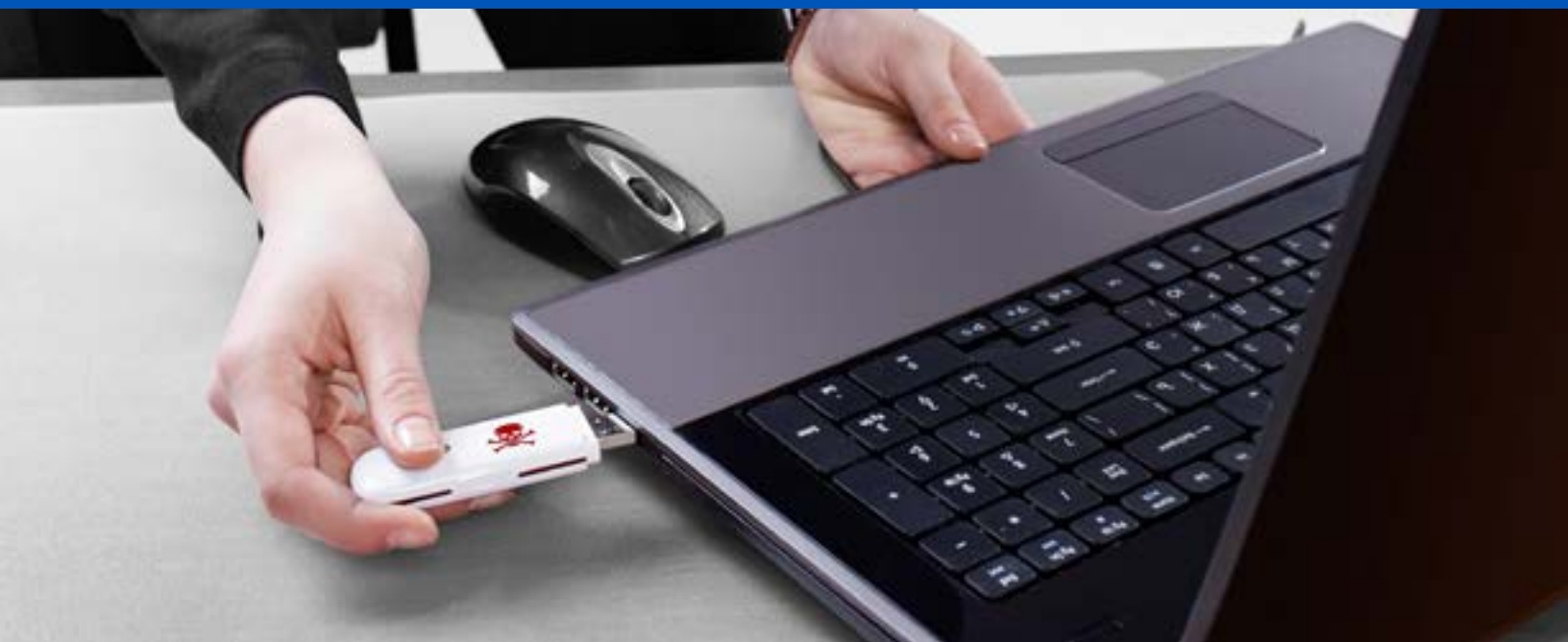
Ontrack®

Recuperación de Datos de Empresas luego de Ataques

2019



Resumen Ejecutivo

Los episodios de ransomware han alcanzado proporciones epidémicas. De acuerdo a algunas investigaciones, hasta un 28% de las organizaciones ha sufrido un ataque de ransomware el año pasado. Y las consecuencias pueden ser severas: desde no poder acceder a los datos de la compañía durante semanas, hasta la eliminación de bases de datos completas y enormes daños a la reputación y la consiguiente pérdida de confianza del cliente.

El FBI recibió 1.493 denuncias de ataques de ransomware en 2018, mientras que las pérdidas sufridas por las víctimas llegaron a los $3.621.857. Aunque eso sólo toma en cuenta los pagos de rescates, no los costos completos. El gobierno de la ciudad de Atlanta, por ejemplo, gastó aproximadamente 2,6 millones de dólares en costos de recuperación, luego de una demanda de rescate de ransomware de aproximadamente $52.000.

Según Symantec, los ataques de ransomware a empresas aumentan un 12% por año. Ésta es una de las principales razones para renovar el énfasis sobre la creación de copias de respaldo actualizadas y exhaustivas, ya que es frecuente que los archivos de respaldo estén incompletos, no tengan el debido cuidado e incluso en algunos casos, estén infectados con el mismo ransomware que infectó los sistemas principales.

Según Symantec, los ataques de ransomware a empresas aumentan un **12%** por año.

Si las copias de respaldo no pueden ofrecer una recuperación adecuada, las alternativas de mecanismos de respuesta incluyen técnicas de recuperación de datos como las de las herramientas de cifrado, la recuperación de datos lógicos directamente a partir de los medios de almacenamiento y el envío de los medios a un laboratorio en donde los técnicos intenten extraer tanta información como sea posible.

Lamentablemente, la epidemia de ransomware ha propiciado el surgimiento de prácticas cuestionables en el campo de la recuperación de datos. Algunas compañías proclaman falsamente contar con tecnología especial para recuperar datos. Cobran una tarifa alta pero, en realidad, lo único que hacen es pagar el rescate. Se descubrió que algunas compañías tenían una relación secreta con cibercriminales. Trabajaban en conjunto para infectar sistemas de empresas y luego lucrar con la “resolución” del problema. Esto puede darle mala fama a todo el ámbito de la recuperación de datos.

Por suerte, existen compañías con buena reputación como Ontrack, que ofrecen soluciones reales cuando los archivos han quedado cifrados con ransomware. Dichas compañías adhieren a los lineamientos del FBI con respecto a no pagar rescates nunca y emplear las tecnologías de recuperación de datos en funcionamiento. Dependiendo de la situación, puede ser posible recuperar la mayoría de los datos perdidos.

Ya que es el líder en el campo de la recuperación de datos para empresas, Ontrack debería ser la primera opción a contactar si las herramientas de respaldo y cifrado no pueden contrarrestar un ataque de ransomware en curso

Epidemia de Ransomware

El ransomware es un tipo de malware que cifra los archivos de los usuarios o impide de alguna otra manera el acceso a ellos. Cuando los usuarios intentan acceder a sus datos, reciben una notificación que solicita el pago de un rescate para poder volver a acceder a los datos.

De acuerdo a la firma de respaldo y ciberseguridad Datto, el ransomware les cuesta a las empresas aproximadamente 75.000 millones de dólares al año. Esta cifra incluye los rescates, los esfuerzos de recuperación subsiguientes, las iniciativas de IT y de las empresas a fines de protegerse frente a otros ataques, como así también los periodos de inactividad, la investigación forense, los costos de capacitación, la restauración y la pérdida de ingresos/ productividad.

Un cálculo más conservador por parte de Cybersecurity Ventures situa a los daños por ransomware en aproximadamente 8.000 millones de dólares durante 2018, con una predicción de alcanzar los 11.500 millones de dólares hacia finales de 2019. Es un aumento sorprendente en comparación a los modestos 325 millones de dólares de cuatro años atrás. En otras palabras, actualmente se produce un ataque de ransomware a una empresa cada 14 segundos.

Sin importar si las cifras son 75.000 u 8.000 millones de dólares, la devastación es muy real para aquellos que sufrieron un ataque de ransomware. En mayo de 2019, por ejemplo, el gobierno de la ciudad de Baltimore sufrió la salida de servicio de los sistemas del gobierno durante más de un mes. Se vieron afectados sistemas vitales para la producción de vacunas, cajeros automáticos, aeropuertos y hospitales. A pesar de que la demanda del rescate era de $76.000, el costo total del la recuperación alcanzó aproximadamente los $20 millones.

De forma similar, el gobierno de la ciudad de Atlanta gastó aproximadamente $3 millones en sus esfuerzos de recuperación cuando quedaron sin acceso cinco departamentos del gobierno local, entre los que se encontraban el de los registros policiales, el de mantenimiento de infraestructura, el del sistema judicial y el de cobros. Según todos los indicadores, las demandas de rescates están aumentando. Lake City, Colorado, pagó $460.000 y Riviera Beach, Florida, pagó $600,0000 para recuperar acceso a sus sistemas.

El FBI recibió **1,493** denuncias por ransomware en 2018, mientras que las pérdidas sufridas por las víctimas llegaron a

Las soluciones para el flagelo del ransomware incluyen herramientas de cifrado sofisticadas que pueden contrarrestar rápidamente algunos de los métodos de cifrado utilizados por esta forma de malware. Sin embargo, las variantes de ransomware se multiplican a gran velocidad. Hace algunos años, las variantes más virulentas de ransomware eran Locky, CryptoLocker y TorrentLocker. Ahora lo son SamSam, CrypoFortress y TeslaCrypt. En algunos meses más, surgirán nuevas variantes. Como resultado de ello, los proveedores de soluciones de mitigación de ransomware deben esforzarse para mantener el ritmo de las nuevas variantes que surgen.

Como si esto fuera poco, ha surgido una economía no visible que le da apoyo a los cibercriminales. Los desarrolladores de ransomware ofrecen soporte tecnológico y las variantes más modernas de ransomware a través de la Dark Web a cambio de una parte del botín. Esto llega al punto de ofrecer el Ransomware-como-Servicio (RaaS) lo que les permite a los criminales robar nombres de usuario y contraseñas sin contar con un conocimiento técnico sofisticado.

No sorprende que el ransomware siga creciendo. El FBI recibió 1.493 denuncias de ataques de ransomware en 2018, mientras que las pérdidas sufridas por las víctimas llegaron a los $3.621.857. Esas cifras, sin embargo, solamente toman en cuenta los pagos de los rescates, sin contemplar las repercusiones de los ataques, los ingresos perdidos o los daños a las relaciones públicas.

El sector empresarial, en particular, está bajo amenaza. El FBI, el Servicio Secreto de Estados Unidos y otras autoridades advierten desde hace años a las compañías de Estados Unidos que ciberespías y ciberladrones de países como China y Rusia tienen como objetivos a sus archivos de computadora. Los delincuentes buscan información relacionada a fusiones, patentes, secretos comerciales, detalles financieros y planes de negocios.

Uno de los aspectos más penosos de este problema es que normalmente se aprovecha de la ingenuidad de algunos empleados. Los correos electrónicos de suplantación de identidad continúan siendo efectivos para engañar al personal y lograr que abran adjuntos o visiten sitios perjudiciales. Esto permite que los delincuentes obtengan credenciales y roben fondos o inicien una infección por ransomware.

Mitigación y Prevención de Ransomware

Debido al continuo éxito de los métodos de suplantación de identidad, la capacitación de los usuarios es la principal línea de defensa contra el ransomware. También deben implementarse tecnologías y prácticas estándares de seguridad de IT, como antivirus, antimalware, prevención/detección de intrusos, cortafuegos, monitoreo de red y controles de acceso. Los puertos que no requieran de una conexión a Internet deben quedar cerrados y aquellos que sí la requieran deben ser cuidadosamente protegidos y monitoreados.

Últimamente han surgido en el mercado programas de heurística y aprendizaje automático que pueden buscar comportamientos de ransomware, como el cifrado por parte de programas no autorizados. Con el respaldo de una inteligencia contra amenazas y demás salvaguardas, un departamento de IT atento puede limitar las posibilidades de una intrusión.

Una vez que una infección queda contenida, por lo general las copias

Además, son necesarias más capas de protección, como copias de respaldo regulares. Estos respaldos deben ser exhaustivos, de fácil recuperación y deben ser probados para comprobar su fiabilidad.

A pesar de esto, el ransomware evoluciona de forma constante y encuentra nuevas maneras de infectar sistemas. Algunas veces, ataca sistemas específicos o bases de datos específicas. Con frecuencia, el malware comienza utilizando derechos de administrador robados para desactivar las copias de respaldo online, especialmente sobre SAN. En esos casos, el malware borrará los sistemas NAS. En otros casos, logra

infiltrarse y cifrar las copias de respaldo también. Algunos ataques de ransomware han estado orientados a aplicaciones de respaldo virtualizado, como Veeam. En vista de lo anterior, no es cuestión de si se producirá un ataque, sino de cuándo se producirá.

Las empresas deben estar preparadas. Las cintas conservadas en un sistema de bibliotecas de cintas pueden resultar sobrescritas, cifradas o deterioradas de alguna otra manera por un ataque de ransomware. Los respaldos desconectados eliminan la posibilidad de una mayor infección, si la copia de respaldo original está libre de malware.

Algunas mejores prácticas han evolucionado, con un detalle de las acciones a iniciar si se detecta un ataque de ransomware. Un principio fundamental es nunca pagar el rescate. El FBI es un firme defensor de no pagar. Y todos los miembros de la Conferencia de Alcaldes de Estados Unidos se comprometieron a nunca pagar un rescate a cibercriminales.

Después de todo, aquellos que paguen el rescate no obtienen ninguna garantía de que sus archivos queden intactos. Es posible que les pidan más dinero o que los sistemas de archivos queden infectados con muchos otros tipos de malware.

En conjunto con el no pago del rescate, las víctimas deben ponerse en contacto inmediatamente con las autoridades. Deben apagar inmediatamente los sistemas infectados y desconectarlos de la red. Los discos críticos deben ser clonados antes de hacer cualquier modificación. Una vez que se detecta un ataque, no debe perderse nada de tiempo. De lo contrario, es posible que la infección se extienda a otros usuarios, sistemas y aplicaciones.

Además, se han desarrollado programas que pueden contrarrestar ciertas variantes de ransomware. El departamento de IT debe ponerse en contacto con proveedores o autoridades para comprobar si la infección puede ser descifrada con facilidad. Actualmente existen más de 100 herramientas de descifrado que es posible utilizar contra más de 400 variantes de ransomware. Un ejemplo: el FBI publicó las claves maestras de descifrado para el ransomware GandCrab para que las víctimas pudieran descifrar los archivos infectados por GandCrab. De todos modos, hay que tener en cuenta que los cibercriminales logran siempre mantenerse un paso adelante. Cuando ya es posible descifrar una variedad efectivamente, comienzan a desarrollar una variedad alterada, que no es posible descifrar.

Una vez que una infección queda contenida, por lo general las copias de respaldo resultan la mejor opción para recuperar los datos. Los archivos de copia de respaldo correctos, ya sea provenientes de la nube, de aplicaciones de respaldo o de cinta, posibilitan que la organización vuelva al funcionamiento normal de forma rápida.

De todos modos, debe tenerse especial cuidado de comprobar que los archivos de respaldo no estén infectados también. La restauración de archivos que están infectados con ransomware simplemente llevará a una nueva infección de los sistemas de IT. Además, por lo general, los respaldos están incompletos, desactualizados e incluso deteriorados. En esos casos, la mejor opción es ponerse en contacto con un proveedor de recuperación de datos global, con un historial comprobado en el ámbito de la recuperación.

Opciones de Recuperación Más Allá del Respaldo

Aún en caso de que fallen los esfuerzos de descifrado y no se cuente con respaldos o los mismos estén incompletos, dependiendo del tipo de almacenamiento y el tipo de ransomware, tal vez sea posible recuperar los datos. Es posible el soporte de almacenamiento para compañías de sistemas copy-on-write, como NetApp WAFL o Oracle ZFS. Alguno de estos sistemas permiten que un ingeniero de recuperación retroceda en el tiempo a través de las distintas copias disponibles, hasta encontrar una versión no cifrada.

Este enfoque permite que la organización pueda restaurar sus datos, aunque será inevitable algún grado de pérdida de datos, si la copia no infectada tiene una antigüedad de dos semanas, es posible que se pierdan los datos de esas dos semanas. Por lo tanto, resultan críticas la detección e intervención tempranas, de manera de que el cifrado de ransomware afecte a la menor cantidad de copias posible. Cuanto más reciente sea el punto de recuperación, mejor.

Además, existen distintas técnicas disponibles que pueden recuperar datos de discos rígidos, almacenamientos secundarios, unidades de estado sólido, medios removibles y otros medios. Es posible utilizar estas técnicas para restaurar datos borrados, inaccesibles, deteriorados, dañados o reformateados, cuando han fracasado otros métodos.

El enfoque más simple son las herramientas basadas en software. Es posible utilizarlas en las instalaciones del usuario o de forma remota, para recuperar archivos que, de otra manera, se perderían. Las herramientas de recuperación por software ayudan a resolver problemas de pérdida de datos lógicos como borrado accidental y eliminación de particiones. También es posible recuperar archivos de la papelera de reciclaje, de instantáneas de volúmenes, y es posible realizar una recuperación de datos en crudo utilizando una búsqueda de firmas.

Si esto no resuelve el problema, es momento de solicitar una recuperación de datos en laboratorio. Incluso si los archivos están dañados, deteriorados o parcialmente cifrados, un laboratorio con buena reputación puede alcanzar el éxito en la recuperación de los datos. Es posible examinar las unidades defectuosas para verificar cuáles son los datos que es posible extraer, ya sea debido a fallas lógicas o físicas.

Ya sea a causa de una falta de actualizaciones del sistema operativo, soldaduras de baja calidad, componentes defectuosos, defectos de fabricación, como así también una amplia gama de situaciones de daño por desastres, caídas, roturas, agua, fuego o sobretensión, con frecuencia los servicios en laboratorio logran buenos resultados para recuperar datos que los usuarios creían perdidos para siempre. En el laboratorio es posible resolver incluso las fallas mecánicas o físicas como los contactos de cabezales, fallas de firmware y sectores defectuosos, con cierto grado de éxito.

Sin embargo, hay que tener en cuenta que existen algunas ofertas de servicios de recuperación de datos que son fraudulentas. Generalmente, es posible identificarlas por lo desproporcionado de la promesa de recuperación. Si garantizan una recuperación de datos cercana al 100%, es sospechoso. Algunos servicios afirman contar con el ingrediente secreto que desbloquea instantáneamente sistemas cifrados. Lo que hacen realmente es pagar el rescate y cobrar una tarifa abultada. Algunos de ellos incluso en connivencia con los cibercriminales. Por lo tanto, resulta esencial realizar la debida diligencia al momento de seleccionar una firma a la cual encomendarle la recuperación de

almacenamiento y las estructuras de datos de disco. Pueden reconstruir el RAID, los sistemas de archivos y datos a nivel de bloque. En muchos casos, los principales laboratorios pueden recuperar una cantidad de información sorprendentemente alta, que se creía perdida para siempre.

Servicios de Recuperación de Datos de Ontrack luego de Ataques de Ransomware

Ontrack es el líder del mercado en el ámbito de la recuperación de datos. A partir de una presencia global que abarca Europa, Norteamérica y APAC, Ontrack puede recuperar datos de virtualmente cualquier medio físico (HDD, SSD, cinta, smartphone, RAID, SAN, servidor o base de datos de Oracle y SQL), como así también a partir de pérdidas de datos lógicos y archivos borrados. Con el respaldo de una suite de herramientas de recuperación bajo derechos de propiedad y un experimentado equipo de recuperación de datos, Ontrack aporta una vasta experiencia en resolución de situaciones de pérdidas de datos, desde lo cotidiano a lo extremo. Esto incluye el borrado accidental, deterioro de medios, daño por agua o fuego, impactos y más, ya sea en instalaciones o de forma remota.

A lo largo de los años, Ontrack ha establecido una colaboración con todos los fabricantes principales de medios y almacenamientos. Esto le permite a la compañía tener un conocimiento profundo de cada tipo de sistema de archivos, plataforma de almacenamiento, medios y firmware, para poder encontrar cualquier tipo de datos recuperables y recomponer esos datos.

Ontrack sigue estrictos protocolos de seguridad de IT y realiza auditorías todos los años. Los antecedentes del personal son verificados antes de su contratación y la seguridad de las instalaciones está protegida con cámaras y accesos seguros, bajo certificación SAS70. Nuestro personal de recuperación de datos y de laboratorio cuenta con el respaldo de un equipo de 200 ingenieros de investigación y desarrollo. Hemos desarrollado más de 500 herramientas de software y hardware de recuperación de datos, bajo derechos de propiedad intelectual. Con nuestro software de imágenes bajo derechos de propiedad, por ejemplo, es posible tomar la imagen de una unidad desde atrás hacia adelante o desde cualquier punto, evitando las áreas dañadas de las placas. Este proceso preserva la unidad original, al tiempo de que aumenta la cantidad de datos que es posible recuperar. Para el caso de las SAN y el RAID, los ingenieros pueden tomar una imagen de cada unidad y reconstruir el RAID o hacer un striping de datos para recuperar los datos.

Los dispositivos y medios pueden enviarse al laboratorio o es posible realizar un una Recuperación de Datos por Servicios en Sitio, en las instalaciones del usuario, para aquellas situaciones de pérdida de datos lógicos más críticas y sensibles. Otra opción es la recuperación remota, utilizando avanzadas herramientas de recuperación de software.

Una empresa química suiza multinacional sufrió un ataque de ransomware que se apoderó de un sistema NetApp, utilizando privilegios de administrador obtenidos por suplantación de identidad. El ransomware formateó todos los discos rígidos al 30% y creó un nuevo conjunto. Ontrack pudo reconstruir el RAID y el sistema de archivos y restaurar los datos del cliente.

Resumen

Si el ransomware supera el perímetro de la red y no se dispone de una copia de respaldo completa, tal vez sea aún posible recuperar los datos. Cada situación requiere de un enfoque distinto de recuperación de datos. Aunque solamente debe confiarse la recuperación de datos luego de ataques de ransomware a proveedores globales con experiencia comprobada en sistemas empresariales. Ontrack cuenta con una extensa experiencia en la recuperación de datos de todos los medios y plataformas de almacenamiento principales.

Un principio firme de la política de Ontrack es nunca pagar rescates. En lugar de ello, Ontrack se concentra en recuperar la mayor cantidad de datos posible utilizando técnicas avanzadas. Ontrack cuenta con todas las capacidades, herramientas e instalaciones internas requeridas para la exhaustiva recuperación de datos empresariales.

Para obtener más información, visita www.ontrack.com/es o llama al 38 900 838 188.