G DATA TechPaper

Ransomware

G DATA Software AG | Septiembre 2017

Contenidos

Introducción

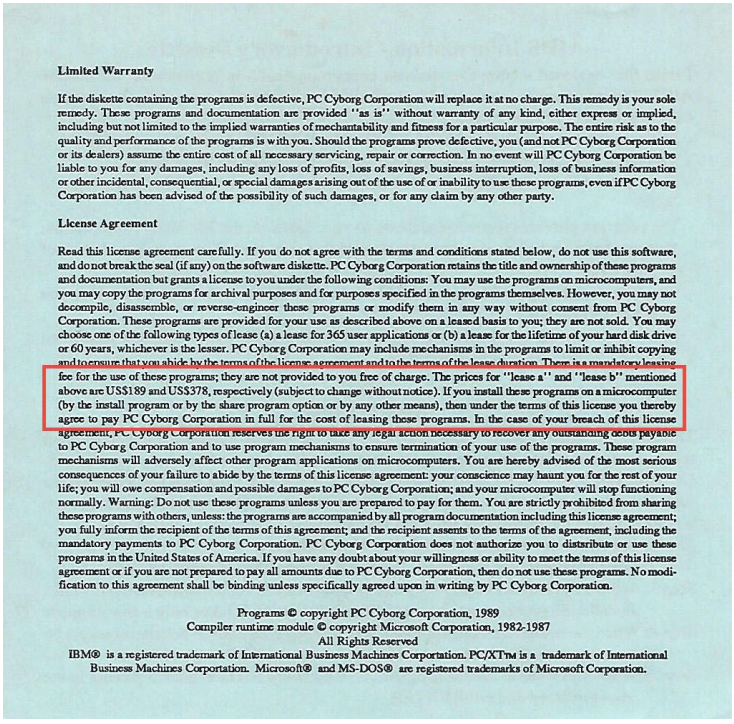
El ransomware ha evolucionado hasta convertirse en una de las amenazas más peligrosas tanto para usuarios domésticos como empresas. Con más de 4.000 ataques diarios y perspectivas de duplicarse en 2017, el riesgo de perder archivos personales, planes de negocio o información de clientes es cada vez mayor[1]. El objetivo de este documento es explicar qué es un ransomware y cómo funciona, para ayudar a evitar este tipo de infecciones.

1. ¿Qué es el ransomware?

Técnicamente, el ransomware es solo un tipo de malware, otra forma de software malicioso. Sin embargo, para sus víctimas se distingue de otras amenazas por una característica muy singular. Mientras que por regla general el malware infecta los dispositivos para usarlos como parte de una botnet o robar la información almacenada en ellos para venderla posteriormente en la dark web, los creadores del ransomware pretenden acelerar el proceso extorsionando directamente a las víctimas. Para ello, el ransomware bloquea los equipos y/o cifra la información almacenada en ellos hasta que la víctima realiza el pago de un rescate o chantaje.

1.1. Historia

En los últimos años, el ransomware ha protagonizado titulares, minutos y portadas de los medios de comunicación de masas más reputados. Usuarios particulares, pequeños negocios y grandes multinacionales, todo el mundo se ha convertido en una víctima potencial. Sin embargo, no se trata de un fenómeno nuevo y su historia se remonta a finales de los 80. En el invierno de 1989, se distribuyeron por primera vez más de 10.000 disquetes infectados con ransomware entre instituciones médicas, investigadores y particulares. Los disquetes contenían supuestamente información sobre el virus del SIDA, una verdadera epidemia entonces, pero usaba en realidad métodos criminales para obligar a aceptar un acuerdo de licencia y, posteriormente, bloquear el PC y “cifrar” archivos. Luego reclamaba 189 dólares que debían ser enviados a una oficina postal de Panamá. Técnicamente, este primer ransomware no era muy sofisticado y los archivos y programas de los equipos infectados pudieron restaurarse a partir de un antídoto creado sin demasiadas complicaciones.



Limited Warranty

If the diskette containing the programs is defective, PC Cyborg Corporation will replace it at no charge. This remedy is your sole remedy. These programs and documentation are provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of mechantability and fitness for a particular purpose. The entire risk as to the quality and performance of the programs is with you. Should the programs prove defective, you (and not PC Cyborg Corporation or its dealers) assume the entire cost of all necessary servicing, repair or correction. In no event will PC Cyborg Corporation be liable to you for any damages, including any loss of profits, loss of savings, business interruption, loss of business information or other incidental, consequential, or special damages arising out of the use of or inability to use these programs, even if PC Cyborg Corporation has been advised of the possibility of such damages, or for any claim by any other party.

License Agreement

Read this license agreement carefully. If you do not agree with the terms and conditions stated below, do not use this software, and do not break the seal (if any) on the software diskette. PC Cyborg Corporation retains the title and ownership of these programs and documentation but grants a license to you under the following conditions: You may use the programs on microcomputers, and you may copy the programs for archival purposes and for purposes specified in the programs themselves. However, you may not decompile, disassemble, or reverse-engineer these programs or modify them in any way without consent from PC Cyborg Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the following types of lease (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs; they are not provided to you free of charge. The prices for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of your breach of this license agreement, PC Cyborg Corporation reserves the right to take any legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing these programs with others, unless: the programs are accompanied by all program documentation including this license agreement; you fully inform the recipient of the terms of this agreement; and the recipient assents to the terms of the agreement, including the mandatory payments to PC Cyborg Corporation. PC Cyborg Corporation does not authorize you to distribute or use these programs in the United States of America. If you have any doubt about your willingness or ability to meet the terms of this license agreement or if you are not prepared to pay all amounts due to PC Cyborg Corporation, then do not use these programs. No modification to this agreement shall be binding unless specifically agreed upon in writing by PC Cyborg Corporation.

Programs © copyright PC Cyborg Corporation, 1989
Compiler runtime module © copyright Microsoft Corporation, 1982-1987
All Rights Reserved
IBM® is a registered trademark of International Business Machines Corportation. PC/XTtm is a trademark of International Business Machines Corportation. Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation.

Figura 1: Acuerdo de Licencia. Disquetes con ransomware. 1989

[1] Fuente: United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS); BBR Services.

En 1996 los investigadores utilizaron por primera vez el concepto de criptovirología que, básicamente, venía a describir el uso de la criptografía en la creación de software malicioso[2]. Se necesitó entonces alrededor de una década hasta que apareció el primer ransomware de distribución masiva con técnicas modernas de cifrado, como *PGPCoder* (2005) o *Archiveus* (2006). Mientras que algunos tipos de ransomware "solo" bloqueaban el PC, haciéndose pasar a veces por instituciones o agencias de la ley, el ransomware de cifrado se convirtió rápidamente en el tipo de ransomware más extendido y utilizado por los cibercriminales.

1.2. El ransomware en la actualidad

A medida que la ciencia de la criptografía avanzaba, los cibercriminales mejoraban la sofisticación de sus amenazas. Mientras que los ransomwares que bloqueaban los ordenadores no dejaban ningún daño permanente una vez que eran eliminados, la aparición del cifrado de archivos significa que incluso cuando el ransomware es eliminado sus daños son irreversibles y los archivos no pueden ser recuperados. Las amenazas actuales se basan en claves de descifrado que solo se pueden conseguir si ha habido algún error de implementación por parte de los creadores del malware. Las infecciones de ransomware, por tanto, deben ser evitadas y los usuarios y administradores de sistemas deben estar seguros de que pueden recuperar sus sistemas después de un ciberataque de ransomware.

A finales de 2013, Cryptolocker se convirtió en uno de los tipos de ransomware más agresivos y peligrosos y desde entonces han aparecido numerosas variantes formando una extensa y prolija familia de ransomwares más o menos emparentados. Todos ellos tienen en común su capacidad para cifrar la información almacenada en los equipos de sus víctimas y enviar la clave de recuperación al atacante. Para acceder de nuevo a los archivos (fotos, agendas y todo tipo de información personal y profesional), se obliga a las víctimas a pagar un rescate a cambio de la mencionada clave.

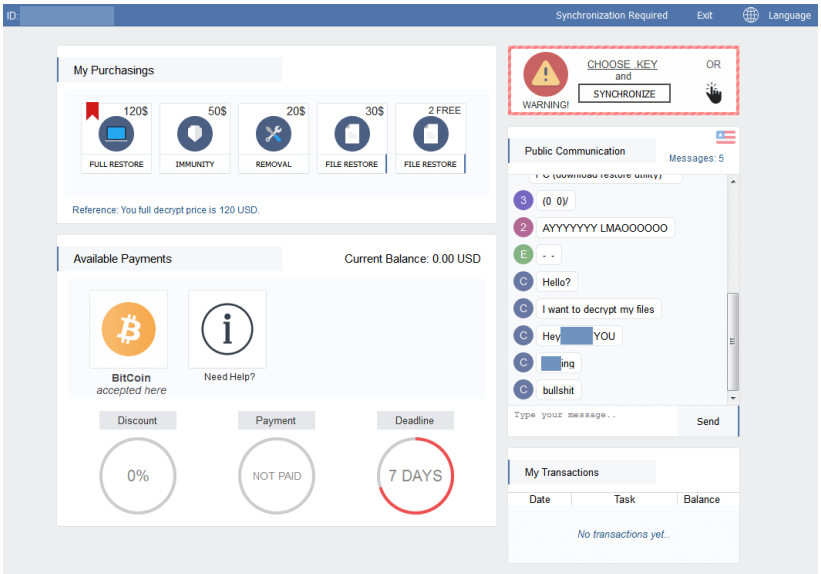


Figura 2: El ransomware Spora ofrece un chat para guiar a las víctimas en el proceso de pago

Otros ejemplos de malware, como Locky, WannaCry o Spora, difieren en su implementación pero mantienen la esencia de su funcionamiento. Y la realidad es que nos enfrentamos a amenazas cada vez más sofisticadas que reflejan el poder de la industria cibercriminal. Aunque hay una gran cantidad de ransomwares que "solo" cifran los archivos y muestran un mensaje solicitando el rescate, otros ya llegan apoyados por complejas infraestructuras que incluyen páginas web, sistemas de chat y hasta diferentes opciones de pago.

[2] Fuente: Adam Young and Moti Yung, Cryptovirology: Extortion-Based Security Threats and Countermeasures, IEEE (1996).

1.3. Distribución y víctimas

El ransomware utiliza las mismas formas de propagación que cualquier otro tipo de malware. Las más habituales son:

- Correos electrónicos con adjuntos y/o enlaces maliciosos
- Websites infectadas
- Redes de anuncios online maliciosos

A pesar de que los profesionales de la seguridad y los administradores de sistemas llevan años advirtiendo de la necesidad de no hacer clic en los enlaces maliciosos o archivos adjuntos procedentes de remitentes desconocidos, el spam se mantiene como el principal vector de infección. El ransomware a menudo se esconde en documentos de texto con macros habilitadas, pero sus archivos ejecutables pueden ser camuflados en cualquier tipo de adjunto. Además del spam, los cibercriminales pueden infectar páginas web capaces de descargar el virus tras la visita de cualquier internauta. O incluso sitios web que no han sido atacados pueden funcionar como aspersores de ransomware si alojan anuncios que, procedentes de redes que no los auditan suficientemente, incluyen código malicioso.

Por regla general, los cibercriminales no tienen objetivos concretos y prefieren distribuir sus «creaciones» a través del mayor número posible de canales, buscando un público masivo y heterogéneo, de forma que el riesgo de que tarde o temprano nos encontremos con uno de estos ransomwares es muy elevado. Y tampoco les importa si la víctima es un usuario particular o una empresa, en los dos casos hay muchas probabilidades de que paguen el rescate si los datos cifrados son valiosos para ellos. Eso no significa que el impacto sea igual en todos los casos. Los hospitales, por ejemplo, han sido víctimas recurrentes del ransowmare, entre otras razones por funcionar con infraestructuras antiguas y vulnerables y ofrecer una superficie de exposición con muchos dispositivos conectados. Además, proporcionan cuidados críticos y para funcionar correctamente necesitan acceder en tiempo real a información actualizada de los pacientes, historiales médicos y de prescripción de fármacos, y cualquier retraso puede suponer un riesgo serio para la salud de los pacientes. En el peor de los casos, un ransomware podría acabar con la vida de inocentes y las instituciones sanitarias tendrían que enfrentarse a procesos legales y fuertes indemnizaciones[3].

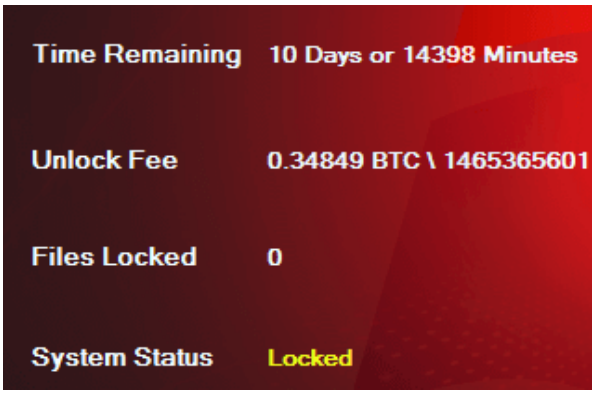


Figura 3: Manamecrypt muestra un contador regresivo para presionar a sus víctimas.

El ransomware no solo usa las últimas tecnologías para mejorar la eficacia de sus cifrados. Además, los cibercriminales han desarrollado ciertas técnicas para apremiar a sus víctimas a que paguen cuanto antes. Muchas variantes amenazan ya con eliminar los archivos cifrados o las propias claves de recuperación si no se produce el pago de los rescates en un plazo de tiempo determinado. Otra familia de ransomware, por ejemplo, ofrecía la posibilidad de recuperar sus archivos si enviaban el propio ransomware a su listado de contactos.

[3] Fuente: https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets

1.4. Modelo de negocio

La razón principal del éxito rotundo del ransomware es que supone un negocio lucrativo, rápido y directo para los cibercriminales. Sin embargo, hay múltiples factores que han favorecido y propiciado su actual modelo de negocio. Uno de ellos es la aparición de monedas alternativas que han permitido a los criminales exigir sus chantajes y mantenerse en el anonimato. La gran mayoría de los ransomwares exigen un pago en Bitcoins, una criptomoneda que no necesita el respaldo de la tradicional cuenta bancaria. Otros admiten todo tipo de tarjetas prepago o dirigen los cobros a través de múltiples servicios que facilitan la ocultación de identidades.

En segundo lugar, la tecnología del ransomware es fácilmente accesible y está al alcance de cualquiera. Los cibercriminales no necesitan desarrollar sus propios métodos de cifrado, no tienen que ser expertos ni necesitan ninguna formación, tan solo tienen que apostar por alguna de las ofertas de «ransowmare-como-servicio» disponibles en los mercados clandestinos de Internet. Esto significa que solo es necesaria una inversión mínima para poner en marcha una campaña de ransomware.

Finalmente, la infraestructura asociada a este tipo de malware es flexible y volátil, complicando los esfuerzos de las autoridades y policías encargadas de perseguir el cibercrimen para localizar los servidores de pago o distribución y, en consecuencia, la posibilidad de ser atrapado es relativamente baja. La combinación de estos elementos favorece un modelo de negocio que permite a los delincuentes poner en marcha campañas de ransomware rápida y masivamente distribuidas y a muy bajo coste.

2. Protección anti-ransomware

Para muchas de las víctimas, la primera reacción ante un ransomware es acceder al chantaje y pagar. «Después de todo, es la forma más fácil de recuperar la información cifrada», nos justificamos todos. Sin embargo, ninguna evidencia respalda está afirmación y no hay ninguna garantía de que los cibercriminales permitan a la víctima recuperar sus archivos una vez realizado el pago. Además, como los pagos no dejan rastro, tampoco nadie va a devolver el dinero en caso de que la recuperación de los archivos no se produzca, no funcione o sea tan solo parcial. Tampoco existe ninguna garantía de que el propio ransomware no siga en el equipo atacado y vuelva a ponerse en acción demandando un nuevo pago. Después de todo, si los cibercriminales saben que una víctima ha pagado un rescate, la oportunidad de ganar más dinero extorsionando a la misma víctima es mayor que si lo intentan con cualquier otra. Finalmente, el hecho de acceder al chantaje simplemente contribuye a perpetuar su desafortunadamente exitoso modelo de negocio.

2.1. Tecnologías anti-ransomware

La mejor manera de protegerse de estas amenazas es asegurarse de que el ransomware no podrá infectar los equipos atacados. Una buena recomendación es usar una solución de seguridad que incorpore una específica funcionalidad anti-ransomware. Además de la detección tradicional basada en firmas, esta solución debería ser capaz de detectar los habituales comportamientos del ransomware, como el cifrado masivo de archivos, y bloquearlos antes de que se ejecuten.

2.2. Parcheado

Además de una protección *ad-hoc* anti-ransomware, los usuarios, ya sean particulares o empresas, deberían asegurarse de que su sistema operativo, así como todos los programas instalados en sus equipos, están correctamente actualizados. En el caso de los usuarios domésticos, la configuración de sus equipos debería permitir que *'Windows Update'* instale los parches de seguridad de forma automática. Si hablamos de empresas con redes informáticas donde conviven decenas de equipos con diferentes configuraciones, se hace necesario incorporar un gestor de parches como *G DATA Patch Management* que asegure la instalación y el despliegue correcto de todos los parches en los plazos adecuados. Las vulnerabilidades no parcheadas son la principal puerta de entrada del ransomware.

2.3. Copia de seguridad

El éxito del ransomware se basa en algo muy concreto: impedir a la víctima el acceso a sus propios archivos. Saber que tenemos un respaldo de dichos archivos puede ser muy útil en caso de infección. Por este motivo, es imprescindible realizar copias de seguridad de todos los archivos importantes con regularidad. Y para impedir que el ransomware realice un cifrado no solo de los originales, sino de nuestra propia copia de seguridad, esta debería estar almacenada en un medio externo no conectado al equipo que contiene los archivos originales. Los usuarios particulares pueden respaldar cómoda y fácilmente sus archivos usando alguno de los servicios de almacenamiento en la nube más habituales o en algún disco duro externo. Las empresas deben apostar por soluciones profesionales que realicen copias regulares de todos los equipos de la red empresarial en un servidor centralizado y eficazmente protegido dedicado a esta tarea.

2.4. Concienciación

El usuario es un filtro más en la lucha contra el ransomware y, por tanto, todas las medidas anteriores deberían ser completadas por campañas de concienciación / formación dirigidas a los usuarios. Sería conveniente que todos los internautas supieran que solo deben abrirse los archivos adjuntos de correos electrónicos procedentes de remitentes de confianza, siempre y cuando las circunstancias y el contexto avalen que esa persona envía ese archivo. Lo mismo sucede con los enlaces pegados en los correos electrónicos procedentes de remitentes desconocidos que, en su gran mayoría, conducen a páginas con malware o de *phising* capaces de estafar a sus visitantes. Las empresas harían bien e invertir parte de su tiempo en este tipo de formaciones.

3. La propuesta anti-ransomware de G DATA

Las soluciones de G DATA ofrecen una protección integral frente al ransomware, tanto para clientes particulares como empresariales, gracias a la combinación de varias tecnologías (firmas, protección de correo electrónico, detección de exploits, protección web, análisis de comportamientos de archivos y, en el caso de las soluciones empresariales, control de dispositivos y aplicaciones) y a un módulo anti ransomware específicamente diseñado para combatir esta amenaza. Esta tecnología se encarga de detener el cifrado espontáneo de los archivos y detener en seco los procesos que intentan modificarlos. Los administradores de sistemas pueden manejarla desde la consola de administración centralizada (G DATA Administrator).

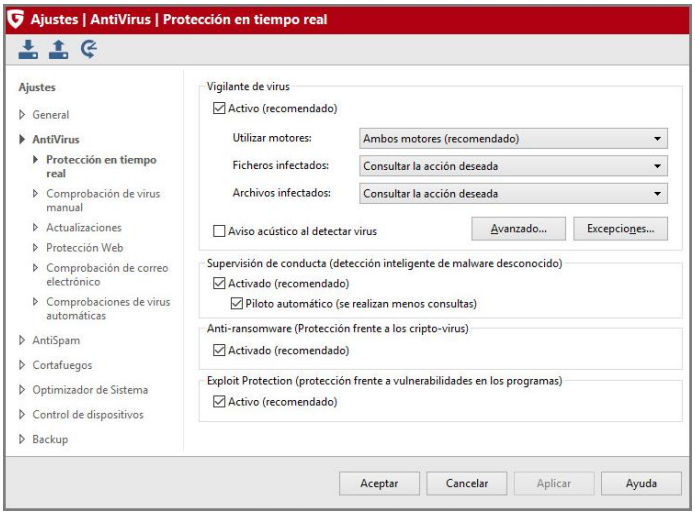


Figura 4: Todas las soluciones de G DATA incluyen una protección Anti-Ransomware dedicada

Además, las organizaciones deberían asegurarse de que disponen de una política de actualización de parches capaz de sellar las vulnerabilidades de los programas instalados en su red en los tiempos y formas adecuados, como por ejemplo *G DATA Patch Management*, compatible con cualquiera de las soluciones para empresas del fabricante alemán.

Por último, es esencial proteger la información de nuestros equipos frente a cualquier pérdida de datos, ya sea motivada por un ransomware o por cualquier otra causa. Tanto *nuestras soluciones para empresas*, como para usuarios particulares G DATA Internet Security y G DATA Total Security, incorporan una función para realizar copias de seguridad regulares.

Más información sobre las soluciones de G DATA en *www.gdata.es*