CryptoLocker Está Evolucionando… Y Es Cada Vez Más Inteligente

En el ambiente que nos rodea vemos que los virus y enfermedades pueden evolucionar, por lo que es lógico que el malware, estafas de hackers y virus informáticos también evolucionen. El virus CryptoLocker, un **tipo de ransomware** que toma como rehén tus archivos hasta que pagues un rescate en ya sea con una transferencia bancaria o con Bitcoins. Sin embargo, las **versiones más recientes** muestran que este código malicioso se ha vuelto más inteligente, poniendo en riesgo grandes proyectos de seguridad y poniendo a prueba los conocimientos de aquellos profesionales de la seguridad informática.

La Evolución De CryptoLocker

Los hackers han adaptado la estafa con la esperanza de aumentar su eficacia. La última versión permite ver una lista de los archivos cifrados y le da la opción para descifrar uno de ellos de **forma totalmente gratuita**. ¡Qué cosa, ¿eh? He aquí un ejemplo de una de estas estafas. Observa el botón «One free decrypt!», justo debajo del temporizador.

¿Por Qué Esta Opción Gratuita?

CryptoLocker hace un trabajo bastante efectivo para apurarlo a pagar el rescate. Amenazan con duplicar el costo para desbloquear cada 24 horas, y también te dicen que la clave de descifrado privada se eliminará en 30 días, creando un sentido de urgencia al usuario infectado.

Pero, realmente confía en **código de malware** que te dice lo que tienes que hacer?

Bueno, eso es exactamente el objetivo de la opción «One free decrypt!». Si un usuario puede descifrar con seguridad uno de sus archivos, les ayuda a confiar en el programa. Pueden decirse a sí mismos, «Hey, este programa puede realmente darme mis archivos de nuevo y sin problemas.» Aunque esta opción puede ser tentadora, puedes terminar pagando una gran cantidad de dinero, y aunque te brinden una gran cantidad de archivos de prueba, créeme, no te gustara seguir pagando lo que ellos te pidan.

Qué hacer si estás infectado

Si crees que esta infección no te puede alcanzar, es mejor que no subestimes el poder de contagio de este malware. Aunque existan nuevas versiones, variantes que son mas inteligentes que la anterior, existen 4 pasos que puedes poner en practica luego de ser infectado:

1. **No hagas caso de la petición de rescate** – Ni siquiera pienses en pagar el rescate. No existe garantía de que volverás a recuperar tus archivos.

2. **Elimine el ransomware desde el ordenador** – Mientras CryptoLocker puede parecer amenazante, es igual que **cualquier otro código de malware**. Hay una serie de empresas y herramientas que se especializan en la eliminación de malware. Es aconsejable quitar el ransomware tan pronto como sea posible con el fin de minimizar el riesgo de que su dispositivo se infecte aun más.
3. **Actualice su antivirus, el software anti-malware e instale actualizaciones del sistema operativo** – Si se infectó, hay una buena probabilidad de que se debía a que el software de protección estaba desactualizado.
4. **Actualice las contraseñas** – No se sabe qué tipo de información ha tenido acceso el programa de **malware a su dispositivo** mientras estaba infectado. Cambiar las contraseñas es una buena idea con el fin de garantizar la seguridad adicional de seguir adelante.

Siempre respalde los archivos

Otro consejo importante que siempre debes de tener en cuenta, es realizar siempre una copia de seguridad de los archivos. Hay una buena probabilidad de que pueda sufrir alguna pérdida y/o daños en los archivos después de una infección, por lo que siempre se debe tener copias de seguridad en un sistema externo, ya sea en otro disco duro o hacer uso de un servicio de almacenamiento de archivos. Si se toman como rehenes a sus archivos, estarán a salvo en otra ubicación ;)

Finalmente

El Malware está en constante cambio. Los hackers son inteligentes y tienen muchas **estrategias para infectar las computadoras**. Además, la mayoría de estas estafas tratan de aprovecharse de un error humano, en lugar de los **errores en el software de seguridad**. Es importante mantenerse al tanto de las formas más importantes y comunes de malware con el fin de protegerte mejor.