios de administrador, es probable que el atacante intente desactivarla. Esto le facilita al atacante la descarga de software adicional, basándose en su evaluación del potencial de abuso del sistema. Tenga en cuenta que, en el siguiente texto, cuando las acciones se describen como realizadas “por el atacante”, es posible que no las realice una persona desde un teclado, sino un software utilizado para automatizar ciertos aspectos de un ataque.

Algunos atacantes intentan introducir el fragmento de código malicioso más pequeño posible para minimizar la detección. A continuación, el malware emplea la estrategia conocida en inglés como “living off the land”, es decir, hace uso de software legítimo (a menudo utilizado por los mismos administradores del sistema), e incluso de las herramientas estándar instaladas junto con el sistema operativo base, para extender su penetración en la red. Por ejemplo, la interfaz PsExec y la Línea de comandos de instrumental de administración de Windows (WMIC) se suelen usar indebidamente para lograr el movimiento lateral en redes comprometidas. Como existen razones válidas para que se estén ejecutando estos programas, detectar su uso indebido por parte de un atacante puede ser difícil, aunque no imposible. Para obtener más información sobre su detección, consulte la sección sobre las herramientas de detección y respuesta para endpoints (EDR) a continuación.

El término movimiento lateral se utiliza para describir la estrategia de afianzarse en un sistema y utilizarlo para infectar otros dispositivos a los que se puede llegar desde allí. Por ejemplo, los atacantes pueden utilizar credenciales comprometidas para infectar un servidor que ni siquiera está presente en la organización objetivo, y luego usar su conexión a la infraestructura principal para entregar el payload con el ransomware.

Además de utilizar la estrategia de “living off the land”, [los ataques de ransomware pueden aprovecharse de vulnerabilidades no corregidas en algún software legítimo del sistema](#). Quizás uno de los ejemplos más arquetípicos es el ransomware WannaCryptor, que se propagó a través del [exploit EternalBlue](#), usando indebidamente una vulnerabilidad de alta severidad en la implementación de SMB de Microsoft. A pesar de que los parches estaban disponibles al público desde hacía dos meses antes de la campaña de WannaCryptor, que comenzó el 12 de mayo de 2017, los atacantes lograron encontrar e infectar más de 200.000 máquinas vulnerables. Incluso en las últimas etapas de este brote, los dispositivos infectados continuaron siendo una amenaza, por ejemplo, cuando los usuarios llevaban, sin saberlo,

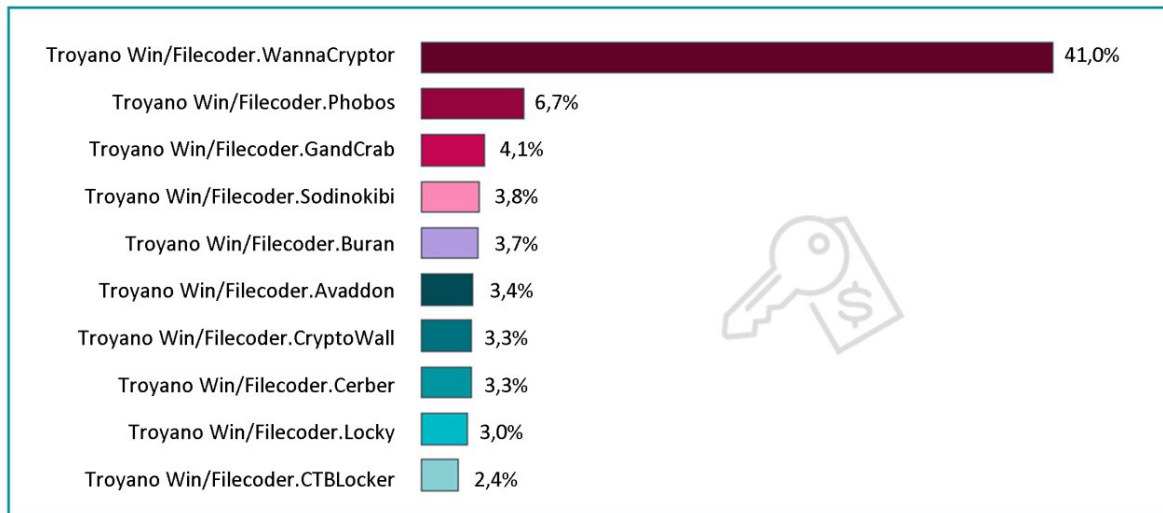


Imagen 3. // Las 10 principales familias de ransomware en el primer cuatrimestre de 2021 (% de detecciones de ransomware). Cuatro años después de su devastador ataque de 2017, WannaCryptor todavía se encuentra entre las familias de ransomware en actividad más detectadas (fuente: [Informe de amenazas de ESET del primer cuatrimestre de 2021](#))

computadoras portátiles infectadas a lo que los administradores consideraban un perímetro seguro.

Naturalmente, en algunos casos existe la posibilidad de que el primer punto de contacto entre el atacante y la organización sea un servidor que aloja una base de datos crítica. Un delincuente oportunista aquí podría decidir que prefiere ahorrar algo de tiempo y esfuerzo y buscará una victoria rápida simplemente robando datos, cifrándolos y pidiendo un recate por los archivos de ese único servidor. Sin embargo, se puede ganar mucho más mediante la persistencia, por lo que es probable que en la mayoría de los casos los operadores de ransomware continúen llevando a cabo un proceso de reconocimiento, incluso después de haber robado los datos y antes de cifrarlos, solo para asegurarse de que tienen suficiente influencia.

Cómo defenderse contra ataques de ransomware por RDP

Es posible defender los sistemas que ejecutan RDP del acceso no autorizado y, por lo tanto, impedirles a los delincuentes usar este vector de ataque cada vez más popular, más allá de que estén intentando acceder para infectar el sistema con ransomware o realizar alguna otra actividad no autorizada. Si bien en esta sección hablamos de las estrategias defensivas en general, en la sección titulada “[Cómo proteger el RDP del ransomware](#)” proporcionamos una lista más específica de las técnicas contra el ransomware.

Seguramente su organización ya contará con algunas políticas para abordar la seguridad del acceso remoto. Quizá tenga reglas que requieran que todo acceso vía RDP pase a través de una VPN (red privada virtual), esté protegido mediante autenticación multifactor (MFA), limitado a roles específicos, en sistemas específicos configurados de forma segura, con parches instalados de inmediato,

monitoreados constantemente, con los firewalls que corresponden y con tareas periódicas de creación de backup.

Sin embargo, por más que ya haya implementado todas estas reglas o esté trabajando para implementarlas, las reglas por sí solas no garantizarán la seguridad total de su acceso remoto. Aún necesitará asegurarse de que todos cumplan con las reglas, y al mismo tiempo estar preparado para manejar un ataque que en muchos casos logra su cometido a pesar de la existencia de reglas.

Un primer paso fundamental en la defensa contra los ataques de ransomware mediante RDP es hacer un inventario de todos los activos conectados a Internet. Por más que parezca una afirmación obvia decir que uno no puede defender un sistema si no sabía que existía, según nuestras investigaciones, el siguiente es un escenario bastante común: una organización es atacada a través de un activo conectado a Internet que el personal de seguridad de la organización no sabía que existía hasta después del ataque.

Es necesario que se implementen procesos para garantizar que eso no suceda en su organización. Por ejemplo, no debería ser posible que un proveedor o un empleado conecte un servidor físico o virtual a la red corporativa y a Internet, a menos que ese servidor esté configurado de forma segura; dicha configuración debe haberse hecho antes de que el servidor aparezca online, en particular si el servidor está ejecutando RDP con una cuenta de administrador de dominio.

Cuando haya terminado de crear el inventario de todos los activos conectados a Internet, debe documentar cuáles tienen habilitado el acceso remoto y luego decidir si realmente es necesario. Si el acceso es necesario, exíjales a los usuarios de dichas cuentas que creen contraseñas largas. ¿Cuán largas? Aunque las contraseñas de 15 caracteres o más pueden parecer imposibles de recordar, son fáciles si [se usan frases de contraseña](#). Además, las contraseñas de esa longitud no necesitan tener reglas de complejidad, que según las investigaciones tienden a empujar a las personas a prácticas deficientes en el uso de contraseñas. Una vez que estableció requisitos estrictos para la longitud de la contraseña de las cuentas, determine si es factible o no limitar esos sistemas a la red interna y hacer que se acceda remotamente mediante una VPN corporativa.

Si es necesario acceder a un sistema desde la Internet pública a través de RDP, y el uso de una VPN no es factible, al menos instale una solución MFA para que su protección no dependa únicamente de las contraseñas del usuario. Pero asegúrese de no utilizar una solución MFA basada en SMS. Los delincuentes tienen muchas formas de interceptar los SMS de autenticación.

Si se ve obligado a confiar en las contraseñas porque la solución MFA no está disponible, posiblemente debido a una política presupuestaria miope, al menos bloquee el acceso a posibles intrusos cuando detecta repetidos intentos por adivinar las credenciales. Establezca un límite de tres intentos de inicio de sesión no válidos, tras los cuales no se reconocerá ningún otro intento de inicio de sesión durante un período de tiempo establecido; por ejemplo, tres minutos. La [Imagen 5](#) muestra cómo se ve en Windows.

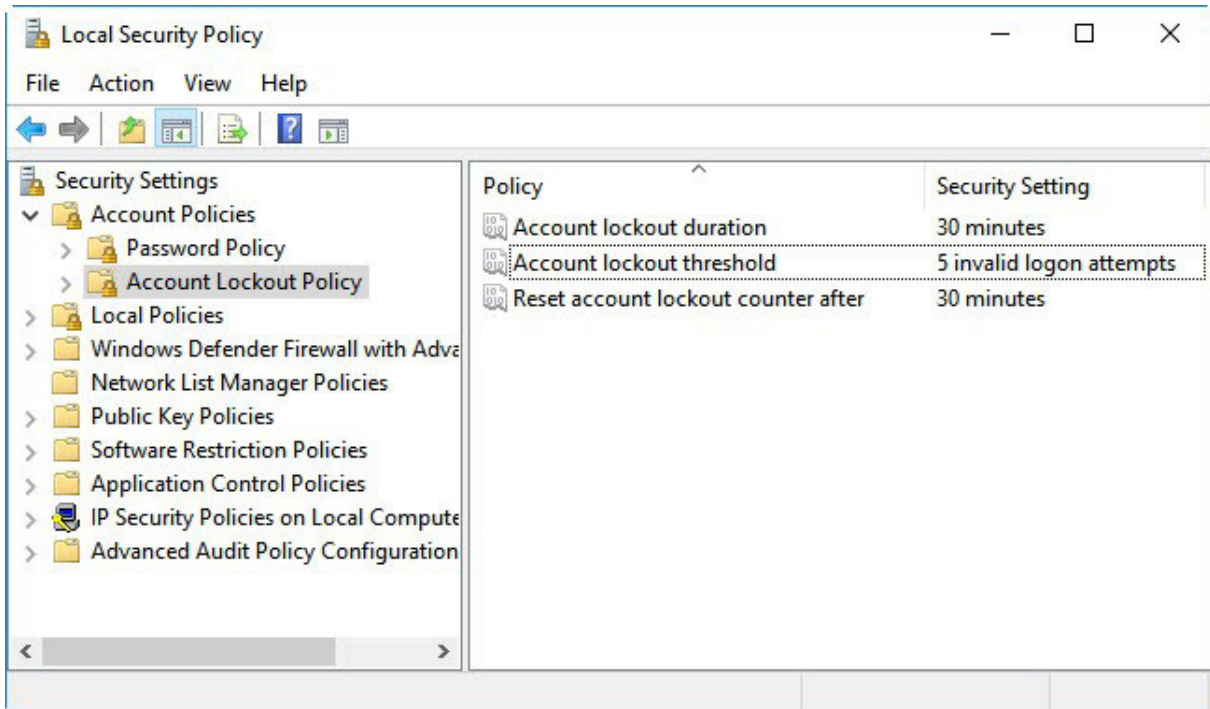


Imagen 5. // Política de bloqueo de cuenta

También puede cambiar el puerto de escucha RDP de 3389 a otro, para que sea un poco más difícil para los atacantes encontrar las máquinas accesibles. Puede hacerlo desde la configuración del sistema, aunque también necesitará cambiar las reglas de firewall para acomodar el puerto designado. Recuerde que esto es meramente "seguridad por oscuridad" y no debe confiar en que mantendrá seguros los sistemas RDP (consulte la sección "[Cómo proteger el RDP del ransomware](#)" para obtener más detalles).

El fortalecimiento de la seguridad y la aplicación de parches es algo que debe realizarse en todos los dispositivos que son accesibles en forma remota. Además de cerciorarse de que todas las vulnerabilidades de seguridad estén identificadas y remediadas, debe verificar que todos los servicios y componentes no esenciales se hayan eliminado o deshabilitado, y que la seguridad esté configurada en el máximo nivel.

Por ejemplo, en sistemas Windows puede usar las Directivas de restricción de software (SRP) para impedir que los archivos se ejecuten desde carpetas como AppData y LocalAppData, que a veces son utilizadas por malware. También puede usar AppLocker para controlar qué aplicaciones y archivos pueden ejecutar los empleados en sus máquinas. Por supuesto, la última línea de defensa contra el ransomware por RDP es un sistema completo y bien probado de creación de backups y recuperación. Dado que los backups son la clave para sobrevivir al ransomware independientemente del vector de ataque, lo analizaremos tras considerar tres vectores más: el correo electrónico, la cadena de suministro y las vulnerabilidades.

Protocolo SMB, en segundo lugar tras el RDP

El protocolo Bloque de mensajes del servidor (SMB), que se utiliza sobre todo para compartir archivos e impresoras en redes corporativas, también se puede usar indebidamente como un servicio remoto para introducir el ransomware. En el primer cuatrimestre de 2021, las tecnologías de ESET [bloquearon](#) 335 millones de ataques por fuerza bruta a servicios SMB orientados al público. Aunque esto representa una disminución del 50% en comparación con los últimos cuatro meses de 2020, los ataques a través de SMB siguen siendo una amenaza importante. Además, el ransomware WannaCryptor (también conocido como WannaCry), que abarcó el 41% de las detecciones de ransomware en este mismo primer cuatrimestre de 2021, se propaga mediante el aprovechamiento de vulnerabilidades en el protocolo SMBv1.

Siga estos consejos para protegerse contra las amenazas dirigidas al protocolo SMB:

- [Deshabilite SMBv1 y SMBv2](#), tenga en cuenta que deberá gestionar cualquier dependencia existente en estas versiones obsoletas.
- Actualice a la última versión del protocolo SMB, que actualmente es SMBv3.
- Utilice la configuración de la directiva de grupo para asegurar que se requiera la firma de SMB entre los hosts y los controladores de dominio para evitar ataques de reproducción en su red.
- Bloquee los puertos TCP 445 y 139, y los puertos UDP 137 y 138 de Internet. Esto impedirá el acceso a todas las versiones de SMB fuera de su red.

Cómo proteger el RDP del ransomware

Le recomendamos considerar la siguiente recopilación de estrategias y técnicas:

1. Documente el problema

Cómo proteger el RDP del ransomware

Le recomendamos considerar la siguiente recopilación de estrategias y técnicas:

1. Documente el problema

Asegúrese de que todos los activos conectados a Internet de su organización sean conocidos por las personas a las que se les ha asignado la tarea de protegerlos. Disponga de un proceso para garantizar que se incluyan todos los dispositivos nuevos.

2. Limite los activos expuestos

Asegúrese de que ningún activo digital sea accesible de manera remota directamente desde Internet, a menos que haya sido aprobado para usarse de esa manera y esté configurado adecuadamente. Revise por qué no se puede proporcionar acceso al activo a través de una VPN. Deshabilite el protocolo RDP siempre que no sea necesario (estos artículos muestran cómo hacerlo en diferentes versiones de Microsoft Windows: [Server 2019](#); [Server 2016](#); [Server 2008/R2](#); [Windows 10](#); [Windows 8](#); [Windows 7](#)).

3. Proteja los activos expuestos

Si definitivamente tiene que usar RDP sin una VPN, asegúrese de seguir la mayor cantidad que pueda de estos consejos:

- a. Cambie la contraseña de la cuenta de usuario a la que se está conectando en la máquina remota con regularidad. Asegúrese de cambiar la contraseña predeterminada que a veces se genera automáticamente para las instancias en la nube.
- b. Haga cumplir la complejidad de la contraseña (es obligatorio que sea una frase de contraseña larga que contenga más de 15 caracteres, sin frases relacionadas con la empresa, con los nombres de productos o con los usuarios).
- c. Establezca un límite de bloqueo de cuenta para bloquear el acceso remoto después de cierta cantidad de intentos fallidos consecutivos de inicio de sesión. Al configurar su computadora para que bloquee una cuenta durante un período de tiempo tras una serie de conjeturas incorrectas, obstaculizará a los atacantes que utilizan herramientas automáticas de adivinación de contraseñas (ataque por fuerza bruta). Para establecer una política de bloqueo de cuenta en Windows: Vaya a Inicio --> Programas --> Herramientas administrativas --> Directiva de seguridad local En Directivas de cuenta --> Directivas de bloqueo de cuenta, introduzca valores para las tres opciones: tres intentos no válidos con una duración del bloqueo de tres minutos son opciones razonables.
- d. Pruebe e instale los parches para todas las vulnerabilidades conocidas y asegúrese de que las más conocidas y obvias, como BlueKeep y EternalBlue, se encuentren entre los defectos corregidos. Si los parches no se pueden instalar en una computadora determinada, planifique su reemplazo oportuno.
- e. Utilice la Autenticación a nivel de red para mejorar la seguridad del host de sesión de escritorio remoto, ya que de esta forma le exige al usuario que esté autenticado en el servidor host de sesión de escritorio remoto antes de crear una sesión.
- f. Cambie el puerto predeterminado para RDP (3389), pero tenga en cuenta que esto es simplemente "seguridad por oscuridad" y no debería ser la única medida que tome. Para cambiar el puerto, edite el siguiente valor de registro (ADVERTENCIA: no lo intente a menos que esté familiarizado con el Registro de Windows y los protocolos TCP/IP): HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber.
- g. Restrinja las direcciones IP públicas que se pueden conectar a través de RDP. Esto puede resultar engorroso si los usuarios remotos no tienen direcciones IP estáticas; por ejemplo, cuando están de viaje o trabajan desde su casa.
- h. Utilice más de un factor de autenticación. Hay tres factores posibles: algo que uno sabe, como el nombre de usuario y la contraseña; algo que uno es, como la huella dactilar o de voz; y algo que uno tiene, como el teléfono, que puede recibir un código de acceso de un solo uso o ejecutar una aplicación de autenticación que generará el código cuando lo necesite. Sin embargo, si usa como segundo factor un código enviado a un teléfono, evite los códigos por SMS, porque los delincuentes ya se las ingeniaron para interceptar este tipo de mensajes de autenticación (como se describe en [este artículo](#)). Existen buenas soluciones MFA que aprovechan el uso generalizado de los teléfonos inteligentes pero no se comunican por SMS (como [ESET Secure Authentication](#)).
- i. Fortalezca los permisos y derechos de los usuarios. Deshabilite los archivos que se ejecutan desde las carpetas AppData y LocalAppData. Bloquee la ejecución desde el subdirectorio Temp (que por defecto forma parte del árbol AppData). Bloquee los archivos ejecutables que se ejecutan desde los directorios de trabajo de diversas utilidades de descompresión (por ejemplo, WinZip o 7-Zip). Además, si cuenta con un buen producto de protección para endpoints puede crear reglas HIPS para permitir que solo ciertas aplicaciones se ejecuten en la computadora y bloquear todas las demás de forma predeterminada.

- j. Exija el uso de contraseñas únicas y derechos de administrador para las cuentas locales que necesiten acceder a los servidores (por ejemplo, se puede implementar el servicio LAPS u otro servicio confiable de administración de contraseñas). Adicionalmente, restrinja los derechos de acceso al servidor para un grupo limitado de usuarios. Esto reduce la superficie de ataque de los servidores, ya que limita la cantidad de usuarios que pueden acceder a ellos.
- k. Configure el nivel de cifrado de la conexión del cliente RDP en "alto", si es posible. De lo contrario, use el nivel de cifrado más alto disponible para las conexiones.
- l. Instale una puerta de enlace VPN que sirva como mediador para todas las conexiones RDP desde fuera de su red local.
- m. Proteja con contraseña la solución de seguridad de sus endpoints para evitar que usuarios no autorizados puedan cambiar la configuración, deshabilitar la protección o incluso desinstalar el producto (pero use una contraseña diferente a la del inicio de sesión en RDP).
- n. Habilite el [bloqueo de exploits](#) en su software de seguridad para endpoints. Se trata de una [tecnología](#) para detectar anomalías, no basada en firmas, que monitorea el comportamiento de las aplicaciones que suelen ser atacadas por exploits con mayor frecuencia.
- o. Aísle las computadoras no seguras a las que se deba acceder desde Internet usando RDP.
- p. Si todo el personal y los proveedores se encuentran en un mismo país o en una lista reducida de países, considere bloquear el acceso de los países excluidos mediante el bloqueo GeoIP en la puerta de enlace VPN de modo de evitar conexiones de atacantes extranjeros.

ATAQUES DE RANSOMWARE POR CORREO ELECTRÓNICO

Como le dirá cualquier experto en seguridad con experiencia: las amenazas a los sistemas de la información son acumulativas. Por ejemplo, el hecho de que el foco de atención de algunos delincuentes haya cambiado a servidores con acceso remoto habilitado para distribuir ransomware, no significa que pueda ignorar los demás vectores de ataque. Algunos todavía siguen usando archivos adjuntos a correos electrónicos para instalar malware como etapa inicial de una infección que termina con ransomware.

Los ciberdelincuentes pueden usar este vector para entregar downloaders, que instalan malware en la máquina del destinatario del correo electrónico, o para lograr afianzarse en una máquina que está dentro de la red de una organización. Esta presencia les sirve de base para luego intentar robar los datos valiosos y cifrar los archivos de toda la organización, para más tarde hacer un pedido de rescate muy grande, como suele ser el caso de los ataques de ransomware dirigidos a través de RDP.

En particular, el correo electrónico es uno de los vectores principales de las botnets, como Trickbot, Qbot y Dridex, que suelen utilizar documentos de Microsoft Office con macros maliciosas para la intrusión inicial y descargar ransomware como payload final. Algunas de las relaciones conocidas entre las familias de botnets y ransomware incluyen [Emotet](#) con Qbot, [Trickbot](#), [Ryuk](#) y Conti; [Dridex](#) con FriedEx (también conocido como BitPaymer); [Nemuco](#) con [Avaddon](#), Dridex, Ursnif y Trickbot; y [SmokeLoader](#) y [Zloader](#) con LockBit y Crysis.

La policía logró desactivar a [Emotet](#) a principios de 2021, lo que provocó una fuerte disminución en la cantidad de downloaders que se distribuían a través del correo electrónico. Describimos los impactos de las campañas de [Emotet](#), tanto antes como después de su intervención, en el [Informe de amenazas de ESET del primer cuatrimestre de 2021](#), en el [Informe de amenazas de ESET del cuarto trimestre de 2020](#) y en el [Informe de amenazas de ESET del tercer trimestre de 2020](#).

A pesar de la disminución significativa de los downloaders, los actores maliciosos que utilizan macros infectadas siguieron siendo la principal amenaza de correo electrónico en 2021. En enero, incluso se produjo un aumento en los correos electrónicos que entregaban documentos de Office maliciosos con los downloaders Dridex y Emotet.

En octubre de 2020, otra botnet popular, [Trickbot](#), sufrió la interrupción de una parte de su infraestructura. Sin embargo, parece haber sido solo un revés temporal, ya que sus operadores no tardaron mucho en lanzar una [nueva campaña de phishing](#) en enero de 2021 dirigida a empresas de seguros y servicios jurídicos en América del Norte. Parece que será necesario hacer un esfuerzo aún mayor en el futuro para deshacerse de Trickbot para siempre.

A la hora de proteger a su organización contra ataques de ransomware provenientes del correo electrónico, la primera línea de defensa es filtrar todo el correo entrante en busca de spam y mensajes de phishing. De hecho, ya existían varias buenas razones para hacerlo incluso antes de que el correo electrónico se convirtiera en un canal de entrada para el ransomware, y muchas organizaciones ya cuentan con un filtrado básico de spam y detección de phishing.

Es posible que desee ir un paso más lejos e implementar el bloqueo de todos los tipos de archivos adjuntos que su empresa normalmente no espera recibir por correo electrónico; sin embargo, esta estrategia solo será adecuada para ciertos tipos de negocio y probablemente necesitará cambiar algunos hábitos de trabajo. Por ejemplo, si los empleados acostumbran enviarse hojas de cálculo de Excel y documentos de Word por correo electrónico, es posible que la organización deba adoptar primero una solución o un marco de colaboración seguro para compartir archivos, y hacer que el personal comience a utilizar la nueva modalidad antes de bloquear rigurosamente los archivos adjuntos al correo electrónico con un filtrado más estricto.

Asegúrese de que todos los endpoints estén ejecutando un software de protección para endpoints (EPP) de alta calidad para evitar que los empleados accedan a páginas web que se sabe que alojan malware. Es posible que también desee utilizar el filtrado de contenido web como capa adicional de protección. Además de bloquear sitios web maliciosos, un filtro de contenido web puede impedir que los empleados visiten sitios web que se consideran inapropiados en el ámbito laboral.

Su solución EPP debe poder administrarse de manera centralizada para hacer cumplir las políticas de seguridad relevantes, como evitar que se desactive la protección en los equipos o que se inserten medios extraíbles. Asegúrese de que todos los dispositivos estén ejecutando la última versión del producto de seguridad y que estén recibiendo correctamente las actualizaciones. Si su proveedor de EPP tiene un componente en la nube, asegúrese de que esté activado, ya que permite una reacción aún más rápida a las nuevas amenazas. El componente en la nube de ESET se llama [LiveGrid® y, en algunos productos, ESET Dynamic Threat Defense](#).

Los proveedores de servicios gestionados que se encargan de configurar los productos de ESET implementados en las redes de sus clientes encontrarán sugerencias de configuración contra ransomware [aquí](#).

La instalación rápida y completa de los parches para sistemas operativos y aplicaciones ayudará a evitar que el ransomware ingrese a través de archivos adjuntos de correo electrónico o descargas no autorizadas. La configuración segura también puede resultar útil. Por ejemplo, considere usar la Política de grupos para deshabilitar completamente las macros de Microsoft Office. Esto limitará la superficie de ataque del ransomware, aunque es posible que no sea factible si el flujo de trabajo de la organización se basa en macros.

Hoy en día, no cabe duda de que la seguridad es una responsabilidad compartida. Asegúrese de mantener actualizada la capacitación en ciberseguridad de sus empleados para que refleje las últimas tendencias en el panorama de amenazas. Como se indica en la capacitación gratuita de [concientización sobre seguridad cibernética](#) de ESET: "Logrará reducir la cantidad de incidentes de malware con los que

tiene que lidiar su empresa si les informa a los empleados qué buscar y qué evitar en relación con el phishing y otros contenidos maliciosos.”

Deje en claro a los empleados que deben informar de inmediato, ya sea a la mesa de ayuda o al equipo de seguridad, cuando detectan un mensaje o archivo adjunto sospechoso. Además del potencial para prevenir o limitar el daño, las advertencias tempranas ayudan a la organización a ajustar sus filtros de contenido y correo no deseado, así como a reforzar sus firewalls y otras defensas.

ATAQUES DE RANSOMWARE POR CADENA DE SUMINISTRO

Un vector de ataque de ransomware que merece especial atención en la actualidad es la cadena de suministro de software. Así como el ransomware se remonta al siglo pasado, los riesgos en la cadena de suministro de software también. Cuando el vector de ataque principal para los virus informáticos eran los discos de computadora, y estos eran la forma principal en que las personas adquirían software, el malware a veces terminaba en discos de producción o en los discos de software de prueba que solían distribuirse con revistas de informática.

En 2017, ESET [descubrió](#) que [los delincuentes utilizaban un software de contabilidad legítimo para impulsar el malware NotPetya/DiskCoder.C](#). Los atacantes penetraron en los servidores de actualización de la empresa de software y añadieron su propio código a los archivos legítimos de actualización de la aplicación. Cuando los usuarios del software de contabilidad hacían clic para instalar las actualizaciones del programa, también estaban instalando un backdoor, lo que abrió el camino para lo que se convirtió en el ataque cibernético más devastador de la historia. La primera línea de defensa contra este tipo de ataques es tener un buen producto de protección para endpoints que incluya herramientas de EDR.

De esta forma, debido al impacto que pueden provocar estos ataques y a las mitigaciones que luego pueden requerir, los investigadores y administradores de seguridad deben mantenerse atentos. [El 2 de julio de 2021 se produjo una serie de eventos con el software de administración de TI de Kaseya para proveedores MSP](#), con características similares a las de un ataque de ransomware en la cadena de suministro y que utilizaba el troyano Win32/Filecoder.Sodinokibi.N. La investigación subsiguiente demostró que el ataque aprovechaba una vulnerabilidad o-day que, al involucrar la cadena de suministro, provocaba una reacción rápida. Kaseya, por su parte, se apresuró a gestionar el incidente y envió notificaciones a los clientes potencialmente afectados aconsejándoles que cerraran de inmediato los servidores VSA locales que podrían haber sido comprometidos.

La creciente intensidad de los ataques a la cadena de suministro también está documentada en una gran cantidad de artículos de investigación de ESET [publicados](#) en los que se utilizó este vector de ataque. Entre noviembre de 2020 y febrero de 2021, ESET descubrió cuatro casos de ataques a la cadena de suministro, un número muy alto en comparación con años anteriores.

Defenderse contra este tipo de ataque implica mantenerse al día con los parches, usar software de protección para endpoints, utilizar [soluciones EDR](#) y educar a los usuarios sobre los correos electrónicos no solicitados que los persuaden para que visiten sitios web desconocidos.

ATAQUES DE RANSOMWARE POR APROVECHAMIENTO DE VULNERABILIDADES

Si bien los ciberdelincuentes pueden beneficiarse tanto de las vulnerabilidades conocidas como de las desconocidas, el uso de vulnerabilidades o-day por lo general pertenece al mundo de los grupos APT y los actores maliciosos patrocinados por Estados. Más allá de la amenaza que supone el aprovechamiento de vulnerabilidades o-day, las vulnerabilidades conocidas proporcionan un dolor de

cabeza más que suficiente para los administradores de seguridad, investigadores y dueños de empresas por igual.

Un ejemplo es el hecho de que casi todos los fabricantes de seguridad cibernética todavía siguen detectando el exploit EternalBlue (de 2017) y sus muchas variantes, como así también el aprovechamiento continuo de vulnerabilidades en el protocolo SMBv1 de Microsoft para el intercambio de archivos. La larga vida útil de las vulnerabilidades y amenazas como WannaCryptor (también conocido como WannaCry) generalmente se debe a la falta de instalación de actualizaciones y parches en empresas e instituciones.

Paralelamente, la creciente complejidad del panorama de amenazas ha producido nuevas herramientas para combatir tipos de ataques más modernos, pero estas herramientas también implican una carga técnica adicional: estar atento a las vulnerabilidades de los productos y llevar a cabo una administración cuidadosa de los parches.

Es necesario destacar el enorme aumento en el uso y la dependencia de las VPN para los negocios y para el uso personal. Aquí me vienen a la mente dos casos en los que las vulnerabilidades identificadas en los servicios VPN de [Pulse Secure](#) y [Fortinet](#) permitieron la proliferación de ransomware entre los clientes. El uso de las VPN en grandes instituciones y empresas, si bien es altamente efectivo, añade una responsabilidad adicional con respecto a la actualización del producto cuando sea necesario. Este enfoque en las actualizaciones oportunas debe acompañarse por la implementación de la autenticación en varias fases para iniciar sesión en sus respectivos servicios VPN. Si surge la sospecha de un abuso de credenciales, las organizaciones deben restablecer las cuentas por completo.

Estos desafíos también se reflejan en el aumento global en el uso de grandes plataformas de productividad y colaboración. En marzo de 2021, estalló una actividad frenética entre los actores de amenazas, los principales fabricantes de software y la industria de la ciberseguridad en general cuando se descubrió que Microsoft lanzó actualizaciones de emergencia para corregir cuatro fallas o-day que afectaban a las versiones 2013, 2016 y 2019 de Microsoft Exchange Server. Posteriormente, se observó que los actores de amenazas aprovechaban las vulnerabilidades in-the-wild para acceder a los servidores de Exchange locales, lo que les permitía robar correos electrónicos, descargar datos e infectar máquinas con malware para obtener acceso a largo plazo en las redes de las víctimas.

Este evento a gran escala dejó a los [servidores de Exchange bajo el asedio de al menos 10 grupos APT](#). Los pensamientos de los investigadores de ESET se centraron rápidamente en comprender cuántas organizaciones habrían sido estudiadas e infiltradas por los delincuentes para futuros ataques, incluyendo de ransomware. ¿Cómo es el mecanismo más probable? Al afianzar su presencia en un servidor de Microsoft Exchange, los atacantes logran tener un acceso privilegiado a la empresa, posiblemente con derechos de administrador, y luego, con el tiempo, planean un próximo ataque.

Como se mencionó anteriormente en la sección sobre ataques a la cadena de suministro, el [ataque](#) de ransomware a Kaseya VSA afectó a más de 50 proveedores MSP y tuvo un impacto en más de 1.000 clientes finales. Los atacantes utilizaron una serie de vulnerabilidades o-day, incluyendo CVE-2021-30116, para comprometer Kaseya VSA, una herramienta de software de administración de TI muy popular entre los MSP. Los atacantes afirmaron haber atacado más de un millón de sistemas, lo que podría ser una exageración. La telemetría de ESET reveló víctimas en 17 países, entre los que se encuentran el Reino Unido, Sudáfrica, Canadá, Alemania y los Estados Unidos.

Si bien los primeros indicios de que los problemas de Kaseya se debían a un ataque a la cadena de suministro no se confirmaron, un ataque o-day de este tipo es muy grave y, de hecho, repercutió en la cadena de suministro. En resumen, debido a la popularidad de los sistemas de Kaseya, los impactos incluso se registraron en las empresas que apenas estaban conectadas tangencialmente a su plataforma VSA para MSP. A partir del 2 de julio, por ejemplo, la cadena de supermercados escandinava Coop tomó medidas para cerrar aproximadamente 500 tiendas debido al hecho de que el procesador

de pagos de terceros y el [proveedor de su sistema de caja registradora/PoS](#) utilizaban sistemas alojados en Kaseya. Por lo tanto, aunque Coop no estaba involucrado en forma directa, sí se vio significativamente afectado por depender de otro servicio que se cerró debido al ataque a Kaseya.

Los administradores de TI, los CISO y los miembros de la alta gerencia deberían haber tomado nota de la escala y el impacto de los incidentes de Microsoft Exchange y Kaseya para actualizar su enfoque tanto en el entorno de amenazas como en el impacto empresarial que puede tener el ransomware. Para obtener más información, consulte algunas de las vulnerabilidades mencionadas con más frecuencia en los informes públicos:

- [Kaseya VSA](#)
- [Pulse Connect Secure](#)
- [Citrix Hypervisor](#)
- [Fortinet VPN](#)
- Microsoft Exchange Server: lea la historia destacada en nuestro último [informe de amenazas](#)
- [Citrix Application Delivery Controller y Gateway](#)
- [Controles comunes de Microsoft Office](#)
- [Windows Win32k](#)
- [Accellion File Transfer Appliance](#)

NUBES Y SEGMENTOS

Independientemente del vector de ataque empleado por el ransomware, si ingresa a su organización, es muy probable que intente propagarse a tantas máquinas como pueda, lo que posiblemente afectará todas las operaciones de su empresa. Está claro que limitar la cantidad de máquinas a las que un atacante puede llegar desde un único punto de entrada tiene importantes beneficios como estrategia defensiva. Existen varios enfoques para implementar una estrategia de este tipo, el más importante de los cuales es la segmentación de la red.

El análisis de los detalles de la arquitectura de red está fuera del alcance del presente documento, y transformar una red “plana”, amplia y fácilmente transitable en una red segmentada puede ser desafiante y costoso (este [informe de KPMG](#) ofrece una perspectiva útil). No obstante, toda organización necesita comprender las fortalezas y debilidades de seguridad de su arquitectura de red actual. Una auditoría simple basada en preguntas y respuestas puede mejorar esa comprensión. Pregúntese: “¿Puedo ir de acá hasta allá?” o “¿Qué impide que alguien pueda llegar desde allá hasta acá?”.

Una estrategia de arquitectura de sistemas popular en los últimos años ha sido mover datos a la nube, pero la nube no proporciona inmunidad automática contra los ataques de ransomware (a pesar de los esfuerzos de proveedores poco escrupulosos para crear la impresión de que la nube es seguridad). De hecho, el bajo costo y la relativa facilidad con la que se pueden aprovisionar nuevos servidores en la nube y conectarlos al resto de la infraestructura digital de la organización ha convertido a la nube en un terreno de caza fértil para los delincuentes. Sin duda, cualquier uso de la nube por cualquier parte de la organización debe estar debidamente autorizado y configurado de manera segura. Además, como todos los demás sistemas, los que están en la nube deben tener programado un régimen apropiado de creación de backups y recuperación.

LOS PARCHES Y LOS BACKUPS COMO DEFENSAS CONTRA EL RANSOMWARE

La instalación de parches y la creación de backups son dos aspectos del funcionamiento y la administración de sistemas que desempeñan un papel fundamental en la defensa contra un ataque de ransomware. Al mantener un sistema con los parches al día, se cierran las posibles vías de ataque y puede evitar que el ransomware ingrese a su organización o, si lo hace, reducir el daño que pueda causar.

Por supuesto, como sabe todo administrador de sistemas, la aplicación de parches puede ser mucho más complicada de lo que parece. Los parches y las actualizaciones deben probarse antes de su implementación. Algunos de los sistemas de su organización pueden depender de software que deja de funcionar cuando actualiza a la última versión de una aplicación o sistema operativo. Sin embargo, el elevado costo de un ataque de ransomware dentro de su red justifica el esfuerzo de abordar esos desafíos y mantener un régimen de instalación de parches rápido y completo para que el ransomware se quede afuera.

Se suele decir que si el ransomware ingresa a su organización (ya sea a través de RDP, el correo electrónico, la cadena de suministro de software o un empleado con malas intenciones), un programa de backup y recuperación completo y adecuadamente administrado es un mecanismo de defensa vital y constituye un elemento crucial para la recuperación posterior.

Hay mucha verdad en esta afirmación y son varias las buenas razones para tener un programa de este tipo; pero recuerde que algunos ataques de ransomware se ejecutan en un período de tiempo prolongado, durante el cual también puede haber hecho un backup del ransomware, comprometiendo así la posibilidad de lograr una restauración sin problemas. Es por eso que el backup no es una defensa para configurar y olvidarse; debe ser monitoreado y administrado, y el proceso de recuperación debe probarse con regularidad.

En estos días, existen más opciones que nunca para hacer backups y recuperar los datos, en especial gracias al almacenamiento en la nube, ya sea de manera remota, local o híbrida. Sin embargo, también hay más datos para respaldar, desde más ubicaciones. A menos que tenga una estrategia de backup completa, siempre existe la posibilidad de que los actores que suministran el ransomware encuentren aquel dispositivo que olvidó incluir en el último backup.

Según Xopero, empresa experta en backups y miembro de la [Alianza Tecnológica de ESET](#), un backup completo incluye los datos y el estado del sistema en todas los endpoints, servidores, buzones de correo, unidades de red, dispositivos móviles y máquinas virtuales.

El análisis detallado de la estrategia de backup y recuperación para grandes corporaciones está fuera del alcance del presente white paper, pero debe quedar claro que contar con una estrategia de este tipo es más crítico que nunca. El ransomware simplemente se suma a la larga lista de razones por las que su organización no debe escatimar en esta parte del programa de TI. Sin embargo, existen algunas advertencias específicas para el ransomware. Por ejemplo, cuando el almacenamiento está "siempre activo", su contenido puede ser vulnerable al ransomware de la misma manera que lo es el almacenamiento local u otro conectado a la red.

Para evitar que lo intercepte el ransomware, opte por un almacenamiento externo que:

- no esté online en forma rutinaria y permanente;
- proteja los datos respaldados de modificaciones o sobrescrituras automáticas y silenciosas por malware cuando la instalación remota esté online;

- proteja las generaciones anteriores de datos respaldados contra las infecciones, de modo que incluso si ocurre un desastre en los últimos backups, al menos pueda recuperar algunos datos, incluyendo las versiones anteriores de los datos actuales; y
- proteja al cliente detallando las responsabilidades legales o contractuales del proveedor, por ejemplo, que indique qué sucede si el proveedor cierra, etc.

Tampoco subestime la utilidad de los medios de una sola escritura para archivar datos. Los archivos almacenados en medios que no se pueden reescribir son inmunes a los abusos del ransomware.

Por supuesto, existen muchas otras razones por las que su organización necesita implementar un programa de backup y recuperación, por ejemplo, en caso de incendios, inundaciones, daños por tormentas, etc.

CÓMO RESPONDER A UN ATAQUE DE RANSOMWARE

Además de erigir defensas contra el ransomware, todas las organizaciones deben estar preparadas para responder a cualquier ataque que logre penetrar dichas defensas. Durante esta preparación, es fundamental actualizar las políticas de seguridad corporativas para que abarquen el ransomware. Estas políticas deben especificar cómo deben responder los empleados de todos los niveles de la empresa a las demandas del ransomware. Asegúrese de que sus políticas respondan estas preguntas:

- ¿A quién deben informar los empleados si sospechan de la existencia de un ransomware?
- ¿Cuál es la política de la empresa sobre el pago de rescates de ransomware?
- ¿Quién será el encargado de pagar o negociar los pagos de rescate? Las políticas deben diseñarse para evitar los siguientes problemas:
 - Empleados que no informan sospechas de ransomware por temor a represalias.
 - Administradores de redes que prefieren pagar rescates porque es más fácil que recuperar sistemas a partir de backups.
 - Divulgación no autorizada de información sobre ataques de ransomware reales o sospechados.
- ¿Qué pasos está obligada a tomar la organización en caso de una vulneración de datos?
- ¿Cuál es la política de la empresa sobre el apagado de las máquinas afectadas? ¿Quién da esta orden? Apagar las máquinas elimina la evidencia potencial almacenada en la memoria y puede considerarse que no cumple con las regulaciones.

Después de actualizar las políticas de seguridad de la información para incluir la amenaza de ransomware, debe asegurarse de que sus programas de capacitación de empleados y concientización sobre seguridad incluyan contenido apropiado relacionado con el ransomware.

También querrá asegurarse de que sus planes de recuperación ante desastres, respuesta ante incidentes y crisis estén preparados en caso de un ataque de ransomware. A continuación, se muestra un resumen del terreno que debe cubrir su plan de respuesta:

- Ante los primeros signos de ataque, notifique al personal designado.
- Aísle y analice las máquinas afectadas.
- Apagado de equipos: Si no es posible aislar las máquinas afectadas, tome una imagen del sistema y una captura de memoria, luego apáguelas para evitar una mayor propagación del ransomware.
- Una vez confirmado el ataque, active su equipo de respuesta ante incidentes/crisis.
- Alerte al asesor legal.

- Comuníquese con proveedores que puedan ayudarlo.
- Recuerde a los empleados la política de prensa y redes sociales
- Evalúe el alcance del ataque y los detalles específicos del ransomware (por ejemplo, si hay una clave disponible).
- Póngase en contacto con la policía.
- Prepare una declaración de contención.
- Si los archivos fueron cifrados, determine si se pueden restaurar desde el backup.
- Mantenga a los empleados actualizados sobre el estado del ataque.

RULE NAME (54)	SEVERITY SCORE	TAGS	CATEGORY	ENABLED	VALID	LAST CHANGE DATE	SEVERITY	HIT COUNT
File used by DiskCryptor application has been written [C0618]	89	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:42 AM	High	0
RAR encrypts and detests files [B0901]	84	MITRE Tactic: Coll... MITRE Tactic: Imp... Ransomware Beh... Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	High	0
Archive Utility (7Zip) encrypting and deleting files [E0617]	84	Data Encryption MITRE Tactic: Coll... MITRE Tactic: Imp... Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:43 AM	High	0
Archive Utility (PKZIP) encrypting and deleting files [E0604]	84	Data Encryption MITRE Tactic: Coll... MITRE Tactic: Imp... Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:43 AM	High	0
Filecoder behavior [I0601]	81	MITRE Tactic: Imp... Ransomware Beh... Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:45 AM	High	6
Filecoder behavior [I0601]	81	MITRE Tactic: Imp... New	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:45 AM	High	0
File with extension used by Win32/Filecoder:JICWare has been written [C0615]	80	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	High	0
Win32/Filecoder:WannaCryptor clue has been found [C0614]	80	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	High	0
File with extension used by Win32/Filecoders:Crysis has been written [C0613]	80	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	High	0
File with extension used by Win32/Filecoder:CaracraB has been written [C0609]	80	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	High	0
File with extension used by Win32/Filecoder:HydraCrypt has been written [C0604]	80	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	High	0
Ransomware behavioral detection - filecoders [C0616]	80	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:42 AM	High	2
File used by Win32/Diskcoders D has been written [C0617]	80	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	High	0
File used by Win32/Diskcoders C has been written [C0616]	80	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	High	0
Encryption of files [B0602]	79	MITRE Tactic: Coll... MITRE Tactic: Imp... Ransomware Beh... Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	Medium	2
Ransomware file was written - filecoders [C0611]	78	MITRE Tactic: Imp... Ransomware IOC Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:41 AM	Medium	5
File with unexpected extension is written into locations: filebin [C0606]	73	MITRE Tactic: Imp... Suspicious Files Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:42 AM	Medium	920
Archive Utility (7Zip) encrypting files [E0608]	70	Data Encryption MITRE Tactic: Coll... MITRE Tactic: Imp... Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:43 AM	Medium	0
Archive Utility (WinZip) encrypting files [E0607]	70	Data Encryption MITRE Tactic: Coll... MITRE Tactic: Imp... Updated	Ransomware / Filecoders	Enabled	Valid	Jun 2, 2021, 7:07:43 AM	Medium	0

Imagen 6. // Panel de control de ESET Enterprise Inspector con reglas relacionadas con el ransomware

- Si es necesario, active su plan de continuidad empresarial.
- Recopile registros relevantes y posibles indicadores de sistemas comprometidos, como archivos binarios, notas de pedidos de rescate, direcciones IP, entradas de registro u otros archivos.
- Documente la investigación inicial del ataque y las medidas tomadas para remediarlo.

Es una buena idea tener al menos un escenario de ransomware en su manual de estrategias de planificación de crisis y analizarlo en un ejercicio de mesa con el personal relevante, incluyendo los directores. Esto puede revelar brechas en los planes de backup y recuperación, y ayudarlo a anticipar el impacto de no poder acceder a los servicios básicos debido a que los sistemas están cifrados (como el correo electrónico, las comunicaciones VoIP y el acceso a Internet).

DETECCIÓN Y RESPUESTA PARA ENDPOINTS

Existe una categoría de software de seguridad que puede ayudar a limitar el impacto de los ataques de ransomware y fortalecer su respuesta: se trata de las herramientas de detección y respuesta para endpoints, o EDR para abreviar. Ya sea como un conjunto de herramientas desarrolladas internamente o como un producto de seguridad integrado, la solución EDR puede ayudar en los esfuerzos manuales de cacería de amenazas en sus redes, así como a automatizar una amplia gama de medidas defensivas.

La Imagen 6 muestra varias reglas de EDR relacionadas con el ransomware diseñadas para alertar al personal de seguridad sobre actividades sospechosas (esta solución de EDR en particular es ESET Enterprise Inspector).

Una herramienta de EDR es capaz de monitorear todos los endpoints de su organización en busca de actividad anómala y sospechosa, como los cambios de las extensiones de archivos, que normalmente se observan durante los ataques de ransomware. Su equipo de seguridad definitivamente querrá que le notifiquen de inmediato sobre la presencia de herramientas de ataque como Mimikatz, creada para robar las credenciales de usuario de la memoria, o Cobalt Strike, usada a menudo por los atacantes para lograr persistencia en el sistema y ejecutar comandos de forma remota.

Los primeros signos de advertencia de intrusión se pueden configurar mediante reglas y alarmas. Se pueden refinar constantemente con datos nuevos provenientes de diversas fuentes de inteligencia de amenazas, como las listas de indicadores de sistemas comprometidos (IoC). Una buena solución de EDR incluirá reglas que le permitan al operador encontrar los sistemas comprometidos inmediatamente cuando se acciona la regla, aislar esos sistemas y luego diagnosticar el problema, incluyendo la reversión del historial de comandos ejecutados por los sistemas afectados. Estas capacidades demuestran que una solución de EDR incrementa la capacidad de su equipo de seguridad para frustrar ataques, responder a ataques y realizar análisis forenses después de un ataque.

DOS PALABRAS SOBRE EL PAGO DEL RESCATE

Esas palabras son: NO PAGUE. ¿Por qué? Porque [pagarle al delincuente que ha cifrado sus archivos significa que:](#)

- Está validando el modelo de negocio detrás del crimen.
- Está fomentando una mayor actividad delictiva.
- Está permitiendo que las bandas de ransomware investiguen las vulnerabilidades o-day y desarrollen nuevos exploits para aprovecharlas.
- Puede volver a ser víctima de futuros ataques y nuevas demandas de dinero.

Además, pagar a los delincuentes que han cifrado sus archivos de ninguna manera garantiza que obtendrá la clave de descifrado; después de todo, no es como si pudiera llevarlos a los tribunales o denunciarlos a Defensa al Consumidor. Existen numerosas razones por las que, aunque pague el rescate, es posible que no recupere sus archivos:

- Algunos de los datos pueden haberse dañado durante el proceso de cifrado y, por lo tanto, no se puedan recuperar.
- La herramienta de descifrado proporcionada puede incluir otro malware, no funcionar correctamente o ser mucho más lenta que la recuperación desde los backups.
- Existen numerosas formas en las que puede fallar el proceso de entrega de la clave de descifrado.
- El atacante actúa de mala fe y [no tiene ninguna intención de proporcionarle la clave de descifrado.](#)

Todo esto debería ser motivo suficiente para disuadir a las organizaciones de pagar las demandas del ransomware. De todas formas, para subrayar nuestro consejo, esto es lo que [dice](#) el FBI al respecto: "Pagar un rescate no le garantiza a la organización que recuperará sus datos; hemos visto casos en los que las organizaciones nunca obtuvieron la clave de descifrado después de haber pagado el rescate. Pagar un rescate no solo anima a los ciberdelincuentes actuales a atacar a más organizaciones, sino que también ofrece un incentivo para que otros delincuentes se involucren en este tipo de actividad ilegal. Y finalmente, al pagar un rescate, la organización podría estar financiando inadvertidamente otras [actividades ilícitas asociadas con los delincuentes](#)".

En la práctica, parece haber dos argumentos para pagar el rescate. El primero es “no podemos restaurar la información cifrada de los backups”. Esto podría deberse a que las copias de seguridad no existen, o existen pero están incompletas o dañadas de alguna manera. Sin embargo, puede haber otras alternativas. Antes de decidir enviar el dinero, consulte con su proveedor de software de seguridad (a) en caso de que esta sea una de las raras situaciones en las que ya exista una herramienta de descifrado disponible, lo que hace posible la recuperación sin pagar el rescate, y verifique (b) si se sabe que pagar el rescate no dará como resultado la recuperación de esa variante de ransomware en particular.

El segundo argumento común para pagar el rescate es que “es más barato que restaurar desde los backups”. Si esta afirmación se basa únicamente en cálculos de tiempo y mano de obra, podría ser técnicamente correcta, pero la decisión de pagar es, sin embargo, profundamente defectuosa por las razones expuestas anteriormente, en particular la falta de confiabilidad de las promesas de descifrado, la probabilidad de ser atacado nuevamente tras el primer pago (después de todo, usted no está tratando con ciudadanos respetuosos de la ley) y, por último, que con su pago está sustentando un ejercicio criminal, por lo tanto, está ayudando a aumentar la probabilidad de que se efectúen nuevos ataques a otros.

Quizás haya escuchado que algunos actores de ransomware ofrecen a las víctimas pruebas de que el descifrado funciona. Esto ocurre, pero puede provocar aún más problemas. Suponga que los atacantes le piden que les envíe un archivo cifrado que luego descifran y le devuelven como prueba de buena fe. Usted acaba de facilitar la divulgación del contenido de ese archivo a personas de dudoso carácter moral y, en caso de que el archivo contenga información de identificación personal, es probable que haya cometido un delito en virtud de una o más leyes de privacidad nacionales y regionales, que cada vez son más numerosas y estrictas.

Además, tenga en cuenta que eliminar el ransomware activo con software de seguridad no es de ninguna manera lo mismo que recuperar datos. Eliminar el ransomware y luego decidir pagar significa que es posible que los datos ya no se puedan recuperar incluso con la cooperación de los delincuentes, porque el mecanismo de descifrado suele ser parte del mismo malware. En otras palabras, si decide pagar, proceda con precaución.

EL FUTURO DEL RANSOMWARE

Exigir dinero para restaurar el acceso a sistemas y datos apunta a la “D” en la tríada de la CID, el clásico modelo de políticas de seguridad basado en la Confidencialidad, la Integridad y la Disponibilidad de la información. En esencia, el ransomware aprovecha la dependencia que la organización tiene de la tecnología y, por lo tanto, cuanto más dependen las organizaciones de la tecnología, mayor es el alcance del ransomware. Eso significa que podemos esperar que el ransomware persista y evolucione en el futuro (a menos que haya cambios imprevistos en la política y la economía globales).

Basándonos en nuestra experiencia con código malicioso desde finales de la década de 1980, podemos decir que las amenazas de malware tienden a evolucionar de la siguiente forma:

- se descubren vulnerabilidades en una nueva tecnología y se discute su potencial de abuso criminal;
- comienzan los esfuerzos para remediar y mitigar esas vulnerabilidades;
- los intentos de abuso criminal de la última tecnología son pocos al principio porque los criminales están ganando dinero fácilmente con las estrategias ya establecidas;
- al no haber un abuso delictivo generalizado, los esfuerzos de remediación y mitigación pierden fuerza;
- finalmente, los delincuentes descubren que esta “nueva” tecnología está lista para su aprovechamiento;

- surge una nueva tendencia de malware.

Algunos ejemplos incluyen ataques de denegación de servicio distribuidos que aprovechan los equipos de vigilancia conectados a Internet (Mirai) y la aparición de malware para routers (VPNFilter). En lo que respecta al ransomware, el crecimiento explosivo en el despliegue de dispositivos de la IoT (Internet de las cosas) mal protegidos está creando un panorama fértil para esfuerzos criminales futuros, al igual que el uso cada vez mayor de sistemas de control industrial conectados a Internet, edificios inteligentes y vehículos, incluyendo los vehículos autónomos (consulte el artículo "[RoT: el ransomware de las cosas](#)" y el webinar "[El ransomware desde el lado oscuro](#)").

Son varios los escenarios posibles en caso de que una caída en los ingresos de los delitos cibernéticos más establecidos lleve a los delincuentes a buscar nuevos modelos de ataque. El malware para routers podría limitar o bloquear el tráfico a menos que se pague un "peaje", con la amenaza de dañar el firmware del router o revelar el contenido del tráfico si la víctima intenta eliminar el malware.

Asimismo, se podrían bloquear remotamente vehículos, casas y edificios para extorsión. La manipulación de los BAS (sistemas de automatización de edificios), capaces de controlar el acceso al edificio, la calefacción, la ventilación y el aire acondicionado, podría servir como base para métodos de extorsión, y [ya estamos viendo señales de esto](#). En cuanto a los robots comerciales, ya se ha demostrado la viabilidad de que sufran ataques de ransomware.

Estos escenarios de ransomware en evolución tienen múltiples implicaciones para las empresas. Le recomendamos prepararse de la siguiente manera:

- Empiece a contemplar estas amenazas potenciales en su estrategia y planificación de gestión de riesgos.
- Comience ahora mismo a manejar los activos que puedan convertirse en objetivos del ransomware: dispositivos de la IoT, routers de oficinas pequeñas y domésticas, robots, sistemas de control, sistemas autónomos.
- Haga un seguimiento de los informes de vulnerabilidades relacionados con estos activos.
- Mantenga al día los parches y las actualizaciones de firmware para estos activos.
- Segmente los dispositivos de la IoT y otras nuevas tecnologías de las redes de producción.

CONCLUSIÓN

Los datos, las técnicas y los casos del mundo real presentados en este documento muestran que el ransomware realmente se ha convertido en la amenaza cibernética más importante en la actualidad. Su aumento se puede atribuir en gran medida al desarrollo de la técnica de doble extorsión (o doxing), iniciada en 2019 por la banda Maze, ahora retirada. Además de cifrar los dispositivos de sus víctimas, los operadores de este infame grupo de ransomware también robaban los datos más valiosos y confidenciales, y luego amenazaban con publicarlos.

Otros actores de ransomware pronto siguieron su ejemplo, añadiendo más piezas a esta base efectiva de doble extorsión. Se introdujeron nuevos métodos, dirigidos no solo a los datos de las víctimas, sino también a sus sitios web, empleados, socios comerciales y clientes, con el objetivo de aumentar la presión y, por lo tanto, la disposición a pagar.

Aprovechando el caos y la inseguridad de la pandemia, las bandas de ransomware también comenzaron a acceder a los sistemas mediante fuerza bruta a través del protocolo RDP, transformándolo finalmente en una de sus principales vías de ataque. Sin embargo, las campañas de [malspam](#) que entregaban macros maliciosas, enlaces peligrosos y binarios de botnets no desaparecieron; por el contrario,

siguieron bombardeando a las víctimas potenciales además de los miles de millones de ataques de adivinación de contraseñas.

Debido a la mayor efectividad de las técnicas de extorsión y los nuevos canales de distribución, se estima que cientos de millones de dólares han terminado en las cuentas de estos ciberdelincuentes técnicamente habilidosos, lo que les permite desarrollar su modelo de negocio de ransomware como servicio e incorporar numerosos nuevos afiliados. Aliviados del “trabajo sucio”, algunas de las bandas comenzaron a adquirir vulnerabilidades o-day y a comprar credenciales robadas, lo que expandió aún más el grupo de víctimas potenciales.

El creciente número de incidentes de ransomware conectados indirectamente a ataques a la cadena de suministro representa otra tendencia preocupante que podría indicar la dirección en la que estas bandas se encaminarán a continuación.

Como el dinero, la ambición y la determinación están principalmente del lado de las bandas de ransomware, aprender de las historias de pesadilla y los análisis que se informan a diario en los medios se ha convertido en una necesidad para todo profesional de TI y seguridad. Se ha demostrado una y otra vez desde principios de 2020 que la aplicación de políticas, la configuración adecuada y las contraseñas seguras combinadas con la autenticación en varias fases pueden ser elementos decisivos en la lucha contra el ransomware. Muchos de los incidentes mencionados en este documento también destacaron la importancia de la instalación oportuna de parches, ya que las vulnerabilidades conocidas se encuentran entre los vectores de ataque de estos ciberdelincuentes.

Para contrarrestar las vulnerabilidades o-day, las botnets, el malspam y otros métodos técnicamente más avanzados, se necesitan tecnologías de seguridad adicionales: por un lado, una solución de protección para endpoints de varias capas, capaz de detectar y bloquear amenazas entrantes provenientes del correo electrónico, enlaces, RDP y otros protocolos de red; y por el otro, una herramienta de respuesta y detección para endpoints que monitoree, identifique y aisle anomalías y signos de actividad maliciosa en el entorno de una organización.

Las nuevas tecnologías, si bien aportan beneficios a la sociedad, también constituyen un campo de oportunidades en constante expansión para los ciberdelincuentes. Esperamos que, al explicar la gravedad que ha adquirido la amenaza del ransomware y lo que se puede hacer para defenderse de ella, el presente documento ayude a que se protejan esos beneficios tecnológicos y a la vez se minimicen las pérdidas causadas por los malos actores.

ACERCA DE ESET

Por más de 30 años, ESET® ha estado desarrollando software y servicios de seguridad informática líderes en la industria para proteger a las empresas, la infraestructura crítica y los consumidores en todo el mundo ante las amenazas digitales cada vez más sofisticadas. Desde la seguridad para endpoints y dispositivos móviles hasta la detección y respuesta para endpoints, además del cifrado y la autenticación en varias fases, las soluciones de alto rendimiento y fáciles de usar de ESET brindan protección y supervisión en forma discreta las 24 horas, los 7 días de la semana, y actualizan las defensas en tiempo real para mantener a los usuarios seguros y a las empresas funcionando sin interrupciones. Las amenazas en evolución exigen que las empresas de seguridad de TI también estén en constante evolución para permitir el uso seguro de la tecnología. ESET cuenta con el respaldo de sus Centros de investigación y desarrollo distribuidos en todo el mundo, que trabajan para apoyar nuestro futuro compartido. Para obtener más información, visite www.eset-la.com o síganos en [LinkedIn](#), [Facebook](#) y [Twitter](#).



ENJOY SAFER TECHNOLOGY™