RANSOMWARE: UNA PERSPECTIVA CORPORATIVA

Author:
Stephen Cobb

2018

ENJOY SAFER TECHNOLOGY™

CONTENIDO

OBJETIVOS Y RESUMEN EJECUTIVO

Los objetivos de este documento son explicar por qué el ransomware sigue siendo una amenaza seria para tu organización – sin importar el tamaño – y qué puede hacer tu organización para reducir la exposición a, y los daños de, ataques de ransomware. Se hace referencia a tres vectores de ataque, en el siguiente orden: acceso remoto, correo electrónico y *supply chain*. Dirigido en principio a una audiencia ejecutiva, este documento debería ser útil para CEOs, CIOs, CISOs, y gestores de riesgo (risk managers). Los aspectos más técnicos de la respuesta al ransomware se incluyen en el Apéndice B.

LA AMENAZA DEL RANSOMWARE

Un ataque de ransomware puede definirse como un intento de extorsionar a una organización denegando el acceso a su información. El ransomware es un tipo de malware, término colectivo para todas las formas de código malicioso, incluyendo los virus informáticos y gusanos.

Los ataques de ransomware difieren de la denegación de acceso a la información al eliminarla o borrarla por completo, aunque algunos malware que se presentan a sí mismos como ransomware puede destruir la información (wiperware) y/o dejar a los sistemas inoperables (brickware). Por ejemplo, el conocido y extremadamente costoso brote de malware llamado NotPetya/Diskcoder.C suele ser asociado con WannaCryptor/WannaCry cuando se habla de ransomware; sin embargo, NotPetya era una combinación de wiperware y brickware, eliminando la posibilidad de descifrar archivos, y modificando a su vez el código MBR (registro de arranque principal o maestro, por sus siglas en inglés) **"de manera tal que la recuperación no fuera posible"**.

Un ataque de ransomware difiere también de un ataque de denegación de servicio (DoS), que no permite el acceso a los sistemas al sobrecargarlos de tráfico, pero no daña intencionalmente la información. La capacidad de llevar a cabo un ataque DoS podría utilizarse por un extorsionista para amenazar al operador de un sitio web comercial, **demandando un pago a cambio** de no dejar su sitio temporalmente inhabilitado. Esta clase de ataques suelen ir dirigidos a organizaciones que operan sitios de ventas, ya que dejarlos sin funcionamiento por un breve período de tiempo puede afectar sus ingresos ampliamente. También vemos **ataques DoS utilizarse para el hacktivismo,** así como para **atacar competidores.**

La idea de secuestrar información y sistemas no es nueva. Donn Parker citó un caso de 1971 en su emblemático libro *Crime by Computer*. La mayoría de los expertos en seguridad consideran al **troyano AIDS de 1989 del Dr. Popp** como la primera pieza de ransomware basado en cifrado, es decir que los archivos de la víctima eran cifrados por el atacante, quien prometía descifrarlos a cambio de un pago.

Afortunadamente, este primer intento no se convirtió en una tendencia, y pasaron algunas décadas hasta que el ransomware se volvió protagonista del crimen informático. Si bien el brote de WannaCryptor en 2017 logró acaparar varios titulares en las noticias en el mundo, el ransomware ha estado dominando las noticias sobre malware durante los últimos cinco años. Por ejemplo, una de las cinco páginas más visitadas en el **portal de noticias WeLiveSecurity** es el artículo **"11 cosas que puedes hacer para protegerte contra el ransomware, incluyendo Cryptolocker"**, escrito por la investigadora de ESET Lysa Myers en 2013. Aquí enumeramos algunos otros números que reflejan la escala del problema del ransomware:

- Los ataques de ransomware aumentaron un 350% a nivel mundial, de 2016 a 2017 (Dimension Data, 2018)
- El 48% de los consultores de informática a lo largo de 22 industrias diferentes notaron un aumento en las consultas de soporte relacionadas al ransomware en el último año (Intermedia, 2017)
- El 25% de los reclamos de seguros infomáticos en 2017 fueron por ransomware (AIG, 2018)
- Las pérdidas totales por el ransomware WannaCry podrían alcanzar los $4 billones (Cyence, 2017)
- El 72% de las empresas afectadas por el ransomware perdió acceso a su información por al menos dos días; el 32% perdió acceso durante 5 días o más (Intermedia, 2017)

Lamentablemente, aun existiendo números como estos, las organizaciones siguen siendo golpeadas por ataques costosos de ransomware, aun cuando han comenzado a circular rumores sobre la muerte del ransomware.

SÍ, EL RANSOMWARE SIGUE SIENDO UNA AMENAZA SERIA

Si tu organización ha sido víctima de ransomware recientemente, entonces el objetivo de este White Paper – explicar por qué el ransomware sigue siendo una amenaza seria para tu organización – podrá sonar como una obviedad. Sin embargo, si tu organización no ha sido afectada por esta amenaza en el último tiempo, podrías estar bajo la ilusión – creada por algunos titulares durante 2018 – de que el ransomware está comenzando a desaparecer:

- **The Decline of Ransomware and the Rise of Cryptocurrency Mining**
- **Cybercriminals Move from Ransomware Attacks to Crypto Mining**

- **Why cryptomining is the new ransomware**
- **Ransomware is so 2017**
- **Banking Trojans Replace Ransomware As Top Malware In Email For First Time Since 2016**

Por supuesto, los titulares no cuentan la historia complete, y en algunos de estos artículos hallarás alertas sobre el ransomware aun siendo una amenaza. Sin embargo, el uso de términos como "ascenso y caída" para describir las tendencias de malware opaca dos realidades importantes de la ciberseguridad: los riesgos de los sistemas de información son cumulativos, y la actividad criminal es difícil de medir (especialmente en el ciberespacio).

Toma en consideración lo que ha sucedido con la minera ilegal de criptomoneda, el uso no autorizado de recursos informáticos para crear valor monetario en formato de moneda digital, como Bitcoin, Ethereum o Monero. Los investigadores de seguridad han documentado una tendencia en este tipo de actividad en 2018: criminales utilizando técnicas variadas asociadas al phishing y otras formas de distribución de malware para poder ingresar sus códigos de minería generadores de valor en tus computadores. Sin embargo, es importante destacar que este tipo de minería de criptomoneda es más fácil de detectar y rastrear para los proveedores de seguridad que algunas otras formas de de cibercrimen.

En resumen, los titulares de arriba reflejan el hecho de que, mientras las detecciones de criptominería han ido en aumento, algunos de los principales indicadores de actividad de ransomware han ido disminuyendo. Pero para ser claros, el ransomware sigue siendo una amenaza para tu organización. De hecho, el peligro de esta amenaza podría estar en su máximo. ¿Por qué? Porque en los últimos dos años algunos criminales han estado perfeccionando una manera de abordar el ransomware diferente, más apuntada, para la cual las métricas resultan más difíciles de obtener.

Hemos visto un viraje en la tendencia de apuntar a grandes grupos de personas, demandando modestas sumas de dinero por un rescate, hacia una de solicitar grandes rescates de grupos de víctimas más selectos y adinerados (que no pueden permitirse perder el acceso a su información). Esto ha dado como resultado los siguientes titulares (en inglés):

- **Atlanta ransomware attack may cost another $9.5 million to fix**
- **City of Farmington, N.M., recovering after SamSam ransomware attack**
- **Davidson County, N.C., Still Reeling from Ransomware Attack**
- **Ransomware Attacks Against Riverside, Ohio, Worse than Initially Thought**
- **Ransomware strikes CDOT for second time even as agency still recovering from first SamSam attack, Denver, CO**
- **MVSU Campus Loses Internet After Ransomware Attack, Itta Bena, MS**
- **Ransomware costs continue to climb for Wasaga Beach, Ontario, Canada**
- **Ransomware recovery a work in progress, Coweta County, GA**
- **Ransomware attack forces town's employees to go back to typewriters, Anchorage, AK**

Si bien perder fotografías familiares por culpa del ransomware puede ser doloroso, estos titulares tratan de crímenes cibernéticos que han causado grandes pérdidas financieras, e impactado sobre millones de personas.

Por ejemplo, luego de que la Ciudad de Atlanta se negara a pagar los $50.000 dólares que el ransomware solicitaba, los costes siguieron en aumento (**y podrían llegar a los $17 millones**). Cinco departamentos de la ciudad han tenido que hacer su trabajo sin computadores durante una semana: Correcciones, Administración de Cuencas Hidrográficas, Recursos Humanos, Parques y Recreación y Planificación Urbana. Los servicios impactados por los ataques incluyeron al servicio de pago en línea de los impuestos de agua y tickets de tráfico. También fue dado de baja el servicio Wi-Fi del Aeropuerto Internacional de Atlanta Hartsfield-Jackson, durante una semana.

Si prestas atención a los ataques mencionados, verás que en todos los casos la víctima es una organización del sector público. ¿Significa esto que el sector privado está a salvo de dichos ataques? Desafortunadamente, la respuesta es no. Las empresas comerciales gozan de inmunidad no sectorial del ransomware dirigido (o cualquier otra forma de cibercrimen, en realidad).

APUNTANDO A ESCUELAS, HOSPITALES Y CORPORACIONES

El motivo por el cual vemos titulares que hablan de ransomware en el sector público es justamente que son públicos, y ciertos servicios públicos se vieron afectados. Pero eso no significa que los criminales estén limitando sus objetivos de víctimas al sector SLED (State and Local Government and Education). Observa este otro grupo de titulares (en inglés):

- **Ransomware attack targets Adams Memorial Hospital, Decatur, IN**
- **ECMC spent nearly $10 million recovering from massive cyberattack, Buffalo, NY**
- **Hospital pays $55,000 ransom; no patient data stolen, Greenfield, IN**
- **Allscripts sued over ransomware attack, accused of 'wanton' disregard**
- **LabCorp 90% recovered from SamSam ransomware attack, Burlington, NC**

Estas organizaciones están dentro del sector de la salud, otro sector en el que se hace difícil esconder un ataque de ransomware que impacta servicios, especialmente cuando las regulaciones gubernamentales pueden requerir su divulgación, y la **seguridad de los pacientes entra en riesgo**.

¿Pero qué sucede con las organizaciones que no tienen la obligación de dar a conocer información sobre las brechas de seguridad? Es lógico asumir que una empresa comercial que es víctima de un ataque de ransomware intentará evadir los titulares en cuanto le sea posible. Y eso significa que no podemos depender de los reportes de ataques de ransomware publicados para evaluar la escala de la amenaza. Lo que sí conocemos, gracias a dialogar con equipos de soporte de Proveedores de Servicios Gestionados y proveedores de seguridad, es que el ransomware sigue siendo un crimen costoso que no escasea en víctimas.

Sabemos también que un número de estos ataques de ransomware de 2018 en entidades de gobierno y servicios de salud involucró a una familia

de ransomware conocida como SamSam (detectada por los productos de ESET como **MSIL/Filecoder.Samas**). SamSam ha estado presente desde 2016, explotando varios vectores de ataque diferentes, pero a principios de 2018 los investigadores comenzaron a sospechar que los ataques de SamSam estaban penetrando organizaciones "con ataques de fuerza bruta sobre endpoints RDP" (**Departamento de Salud y Servicios Sociales de los Estados Unidos**

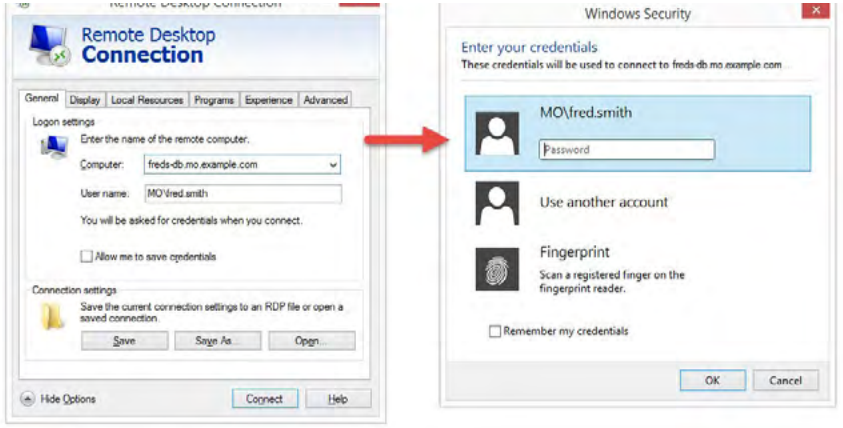
EL FACTOR RDP

Un endpoint RDP es un dispositivo, al igual que un servidor de base de datos, que está ejecutando un software de protocolo de escritorio remoto (RDP, por sus siglas en inglés), para que el dispositivo pueda ser accedido a través de una red, por ejemplo, Internet. Si un nombre de usuario y contraseña son requeridos para acceder al dispositivo, entonces el atacante, habiendo identificado al servidor como un objetivo de ataque, hará varios intentos para adivinar las credenciales, generalmente a altos niveles de velocidad, por ello el término: ataque de fuerza bruta. Al no haber un mecanismo que limite los múltiples intentos errados, dichos ataques pueden ser muy efectivos.

Obtener acceso no autorizado a dispositivos que se ejecutan con servidores RDP puede requerir un esfuerzo inicial mayor que con el ransomware enviado por correo, pero aquel vector ofrece a los atacantes varios beneficios, como el potencial para evadir la protección endpoint y comprometer rápidamente múltiples sistemas dentro de una única organización. Veamos el ataque de ransomware mediante RDP contra Lab Corp, uno de los laboratorios clínicos más grandes de Estados Unidos, en julio de 2018; si bien la compañía logró contener el ataque dentro de los primeros 50 minutos desde que se inició, ya había impactado para ese momento 7000 sistemas y 350 servidores de producción (**CSO**).

Los ataques mediante RDP pueden pasar desapercibidos para muchos métodos de detección, resultando en menos métricas y conciencia sobre el peligro de las amenazas. Por ejemplo, cualquier organización que cuente con un programa de seguridad informática estable será capaz de detectar y bloquear una pieza de ransomware enlazada a un archivo adjunto en un correo. Esta clase de incidentes suelen ser registrados y reportados por programas de protección endpoint, y los proveedores de dichos programas conforman sus estadísticas de tendencias de amenazas a través de estos reportes. Lo mismo puede decirse de los intentos de engañar a los usuarios para que ingresen a sitios infectados que propagan ransomware. Sin embargo, si un atacante con privilegios de administrador de un sistema en un servidor comprometido apaga la protección endpoint antes de dirigir el ransomware para que cifre los archivos de esa máquina, el ataque bien podría eludir los típicos parámetros del malware.

El objetivo del RDP es habilitar los recursos informáticos de una organización para que puedan ser accedidos remotamente. Hay numerosas razones legítimas para implementar RDP – por ejemplo, proveer a una amplia base de datos central, o ejecutar una aplicación especializada de software compartida entre múltiples usuarios.

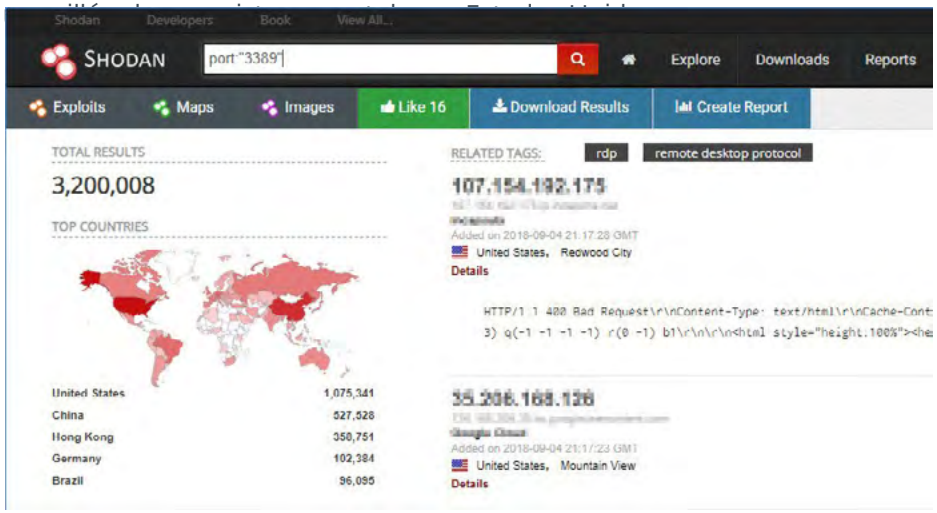


dos formas en las que las organizaciones utilizan RDP. La primera es para administrar programas que se ejecutan en un servidor, por ejemplo, un sitios web o base de datos en el back-end. En este escenario, el administrador de sistemas abre el puerto 3389 al mundo externo para permitir la administración remota mediante una cuenta de administrador. Un segundo uso del RDP es para permitir que múltiples usuarios sin permiso de administrador ingresen a un sistema compartido para hacer tareas diarias. Esto puede realizarse dentro de la red de la compañía, o a través de internet, en cuyo caso el puerto 3389 se vuelve accesible al mundo externo.

Para quienes tienen intenciones maliciosas, hallar cualquiera de estos tipos de servidor, accesibles al mundo externo, y luego utilizarlos para ejecutar sus ataques resulta bastante sencillo, porque:

- Los servidores vulnerables son fáciles de hallar
- Es sencillo para los atacantes posicionarse en servidores RDP si éstos están en su configuración predeterminada
- Muchos servidores RDP tienen configuraciones débiles o predeterminadas
- Las herramientas y técnicas para obtener privilegios y así derechos de administrador en servidores RDP comprometidos son ampliamente conocidas y fáciles de conseguir

Los servidores ejecutados en RDP pueden identificarse por motores de búsqueda especializados, como **Shodan**, que examinan Internet constantemente en búsqueda de dispositivos conectados y reúne información sobre ellos. El 1 de septiembre de 2018, Shodan indicó que había cerca de 3 millones de sistemas en Internet utilizando el **puerto 3389** (puede ser necesario registrarse para ver los resultados filtrados de Shodan). Como podrás ver en la interfaz de Shodan en la Figura 2, Más de



Modificando la búsqueda, se hallaron más de dos millones de equipos ejecutando RDP explícitamente. Para un atacante, todas aquellas máquinas son objetivos potenciales de ser explorados. Si bien ingresar a un servidor RDP suele requerir un nombre de usuario y contraseña, éstas pueden resultar sorprendentemente sencillas de adivinar por los atacantes, y muchos harán uso de ataques de fuerza bruta (intentos repetidos de ingresar utilizando una base de datos de posibles credenciales).

Para los atacantes que cuentan con fondos suficientes, adquirir acceso a servidores comprometidos puede ser un atajo. En los mercados de la dark web se ofrecen credenciales de servidores. Por ejemplo, el sitio xDedic provee a potenciales compradores de una amplia variedad de información sobre sus ofertas de servidores, permitiéndoles definir objetivos tanto geográfica como logísticamente, (filtras y eliges por versión de SO, CPU, RAM, velocidad de conexión, aplicaciones instaladas, estado de blacklist,

antivirus instalado, y más). Para saber más sobre las credenciales en el mercado negro, mira el Apéndice A.

Ten en cuenta que los ataques dirigidos de ransomware no son la única razón para adquirir credeciales de servidores vulnerados. De hecho, la documentación de xDedic enlista 12 usos diferentes para un servidor comprometido, incluyendo el envío de spam, hospedaje de malware, cracking de contraseñas, minería de criptomonedas y una serie de actividades para la cual es deseable el anonimato, y no la atribución; piensa en las compras fraudulentas y el lavado de dinero. El sitio también ofrece herramientas para explotar servidores una vez que obtienes acceso.

"Pívot" y "vivir de la tierra"

Para el atacante, un servidor comprometido puede significar mucho más que solicitar dinero para descifrar los archivos de esa máquina, especialmente si el servidor puede significar un punto de entrada a una red de dispositivos completa, deshabilitando potencialmente el cifrado a gran escala de información crítica. Eso es lo que sucedió en muchos de los casos presentados en los titulares citados anteriormente, y las técnicas para llevar a cabo este tipo de ataques no son ningún secreto.

Además de lograr acceso remoto, el atacante querrá aprender más sobre el equipo comprometido, evaluando su potencial para abusarlo, incluyendo el mapeo de conexiones a otros sistemas. Si el acceso no se consiguió con credenciales de administrador, diversas técnicas pueden utilizarse para "escalar privilegios" a nivel de '*admin*'. Si hay protección endpoint instalada en el sistema, y ésta puede ser apagada por el usuario que tiene privilegios de administrador, el atacante probablemente lo haría. Esto le facilita la descarga de software adicional, en base a una evaluación del potencial de abuso del sistema. (Ten en cuenta que cuando se describen las acciones como llevadas a cabo "por el atacante" no necesariamente se realicen por una persona con un teclado, sino con un software utilizado para automatizar ciertos aspectos del ataque).

Ciertos atacantes intentarán introducir la menor cantidad de código malicioso como sea posible para minimizan las chances de una detección. Implementarán en cambio una estrategia de "vivir de la tierra", utilizando software legítimo para extender la penetración de la red. Por ejemplo, el malware NotPetya utilizaba dos herramientas populares, PsExec y Windows Management Instrumentation Command-line (WMIC) para lograr un movimiento lateral en la red comprometida. Existen razones válidas para que se ejecuten estos programas, por lo cual detector un uso abusivo por un atacante puede ser difícil, aunque no imposible (mira la última discusión de herramientas EDR).

El término "pívot" se usa para describir la estrategia de obtener acceso a un sistema y utilizarlo para comprometer todos los dispositivos que puedan ser alcanzados desde allí. Por ejemplo, en el ataque a un hospital en Greenfield, Indiana, citado anteriormente, los atacantes "utilizaron credenciales de acceso comprometidas para apuntar a un servidor localizado en el centro de respaldo informático de emergencia que empleaba el hospital – ubicado a varios kilómetros de distancia del campus central – e hicieron uso de las conexiones electrónicas entre el sitio de backup y el grupo de servidores en el campus central del hospital para ejecutar SamSam" (Reporte del **Departamento de Salud y Servicios Sociales de los Estados Unidos**).

Además de vivir de la tierra, los ataques de ransomware pueden sacar ventaja de las vulnerabilidades que no tiene parches en sistemas de software legítimos. Por ejemplo, hay ransomware que se distribuye el **exploit de EternalBlue**, que apunta a una vulnerabilidad en algunas versiones de la implementación del protocolo SMB (Server Message Block) de Microsoft (mira el **boletín de seguridad de Microsoft MS17-010**, en inglés). En los casos no emparchados del protocolo de intercambio de archivos de la red fueron abusados por el infame ransomware WannaCry

(excepto en los sistemas que estaban ejecutando productos de seguridad endpoint que bloqueaban **EternalBlue**).

Es posible que, en ciertos casos, el primer punto de contacto de un atacante con una organización sea un servidor ejecutado una base de datos crítica para la empresa, en cuyo caso un criminal oportunista podría decidir ahorrar algo de tiempo y esfuerzo y buscar una victoria rápida cifrando y secuestrando los archivos utilizados por ese único activo.

Defendiéndote de los ataques de ransomware mediante RDP

Afortunadamente, es posible proteger los servidores que ejecutan RDP contra acceso no autorizado, y privar a los criminales de este vector de ataque cada vez más popular, ya sea que estén proveyendo ransomware o involucrados en el abuso de algún otro acceso no autorizado al sistema. Si bien en esta sección hablamos de estrategias para protegerse, ofrecemos una lista más específica de técnicas anti-ransomware en el Apéndice B.

Por supuesto, tu organización podría contar ya con las políticas adecuadas en relación a la seguridad de accesos remotos. Podrías tener reglas que requieran que todos los accesos de RDP sean conducidos por una VPN, asegurados por 2FA (doble factor de autenticación), limitados a roles específicos, en sistemas específicos que estén configurados adecuadamente, emparchados rápidamente, monitoreados constantemente, reforzados apropiadamente mediante un firewall, y respaldados regularmente.

Sin embargo, debe decirse que, ya sea que tengas dichas reglas establecidas o estés trabajando en establecerlas, las reglas por sí solas no asegurarán que el acceso remoto no sea vulnerado. Debes asegurarte que todos están cumpliendo con ellas, y estar preparado a la vez para manejar un ataque que podría ser exitoso a pesar de esas reglas.

Un primer paso clave para defenderse contra ataques de ransomware mediante RDP es hacer un inventario de tus activos con acceso desde Internet. Decir que un sistema no puede ser protegido si no eres consciente de su existencia parece algo obvio, pero, basándonos en nuestras investigaciones, el siguiente escenario no parece tan inusual: una organización es atacada mediante un activo conectado a Internet del cual los encargados de seguridad de la organización no tenían conocimiento antes de suceder el ataque.

Para asegurar que eso no suceda en tu organización, necesitas de procesos. Por ejemplo, no debería ser posible ni para un contratista ni para un empleado conectar un servidor físico o virtual a la red de la compañía o a Internet, a no ser que ese servidor este correctamente configurado; dicha configuración debe darse antes de que el servidor se conecte, especialmente si el mismo ejecuta protocolo RDP con una cuenta de administrador.

Caso de estudio: el incidente de seguridad de CDOT

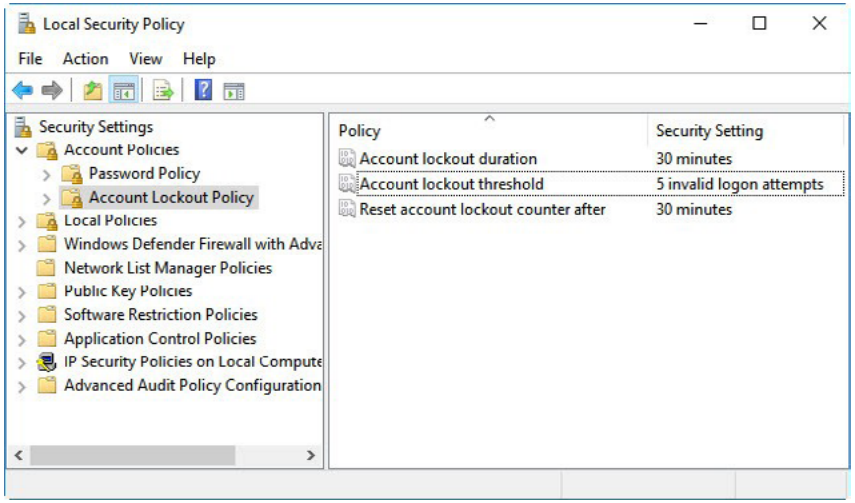
Según un reporte lanzado al público, el vector de ataque de ransomware al Departamento de Transportes de Colorado (CDOT, por sus siglas en inglés), que ocurrió en febrero de 2018, fue un servidor virtual conectado a Internet que fue comprometido dentro de los dos días posteriores a su creación. Los atacantes "ingresaron a la cuenta de Administrador utilizando aproximadamente 40.000 intentos de contraseñas hasta que la misma se vio comprometida".

Una vez que hayas terminado de crear tu inventario de activos con acceso desde Internet, debes documentar cuáles tienen habilitado el acceso remoto, y luego decidir si ese acceso es necesario. Si lo es, determina luego si es o no posible ubicar esos sistemas en la red interna y acceder a ellos

utilizando una VPN corporativa.

Si un sistema debe estar habilitado para ser accedido desde Internet público via RDP, y utilizar una VPN no es posible, instala al menos el 2FA, para que tu protección no dependa únicamente de contraseñas. Pero asegúrate de utilizar una solución de doble factor que no esté basada en SMS. Los criminales tienen múltiples maneras de frustrar la autenticación basada en SMS (comúnmente desarrollado por creadores de malware que apuntan a clientes de bancos en Europa, donde el 2FA basado en SMS ha sido utilizado durante años para confirmar las transacciones bancarias).

Si te ves obligado a depender de contraseñas porque el 2FA no está disponible – posiblemente debido a políticas presupuestarias limitadas – al menos pon un freno a los atacantes que realizan múltiples intentos repetidos por adivinar las credenciales. Establece un máximo de quizás cinco intentos de ingreso inválidos, después de los cuales los intentos no son reconocidos por un período de tiempo establecido, por ejemplo, 30 minutos. En la Figura 3 puedes ver cómo se refleja esto en Windows.



También puedes modificar el puerto RDP "en escucha", de 3389 a algo distinto, para dificultar a los atacantes que encuentres las máquinas accesibles. Esto puede lograrse desde los ajustes del sistema, pero necesitarás también modificar las reglas del firewall para adaptar el puerto designado. Ten en cuenta que esto no es más que seguridad por oscuridad, y no debería dependerse de ello para mantener protegidos a los sistemas RDP (mira el Apéndice B para más detalles).

La securización y el emparchado debería realizarse para todos los dispositivos con acceso remoto. Uno de los motivos por los que el ransomware WannaCry se distribuyó tan rápido, fue el alto número de versiones obsoletas del protocolo SMB, sin emparchar. Aparte de asegurarte que todas las vulnerabilidades de seguridad han sido identificadas y remediadas, querrás tener certeza de que todos los servicios y componentes no esenciales han sido eliminados o deshabilitados, y que los ajustes se han realizado para garantizar la máxima seguridad. Por ejemplo, en los sistemas de Windows puedes utilizar Directivas de Restricción de Software (SRP, por sus siglas en inglés) para prevenir que los archivos se ejecuten desde carpetas como AppData y LocalAppData, que a veces son utilizadas por el malware.

Por su puesto, la última línea de defensa contra el ransomware vía RDP es un sistema de recuperación y backup comprehensivo y probado. Dado que el backup es clave para sobrevivir al ransomware, sin importar cuál sea el vector, el tema entrará en discusión, tras considerar otros dos vectores.

Ransomware mediante correo electrónico y otros vectores

Como dirá cualquier experto en seguridad: las amenazas que atacan sistemas de información son acumulativas. Por ejemplo, solo por el hecho de que ciertos criminales se hayan enfocado en servidores con acceso

remoto habilitado como sus nuevos vectores de ataque de ransomware, no significa que puedas ignorar otros vectores. Algunos siguen utilizando adjuntos de correo para instalar ransomware. Pueden hacerlo para instalarlo en la máquina del receptor, o para obtener acceso a un dispositivo conectado a la red de una organización. Ese acceso puede ser la base para intentar cifrar archivos de la compañía, previo a solicitar grandes sumas de dinero para devolver la información, como en el caso de los ataques de ransomware dirigidos vía RDP descriptos anteriormente.

Cuando se trata de proteger a tu organización contra ataques de ransomware a través del correo, la primera línea de defensa es filtrar todos los correos recibidos en busca de spam y phishing. Ya existían varios motivos válidos para hacer esto incluso antes de que el correo se convirtiera en una vía para los ataques, y muchas organizaciones ya cuentan con filtrado básico de spam y detección de phishing establecidos.

Tal vez quieras ir más allá e implementar un bloqueo a todos los tipos de adjuntos que tu organización no suele utilizar; sin embargo, la posibilidad de implementar esta estrategia dependerá del tipo de negocio en el que te desempeñes, y podría involucrar algunos cambios de tus hábitos laborales (por ejemplo, si los empleados suelen enviar correos entre ellos de hojas de cálculo de Excel y documentos de Word, la compañía debería adquirir una solución de seguridad para proteger archivos compartidos.

Luego, querrás asegurarte de que todos tus endpoints están siendo asegurados por un software de protección endpoint de máxima calidad, que evitará que los empleados visiten sitios web conocidos por alojar software. Es recomendable también utilizar un filtro de contenidos web como capa de protección adicional (además de bloquear sitios maliciosos, un filtro de contenidos web puede prevenir que los empleados visiten sitios no apropiados para el espacio de trabajo).

Tu protección endpoints debería administrarse de forma centralizada para reforzar las políticas de seguridad relevantes, como limitar la habilidad para apagar la protección antivirus o introducir medios extraíbles. Asegúrate que todos los endpoints estén ejecutando la última versión del producto, y que éste está llevando adelante las actualizaciones de forma exitosa. Si tu proveedor de seguridad tiene un componente en la nube, asegúrate de que esté encendido, ya que permitirá una reacción aun mayor ante nuevas amenazas (ESET llama a este componente LiveGrid®).

El emparchado inmediato y exhaustivo de los sistemas operativos y las aplicaciones ayudarán a prevenir el ingreso de ransomware por medio de adjuntos de correo electrónico o al visitar un sitio web infectado. Una configuración segura también puede ser de ayuda. Por ejemplo, considera utilizar una Directiva de Grupo para deshabilitar por completo las macros (que automatizan tareas preconfiguradas) de Microsoft Office. Esto limitará las posibilidades de un ataque de ransomware, aunque puede no ser una posibilidad si el flujo de trabajo de la organización depende de las macros.

Estos días, no cabe mucha duda de que la seguridad es una responsabilidad compartida, así que asegúrate que el entrenamiento en ciberseguridad de tus empleados esté al día y refleje las últimas tendencias en el ransomware que llega por correo. Según Ben Reed, quien lideró el desarrollo del **entrenamiento gratuito de concientización en ciberseguridad** de ESET: “Puedes reducir el número de incidentes de malware a los que se enfrenta tu compañía haciendo saber a tus empleados a qué deben prestar atención y qué deben evitar a la hora de tratar el phishing u otros contenidos maliciosos”.

Asegúrate de dejar en claro a tus empleados que deben reportar cualquier mensaje y adjunto sospechoso al equipo de seguridad de inmediato. Además de prevenir o limitar el daño, las advertencias tempranas pueden ayudar a la organización a modificar sus filtros de contenido y spam, y reforzar su firewall u otros medios de defensa.

RANSOMWARE, CADENA DE SUMINISTRO E INFECCIONES VÍA SITIOS WEB

Otros dos vectores de ataque de ransomware que despertaron la atención estos días son la cadena de suministro y las infecciones mediante sitios web comprometidos. Así como el ransomware, los riesgos de la cadena de suministro de software también surgieron durante el siglo pasado. Allá cuando el principal vector de ataque para virus informáticos eran los 'diskettes', y éstos a su vez eran la vía principal para adquirir software, el malware acababa localizado en diskettes de producción, o **aquellos de software de prueba** que solían distribuirse con las revistas de informática.

El pasado año, en una galardonada pieza de investigación, ESET descubrió que una aplicación legítima de software contable era utilizada por criminales para instalar el malware **NotPetya/DiskCoder.C.** Loa atacantes penetraron los servidores actualizados del software de la compañía y agregaron su propio código a los archivos legítimos de actualización de la aplicación. Cuando los usuarios del software contable hacían clic para instalar las actualizaciones del programa, también instalaban un backdoor, abriendo el camino para el ransomware. La primera línea de defensa contra este tipo de ataques es un producto de protección endpoint de calidad, respaldado por tecnología EDR (Detección y Respuesta).

Una versión particular de la distribución de malware por cadena de suministro es el "abuso" de sitios de cracking. Éstos existen para compartir información sobre cómo modificar las restricciones de software legítimo, incluyendo código que puede ser descargado para quebrar esas restricciones. En 2018, los investigadores descubrieron que el ransomware GandCrab, detectado por ESET como **Win32/Filecoder.GandCrab,** había simulado ser un código de cracking gratuito disponible para descargar (según reportó **Bleeping Computer**).

Los riesgos de esta vía de ataque pueden reducirse mediante productos de protección endpoint junto con la educación de los empleados sobre los peligros de dichos sitios, así como su dudosa legalidad y ética.

Los investigadores también han detectado un resurgir de sitios infectados como vector para llevar a cabo ataques de ransomware, comprometiendo a los visitantes de ciertos sitios. Un fragmento de ransomware detectado por ESET como Win32/Filecoder.Princess se ha distribuido utilizando esta técnica (un agradecimiento aquí a Malwarebytes Labs). Para ejecutar un ataque a través de sitios web, el actor instala código conocido como *exploit* kit en un sitio web. Puede tratarse de un sitio legítimo que ha sido comprometido para este propósito o un sitio creado por el atacante para que las víctimas sean dirigidas allí. Cuando alguien visita un sitio que almacena un exploit kit, el malware comprometerá la máquina del visitante utilizando uno de muchos exploits diferentes, en base a la configuración del equipo (por ejemplo, si el equipo ejecuta una versión del buscador web no emparchada, una vulnerabilidad conocida en esa versión del buscador puede ser explotada). Defenderse de este tipo de ataques implica estar al día con los parches, utilizando software de protección endpoint, y educando a los usuarios sobre los correos no solicitados que los incentivan para visitar sitios web no familiares.

NUBES Y SEGMENTOS

Sin importar cuál sea el vector de ataque implementado por el ransomware, si ingresa a tu organización hay grandes posibilidades de que intente expandirse por la mayor cantidad de máquinas que pueda.

En el caso de Lab Cort, citado anteriormente, miles de máquinas fueron afectadas en menos de una hora. Cuando NotPetya infectó la red del gigante de transporte marítimo Maersk, impactó rápidamente **45.000 equipos y 4.000 servidores.** Por supuesto, limitar el número de máquinas que están al alcance del atacante desde un único punto de entrada tiene grandes beneficios como estrategia de defensa. Existen varias maneras de abordar la implementación de dicha estrategia, entre las que destaca la segmentación de la red.

Discutir sobre la arquitectura de la red está fuera del alcance de este documento, y transformar una red "plana" amplia en una segmentada puede ser desafiante y costoso (**este reporte de KPMG** brinda una perspectiva útil). Sin embargo, toda organización necesita comprender las fortalezas y debilidades de seguridad de su arquitectura de red actual. Una simple auditoría con entrevistas puede mejorar la comprensión, al preguntar "¿puedo llegar de aquí hasta allí?" o "¿qué está frenando que alguien llegue de aquí hasta allí?"

Si esas preguntas hubieran sido hechas en Target antes de la brecha de noviembre de 2013, la compañía podría haber evitado la infame intrusión que comenzó como un correo de phishing que incluía un troyano – clickeado por un empleado en uno de los más grandes contratistas de HVAC (sistemas de ventilación, calefacción y aire acondicionado, por sus siglas en inglés) del comercio – y acabó como un malware en las terminales de punto de venta en sus locales. Si mediante estas mismas conexiones se hubiera desplegado un ataque de ransomware, el daño a Target podría haber sido mucho mayor que el masivo robo de tarjetas de crédito que tuvo lugar.

Una popular estrategia de arquitectura del sistema en años recientes ha sido mover información a la nube, pero la nube brinda inmunidad no automática de ataques de ransomware (a pesar de los esfuerzos de los proveedores menos escrupulosos por crear la impresión de que la nube = seguridad). De hecho, el bajo costo y la relativa facilidad con que los nuevos servidores pueden ser provistos en la nube y conectados al resto de la infraestructura digital de la organización, ha convertido a la nube en un campo fértil para los cibercriminales en busca de víctimas. El ataque de ransomware en CDoT citado previamente llegó mediante un servidor virtual conectado a internet que fue comprometido por un ataque de fuerza bruta a dos días de su creación. Por supuesto, cualquier uso de la nube por cualquier parte de la organización necesita estar autorizado y configurado apropiadamente. Además, como todos los otros sistemas, aquellos ubicados en la nube deben ser parte de un régimen de backup y recuperación apropiado.

PARCHES Y BACKUP COMO DEFENSA CONTRA EL RANSOMWARE

Los parches y el backup son dos aspectos de la operación y administración de sistemas que juegan roles vitales en la defensa contra los ataques de ransomware. Emparchar los sistemas cierra potenciales vías de ataque, y puede prevenir que el ransomware ingrese en tu organización, o en caso de que lo haga, reduce el daño que puede causar. Por ejemplo, las organizaciones que emparcharon adecuadamente el servicio de Windows de File and Printer Sharing a partir del Microsoft Security Bulletin MS17-010, estuvieron protegidas ante el exploit EternalBlue utilizado para distribuir WannaCryptor y NotPetya entre las organizaciones.

Por supuesto, como todo administrador de sistemas sabe, emparchar puede ser bastante más complejo de lo que parece. Los parches y las

actualizaciones necesitan ser puestos a prueba antes de implementarse. Ciertos sistemas dentro de tu organización podrían tener dependencias de software que se rompan al actualizar a la última versión de una aplicación o sistema operativo. Sin embargo, el alto costo de que el ransomware ingrese a tu red – en los cientos de millones de dólares para algunas compañías alcanzadas por NotPetya – justifica el esfuerzo de enfrentar estos desafíos y mantener un régimen de parches completo y a tiempo para evitar el ransomware.

Suele decirse que, si se produce un ataque de ransomware en tu organización – ya sea por RDP, correo, cadena de suministro del software o un actor malicioso interno – un programa comprehensivo y bien administrado de backup y recuperación puede ser tu mejor método de defensa. Hay mucho de realidad en esto – y son varias las razones para tener dichos programas – pero ten en cuenta que ciertos ataques de ransomware se ejecutan a través de un período de tiempo, durante el cual el ransomware puede también ser respaldado, comprometiendo la posibilidad de una recuperación sencilla. Por tal motivo, el backup no es un medio de defensa que instalas y lo olvidas, sino que debe ser monitoreado y administrado, y el proceso de recuperación debe ser probado regularmente.

Afortunadamente, cada vez existen más opciones de backup y recuperación, destaca el almacenamiento en la nube, ya sea remoto, on premise, o híbrido. Sin embargo, también se ha incrementado la cantidad de información que debe respaldarse, de más sitios. A menos que cuentes con una estrategia de backup comprehensivo, siempre existirá la posibilidad de que quienes lanzan el ataque hallen ese único dispositivo que no ha sido respaldado. De acuerdo a los expertos en backup de **Xopero,** miembro de ESET Technology Alliance, un backup comprehensivo incluye información y estado del sistema de todos los endpoints, servidores, casillas de correo, unidades de red, dispositivos móviles y máquinas virtuales.

Una discusión detallada sobre la estrategia de backup y recuperación corporativa va más allá del alcance de este White Paper, pero debería quedar en claro que contar con dicha estrategia es más crítico hoy que nunca antes. El ransomware simplemente se suma a la larga lista de razones por las cuales tu organización debería no escatimar en gastos cuando se trata de este segmento del programa de IT, pero, como remarcó quien fue Senior Research Fellow de ESET, David Harley, en "Trends 2018: The ransomware revolution", existen ciertas advertencias específicas para el ransomware. Por ejemplo, "si el almacenamiento se encuentra "siempre encendido", su contenido puede ser vulnerable a las infecciones de ransomware de la misma manera que el almacenamiento local". Harley recomendaba que el almacenamiento fuera del sitio:

- No permanezca online de manera habitual ni permanente
- Proteja los datos almacenados cuando el centro remoto esté online, de modo que un malware no pueda modificarlos o sobrescribirlos en forma automática y silenciosa
- Proteja de infecciones a las generaciones anteriores de datos respaldados para que, incluso si ocurriera un desastre que afectara a los últimos backups, al menos puedas

recuperar algunos datos, incluyendo las versiones anteriores de los datos actuales

- Proteja al cliente explicando las responsabilidades legales y contractuales del proveedor, indicando qué pasará si el proveedor cierra la empresa, etc.

Harley advirtió también sobre los peligros de subestimar la utilidad de los medios de una sola escritura para archivar información, resaltando que los archivos almacenados en medios que no pueden sobreescribirse son inmunes al ransomware.

Por supuesto, existen muchas otras razones por las que tu organización necesita una solución de backup y recuperación – como el rescate del fuego, inundaciones, daños por tormentas, y más – y hay una razón por la que el backup no.

RESPONDIENDO A UN ATAQUE DE RANSOMWARE

Además de establecer defensas contra el ransomware, toda organización necesita estar preparada para responder a cualquier ataque que logre penetrar esa protección. Por ello es fundamental contar con políticas de seguridad empresariales actualizadas para abarcar al ransomware. Debes detallar las formas en que debe responder cada empleado en cada nivel a las demandas del ransomware. Asegúrate de que tus políticas respondan a las siguientes preguntas:

- ¿A quién deberían reportar los empleados una sospecha de ransomware?
- ¿Cuál es la política de la empresa sobre el pago de las demandas del ransomware?
- ¿Quién está habilitado para negociar los pagos demandados?

Las políticas deberían formularse para evitar los siguientes problemas:

- Que los empleados no reporten sospechas de ransomware por miedo a una represalia
- Que los administradores de la red paguen el rescate porque es más sencillo que recuperar los sistemas desde el backup
- La divulgación no autorizada de información sobre ataques de ransomware sospechados o reales

Tras actualizar tus políticas de seguridad de la información para abordar al ransomware, debes asegurarte de que tus programas de entrenamiento de empleados y concientización en seguridad incluye contenido relacionado al ransomware apropiado.

También deberías querer asegurarte de que tu plan de Respuesta ante Incidentes/Crisis esté listo en caso de un ataque de ransomware. Aquí hay un esquema de lo que debería cubrir tu plan de respuesta:

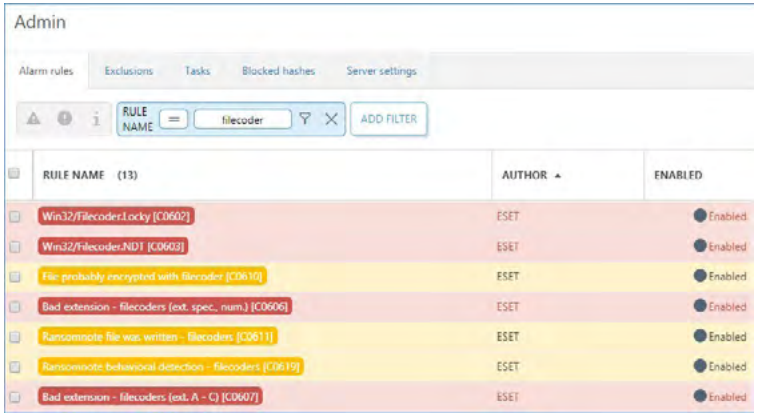
- Ante los primeros signos de un ataque, notifica al personal designado
- Aísla y analiza los equipos afectados
- Si se confirma un ataque, activa al equipo de Respuesta ante Incidentes/Crisis
- Alerta al consejo legal
- Contacta a los proveedores que estén dispuestos a asistir
- Recuerda a los empleados de la política de prensa y redes sociales
- Evalúa el alcance del ataque y las características del ransomware (si es posible)
- Contacta a la policía

- Prepara un comunicado para el público
- Si los archivos han sido cifrados, determina si pueden recuperarse mediante las copias de backup
- Mantén a los empleados al día con el estado
- Si es necesario, activa un plan de continuidad del negocio

Es una buena idea tener al menos un escenario de infección de ransomware en tu proyecto de plan de crisis, y repasarlo en las reuniones con personal relevante, incluyendo ejecutivos. Esto puede revelar huecos en los planes de backup y recuperación, y ayudarte a anticipar el impacto de no ser capaz de acceder a servicios básicos, debido a que los sistemas han sido cifrados (servicios como el correo, móviles VoIP y acceso a Internet).

DETECCIÓN Y RESPUESTA DE ENDPOINTS

Existe una categoría de software de seguridad que puede ayudar a limitar el impacto de los ataques de ransomware y reforzar tu respuesta ante ellos: las herramientas de detección y respuesta de endpoint, o simplemente EDR. Ya sea como una colección de herramientas desarrolladas internamente o un producto de seguridad integrado, el EDR puede utilizarse para cooperar en los esfuerzos de búsqueda de amenazas manuales en tu red, así como automatizar un amplio grupo de medidas de protección. En la Figura 4 podrás ver diversas reglas de EDR relacionadas al ransomware diseñadas para alertar al personal de seguridad sobre actividad sospechosa (este EDR se llama ESET Enterprise Inspector).



Un EDR puede monitorear todos los endpoints de tu organización en busca de actividad sospechosa, como la modificación de la extensión de archivos que suele ser común en ataques de ransomware. Definitivamente, tu equipo de seguridad querría estar al tanto de la presencia de herramientas de ataque como Mimikatz, creada para robar credenciales de usuario de la memoria, o xDedicRDPPatch, utilizado para la creación de usuarios adicionales una vez que hayas accedido al servidor vía RDP (disponible desde el sitio xDedic previamente mencionado).

Las alertas tempranas de signos de intrusión pueden codificarse como reglas y alarmas. Esto puede refinarse con nueva información de inteligencia de amenazas, como indicadores de compromiso (IOC) constantemente. Un buen EDR tendrá reglas que le permitan al operador hallar sistemas comprometidos al momento en que una regla se activa, aislar esos sistemas y hacer un diagnóstico del problema, incluyendo un retroceso al historial de comandos ejecutados por los sistemas afectados. Estas capacidades significan que un EDR puede incrementar las habilidades del equipo de seguridad para frustrar ataques, responder a ellos y realizar análisis forenses una vez ocurridos.

UNA PALABRA SOBRE LOS PAGOS DE RESCATE

La palabra es: no. ¿Por qué? Porque pagar a un criminal que ha cifrado tus archivos significa:

- Estás validando el modelo de negocio detrás del crimen
- Estás incentivando la actividad criminal
- Podrías verte afectado por futuras demandas de dinero y futuros ataques

Además, pagar a los criminals que han cifrado tus archivos no garantiza que consiga la llave de descifrado; después de todo, no es como si puedieras iniciar un juicio o reportarlos ante el el Better Business Bureau. Hay múltiples razones por las cuales pagar podría no significar que recuperes tus archivos:

- El ransomware no funciona correctamente – los errores de codificación en el malware son muy comunes
- Hay numerosas maneras en las que el proceso para entregar la llave de descifrado puede fallar
- El atacante actúa simplemente por maldad y no planea entregar las llaves de descifrado

Los motivos mencionados deberían ser suficientes para frenar a las organizaciones de que paguen a las demandas de ransomware, pero para resaltar esta recomendación, esto es **lo que tiene para decir el FBI sobre efectuar los pagos:**

"Pagar un rescate no garantiza a una organización la recuperación de su información – hemos visto casos en los que las organizaciones nunca obtuvieron una llave de descifrado tras pagar. Hacerlo no solo anima a los criminales a apuntar a más organizaciones, ofrece también un incentivo para que nuevos cibercriminales se involucren en este tipo de actividad ilegal. Y finalmente, al pagar el rescate, una organización puede estar sin notarlo financiando otra actividad ilegal asociada con los criminales".

En la práctica, parece haber dos argumentos para pagar un rescate, el primero "no podemos recuperar la información cifrada con las copias de backup". Esto puede deberse a que los respaldos no existen o que sí lo hace, pero de alguna manera están dañados. Sin embargo, puede haber alternativas a pagar. **Como ha sugerido David Harley:** "Antes de pagar, comprueba con tu proveedor de seguridad (a) si es posible algún otro método de recuperación sin pagar el rescate (b) si es sabido que pagando no se puede recuperar la información de esa variante de ransomware específica.

El otro argumento para pagar el rescate es que "es menos costoso que recuperarlo desde copias de backup". Si esta afirmación se basa únicamente en cálculos de tiempo y trabajo, podría ser técnicamente correcto, pero de todas maneras la decisión de pagar está profundamente afectada por las razones ya mencionadas, principalmente la poca fidelidad de las promesas de descifrado y la probabilidad de ser atacado nuevamente tras el primer pago – después de todo, no estás lidiando con ciudadanos que se guíen por las leyes.

Quizás hayas oído que algunos de los criminales que ejecutan el ransomware ofrecen a sus víctimas pruebas de que el descifrado funciona. Esto sucede, pero puede llevar incluso a más problemas, como en la reciente brecha de **Health Management Concepts**. Imagina que los atacantes te han hecho enviarles un archivo cifrado que luego ellos pueden

descifrar y reenviarte como evidencia de su buena fe; solo has facilitado la divulgación de los contenidos que ese archivo poseía entre sujetos de dudosa moral.

Y aquí hay otro problema a considerar, **resaltado por David Harley:** "recuerda que una cosa es eliminar un ransomware activo con un software de seguridad que detecta ransomware y otra muy distinta es recuperar datos cifrados: si eliminas el ransomware y luego decides pagar, es posible que los datos ya no se puedan recuperar, incluso con la cooperación de los delincuentes, porque el mecanismo de descifrado es parte del malware". En otras palabras, si decides pagar, avanza con precaución.

EL FUTURO DEL RANSOMWARE

Demandar dinero para recuperar el acceso al sistema y la información apunta a la "D" de CID, la clásica tríada de seguridad de Confidencialidad, Integridad y Disponibilidad. En esencia, el ransomware se aprovecha de la dependencia de una organización en su tecnología, por ello cuanto más dependan ellas de la tecnología, mayor será el alcance del ransomware. Eso significa que podemos esperar que el ransomware persista y evolucione a futuro (a menos que surjan cambios inesperados en la política y economía global).

Basándonos en nuestra experiencia con códigos maliciosos durante los últimos 30 años, podemos decir que las amenazas de malware tienden a evolucionar de la siguiente manera:

- Se descubren vulnerabilidades en nuevas tecnologías y se pone en discusión su potencial para ser abusado por criminales
- Comienzan los esfuerzos por remediar y mitigar esas vulnerabilidades
- Los intentos de ataque a estas últimas tecnologías son raros en un comienzo, dado que los criminales siguen haciendo dinero fácil con estrategias ya establecidas
- Al no registrarse amplio abuso criminal, los esfuerzos de remediación y mitigación pierden fuerza
- Eventualmente, los criminales descubren que esta "nueva" tecnología está allí para ser explotada
- Emerge una nueva tendencia de malware

Algunos ejemplos recientes pueden ser los ataques distribuidos de denegación de servicio que se aprovecharon del equipamiento conectado de vigilancia (**Mirai**) y el surgimiento del malware en router (**VPNFilter**). En cuanto al ransomware, el enorme crecimiento del lanzamiento de dispositivos IoT sin protección está creando un suelo fértil para futuros intentos de ataque, como también lo hacen el aumento en el uso de sistemas de control industrial conectados a Internet, edificios y automóviles inteligentes, incluyendo los autónomos (mira el artículo "**RoT: el ransomware de las cosas, en detalle**" y accede al webinario "**Ransomware Today: What's New, What's Coming Next**", en inglés).

Si una caída en los ingresos de crímenes más establecidos lleva a los criminales a perseguir nuevos esquemas, pueden darse varios escenarios. El malware en routers podría limitar o bloquear el tráfico hasta que se realice un pago, con el respaldo de amenazas de bloquear el router, o revelar el contenido del tráfico, si intentas remover el malware.

La cerradura remota de vehículos, hogares y edificios podría ser abusada para la extorsión. La manipulación de los sistemas de automatización integral de inmuebles (inmótica), así como los que ganan control de sistemas HVAC (climatización) pueden servir como base para esquemas de extorsión (ya vemos signos de esto). En cuanto a robots comerciales, la viabilidad de los ataques de ransomware ya ha sido demostrada.

Estos escenarios de ransomware en crecimiento tienen múltiples implicancias para las corporaciones. Las siguientes reacciones son recomendadas:

- Comienza a abordar estas potenciales amenazas en tu estrategia de gestión de riesgos
- Comienza a registrar aquellos activos que pueden ser víctimas de ransomware: dispositivos IoT, routers SOHO, robots, sistemas de control, sistemas autónomos
- Haz un seguimiento de los reportes de vulnerabilidades relacionados a estos activos
- Mantente al día con los parches y actualizaciones de firmware de estos activos
- Segmenta los dispositivos IoT y otras nuevas tecnologías de redes de producción

Estas recomendaciones ayudarán también a tu organización a defenderse contra otra tendencia que surge en la evolución del crimen online: la criptominería, el uso no autorizado de los recursos de un computador para generar criptomonedas, como Bitcoin, Litecoin, Ethereum y Monero. Como se mencionó anteriormente, ya son muchos los criminales que ven la criptominería como flujo de ingresos adicional. También fue dicho que las amenazas cibernéticas tienen a acumularse, y parece lógico predecir una futura mezcla entre el ransomware y la minería. Por ejemplo, los sistemas comprometidos podrían quedar secuestrados hasta que se hubiera minado cierta cantidad de moneda digital. Como alternativa, una organización con una amplia cantidad de dispositivos IoT puede ser comprometida mediante un esquema de criptominería y luego recibir una oferta extorsiva: paga X cantidad, y frenamos la minería.

RESUMEN

Durante varias décadas, hemos sido testigos de una lucha global por prevenir que códigos maliciosos quebranten la tecnología de la que hoy prácticamente depende la vida moderna. Las partes de esta lucha incluyen, de un lado, a los criminales motivados por lo financiero, activistas guiados por agenda, agentes de gobiernos con una ética cuestionable, y ocasionalmente algunos adictos de la codificación encapuchados que no han analizado a fondo lo que hacen. Del otro lado están las compañías y los consumidores y cualquier organización que posea información que puede ser aprovechada o destruida por alguien con intenciones maliciosas.

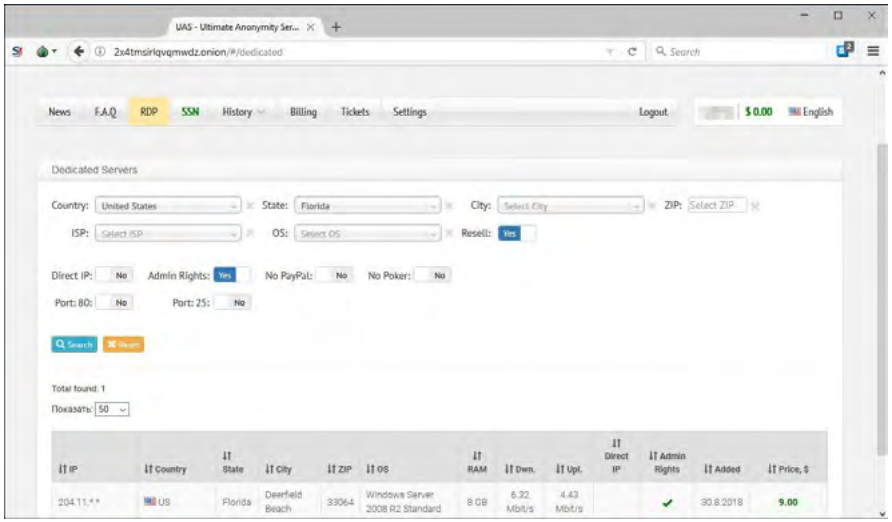
Para tener la ventaja en esta lucha debe primero entenderse a los atacantes y las vías de ataque. Naturalmente, estos evolucionan con el tiempo, pero de forma acumulativa. El hecho de que el abuso criminal de los recursos de un computador para minar criptomoneda haya surgido recientemente no significa que exista una escasez de criminales para desarrollar e implementar técnicas de explotación RDP para crear vectores de ataque redituables para el ransomware. Asimismo, reducir el uso de RDP en tu organización – algo que debe hacerse por varias buenas razones – no significa que las capacitaciones sobre anti-phishing deban dejarse de lado.

Junto con una educación del empleado efectiva, necesitas: políticas de seguridad sólidas que se apliquen de forma exhaustiva y se refuercen con rigurosidad; la combinación correcta entre productos de seguridad y herramientas, incluyendo backup y sistemas de recuperación probados; y un plan de respuesta a incidentes constantemente actualizado. Incluso con todo esto aplicado, además de la constante vigilancia, no tienes garantizada la inmunidad ante un ataque; sin embargo, puedes aumentar en gran medida las posibilidades de evitar a los atacantes y recuperarte de un ataque.

Hasta que las economías globales mejoren dramáticamente y sus gobiernos logren frenar las tensiones mundiales, la lucha contra el cibercrimen no solo continuará, también se expandirá, junto con los beneficios que la sociedad obtiene de las nuevas tecnologías. Tal vez, con algo de suerte, al explicar por qué el ransomware sigue siendo una amenaza seria para tu organización y qué puede hacerse para defenderse contra él, este White Paper te ayudará a asegurar esos beneficios y minimizar, a la vez, las pérdidas causadas por actores maliciosos.

APÉNDICE A

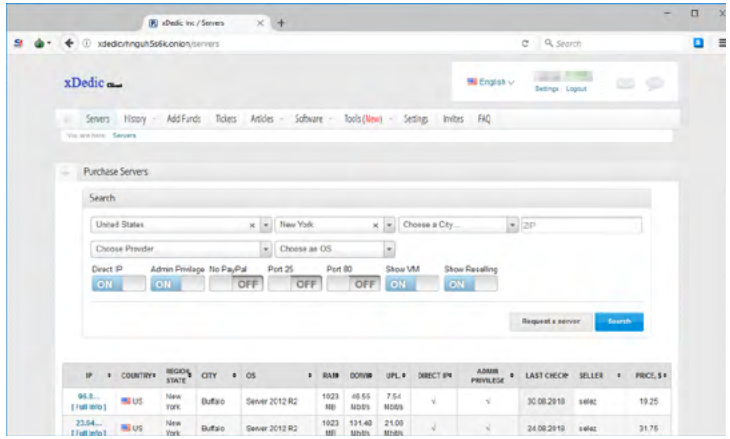
Los ataques de ransomware via RDP están impulsados por la disponibilidad comercial de credenciales comprometidos en el mercado negro. En la Figura A1 podrán ver cómo se ve uno de estos mercados, Ultimate Anonymity Services, o UAS, ante un cliente en busca de credenciales para comprar que le garanticen derechos de administrador a un servidor RDP en Florida:



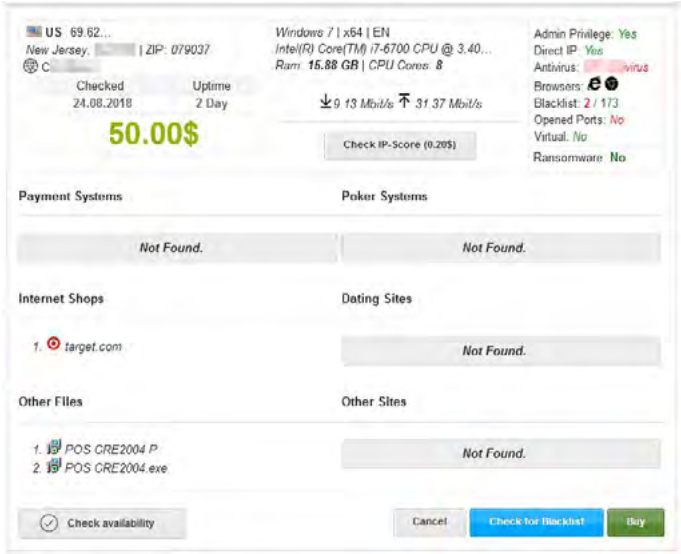
Observa la amplitud de filtros de búsqueda que permiten a los compradores especificar la selección de sus víctimas. Mira también el nivel d detalle que provee sobre los ítems listados. El precio por las credenciales del servidor de Windows mostradas aquí es de US$9.00. Un mercado RDP más amplio, pero más costoso, es xDedic (para servidores dedic-ados). Desde sus orígenes en 2014, xDedic ha atraído cientos de vendedores de credenciales de todo el mundo – gente que vulnera servidores para obtener acceso y luego enlistar esos accesos para vender.

Sorprendentemente, xDedic no comenzó a operar en la dark web, pero fue movido detrás de un paywall en la red Tor tras varias investigaciones y artículos de investigadores en seguridad (mención especial a Kespersky). Actualmente, los aspirantes a criminales deben adquirir un invite de $200 para conseguir una cuenta de xDedic. Además, deben rápidamente depositar $50 en la cuenta, suma que se pierde si no se la utiliza para realizar compras dentro de los 30 días.

Para criminales con necesidades específicas, la interfaz web de xDedic ofrece filtros, como los de UAS. En la Figura A2 podrás ver como se ve xDedic ante un cliente que busca servidores con acceso IP directo y privilegios de administrador en el estado de Nueva York:



Cualquier cliente de xDedic que piense en adquirir accesos a servidores particulares, puede obtener un amplio rango de detalles antes de comprar. Si bien la dirección IP exacta de los objetivos no es revelada sin realizarse el pago, es posible saber dónde están ubicadas las máquinas, sus especificaciones técnicas, velocidad de conexión a Internet, y si se trata de una máquina virtual o no. También puedes conocer qué antivirus está ejecutando y si dicha dirección IP ha sido ingresada en la lista negra de las organizaciones que luchan contra el spam y el alojamiento de malware. La información es presentada de forma eficiente en una ventana emergente, como se observa en la Figura A3.



Como verás, en este servidor se ha detectado un ejecutable de software de un punto de venta, lo que podría responder al precio relativamente elevado. Este servidor podría ser un objetivo atractivo para un criminal que busca robar información de tarjetas de crédito, y es importante destacar que no todos los que están en el mercado en busca de un servidor comprometido busca cifrar su contenido mediante un ataque de ransomware. Hay múltiples razones por las que los criminales quieren hacerse con servidores conectados a internet, y por lo tanto muchas razones por las que tu organización debería tener programa de defensa ante accesos remotos integral.

APÉNDICE B: ASEGURANDO EL RDP CONTRA EL RANSOMWARE

Una colección de estrategias y técnicas a considerar:

1. Documenta el problema

Asegúrate de que quienes están a cargo de proteger los activos de tu organización conectados a internet conozcan la existencia de todos ellos. Aplica un proceso que asegure que los dispositivos nuevos sean incluidos.

2. Limita los activos expuestos

Asegúrate de que no haya activos digitales accesibles de forma remota directamente desde internet a menos que haya sido aprobados para utilizarse de esa manera y apropiadamente configurados. Pregunta por qué el acceso al activo no puede ser provisto por una VPN (Red privada virtual). Deshabilita el RDP cada vez que éste no sea requerido (este artículo muestra cómo hacerlo en diferentes versiones de Microsoft Windows (en inglés): **Server 2016**; **Server 2008/R2**; **Windows 10**; **Windows 8**; **Windows 7**; Windows XP).

3. Protege los activos expuestos

Si no tienes más alternativa que utilizar RDP sin una VPN, asegúrate de llevar a cabo las siguientes acciones, lo máximo que puedas:

a. Cambia la contraseña por defecto de administrador.

b. Refuerza la complejidad de la contraseña (largo, mezcla de caracteres, etc.).

c. Establece un límite de intentos de acceso remoto tras un número de intentos fallidos de acceso consecutivos.

Al configurar tu computador para que bloquee una cuenta durante un período de tiempo tras varios intentos incorrectos por acceder, obstruirás a los atacantes que utilizan herramientas automatizadas de acierto de contraseñas (ataque de "fuerza bruta"). Para establecer una política de lockout en Windows:

Ve a Inicio--> escribe **secpol.msc** y presiona Enter-->Configuración de seguridad-->Directivas Locales

Bajo Directivas de Cuenta-->Directiva de bloqueo de cuenta, establece valores para las tres opciones. 3 intentos fallidos con un bloqueo de 3 minutos es una opción razonable.

d. Utiliza Autenticación a nivel de red para reforzar la seguridad del servicio de rol Host de Sesión al solicitar al usuario una autenticación previa a la creación de dicha sesión.

e. Modifica el Puerto por defecto de conexión RDP, el 3389 (pero ten en cuenta que esto solo es seguridad por oscuridad, y no debería ser la única medida a tomar).

Para modificar el Puerto, edita la siguiente clave de registro (ADVERTENCIA: no realices esta acción si no estás familiarizado con el Registro de Windows TCP/IP): HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp.

f. Restringe las direcciones IP públicas que pueden conectarse via RDP (esto puede ser engorroso si los usuarios remotos no tienen direcciones IP estáticas, por ejemplo, cuando viajan o trabajan desde sus hogares).

g. Utiliza más de un factor de autenticación. Hay tres posibilidades: algo que sepas, como nombres de usuario y contraseñas; algo que eres, como huellas o registros de voz; algo que tienes, como tu móvil, al que puede enviarse un código de uso único.

Sin embargo, si utilizas códigos enviados a tu móvil como segundo factor, evita recibirlos por SMS, dado que los criminales tienen en su historial varios triunfos sobre la autenticación basada en SMS (como describimos en **este artículo**). Hay buenas soluciones de 2FA que hacen uso de la ubicuidad de los móviles, pero no se comunican por SMS (como **ESET Secure Authentication**).

h. Refuerza los permisos y derechos de usuario. Deshabilita los archivos que se ejecutan de las carpetas AppData y LocalAppData. Bloquea la ejecución del subidirectorio Temp (parte del árbol de AppData por defecto). Bloquea archivos ejecutables que se ejecutan en directorios de trabajo de varios software compresión (por ejemplo, WinZip o 7-Zip). Además, si tienes un buen producto de protección endpoint puedes crear reglas de HIPS para permitir que solo ciertas aplicaciones se ejecuten en el computador y bloqueen a todas las demás por defecto).

i. Protégé tu protección endpoint con contraseña para prevenir la modificación de la configuración no autorizada, deshabilitando la protección o incluso desinstalando el producto (pero usa diferentes contraseñas de las que utilizaste para las credenciales de acceso de la conexión RDP).

AGRADECIMIENTOS:

Este White Paper debe mucho al trabajo de mis queridos colegas de ESET James Rodewald, Ben Reed, Fer O'Neil, y David Harley, y mi talentoso equipo: Aryeh Goretsky, Bruce P. Burrell, Cameron Camp, y Lysa Myers.

ACERCA DE ESET

Durante 30 años, ESET® ha desarrollado software de seguridad IT y servicios para empresas y consumidores líderes en la industria alrededor del mundo. Con soluciones que abarcan endpoints y seguridad móvil, hasta cifrado y doble factor de autenticación, los productos de alto rendimiento y facilidad de uso de ESET dan a los consumidores y negocios la tranquilidad para disfrutar el potencial absoluto de su tecnología. ESET protege y monitorea sin obstrucciones 24/7, actualizando la defensa en tiempo real para mantener a sus usuarios a salvo y a los negocios funcionando sin interrupciones. Las amenazas evolucionan, lo que requiere una compañía de seguridad que también evolucione. Respaldada por centros de Investigación y Desarrollo alrededor del mundo, ESET se convirtió en la primera compañía de seguridad informática en recibir 100 premios Virus Bulletin VB100, identificando cada malware "in-the-wild" sin interrupciones desde 2003. Para más información, visita www.eset.com/latam o síguenos en LinkedIn, Facebook y Twitter.