Resumen

¿Se puede ignorar el Ransomware?

La Oficina de Abogados del Condado de Pinal, Arizona se vio atacada recientemente por uno de los principales ransomware, el denominado CryptoLocker. Se destruyeron más de 65 000 archivos. Afortunadamente, no se propagó al juzgado y a otras redes de seguridad pública.

El condado no tiene implementada ninguna defensa. No obstante, tenían copias de seguridad, pero restaurar su sistema ha sido un proceso largo ya que se aseguran de que se hayan eliminado todos los rastros de ransomware.

Al final de cuentas, están pagando un alto precio en tiempo y dinero para recuperar su sistema. También están pagando un precio en productividad pérdida y desgaste de la confianza del público. Todo esto podría haberse evitado con la ciberseguridad adecuada.

¿Pagará el rescate de un rey?

En Cisco, ya estamos visualizando el futuro del ransomware, lo que denominamos el marco de rescate de un rey. Creemos que se centrará en:

- El cifrado de las ubicaciones estándares, la personalización de tipos de directorios/archivos y la personalización de blancos
- Marcando sistemas y archivos que ya se han cifrado
- Rescate manual y capacidades de doble plazo
- Personalización basada en el entorno más propagación agresiva

El auge del ransomware

¿Está protegido?

La creciente amenaza para gobiernos estatales y locales

Cuando se trata de malware, actualmente, la mayor amenaza para los gobiernos estatales y locales es la información que se toma como rehén. La táctica conocida como ransomware, se ha venido utilizando por un tiempo ya, aunque recientemente viene consolidándose por haber evolucionado en el tipo más rentable de malware de la historia. En la actualidad, el ransomware va camino a **convertirse en una empresa de USD 1000 millones en 2016**.

Pero los gobiernos estatales y locales no están exentos al ransomware al igual que las autoridades encargadas del orden público, de Detroit a Maine y a Luisiana, las cuales también recibieron ataques (consulte Autoridad encargada del Orden Público es tomada como rehén por el ransomware). Y, lamentablemente, es probable que este éxito esté motivando a muchos adversarios a comenzar a planificar ataques similares de ransomware contra organizaciones como la suya. Si a ello le suma el hecho de que muchos organismos estatales desconocen un conjunto de vulnerabilidades de los servidores, a los atacantes se les presenta una oportunidad única. Por lo que es fundamental que los gobiernos estatales y locales comiencen a hacerse esta pregunta: "¿estamos realmente preparados para defendernos de intentos de hacer que nuestros sistemas críticos de seguridad pública e infraestructura dejen de funcionar?"

¿Qué es el Ransomware?

El ransomware es el nombre dado a una clase de malware que, una vez descargado, cifra datos fundamentales y exige un rescate para liberarlos. Los atacantes que implementan ransomware generalmente intentan atacar a la mayor cantidad de blancos lo más rápidamente posible, por lo que las cargas útiles se entregan a menudo mediante tres métodos:

- **Suplantación de identidad masiva** – correos electrónicos que se aprovechan de usuarios desprevenidos para habilitarse
- **Publicidad maliciosa** – publicidad maliciosa que se aprovecha de usuarios desprevenidos para habilitarse
- **Kits de ataque** – los cuales se aprovechan de las vulnerabilidades de software preexistentes, como las que se encuentran en aplicaciones comunes (Adobe Flash).

VIDEO: Entérese de las mayores amenazas cibernéticas para 2017
Asista ahora

El ransomware apunta específicamente a los archivos de usuarios y evita dañar archivos de sistema para poder notificar al usuario de lo sucedido. También proporciona medios viables para que el usuario pague el rescate para recuperar sus archivos. Una vez que se cifran los archivos, el malware generalmente se autoelimina y deja un mensaje. Este mensaje le dará instrucciones a la víctima sobre cómo realizar el pago y recuperar acceso a sus archivos. Algunas variantes le muestran a la víctima un cronómetro en cuenta regresiva, amenazando con eliminar la herramienta de clave/descifrado si no se recibe el pago antes de que el cronómetro llegue a cero o, en otros casos, con aumentar el precio del rescate.

Resumen

La próxima gran amenaza:
Ransomware de autopropagación

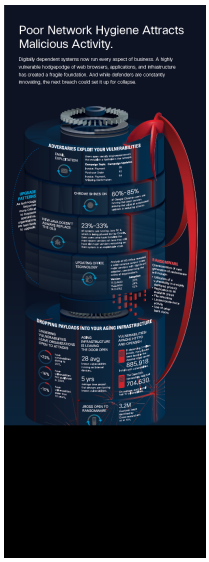
Para mantenerse circulando y propagándose, el ransomware de autopropagación:

- Utilizará una vulnerabilidad en un producto con alto grado de implementación
- Se copiará a todas las unidades (incluidas las unidades locales, remotas, de red y de USB)
- Se agregará o prefijará a archivos, específicamente los ejecutables
- Implementará medidas preventivas para contrarrestar la seguridad
- Utilizará puertas traseras o aprovechamiento

Talos es la organización de inteligencia de amenazas de elite de Cisco, la cual proporciona protección superior para clientes, productos y servicios. Más de 200 investigadores de amenazas a tiempo completo realizan un seguimiento de las amenazas a través de terminales,

VIDEO: Vea cómo Talos ayuda a vencer la amenaza de ransomware de Angler por USD 60M. Ver ahora

redes, entornos de nube, web y correo electrónico para brindar un panorama exhaustivo de amenazas cibernéticas, sus causas raíz y el alcance de los ataques. Luego, correlacionan estos datos en inteligencia de amenazas procesable. Los datos se ingresan automáticamente en los productos de seguridad de Cisco, mejorando su capacidad de detectar nuevas amenazas. Para más información, consulte Cisco Talos.



INFOGRAFÍA: ¿Está quedando vulnerable a ataques de malware no deseados? Ver ahora

Amenaza grande, precio grande

Hay miles de variantes de ransomware, pero las más innovadoras son CryptoLocker y CryptoWall. Los adversarios detrás de estas amenazas llevaron a su malware a todo un nuevo nivel de eficacia mediante un cifrado criptográfico de archivos de sonido. Esta técnica se hizo popular rápidamente y ahora la mayoría del ransomware no puede descifrarse con facilidad. Esto deja a las víctimas sin otra opción que pagar el rescate, el cual se sabe que puede ir de unos cientos a varios cientos de miles de dólares. Lamentablemente, pagando el rescate, las víctimas están financiando contra su voluntad el desarrollo de la próxima generación de ransomware.

Para los atacantes, el método de pago preferido es el Bitcoin (un Bitcoin equivale a aproximadamente USD 556,00) Es un tipo de divisa digital (también conocida como criptomoneda) que utiliza técnicas de cifrado para regular y verificar la transferencia de fondos que no dependen de un banco central. Ha ayudado a la industria del ransomware a prosperar, ya que los usuarios de direcciones de Bitcoin pueden permanecer anónimos.

Los bitcoins también se pueden dividir en fracciones, lo que permite a los atacantes pagar a su equipo completo con tan solo un Bitcoin de manera conveniente y básicamente imposible de localizar. Otra complicación para quienes combaten la amenaza del ransomware es que casi todos los intercambios se realizan a través de Tor, un anonimizador de Internet.

Cómo puede estar seguro

A medida que evoluciona la próxima generación de ransomware, es fundamental que su organización implemente una primera línea de defensa que pueda lograr **tres factores clave**: detener oportunidades de movimiento lateral del ransomware en su red, eliminar su propagación y reducir el tiempo que cualquier atacante tiene de operar en su red. Las mejores prácticas para **aplicar parches a** la infraestructura vulnerable de Internet y **mejorar la administración** de contraseñas también son importantes, al igual **que el control de infecciones del navegador,** para que pueda identificar y corregir amenazas más rápidamente.

Su organización también puede utilizar **la segmentación** de la red (segmentando su red en subredes) para detener, reducir y contener la autopropagación de amenazas. Esto incluye:

- VLAN y subredes que separen en forma lógica el acceso a datos
- Segmentación exclusiva del firewall y gateway
- Firewalls ejecutados en un host con configuración de filtrado de ingreso y egreso
- Aplicación de listas negras y listas blancas
- Permisos de intercambio de red basado en roles (privilegio mínimo)
- Adecuada administración de credenciales

Por último, aconsejamos que su organización implemente una línea de defensa de última línea: **recuperación de** copia de respaldo. Las copias de respaldo fuera del sitio son a menudo su única esperanza de restaurar el servicio sin pagar un rescate. Simplemente asegúrese de que no esté desprotegida ante el riesgo.

Próximos pasos

Para obtener más información acerca de amenazas actuales y emergentes de ransomware y acerca de cómo puede defenderse de ellas, ingrese en http://www.cisco.com/go/ransomware.

Para averiguar cómo su gobierno local o estatal se puede proteger contra las últimas amenazas cibernéticas, ingrese en Ciberseguridad de Cisco para el Gobierno.