Managed secure IT | no matter what

CÓMO INFECTAR UNA COMPUTADORA USANDO RANSOMWARE

Pensar que por su escala destructiva, un ransomware no puede infectar un equipo fácilmente, es subestimarlo y eso acerca a una empresa a convertirse en una víctima más de este tipo tan peligroso de malware usado para extorsionar a empresarios y compañías de toda escala y giro.

Security

Para comenzar, hay que entender que no solo existe un tipo de Ransomware, sino varios.

Este tipo de malware puede dividirse en dos categorías principales: el de cifrado y el que no cifra o Lock screen Ransomware.

El de cifrado, conocido entre los cibercriminales y expertos en seguridad como encrypting ransomware o filecoders, impide el acceso a los datos del usuario cifrando todas las carpetas que haya en un equipo. Al cifrar información sensible, una computadora infectada se hace inútil y se convierte en el vector mediante el cual se propaga una infección de escala internacional.

Solo a través de un respaldo total, la intervención de un experto en seguridad o el pago de un "rescate de información", puede una compañía recuperar la información perdida por este ataque.

El otro tipo de Ransomware más común es el del tipo que no cifra, mismo que trabaja bloqueando el acceso a la computadora infectada o a sus aplicaciones más importantes, reemplazando todas sus funciones por una única: presentar en pantalla un mensaje de rescate que, de no pagarse, no permitirá a nadie interactuar de ninguna manera con el sistema comprometido.

Para infectar un equipo con alguno de estos tipos de Ransomware basta con enviar un correo apócrifo cargado de malware, que cualquier empleado de una compañía abra desde su correo corporativo, infectando en el proceso al resto del sistema.

El correo electrónico es una de las vías de infección más usadas por los cibercriminales, pero también existen otros métodos, como anuncios que llevan a páginas cargadas con malware o archivos en formatos .zip o .rar que no contienen más que instrucciones de secuestro de información.

También es posible infectar una computadora mediante ficheros de clase P2P (pier-to-pier) que vienen en forma de hipervínculos a sitios comprometidos o cadenas de correos masivos, redes sociales, mensajería instantánea o archivos infectados en formatos populares como .mp3, .mp4, .docx o incluso .dmg.

Security

Los portales con más probabilidades de contener archivos corruptos son los de intercambio de contenido audiovisual como los torrents o los clientes de descarga de carpetas.

Un ataque de ransomware también puede llegar de un dispositivo inteligente conectado a una computadora o laptop. También es posible usar un Protocolo de Escritorio Remoto para aprovechar alguna vulnerabilidad en el cerco de protección de cualquier sistema, con el fin de introducir un archivo corrupto por ransomware.

Si la infección tiene éxito, será posible pedir un rescate en criptomonedas, pero si el sistema de una organización está bien protegido o se encuentra respaldado por tecnología basada en el Cloud, las probabilidades de infección se reducen considerablemente.

De las maneras más efectivas en las que una organización puede protegerse de la infección de sus sistemas es actualizando todo el software con el que trabaje el equipo entero, evitando abrir correos electrónicos no solicitados o descargando archivos de sitios no verificados.

Otros medios para protegerse son usando un antivirus potente y actualizado, activando un firewall, realizando respaldos de seguridad constantes y migrando todo el sistema a la nube para mantenerlo alejado de los cibercriminales.

Activar sistemas de autentificación de dos factores y montando redes privadas virtuales o VPNs, también son buenos métodos para protegerse.

Una organización que lleve a cabo estos pasos, difícilmente podrá verse afectada por los cibercriminales y el ransomware que usan para lucrar.

Síguenos en nuestras redes sociales:

MexisMX

Servicios Administrados Mexis, S.A. de C.V.

Mexis TI

Servicios Administrados Mexis, S.A. de C.V.