Artículo

Ransomware (wannacry):

Para

Usuarios y administradores IT.

Soluciones Informáticas Burgos, S.L.
C/ Rosa Chacel, 3 bajo – 09007 Burgos
Tfno.: 947 486402 – Fax: 947 486402
www.sib.es

ÍNDICE

1. Ransomware, definición.

El **Ransomware es un software malicioso** que infecta nuestro equipo desde una ubicación remota y **encripta nuestros archivos** dejándolos inutilizables. Para desbloquearlos el virus lanza una ventana emergente en la que nos pide el pago de un rescate por Bitcoins (dinero de internet). A diferencia de los virus tradicionales no propaga archivos ejecutables detectables por los antivirus si no que aprovecha vulnerabilidades conocidas de las aplicaciones y sistemas operativos no actualizados para ejecutar su código.

En estas últimas fechas, una variante conocida como "Wannacry" está causando graves daños y alerta social gracias a la gran repercusión lograda en los medios de comunicación, por las noticias de infecciones en grandes empresas de todo el mundo (Telefónica, Iberdrola o la mitad de los hospitales británicos, por ejemplo)

En este caso, el virus se propaga utilizando una vulnerabilidad conocida de los sistemas operativos Windows y en particular del sistema SMB, publicada por Microsoft el 14 de marzo de 2017 y parcheada con la actualización de seguridad Microsoft Security Bulletin MS17-010 – Critical Security Update for Microsoft Windows SMB Server (4013389)

El CNI (Centro Criptológico Nacional y Centro Nacional de Inteligencia), en su web ha publicado una herramienta que impide la ejecución de esta variante concreta. CCN-CERT NoMoreCry Tool

2. Que le hace tan peligroso.

La principal cualidad de este tipo de virus y la que le permite ser tan dañino es el control de los eventos: En lugar de crear un virus y dejar que se distribuya y espere su ocasión (método tradicional) El ramsonware se planifica cuidadosamente y se distribuye en oleadas de correos electrónicos o infectando páginas web. Todos los ordenadores que ejecuten el enlace enviado en el correo o hagan click en la web infectada pondrán a prueba las actualizaciones de sus sistemas, si el sistema operativo o aplicación que tiene la vulnerabilidad explotada no está parcheado por las actualizaciones de seguridad se infectará sin remedio. Como ejemplo, si el ataque utiliza una vulnerabilidad de Adobe Acrobat y nuestro ordenador no lo tiene instalado o está correctamente actualizado el ataque no tendrá éxito, en caso contrario una macro empezara a encriptar todos los archivos alcanzables (discos locales, unidades de red compartidas, dispositivos de almacenamiento conectados, etc.) que quedarán inutilizables.

3. Que sucede si me infecto.

En caso de resultar infectado, lo primero es desconectar el PC y apagar la electrónica de red para impedir el proceso de encriptación de archivos y la propagación por la red interna. La tarea de encriptar los archivos lleva tiempo y puede que consigamos salvar carpetas enteras si detenemos el proceso.

El procedimiento más habitual del virus es comenzar a encriptar los archivos de datos locales, continuar con las carpetas de red a las que este ordenador tiene acceso. Esta capacidad le permite encriptar también archivos de copias de seguridad alojados en discos duros externos si estos permanecen conectados al equipo.

Una de las preguntas más habituales entre los usuarios infectados es: ¿Si pago me dan la clave y recuperaré los datos? La respuesta es NO en la mayoría de las ocasiones. Si bien es cierto que este tipo de virus lo distribuyen grupos de delincuentes con afán de lucro y que si nadie recuperara los datos, pocas personas pagarían, su estrategia se basa en recoger los primeros ingresos y cerrar las cuentas para evitar la acción de la justicia. Se le envía la clave a los primeros pagadores para que circule la noticia de que si pagas puedes recuperar los datos.

4. Prevención y herramientas de protección.

Las particularidades de este sistema de malware hacen poco previsible cómo será su siguiente ataque, esto hace difícil plantear una solución única y completa.

Las mejores prácticas para defenderse parten del sentido común, la prevención y la protección.

Prevención:

- Disponer de copias de seguridad diarias, efectuadas en un soporte fuera de línea (unidades de cinta o backup a disco offline) y verificar que se efectúan correctamente. Es muy recomendable disponer de 2 medios de copia de seguridad, una local como la unidad de cinta o los NAS y otra remota como el backup en la nube.
- Mantener un sistema efectivo de derechos de acceso a las carpetas compartidas para minimizar los daños.
- No instalar aplicaciones que no vayamos a usar y las que se instalen que sean originales y actualizadas de forma automática.
- Prudencia en el uso de webs dentro de la red empresarial y en la apertura de correos con enlaces a sitios remotos o archivos adjuntos.

Protección:

- Contar con un antivirus profesional actualizado y correctamente instalado, con actualizaciones on line.
- Mantener actualizado el sistema operativo y las aplicaciones de nuestro ordenador, con los parches de seguridad del fabricante al día.
- Si el presupuesto nos los permite, instalar un cortafuegos con antivirus, antispam, filtrado web y subscripción a un sistema de control de reputación de páginas web. Activar en él el bloqueo de archivos zip, exe, jsp, etc.

Por último y a pesar de la dificultad de criterio que entraña, sea desconfiado y si duda no abra el correo. Piense que los delincuentes utilizan siempre el nombre de grandes corporaciones de las que usted probablemente sea cliente y sea especialmente cuidadoso con correos de operadoras de telefonía, Correos, Amazon, DHL, Seur, grandes bancos, etc. Si recibe un correo con enlace a un sitio web (ej.: pulse aquí para ver su factura) es mejor visitar la web del remitente que hacer click en un enlace que puede llevarnos a otro sitio.