Tecnología

Ransomware: ¿qué es y cómo se previenen estos ciberataques?

Datos secuestrados y una recompensa millonaria: así funciona el ransomware, una modalidad que afectó a miles de empresas esta semana y que es muy común.

MARIANA MALEK
Jueves, 08 Julio 2021 04:00

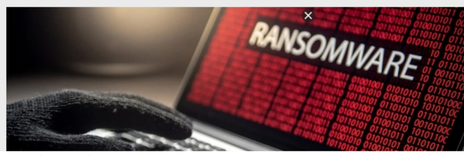

Foto: Shutterstocl

Desde el viernes 2 de julio más de mil empresas de todo el mundo reportaron que fueron víctimas de un ciberataque que secuestró sus equipos y exigió el pago de un rescate para liberar la información. Este tipo de maniobra es conocida como ***ransomware***.

La palabra está compuesta de otras dos en inglés: *ransom* (rescate) y *malware* (software malicioso).

Normalmente el blanco de este tipo de maniobras son empresas que pueden pagar grandes sumas de dinero para recuperar su información. "Los ataques de ransomware lo que buscan es cifrar el contenido de los equipos que son afectados y luego vender la clave para tener el contenido original", explicó a El País El catedrático de ciberseguridad de la Facultad de Ingeniería de la Universidad ORT y encargado de ciberseguridad de MAPFRE, Roberto Ambrosoni.

En el caso de este último ataque masivo, que se considera uno de los más importantes de la historia, el grupo de hackers ruso REvil se hizo cargo del ataque en su portal Dark web, informó la empresa de seguridad informática ESET.

MIRA TAMBIÉN **Ransomware: ¿Qué es y cómo se previenen estos ciberataques?**

"El ataque masivo del **ransomware REvil** apuntó a una cadena de suministro utilizando un instalador de una actualización automática del software de gestión de IT de la compañía Kaseya. En este caso, la actualización con permisos de administrador afectó a los MSP (proveedores de servicios administrados) y estos a su vez infectaron los sistemas de sus clientes con la amenaza, como fue el caso de 11 escuelas en Nueva Zelanda y una cadena de supermercados en Suecia que tuvo que cerrar algunas tiendas, de hecho están regalando la comida fresca para que no se eche a perder, debido al ataque", informó en un comunicado ESET.

Según datos de la telemetría de la misma empresa, se detectaron víctimas del ransomware REvil en Reino Unido, Sudáfrica, Canadá, Alemania, Estados Unidos, Colombia, Suecia, Kenia, Argentina, México, Holanda, Indonesia, Japón, Mauritania, Nueva Zelanda, España y Turquía.
Según informó El País, el pasado martes **REvil** pidió el pago de un rescate de US$ 70 millones en bitcoins, a través de un reclamo publicado en el blog Happy Blog.

¿Qué hacer?

Estar preparado y saber cómo enfrentar este tipo de situaciones es clave para los especialistas en ciberseguridad.

Ambrosoni enfatizó que "como en todo tipo de chantaje económico la recomendación es no pagarlo".

El especialista subrayó que existen formas sencillas para prevenir ser víctimas y perder dinero o información ante este tipo de ataques: "La medida para protegerse es, en primer lugar, contar con respaldos para poder instalar lo que teníamos sin perder la información, de esa manera no te ves obligado al tema del rescate", destacó.

Otra de las medidas es no perder las actualizaciones de seguridad y que los sistemas operativos estén al día: "Es fundamental tener las actualizaciones de los sistemas operativos y los parches instalados porque es la manera que evitamos que a través de virus o ataques se logre generar ransomware en los equipos".

Cómo fue el ataque

Este **ciberataque**.masivo se dio a través de la compañía Kaseya, una empresa de software estadounidense basada en Miami, que desarrolla software para administrar redes, sistemas e infraestructura de tecnología de la información. La empresa tiene 40.000 clientes y y una vez que comenzó el ataque pidió a sus asociados que cerraran los servidores, aunque para muchos fue demasiado tarde.

"El ataque de **REvil** solo cifró los archivos de las víctimas y no robó información previo al cifrado. Por lo que en este caso afecta la continuidad del servicio, pero no hay peligro de una filtración de la información secuestrada", explicó ESET.

MIRA TAMBIÉN **Scraping: ¿qué es y cómo funciona la última estafa de las redes?**

La empresa Kaseya publicó las actualizaciones sobre cómo trabajan sobre el software y los servidores afectados de cara a resolver el problema. Según informó el miércoles, la empresa continuaba con problemas para reiniciar sus servidores y reestablecer el servicio a sus clientes.

Biden en alerta por la situación

El presidente de EE.UU., Joe Biden, se reunió este miércoles con su equipo de seguridad nacional para estudiar una respuesta a los ciberataques como el de este fin de semana contra la firma estadounidense Kaseya, que afectó a un millar de empresas en el mundo.

Aunque inteligencia aún no atribuyó el ataque al grupo REvil, Biden dijo a los periodistas que si tiene algo que compartir con el presidente ruso Vladimir Putin lo hará directamente.