Ransomware: Buenas prácticas de prevención y respuesta

¿Qué es el ransomware?

El ransomware es un tipo de software malicioso que restringe el acceso a un equipo infectado, normalmente mediante la encriptación sistemática de los archivos del disco duro del sistema para a continuación exigir el pago de un rescate, – generalmente en forma de cripto-moneda (p. ej. Bitcoin) –, a cambio de la clave para desencriptar los datos.

¿Cómo se puede evitar una infección por ransomware?

- Asegurándose de que el software antivirus está actualizado.
- Formando a los trabajadores de forma regular para evitar intentos de suplantación de identidad (phishing).
- Sometiendo a los trabajadores a pruebas periódicas a través de campañas contra la suplantación de identidad, monitorizando el resultado de las mismas a traves de los índices de respuesta y estableciendo una política sancionadora formal (tras consultar con los departamentos jurídico y de recursos humanos) para infractores reincidentes.
- Bloqueando emails con extensiones .js, .wsf y .zip y macros en la puerta de acceso o gateways del correo electrónico. Cuando sea posible, habría que deshabilitar los siguientes vectores de ataque comúnmente utilizados: Adobe Flash Player, Java, y Silverlight.
- Si se utiliza JBoss, revisando la información del desarrollador sobre la configuración y endurecimiento.
- Evaluando si la lista blanca de la aplicación es compatible con nuestros sistemas.
- Habilitando ajustes automatizados para el sistema operativo y el navegador web. Una segmentación de red sólida a menudo reduce el impacto del ransomware.
- Permitiendo una gestión de identidad y acceso estricta, utilizando los principios establecidos de privilegio mínimo («necesidad de saber») y limitando los derechos de administración local.
- Invirtiendo en un sistema de detección de intrusiones para monitorizar indicios de actividad maliciosa. Implementando (y testando) un plan con respecto a copias de seguridad y recuperación de datos mantiendo de esta forma los datos sensible debidamente copiados y protegidos en una ubicación independiente y segura (preferiblemente offline). Las copias de seguridad de datos sensibles no deben estar accesibles desde las redes locales.

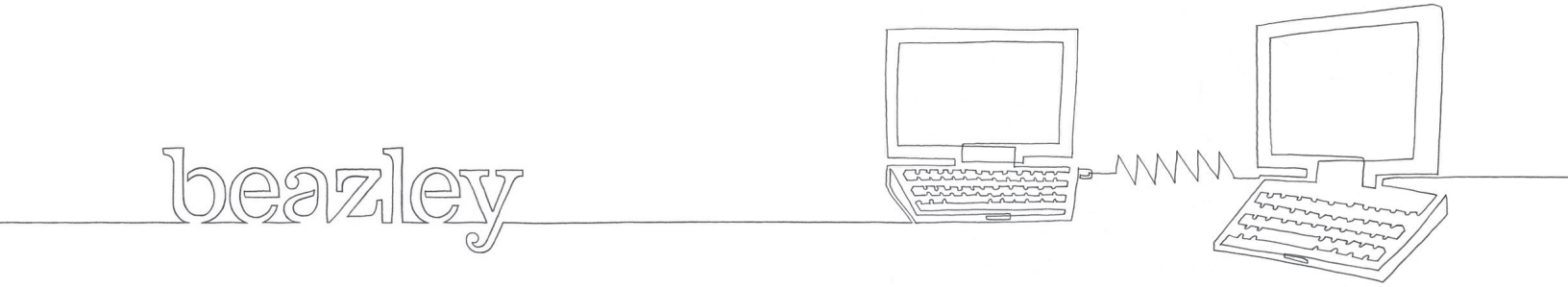
¿Cómo se puede actuar ante una infección por ransomware?

- Los equipos infectados deben desconectarse de la red (tanto de redes por cable como inalámbricas) lo antes posible.
- Hay que evaluar el alcance de la infección, tratar de identificar el tipo de variante de ransomware y determinar si los equipos infectados estaban conectados a discos de red compartidos o no compartidos, a discos duros externos, a USB o a sistemas de almacenamiento en nube. Además podría intentar buscar algún registro o listado de archivo que haya creado el ransomware.
- El ransomware debe eliminarse de los sistemas afectados (existen diversas herramientas de desinfección gratuitas y de pago para estos fines). El sistema operativo debe reinstalarse. Se sugiere llevar a cabo comprobaciones en las herramientas que se utilizan. Beazley no recomienda ningún producto concreto, sin embargo las marcas siguientes ofrecen herramientas de prestigio: BitDefender, Kaspersky Labs, Norton/Symantec y Trend Micro.
- Proceder a la restauración del sistema desde una copia de seguridad fiable. Un plan de copia de seguridad y restauración bien diseñado es una de las medidas de precaución más importantes frente al ransomware.

¿Cómo actuar si no se tiene una copia de seguridad de los datos?

Cuando la restauración desde una copia de seguridad reciente no es posible o ante el riesgo de que las operaciones se queden en un punto muerto, muchas organizaciones optan por pagar el rescate, sobre todo cuando el importe es relativamente bajo. Al hacerlo, estas organizaciones a menudo encuentran dificultades para conseguir el importe necesario de cripto-moneda (p. ej. Bitcoin). Además, se debe dedicar tiempo para pensar y reflexionar sobre cómo se desarrollará la transacción.

- No se puede esperar ningún tipo de honorabilidad por parte de los ladrones; los atacantes podrían coger el dinero y desaparecer, o el código de desencriptación podría no funcionar. Tampoco hay garantías de estar pagando al delincuente correcto.
- Algunos tipos de ransomware se pueden desencriptar con las herramientas adecuadas. Debemos averiguar de qué variante de ransomware se trata y mirar si existe alguna herramienta de desencriptación legal para ello. Hay que tener cuidado con las compañías que dicen poder «romper la encriptación». Muchas variantes de ransomware utilizan encriptaciones de nivel comercial y los ataques por fuerza bruta contra este tipo de ransomware resultan complicados o imposibles. Asimismo, hay que prestar atención a la fuente de cualquier «herramienta de desencriptación» para no causar más daños al descargar otro elemento de malware.



Ransomware: Buenas prácticas de prevención y respuesta

- Debemos pensar cómo y en qué medida debemos contactar con los delincuentes. A menudo, el ransomware que viene acompañado de una exigencia de extorsión cuenta con una línea directa o incluso páginas web específicas para guiar a las víctimas sobre del protocolo de pago.
- Existe la posibilidad de negociar un precio más bajo con los delincuentes, así como intentar ganar más tiempo pidiendoles la extesion del plazo límite.
- Hay que tener en cuenta que lo más probable es que los delincuentes no conozcan qué tipo de datos están en riesgo, y tampoco suelen conocer la ausencia de copias de seguridad. No se debe compartir ningún tipo de información identificativa con ellos. Si se enteran de que los datos son muy sensibles, el rescate exigido podría aumentar de forma significativa.
- Algunos tipos de extorsiones vienen con una «prueba de vida» que podrían ayudarle a comprobar que el delincuente tiene la capacidad de desbloquear los archivos. Es importante tener mucho cuidado y pensar antes de aceptar cualquier archivo de estos delincuentes.
- La adquisición de bitcoin online puede llevar entre 3 a 5 días laborables en algunos casos. Por lo general, se puede adquirir bitcoin a traves de una agencia de cambio o mediador. Las agencias de cambio de prestigio de Estados Unidos exigen el pago a traves transferencia bancaria ACH (por cámara de compensación automática), lo que lleva varios días.
- El proceso se puede agilizar utilizando una tarjeta de crédito o de débito en una agencia de cambio de fuera de Estados Unidos, pero los riesgos son mayores. No todas las agencias son fiables. y aquellas con buena reputación, suelen cobrar una mayor comisión por trasaccion a través de su Web ya que existe un elevado riesgo de fraude.
- Si el importe en bitcoin es relativamente bajo, obtener bitcoin de un cajero automático físico podría ser la opción más rápida. La mayoría de zonas metropolitanas cuentan con una red de cajeros bitcoin físicos donde se puede comprar bitcoin en persona.
- Para poder utilizar los bitcoins adquiridos, es necesario abrir una cartera bitcoin. Los distintos tipos de carteras disponibles son:

  Cartera bitcoin online: de acceso web.

  Cartera bitcoin de hardware: un dispositivo bitcoin físico de su propiedad.

  Cartera bitcoin de software: una aplicación que se instala en el ordenador o en el dispositivo móvil.

  Cartera bitcoin en papel: papel físico con una clave privada.

- Como compañía aseguradora de confianza, no podemos ofrecer garantías con respecto a ninguna agencia de cambio, cartera o transacción con bitcoin. Tampoco podemos garantizar que la transacción conducirá a la recuperación de los datos.

Tengo los bitcoin y la cartera y quiero pagar

Es importante tener en cuenta varias cosas. ¿Está dispuesto a pagar a una fuente desconocida? ¿Debe valorar algún tipo de aspecto de cumplimiento normativo o jurídico antes de utilizar los fondos de la organización para pagar un rescate o realizar un pago a una fuente desconocida?

- Todos los archivos recibidos de los delincuentes deben escanearse en busca de malware.
- Conviene probar la clave de desencriptación en una copia de seguridad de los datos encriptados si es posible, de manera que se pueda comprobar que funciona sin causar ningún problema potencial de corrupción de datos en los datos encriptados.

Todo esto suena demasiado complicado. ¿Puedo pedir ayuda a Beazley?

Por supuesto. Recomendamos ponerse en contacto con los servicios de respuesta ante violaciones de datos de Beazley (Beazley Breach Response Services o Servicios BBR) antes de plantearse el pago de cualquier rescate. También le ofreceremos orientación acerca de las alternativas y posibles proveedores que pueden ayudar en cada paso del proceso, siempre que sea posible.

Contacte con los Servicios BBR en bbr.spain@beazley.com o por teléfono en el +34 51 888 8347.

beazley