6 mejores prácticas para escapar del **ransomware**

Una guía completa para detener los ataques de ransomware.

ManageEngine
IT Management, Simplified

Contenido

- Ciberataques
- ¿Qué es el ransomware?
- Tipos de ransomware
- ¿Cómo funciona?
- Motivos para los ataques ransomware
- ¿Debería pagar el rescate o no?
- Mejores prácticas para estar atento al ransomware
- Escenario del mundo real: Respondiendo WannaCry y

Petya

- Combatir los ataques de ransomware con ManageEngine

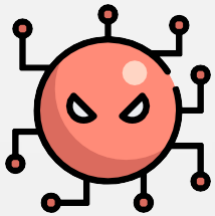
Ciberataques

Un ciberataque es un acto ofensivo contra computadores, redes u otros dispositivos en un intento de robar, cifrar o destruir información de un sistema o red. Una nación, un estado, un individuo, una organización o un grupo pueden orquestar un ataque. Existen diferentes tipos de ciberataques, como los ataques DDoS, los ataques de fuerza bruta, el phishing, el hackeo, los ataques de abrevadero, los ataques de ransomware, y otros. Pero si nos fijamos bien, la mayoría de los ciberataques siguen una de estas cinco estrategias generales.

De estas estrategias, el número cinco ha ganado popularidad recientemente. Esta estrategia es utilizada por los ataques de ransomware, más notablemente el ataque WannaCry que comenzó el 12 de mayo de 2017. WannaCry comenzó a penetrar rápidamente las redes de todo el mundo e infectó más de 400.000 computadores en 150 países, siendo el Servicio Nacional de Salud (NHS) de Inglaterra la principal víctima de este ciberataque.



Bombardear las redes con un tipo de malware continuamente.



Desencadenar diferentes formas de malware para penetrar en las redes.



Irrumpir primero en la red más débil.



Infiltrarse, robar datos y huir.



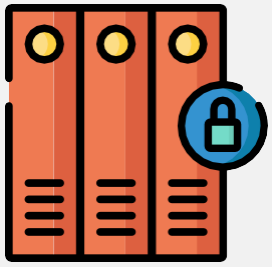
Cifrar archivos y extorsionar a las víctimas para ganar dinero.

¿Qué es el ransomware?

El ransomware es un tipo de malware que cifra un sistema y luego extorsiona a los usuarios o a toda la organización. Básicamente, el ransomware cifra los archivos de la víctima, restringiendo al usuario usar sus propios archivos o documentos, o bloquea el computador para impedir su uso normal y exige un pago como rescate para descifrar los archivos y proporcionar acceso.



Le impide acceder a sus archivos y carpetas.



Bloquea completamente el acceso al sistema.



Exige un rescate para restablecer el funcionamiento del sistema.

Tipo de ransomware

La gente a menudo se confunde sobre los diferentes tipos de ransomware y sus capacidades para cifrar archivos. Actualmente existen tres tipos principales de ransomware, pero a medida que aparecen nuevas versiones, pueden aparecer otras variantes. Los tres tipos de ransomware son:

1. **Ransomware de cifrado**
2. **Ransomware de bloqueo de pantalla**
3. **Ransomware de registro de arranque maestro**



Ransomware de cifrado

Este ransomware cifra sus archivos y carpetas, impidiéndole acceder a sus archivos al bloquearlos con una clave AES-256, que es notoriamente difícil de descifrar. Dependiendo del motivo del hacker, los archivos cifrados se pueden recuperar o no. Después de cifrar sus archivos y carpetas, el ransomware de cifrado muestra un mensaje emergente explicando que sus archivos han sido cifrados y que debe pagar un rescate para que esos documentos sean descifrados. Este es el método que utilizó WannaCry contra sus víctimas.



Ransomware de bloqueo de pantalla

Como su nombre indica, el ransomware de bloqueo de pantalla bloquea la pantalla y pide un rescate. Aunque este tipo de ransomware no cifrará sus archivos, bloqueará inmediatamente todas sus ventanas. Una vez infectado su sistema, no podrá acceder a sus ventanas hasta que pague el rescate o los hackers cancelen el ataque.



Ransomware de registro de arranque maestro

El registro de arranque maestro (MBR) es una parte esencial de un disco duro, que permite el arranque del sistema operativo. El ransomware MBR cambia el MBR, interrumpiendo el proceso normal de arranque al mostrar una demanda de rescate en la pantalla de arranque. Los usuarios ni siquiera pueden arrancar sus sistemas hasta que se paga el rescate. De los tres tipos de ransomware, este posiblemente es el más peligroso.

El ransomware Petya se lanzó inicialmente como ransomware de registro de arranque maestro, pero una vez que los profesionales de seguridad lo descubrieron de inmediato, Petya se actualizó y se lanzó como una nueva variante llamada Wiper. Como su nombre indica, esta variante borrará por completo todo su disco duro y lo dejará con las manos vacías y el sistema en blanco.

¿Cómo funciona el ransomware?

A diferencia de otros ciberataques, el ransomware realmente bloquea los datos de las víctimas en lugar de robarlos o destruirlos. Recientemente, el ransomware de cifrado ha sido el más utilizado. La mayor parte del ransomware entra en una red a través de archivos adjuntos de correo electrónico, redes sociales o sitios maliciosos.

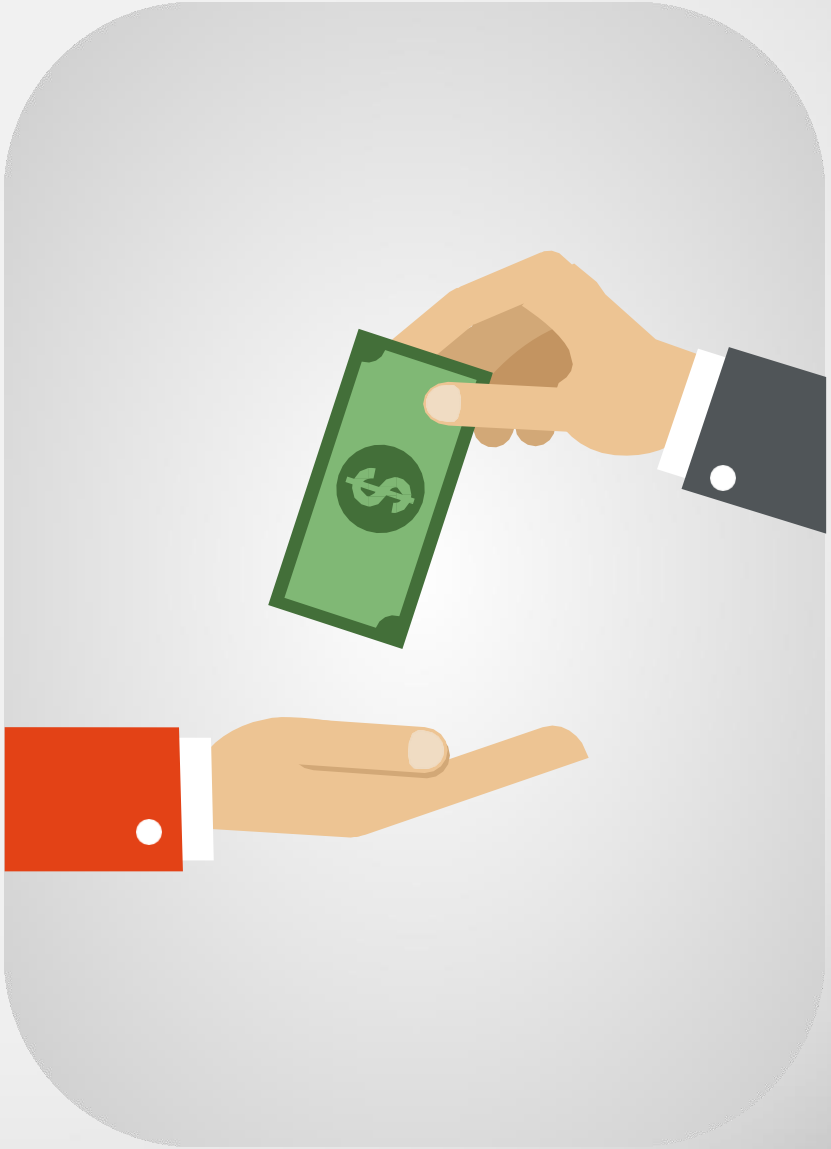
WannaCry infectó los sistemas a través de archivos adjuntos de correo electrónico, pero luego utilizó una vulnerabilidad conocida de Windows, EternalBlue, para propagarse dentro de las redes. Esta técnica de propagación diferencia a WannaCry de la mayoría de los ransomware de cifrado, ya que su exposición no se limitó a los equipos que descargaron directamente el archivo malicioso.

Analicemos el flujo de trabajo típico del ransomware de cifrado en cinco etapas

1. Un usuario descarga un archivo malicioso de una página web o un correo electrónico.
2. El archivo descargado contiene el ransomware, que comienza a infectar el sistema del usuario.
3. Algunos tipos de ransomware se propagan a otros sistemas de la red si ésta contiene vulnerabilidades.
4. El ransomware impedirá el acceso de alguna manera. Muchas versiones de ransomware de cifrado encriptan los archivos de los usuarios a través de la red con AES-256, una clave de un solo uso.
5. El ransomware crea una clave única para cada archivo cifrado (que se utiliza para descifrar los archivos una vez pagado el rescate).

Motivos detrás de estos ataques de ransomware

Generalmente, el principal motivo detrás de cualquier ataque de ransomware es ganar dinero. Con muchas variantes, exigiendo el pago en Bitcoin u otras criptomonedas, a menudo es difícil identificar a los creadores. Aunque WannaCry es el ataque más prolífico hasta la fecha, es probable que los hackers detrás del ataque hayan obtenido aún más ganancias. Se estima que las organizaciones de todo el mundo pagaron en conjunto más de $80.000 para descifrar sus datos antes de que el investigador de seguridad Marcus Hutchins descubriera cómo detener el ataque WannaCry. Haciendo algunos cálculos sencillos, pensemos en una organización que tiene 3.000 sistemas y toda su red queda cifrada. Los hackers exigen a la organización que pague $200 por sistema para descifrar sus archivos. Esto significa que, en teoría, la organización podría acabar pagando $600.000 de rescate. Visto desde la perspectiva de los hackers, pueden ganar mucho dinero en poco tiempo si sólo unas cuantas organizaciones pagan para recuperar sus archivos.



¿Debería pagar el rescate o no?

Pagar un rescate a los hackers nunca va a mantener su red segura. Incluso si una organización decide pagar el rescate para descifrar sus archivos, los hackers pueden utilizar este dinero para crear nuevo malware o ransomware y empezar a atacar de nuevo a la organización. Está claro que pagar el rescate es una solución puntual a un problema continuo.

En definitiva, los expertos en seguridad recomiendan a las víctimas no pagar los rescates y, en su lugar, tratar de prevenir los ataques. En este caso, una buena defensa es realmente el mejor ataque. Lo que deben hacer las organizaciones es utilizar medidas proactivas para prevenir futuras amenazas de ransomware, como las soluciones que se enumeran en la siguiente sección.

Y lo que es más importante, pagar el rescate a una entidad desconocida no garantiza que se descifren los datos cifrados. Del mismo modo, pagar para recuperar los archivos no significa necesariamente que los datos estén seguros. Incluso si los hackers descifran sus datos, no hay garantía de que los datos no hayan sido copiados o almacenados en otro lugar, lo que significa que los hackers podrían utilizar su información confidencial para futuras amenazas.



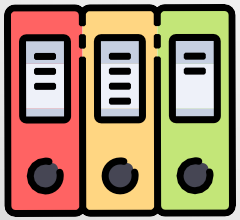
Mejores prácticas para estar atento al ransomware

Ahora que hemos visto lo que no hay que hacer como respuesta a los ataques de ransomware, echemos un vistazo a lo que debe hacer para mantenerse a salvo. Aquí encontrará seis sencillos pasos para proteger sus datos de los ciberataques



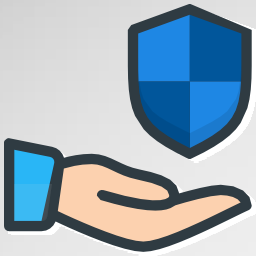
1. Educar a los usuarios sobre los ataques de phishing.

Los ciberdelincuentes suelen enviar correos electrónicos aparentemente inocentes a los usuarios, incitándoles a descargar archivos adjuntos para que los hackers puedan infectar sus sistemas e infiltrarse en su red. Las empresas deben educar adecuadamente a los usuarios y empleados sobre los ataques de phishing, haciendo hincapié en que no deben descargar archivos adjuntos no deseados de direcciones de correo electrónico aleatorias.



2. Hacer una copia de seguridad de sus archivos regularmente.

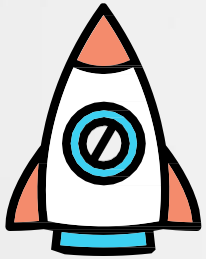
La mejor manera de mantener sus datos a salvo es hacer copias de seguridad de sus sistemas con regularidad. Con las copias de seguridad, los ataques de ransomware no podrán interrumpir el flujo normal de la empresa. Y asegúrese de que la copia de seguridad solo tiene permisos de lectura/escritura para que nadie tenga oportunidad de modificar o borrar sus datos. Una vez que haya hecho una copia de seguridad de sus archivos, asegúrese de comprobar periódicamente el estado de esas copias para detectar inmediatamente cualquier fallo.



3. Estructurar su seguridad.

Divida su red en macrozonas y microzonas para impedir que los hackers accedan a información confidencial. Separe sus computadores en función de su prioridad—crítica, moderada y baja—y proporcione niveles de seguridad basados en la importancia de la red. Por ejemplo, proteja sus servidores de forma más segura que sus computadores o dispositivos de usuario menos importantes.

4. Emplear tecnología de engaño.



Si los datos de su organización tienen que estar protegidos a toda costa, implemente tecnología de engaño para mantenerse a salvo de posibles violaciones de datos. La tecnología de engaño consiste en desplegar un sistema señuelo fuera del firewall, que confunde a los hackers con datos falsos. Como los llamados honeypots, su equipo de seguridad puede identificar las amenazas basándose en varias filtraciones a la vez, todo ello sin poner en peligro sus datos confidenciales. Una vez identificada la amenaza, su organización puede defenderse del ataque respectivamente.

5. Parchear sus sistemas operativos regularmente.



Aunque haya adoptado todas las medidas de seguridad anteriores, su red puede seguir siendo susceptible de sufrir ataques de ransomware si sus sistemas operativos no están actualizados. Para eludir el ransomware completamente debe mantener sus sistemas Windows, Mac y Linux actualizados en todo momento. Implemente los parches faltantes para mantenerse seguro.



6. Actualizar sus aplicaciones de terceros.

Además de sus sistemas operativos, debe asegurarse de que sus aplicaciones de terceros también están actualizadas. Por ejemplo, si existe una vulnerabilidad en su departamento de diseño a través de una aplicación como Adobe Photoshop, los hackers pueden utilizar esta vulnerabilidad para penetrar en su red y empezar a infiltrarse en otros sistemas. Dicho esto, no deje ninguna brecha sin parchear.

Escenario del mundo real: Respondiendo a WannaCry y Petya

En cuanto se corrió la voz sobre los ataques de WannaCry y Petya, nuestro equipo de Desktop Central se puso inmediatamente en contacto con los clientes para ofrecerles un plan de defensa. En primer lugar, pedimos a los clientes que bloquearan los puertos SMB vulnerables que WannaCry y Petya estaban utilizando para propagarse por las redes. Después de bloquear con éxito esos puertos, instamos a los clientes a implementar los parches que faltaban en sus sistemas Windows. Una vez que se aseguraron que todos sus sistemas estaban actualizados, pudieron desbloquear los puertos SMB vulnerables. Con solo seguir estos simples pasos, nuestros clientes pudieron proteger toda su red de estos dos graves ataques de ransomware. Si ya ha penetrado en su red, la mejor estrategia es reducir la propagación del malware bloqueando los puertos SMB afectados y actualizando los demás sistemas de su red. Independientemente de estas medidas, la mejor manera de evitar que el ransomware se convierta un dolor de cabeza para su empresa es disponer de copias de seguridad adecuadas. Cuando se trata de cosas como las copias, puede ser reactivo o proactivo a la hora de proteger su red contra el ransomware. La mayoría de los profesionales de seguridad coinciden en que siempre es mejor ser proactivo y le ayudará a mantenerse protegido.

Combatir los ataques de ransomware con ManageEngine

Los ciberdelitos están evolucionando rápidamente, así que asegúrese de tener la solución correcta para mantenerse alerta y seguro. ManageEngine ofrece cuatro soluciones diferentes para combatir los ataques de ransomware basados en la estructura de su red y otras necesidades. Mitigue los ataques tanto proactiva como reactivamente para mantener seguros los datos de su organización.



Todas las soluciones que se indican a continuación ayudan a corregir las vulnerabilidades automáticamente, manteniendo su red protegida. 24/7

Endpoint Central

Una solución de gestión de endpoints que ayuda a gestionar servidores, desktops, portátiles, smartphones y tablets, todo desde una ubicación central.

PRUEBA GRATIS

Patch Manager Plus

Una solución exclusiva de gestión de parches que ayuda a gestionar Windows, Mac, Linux y más de 250 aplicaciones de terceros desde una ubicación central.

PRUEBA GRATIS

Desktop Central MSP

Una solución de gestión de endpoints diseñada para proveedores de servicios gestionados (MSPs).

PRUEBA GRATIS

Patch Connect Plus

Automatic third-party patch management for Microsoft SCCM.

PRUEBA GRATIS

Beneficios

Utilice cualquiera de las soluciones anteriores y disfrute de una gestión de endpoints sin complicaciones.

- ✓ Prevenir futuros ataques de ransomware.
- ✓ Reducir las brechas de seguridad.
- ✓ Minimizar el tiempo de inactividad
- ✓ Mantener los datos corporativos seguros
- ✓ Evitar la pérdida de datos
- ✓ Mantener la productividad
- ✓ Mantener la imagen de marca, la reputación y la satisfacción del cliente



K. Ryan Coe,
Gestor de redes informáticas

“Desktop Central se ha convertido en una valiosa herramienta en nuestro entorno. Fue muy fácil configurarla. En menos de una hora tenía el servidor funcionando e instalando agentes en toda la red. Mantener nuestros equipos actualizados, a salvo y seguros nos protege tanto a nosotros como a nuestros clientes. Tener la capacidad de parchear, actualizar, instalar y eliminar programas de forma masiva me permite enfocarme en otros proyectos y áreas.”

Pruebe Desktop Central

Desktop Central es una solución unificada de gestión de endpoints que ayuda a gestionar miles de servidores, desktops y dispositivos móviles desde una ubicación central. Automatiza todo el ciclo de vida de la gestión de desktops y dispositivos móviles, desde una simple configuración del sistema hasta una compleja implementación de software. Utilizado por más de 6.000 clientes en todo el mundo, Desktop Central ayuda a las empresas a reducir costos en infraestructura de TI, garantizar la eficiencia operativa, mejorar la productividad y combatir las vulnerabilidades de la red.



Para mayor información por favor visite
www.manageengine.com/latam/desktop-central.

También disponible en

Windows Azure Marketplace | awsmarketplace

Integración con otros productos

SPICEWORKS | servicenow | ManageEngine ServiceDesk Plus

About ManageEngine

ManageEngine integra la TI para los equipos de TI que necesitan ofrecer servicios y soporte en tiempo real. Las empresas emergentes y con larga trayectoria de todo el mundo—más del 60 por ciento de Fortune 500—confían en nuestras herramientas de gestión de TI en tiempo real para garantizar una estrecha alineación con TI y el óptimo rendimiento de su infraestructura de TI, incluidas las redes, los servidores, las aplicaciones, los desktops, entre otros. ManageEngine es una división de Zoho Corporation en oficinas en todo el mundo, incluyendo Estados Unidos, India, Singapur, Japón y China. Para obtener más información, visite https://www.manageengine.com/latam/; siga el blog de la empresa en https://blogs.manageengine.com/espanol, o síganos en Facebook https://www.facebook.com/ManageEngineLA/ y Twitter @ManageEngineLA



Giridhara Raam es un expert en productos ManageEngine, una división de Zoho Corp.

Trabaja con el equipo de gestión de endpoints, comercializando Desktop Central y las herramientas gratuitas de administración de Windows de ManageEngine. Además, también se dedica a la investigación sobre ciberseguridad desde un contexto de gestión de endpoints.


ManageEngine
IT Management, Simplified