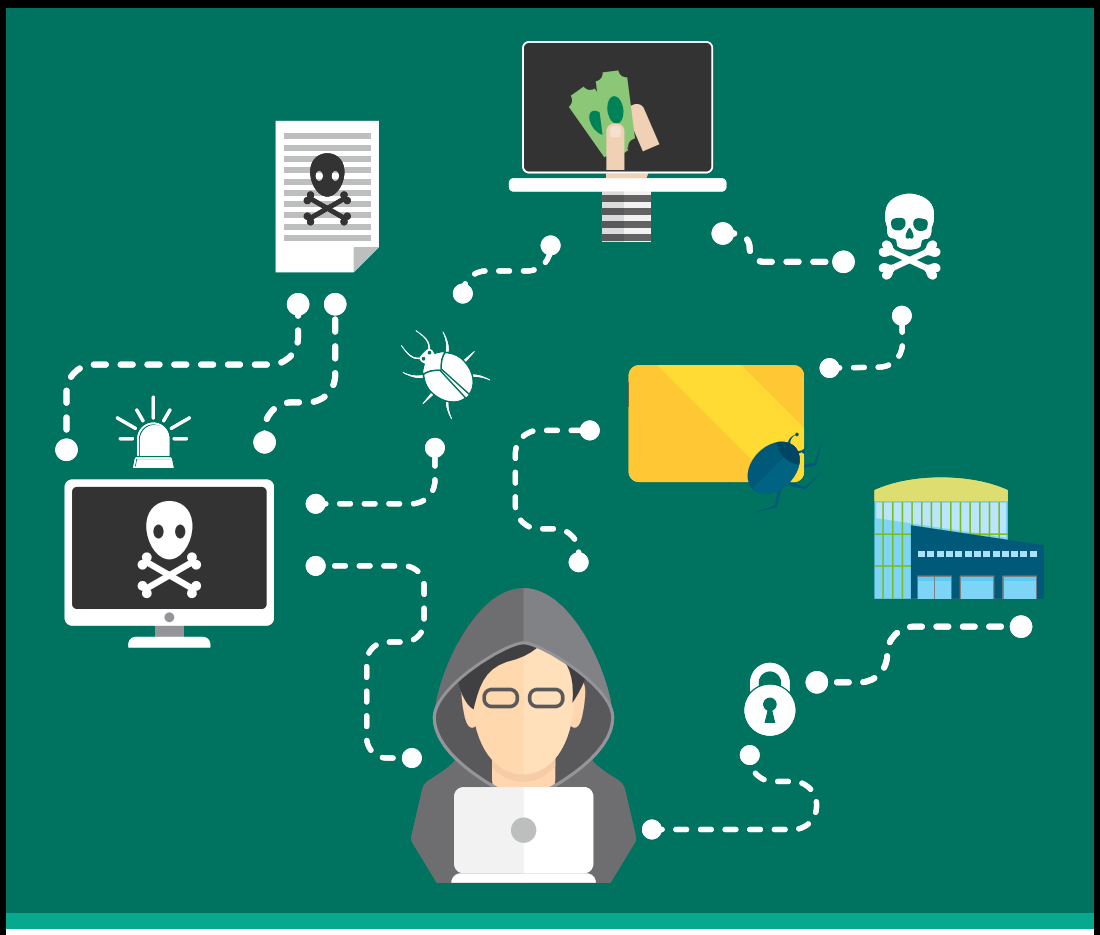
SECURITY [SNAPSHOT]



Cuando los Cifradores Atacan:

Cronología de una infección Ransomware

KASPERSKY lab

¿Qué tan grande es la amenaza de un malware cifrador para las PyMES?

La cantidad total de daños causados por un malware cifrador se puede dividir en dos partes: el rescate y las pérdidas relativas. Partiendo de la encuesta realizada por Karspersky Lab y B2B International a más de 4,000 pequeñas y medianas empresas, podemos ver de cerca los números detrás del daño.

49% Representantes de PyMES consideran que un malware cifrador es una de las amenazas más grandes a las que sus organizaciones se podrían enfrentar.

$99,000 La cantidad promedio de daños causados a las PyMES por un ataque de malware cifrador.

1 de cada 5 Compañías no logran recuperar sus datos después de pagar el rescate.

67% PyMES que reportan la pérdida completa o parcial de datos corporativos debido a un ataque cifrador.

¿Qué es un malware cifrador?

Un malware cifrador es un tipo de ransomware, el malware que intenta obtener un pago de rescate a cambio de desbloquear el acceso a su computadora, su servidor o sus archivos. En el caso del malware cifrador, la información secuestrada se conforma de archivos o datos que están almacenados en un dispositivo infectado. El malware cifra los datos en un formato ilegible, y únicamente puede ser descifrado utilizando la clave de descifrado necesaria, una clave que es otorgada una vez que la víctima ha pagado el rescate exigido.

El malware cifrador es una amenaza peligrosa que hace que la recuperación de sus datos corporativos sea virtualmente imposible. Además, hay que añadir la presión del límite de tiempo, puesto que el rescate debe pagarse en cuestión de días o de lo contrario todos los datos se pierden.

Cronología de un Ataque Cifrado

¿Cómo se desarrolla exactamente un ataque cifrado?
Le mostraremos paso a paso cómo es un ataque y lo que pueda hacer para prevenirlos.

1 El perímetro tiene una brecha.

Los cibercriminales buscan un fácil acceso a sus sistemas, y pueden obtenerlo enviándole un correo electrónico con un archivo adjunto infectado, el cual, abrirán los empleados. También pueden infectar una página web con un malware que usará kits de explotación para identificar las vulnerabilidades del software en la computadora del usuario. Posteriormente, estos kits de explotación se comunican con la computadora y cargan un código malicioso en ella. Normalmente, esto ocurre sin que el usuario se percate que ha cargado un software malicioso.

ELEMENTO DE ACCIÓN:
Instale una solución de seguridad resistente y multicapa que busque malware de manera continua desde diferentes ángulos con el fin de proteger su sistema contra posibles brechas.

2 Descubra y entre en pánico.

A estas alturas, el departamento de TI descubre lo que ha ocurrido y todo se paraliza. Hay muchas preguntas por responder. ¿Cuántas computadoras están infectadas? ¿El servidor está infectado? ¿La información ha sido robada? ¿Tenemos copias de seguridad que puedan restaurar todo para volver a la normalidad, recuperar todo y seguir funcionando como de costumbre?

ELEMENTO DE ACCIÓN:
Para el departamento de TI es un mal día en el trabajo. Nadie quiere enfrentarse a la situación de tener computadoras infectadas, o incluso peor, un servidor entero desconectado. Debe tener un plan de acción detallado con los pasos a seguir en caso de que su compañía sea atacada por un cifrador y tenga que enfrentarse a este tipo de situaciones.

3 ¿Pagamos el rescate?

Muchos de los cibercriminales exigirán un pago en bitcoins, una moneda que no puede ser rastreada por las autoridades. Pero tenga en cuenta que una de cada cinco compañías no recuperan sus archivos, incluso después de haber pagado el rescate.

ELEMENTO DE ACCIÓN:
Nosotros no recomendamos pagar el rescate por múltiples razones. Además del hecho de que no existe la garantía de que los cibercriminales le vayan a dar la clave de descifrado, también está el hecho de que el ransomware no es su único problema. Si pagar el rescate es su única opción, es una señal de que no tiene un plan de recuperación en caso de desastres. Si este es el caso, entonces no será capaz de remediar el ataque y eliminar totalmente la infección de tu infraestructura. Finalmente, todos tenemos que romper el círculo vicioso y dejar de alimentar la máquina cibercriminal. Si los cibercriminales dejan de obtener beneficios, dejarán de desarrollar más ransomware.

4 Tiempo muerto e interrupción del negocio.

Muchos de los malware cifradores le dan un tiempo limitado para pagar el rescate, normalmente tres días. De acuerdo con nuestra encuesta, un 48% de las compañías requieren muchos días para recuperar todos sus datos. Y en ese tiempo, el 41% reporta la pérdida de una cantidad significativa de archivos completos si tardan más de un día en detectar el ataque. Mientras todo esto ocurre, las operaciones normales en su compañía se ven interrumpidas. El tiempo de interrupción depende, principalmente, de las medidas preventivas que haya tomado el personal de TI, incluso antes de que la infección se haya llevado a cabo. ¿Tiene copias de seguridad actualizadas? ¿Ha actualizado y parcheado tu software? ¿El resto de su personal conoce los pasos a seguir para detener la propagación de la infección? Todo esto afecta al tiempo muerto y a las pérdidas a las que se tiene que enfrentar en caso de un ataque.

ELEMENTO DE ACCIÓN:
Prepárese. Actualice sus copias de seguridad. Mantengase al tanto de las novedades de actualizaciones de software y parches. Enseñe a sus empleados las mejores prácticas para el uso de su correo electrónico.

5 Autopsia y reporte forense.

Una de las únicas cosas buenas que se sacan de un ataque es el conocimiento y la comprensión. Lo más probable es que termine como si acabara de hacer un curso intensivo en ransomware, pero, ese conocimiento puede ser utilizado para prevenir otra infección.

ELEMENTO DE ACCIÓN:
Usted y su equipo de TI deben preguntarse lo siguiente: ¿Qué estuvo mal? ¿Cómo nos podemos proteger en un futuro? ¿Necesitamos educar a nuestros empleados? ¿Cuál es nuestro punto más débil? ¿Cómo podemos reducirlo? Haga un análisis y realice los cambios necesarios.

¿Cómo prevenir un ataque de malware cifrador?

Está claro que la prevención es el poder que derrota a los malware cifradores. Estos son los 10 pasos que recomendamos seguir para evitar que un ataque tome desprevenida a su empresa.

1. **HAGA COPIAS DE SEGURIDAD DE SUS ARCHIVOS DE FORMA REGULAR.** La única forma de asegurar que puede manejar inmediatamente un ataque de ransomware es implementando un programa regular de resguardo, así no tendrá que confiar en los cibercriminales para recuperar sus archivos y poder funcionar.

2. **REVISE SUS COPIAS DE SEGURIDAD.** Algunas veces hay cosas que pueden dañar sus archivos. Asegúrese de revisar periódicamente que sus copias de seguridad estén en buenas condiciones.

3. **PROTÉJASE CONTRA ATAQUES DE PHISHING.** Enseñe a sus empleados que no deben abrir archivos adjuntos de un remitente desconocido o incluso archivos sospechosos de amigos en caso de que hayan sido hackeados.

4. **NO CONFÍE EN NADIE.** O bien, confíe, pero asegúrese. Los enlaces maliciosos pueden ser enviados por sus amigos o colegas cuyas cuentas han sido hackeadas. Si los empleados reciben algo fuera de lo común de algún amigo, ellos deberán llamar a esa persona directamente para confirmar el mensaje.

5. **PERMITA LA OPCIÓN "MOSTRAR EXTENSIÓN DE ARCHIVOS" EN LA VENTANA DE CONFIGURACIÓN.** Debido a que los troyanos son programas, los empleados deben estar advertidos de que deben mantenerse alejados de las extensiones como "exe", "vbs" y "scr". Los estafadores pueden usar diferentes extensiones para enmascarar un archivo malicioso como vídeo, foto o documento. .

6. **ACTUALICE SU SISTEMA DE OPERACIONES DE FORMA REGULAR.** Los cibercriminales explotan las vulnerabilidades del software para comprometer los sistemas. Con las herramientas automatizadas de Kaspersky Lab para la evaluación de la vulnerabilidad y la gestión de parches, su sistema será escaneado y los parches serán distribuidos regularmente para mantener su sistema actualizado.

7. **UTILIZA UN ANTIVIRUS RESISTENTE PARA PROTEGER TU SISTEMA DE RANSOMWARE.** Nuestros productos de Kaspersky Lab emplean un sistema de defensa multicapa que comprueba el malware desde diferentes ángulos, asegurándose de no corromper tu sistema.

Pero si el ransomware ataca...

8. **CORTE LA CONEXIÓN A INTERNET INMEDIATAMENTE.** Si descubre un ransomware, apague su conexión a Internet de inmediato. Si el ransomware no elimina la clave de cifrado de los equipos en cuestión, entonces todavía existe la posibilidad de que pueda restaurar sus archivos.

9. **NO PAGUE EL RESCATE.** Si sus archivos se convierten en archivos cifrados, no le recomendamos pagar el rescate, a menos que el acceso instantáneo a alguno de sus archivos sea de gran importancia. Cada pago hará que los criminales prosperen y puedan desarrollar nuevas formas de ransomware.

10. **TRATE DE IDENTIFICAR EL MALWARE.** Si es atacado por un ransomware, trate de encontrar el nombre del malware. Las versiones más antiguas de ransomware solían ser menos avanzadas, por lo que, si es una versión anterior, podrá recuperar sus archivos. Además, los expertos en seguridad cibernética, incluidos los expertos de Kaspersky Lab, colaboran con las fuerzas de seguridad para proporcionar herramientas de restauración de archivos en línea, con la esperanza de detener a los adversarios. Algunas víctimas son capaces de descifrar los archivos sin tener que pagar el rescate. Para comprobar si es posible, visita NoMoreRansom.org

True Cybersecurity for Business

El enfoque de True Cybersecurity de Kaspersky Lab combina la seguridad multicapa con el aprendizaje automático y la inteligencia sobre amenazas asistida por la nube para proteger contra amenazas que pueda enfrentar su negocio. True Cybersecurity no solo previene ataques, sino que también predice, detecta y actúa rápidamente, asegurando al mismo tiempo, la continuidad de tu organización.

Acerca de Kaspersky Lab

Kaspersky Lab es una de las compañías de ciberseguridad de más rápido crecimiento en el mundo y la más grande como propiedad privada. La compañía se encuentra entre los cuatro principales proveedores mundiales de soluciones de seguridad para usuarios finales (IDC, 2014). Desde 1997, Kaspersky Lab ha sido un innovador en ciberseguridad y ofrece soluciones efectivas de seguridad digital e inteligencia contra amenazas para grandes empresas, PyMES y consumidores. Kaspersky Lab es una compañía internacional que opera en 200 países y territorios alrededor del mundo, proporcionando protección a más de 400 millones de usuarios a nivel global. Lee más en latam.kaspersky.com.

Aprenda más acerca de la seguridad de Internet: **www.securelist.com**
Encuentre un socio de negocio cerca a usted aquí.

latam.kaspersky.com
#truecybersecurity

Contáctenos: **latam.kaspersky.com/small-to-medium-business-security/contact-us**