Principales Recomendaciones para Prevenir el Ransomware

El ransomware ha pasado de ser una molestia sin mayor importancia a un sofisticado negocio criminal que genera millones de dólares que, ahora, apunta tanto a individuos como a organizaciones. Se trata de un modelo de negocios delictivo que utiliza software malicioso para retener sus datos personales en forma criptográfica. Si bien se trata de un desafío de urgencia creciente, el ransomware puede prevenirse con la capacitación adecuada, modificaciones específicas en el entorno actual de TI y la tecnología avanzada de endpoints.

¿Qué es el ransomware?

Los atacantes deben seguir cinco pasos para que un ataque de ransomware sea exitoso:

1. **Comprometer y controlar el sistema.** La mayoría de los ataques comienzan con el spear-phishing, a partir del cual se engaña al usuario que recibe un correo electrónico fraudulento para que abra un adjunto infectado que afecta al sistema. Esto puede afectar a una sola computadora, un solo teléfono móvil o a toda una empresa.
2. **Evitar el acceso al sistema.** Una vez infectado, el atacante identifica y encripta ciertos tipos de archivos potencialmente de valor para la víctima, como documentos comerciales en formato .doc, .xls and .pdf; o bien, niega por completo el acceso a todo el sistema por medio de pantallas de bloqueo o tácticas de intimidación.
3. **Alertar al dueño del dispositivo respecto del compromiso, monto de la recompensa y pasos a seguir.** Aunque parezca obvio, los atacantes y las víctimas suelen hablar en idiomas diferentes y tener distintos niveles de capacidades técnicas; por lo tanto, los atacantes deben explicar a las víctimas de forma que puedan comprender lo que ha sucedido y entender los pasos a seguir para desbloquear sus dispositivos.
4. **Aceptar el pago de la recompensa.** El atacante debe tener una manera de recibir los pagos de la recompensa y, al mismo tiempo, eludir a los organismos de cumplimiento de la ley, lo que explica el uso de monedas criptográficas anónimas, como Bitcoin para este tipo de transacciones.
5. **Asegurar la promesa sobre el restablecimiento del acceso total una vez recibido el pago.** El hecho de no poder restablecer los sistemas afectados destruirá la eficacia del esquema, ya que nadie paga una recompensa si no confía en que se le devolverán sus datos de valor.

¿QUIÉN ESTÁ EN RIESGO?

Las corporaciones en la mira. Los ataques de ransomware pueden tener un fuerte impacto público, ya que las operaciones de las organizaciones atacadas pueden ser severamente afectadas o detenidas por completo, como fue demostrado por los recientes ataques a hospitales en los Estados Unidos. Los delincuentes se dieron cuenta de que se trata de un negocio rentable con bajas barreras de entrada. En consecuencia, el ransomware ahora ocupa el lugar de otros modelos de negocios de delitos cibernéticos. Además, los atacantes serán cada vez más sofisticados en su habilidad para determinar el valor de la información afectada, evaluar la voluntad de pago de la organización comprometida y exigir mayores recompensas.

Más plataformas. Si bien, históricamente, los atacantes se enfocaban de manera exclusiva en sistemas de Microsoft® Windows®, el surgimiento del ransomware para Android™ y, tal como descubrió hace poco Palo Alto Networks® en Mac® OS X®, demuestra que ningún sistema puede permanecer inmune a estos ataques. Casi todas las computadoras o los dispositivos con conexión a Internet son víctimas potenciales del ransomware, lo que será una preocupación aún más urgente con la expansión de Internet de las cosas (IoT) y la proliferación de dispositivos adicionales, como la tecnología para vestir y los aparatos domésticos, conectados a Internet.

PREPARARSE Y PREVENIR

Los ataques de ransomware actúan de manera rápida, por lo general en minutos luego de la infección, por lo que es crítico adoptar medidas e implementar controles que atenúen o prevengan los ataques de ransomware. Las próximas dos secciones resumen las recomendaciones más importantes para cumplir con estos dos aspectos.

RECOMENDACIONES PRINCIPALES PARA MINIMIZAR EL IMPACTO DEL RANSOMWARE

1. **Desarrollar e implementar un plan para un programa de concientización destinado a usuarios finales**
   - Obtener aprobación para enviar recordatorios de seguridad a toda la compañía en forma periódica puede ser complicado, pero los usuarios finales más preparados resultarán seguramente en menos incidentes de ransomware.
2. **Revisar/Validar procesos de copia de seguridad de servidores**
   - Algunas organizaciones no se dan cuenta de que sus copias de seguridad están comprometidas, o estaban mal configuradas, hasta que ya es demasiado tarde. Tal vez se necesiten para restablecer el sistema.
   - Comenzar con sus servidores de archivos que alojan la red compartida para los principales departamentos.
3. **Revisar permisos de unidad de red para minimizar el impacto que un usuario único puede generar**

   Revisiones de Privilegio de Usuario Final
   - Designar un gerente de proyectos para que organice la tarea de evaluar los permisos que tienen los usuarios en las unidades de red asignadas. Implementar el principio de privilegios mínimos para reducir el impacto que un usuario individual puede tener en las unidades de red compartidas de la organización.
   - Según el tamaño de la organización, este proceso podría ser una tarea grande y compleja; por lo tanto, comenzar con las ubicaciones de las unidades de red que usan los departamentos principales.

   Revisiones de Privilegio de Usuario Administrador
   - Auditar los roles con privilegios para los equipos de servidores, copias de seguridad y de red par validar el acceso adecuado.
   - Procurar que a los administradores se les asignen cuentas normales y restringidas, que estén separadas de sus cuentas con mayores privilegios.
   - Exigir a los administradores que usen sus cuentas con privilegios solo cuando las necesiten.
   - Eliminar las asignaciones automáticas de unidades de red de las cuentas administrativas, donde sea posible.
   - Restringir las cuentas administrativas para que no reciban correos electrónicos.
4. **Documentar su plan de respuesta ante incidentes de ransomware**
   - Probablemente ya tiene un plan genérico de respuestas ante incidentes, pero es necesario estar preparado para el ransomware, en particular, porque requiere de un proceso muy específico de recuperación que es bastante diferente de otros incidentes de malware.
   - Los casos en los que todos los archivos de la unidad de todo un departamento resultan encriptados pueden ser bastante complejos ya que requieren de la participación de varios equipos: equipos de copia de seguridad, servidor de archivos, endpoints, directorio, etc. Cuanto más se planifique ahora, más rápido será el tiempo de respuesta.

PRINCIPALES RECOMENDACIONES PARA PREVENIR EL RANSOMWARE

1. **Desactivar los archivos de comando con macros en los archivos de MS Office con la política de grupo de AD**
   - Según Microsoft, el 98 % de amenazas dirigidas a Office usan macros. Si se desactivan los archivos de comando con macros en los archivos de MS Office, se podrá detener el ransomware como Locky.
   - Toda la organización no suele requirir los macros de Office, pero es posible que algunos sectores sí los necesiten. Activar los macros solo para excepciones o para departamentos específicos.
   - Office 2016 tiene una función nueva que permite a los administradores bloquear macros para evitar que se procesen en documentos de Word, Excel y PowerPoint que se originan en Internet. Por lo tanto, si se puede actualizar la versión, hágalo y active esta función.
2. **Realizar un recuento y analizar sus procesos de administración de parches mensuales**
   - Muchas organizaciones se esfuerzan por parchar los sistemas en el plazo de 30 días como la versión de parche mensual "Martes de parche" de Microsoft.
   - Revisar sus procesos de parchado y buscar oportunidades para eliminar los obstáculos.
   - Pensar en la posibilidad de implementar un producto de endpoints avanzado que evite los exploits ante parches faltantes y malware.
3. **Realizar un recuento y analizar su protección contra correo no deseado y/o malware entrante**
   - Asegurarse de que el sistema esté configurado para bloquear el correo electrónico entrante según las recomendaciones de su proveedor de servidor (bloquear los ejecutables en los adjuntos, etc.).
4. **Implementar un firewall de nueva generación para proteger la red**
   - Asegurarse de que su firewall bloquee automáticamente las amenazas conocidas según un avance de amenazas que se actualice constantemente.
   - Asegurarse de que su firewall proporcione capacidades de ejecución en modo sandbox para poder detener las amenazas desconocidas (URLs y ejecutables) antes de que lleguen al endpoint. La ejecución en modo sandbox es la mejor manera de detectar variantes nuevas de ransomware que aparecen en forma constante y libremente.
   - Configurar su firewall/proxy para que requiera de la interacción del usuario cuando los usuarios finales se comunican con los sitios web etiquetados como "sin categoría" (por ejemplo, haga clic en el botón "Continuar"). Muchos sitios web no categorizados se usan en campañas de estafas dirigidas para distribuir el malware. Este proceso de dos pasos evita que ciertos tipos de ransomware realicen llamadas externas al servidor de comando y control. Si eso no sucede, es probable que los archivos no estén encriptados.
5. **Implementar protección avanzada de endpoints para proteger los endpoints**
   - El antivirus tradicional no es efectivo contra un malware avanzado, como el ransomware, que cambia en forma continua para evitar su detección. Asegurese de que las medidas de protección de endpoints puedan detectar y prevenir el malware conocido y desconocido así como también los exploits conocidos y desconocidos, incluyendo los días cero.
   - La lista blanca puede funcionar en organizaciones simples y más pequeñas, pero para las empresas en crecimiento, que tienen muchas aplicaciones y mayor complejidad, esto puede requerir rápidamente de mucho trabajo para administrar la lista. La detección basada en técnicas de malware es muy efectiva en la detección de ransomware.
   - Asegurarse de que los sistemas de protección de endpoints cuenten con inteligencia de amenazas en tiempo real de fuentes internas y externas que atraviesan los límites, las geografías y las industrias de la organización.

¿BUSCA MÁS INFORMACIÓN?

Ransomware: paloaltonetworks.com/solutions/initiatives/ransomware
TRAPS: paloaltonetworks.com/products/secure-the-endpoint/traps
NGFW: paloaltonetworks.com/products/secure-the-network/next-generation-firewall