BackupAssist™

BackupAssist™

¿Qué es CryptoLocker?

Se trata de una extorsión virtual, que se apodera de tus documentos, los encripta para que sea imposible acceder a ellos, y pide un pago para desbloquearlos.

¿Cómo entra en tú Red?

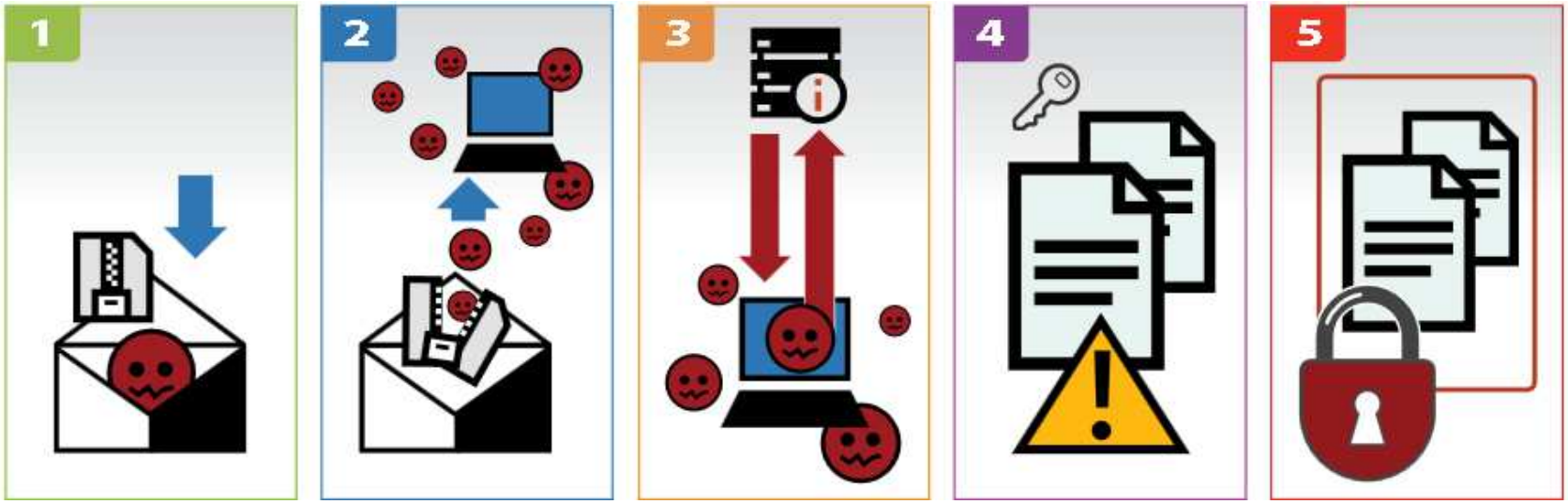
La principal fuente de infección es un correo electrónico de aspecto legítimo con un archivo adjunto que puede verse como un PDF legítimo.

También puede estar infectado por otro ordenador infectado o un sitio web malicioso.

COMO PROTEGERTE DE CRYPTOLOCKER

BackupAssist™

¿Cómo se genera la infección?



La victima recibe un email desde una dirección manipulada confiable, con un adjunto zip o doc que descarga.

BackupAssist™

¿Cómo se genera la infección?

Al abrir el contenido del mensaje se ejecuta el código malicioso e infecta el ordenador.

El virus se comunica con los servidores para generar las llaves de encriptación e intenta transmitirse a otros contactos y usando de la red suplantando la identidad del usuario.

Los archivos del usuario se comienzan a codificar con la llave de encriptación sin que este se entere hasta que es demasiado tarde.

Un mensaje le informa al usuario que sus archivos fueron bloqueados y debe pagar para volver a accederlos.

BackupAssist™

¿Cómo prevenir la infección?

Aunque cuentes con software anti-virus, actualizaciones y políticas de seguridad que mitiguen el riesgo de infección, la forma en que el virus se propaga con extremada facilidad hace que los riesgos sean demasiado altos.

¿Qué sucede si igualmente me infecto?

Las copias de seguridad fuera de línea son fundamentales ya que están desconectadas de la red y se almacenan en un lugar seguro a salvo de infecciones como CryptoLocker

BackupAssist™

¿Cómo proteger mi información con BackupAssist?

COMO PROTEGERTE DE CRYPTOLOCKER

Con el método Archiving de BackupAssist podrá de manera fácil y rentable mediante unidades flash tener una protección de datos multicapa de forma simple y con un coste mínimo.

Generación de Backups de múltiples niveles

Debe rotar los datos resguardados. Si sólo tiene dos copias, puede ocurrir quitar la última copia de seguridad y conectar el segundo dispositivo antes de darse cuenta que CryptoLocker ha infectado sus documentos.

Tener una tercera copia de seguridad de documentos de mayor importancia (con rotación semanal o mensual), y una cantidad de respaldos que garantice su recuperación en cualquier circunstancia.

BackupAssist™

¿Cómo es un Backup Multicapa?

Para que la protección sea efectiva debe involucrar al menos 2 tipos de medios distintos y contar en lo posible con 3 destinos para las copias.

Disco externo

Los discos externos USB suelen ser el medio mas económico, pero se debe contar con varios de ellos y que no se encuentren de forma permanente conectados al servidor para garantizar la integridad de datos.

Ubicación de red

Un NAS permite tener copias online, con una mejor capacidad de tolerancia a infecciones por tener su propio sistema operativo y permisos bien definidos para la copia de datos

Rsync

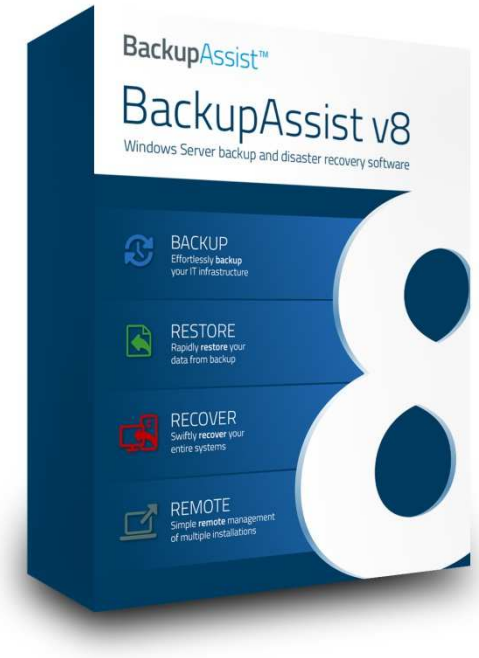
Rsync se puede utilizar tanto para backups a NAS tanto locales como en internet, permitiendo tener copias a salvo de cualquier riesgo/infección de la red local.

COMO PROTEGERTE DE CRYPTOLOCKER

BackupAssist™

Fin de la Presentación

¡GRACIAS!



sistembel@sistembel.com

COMO PROTEGERTE DE CRYPTOLOCKER