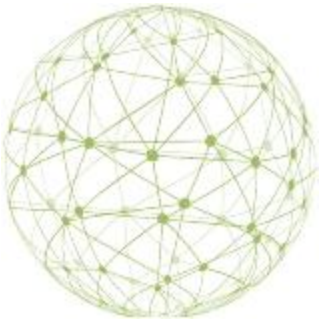

UNA RAPIDA ACCION ADMINISTRATIVA DE IT DESBARATA UN ATAQUE CRYPTOVIRUS CON CARBONITE

"Estoy familiarizado con la forma de trabajo del CryptoVirus y realmente sólo hay dos maneras de obtener los archivos de nuevo: o restaurar a partir de una copia de seguridad o pagar el rescate."
— Chad Mockensturm, Diverse Technology Solutions

Un pensamiento inmediato y una acción rápida de un administrador de sistemas con sede en Ohio salvó de un desastre seguro a un Centro de Salud, cuando un ataque de CryptoVirus amenazó con acabar con cientos de archivos digitales importantes y al servidor en el que residen.

Chad Mockensturm es un asistente de administrador de sistemas de Diverse Technology, un Carbonite Partner certificado. Una parte importante de su trabajo es monitorear y mantener los sistemas informáticos de uno de los clientes de Diverse Technology, un Centro de Salud con base en Ohio. Una noche Mockensturm estaba precisamente monitoreando, cuando recibió una alerta de seguridad.

"Tenemos una consola de gestión corporativa que nos alerta sobre problemas importantes y llegó un mensaje de texto a mi teléfono, que en varias ocasiones un virus fue bloqueado en una de las computadoras de la estación de enfermería ", dijo. "Después nos enteramos de que una de las enfermeras se había conectado en línea para revisar los correos y recibió el CryptoVirus a través de correo electrónico ".

Cuando la enfermera hace clic en el archivo ejecutable, el CryptoVirus encontró su camino de ataque al equipo de enfermería que estaba conectado con el servidor de archivos del centro de salud y empezó a comprometer los archivos importantes. Mockensturm se enteró de que la enfermera había recibido en el escritorio de su ordenador una nota de pedido de rescate, amenazando con destruir los archivos de la instalación de atención médica a menos que el dinero fuera abonado.

Sus Archivos están Encriptados

Para obtener la clave para descrifrar los archivos tiene que **pagar 500 USD/EUR**.
Si el pago no es realizado dentro [incluye una hora especifica], el costo de descrifrar los archivos aumentarán **dos veces y será el pago de 1000 USD/EUR**

"Inmediatamente apagamos la computadora y se procedió a escanear el servidor de archivos para buscar cualquier infección relacionada con el virus. Nos encontramos que había 200-300 archivos que estaban infectados " explicó Mockensturm. "Se examinaron el resto de la red como precaución y luego utilizamos nuestra cuenta de copia de seguridad de Carbonite Server para restaurar copias limpias de los archivos que fueron infectados ".

Que es un Crypto virus?

Hay varios virus del estilo Crypto con diversos nombres, pero la clave a recordar es que todos usa la misma forma de los ransomwares.

''Ransomware' es un virus que infecta un ordenador, cifra los archivos y amenaza con dejarlos inservibles a menos que la víctima pague dinero por un código clave que descifra la información. CryptoVirus como CryptoLocker - uno de los más infames ejemplos, normalmente exigen un rescate en forma de bitcoins, moneda digital que es difícil de rastrear. Algunas variantes Crypto bien conocidos incluyen CryptoWall, TorrentLocker y CryptoDefense".

"La mejor manera de mantenerse alejados de una infección del tipo CryptoVirus es tener cuidado al hacer clic en adjuntos dentro de correos electrónicos", según indica Mockensturm. "Los correos electrónicos que contienen enlaces a CryptoVirus son archivos ejecutables que pueden ser muy convincentes de su origen e incluso pueden parecer como que están viniendo de personas conocidas o lugares familiares".

"Sepa de quién es la dirección de correo electrónico que esta recibiendo", dijo. "Incluso si está viniendo de una persona que crees conocer; deben ser cautelosos cuando abran un correo electrónico."

Pero incluso al más vigilante se le puede engañar de vez en cuando. Es por eso que es también importante crear copias de seguridad de los ordenadores personales y servidores empresariales.

"Siempre es bueno tener una copia de seguridad y la mejor copia de seguridad es la que uno no tiene que recordar en hacerla, ya que se ejecuta en segundo plano y se ejecuta sin problemas " Explicó Mockensturm. "Carbonite es una gran opción"

Source: Chad Mockensturm, Diverse Technology Solutions

Cinco Pasos para defenderse contra un ataque de CryptoVirus

Cuando ataca un CryptoVirus, los usuarios de Carbonite pueden recuperar sus archivos de forma rápida sin tener que pagar el rescate. Aquí hay una guía rápida de obtener los archivos de nuevo después de un ataque de CryptoVirus:

1. Tan pronto que seas consciente del ataque de cryptovirus en el ordenador, en el servidor de ficheros o en la red; apagar de inmediato toda conexión de carpetas compartidas.
2. Utilice su software de antivirus para determinar donde ocurrió la infección. Si no puedes determinar donde se originó la infección usando su software antivirus, hacer click derecho en el archivo infectado para determinar cual fue el último ordenador o usuario que hizo cambios en dicho archivo. Esto les ayudará a determinar el origen de la infección.
3. Evaluar el grado de la infección y el alcance de los daños.
4. Elimine el virus, borrando todos los archivos infectados.
5. Utilice Carbonite para restaurar versiones limpias de los archivos infectados.

Restaurar rapidamente archivos con Carbonite

Diverse Technology Solutions ha estado utilizando Carbonite Server Backup para proteger muchos de los servidores de bases de datos y archivos de sus clientes durante años. Pero en el incidente en el Centro de Salud, fué la primera vez que la compañia tuvo que usar Carbonite para restaurar los archivos infectados por el CryptoVirus.

Para concluir el trabajo, Mockensturm simplemente se loguea en el servidor de archvos del Centro de Salud y abre la consola de Carbonite. Luego realiza una busqueda rápida en la carpeta raiz que contenia todas las subcarpetas y archivos que necesitan ser recuperados.

“Restaure las carpetas a una parte separada del disco duro, borré los archivos originales que fueron encriptados por el virus y copié los nuevos en el mismo lugar,” explicó. “Paso seguido me aseguré de que todos los programas vinculados a estos archivos fueran capaces de funcionar de nuevo sin inconvenientes.”

El proceso fue simple rápido y sin dolor. Mockensturm fue capaz de restablecer copias limpias de los archivos aproximadamente en media hora.

“Estoy familiarizado con el uso de la versión individual de Carbonite y puedo decirles que el uso de la versión Carbonite Server es muy intuitivo. Usted únicamente ingresa a la consola, selecciona la opción de restaurar y escoge los archivos que sedea restaurar y esperar que se descarguen” explicó. “Fué todo muy fácil”.

Nubeseg S.R.L.

http://partners.carbonite.com/nubeseg

ventas@nubeseg.com