Los ciberataques para secuestrar datos se duplicaron en los seis últimos meses

> Ya no hace falta ser un ‘hacker’ experto para dirigir un virus informático; en la internet oscura se ofrece ese servicio a cambio de una cuota. La modalidad de ‘ransomware’ se está popularizando, según un informe anual de amenazas cibernéticas.

El secuestro de datos o ransomware es una de las ciberamenazas más temidas, sobre todo en el ámbito profesional, donde la información es más sensible y muchas veces fundamental para el funcionamiento del organismo o de la empresa (cuando no determinante para su seguridad). Durante los últimos seis meses, las variantes de esta técnica, que consiste en que los ciberdelicuentes cifran los datos y piden un rescate para liberarlos, prácticamente se han duplicado.

Al crecimiento de este tipo de ataque ha contribuido el teletrabajo desde el inicio de la pandemia de covid-19.

El móvil, la tablet o el ordenador del trabajo que utilizas en casa no están conectados a la red del trabajo, que también podría sufrir un ataque, pero en casa estos dispositivos son más fáciles de atacar y por eso concentran ahí sus esfuerzos los ciberatacantes.

A pesar de los esfuerzos y de las acciones a nivel internacional que se llevan a cabo para hacer frente a estos delitos, siguen constituyendo una amenaza importante para las organizaciones, independientemente de su tamaño.

También se ha multiplicado en la primera mitad del año la cifra de borrados de disco, que, según el representante de la compañía, no tiene como objetivo una extorsión, sino “hacer el máximo daño posible”.

Aunque a priori puede resultar una cifra diminuta, es el mismo número de variantes de borrado identificadas desde 2012 hasta el pasado año. Lo que ha desencadenado tal crecimiento en este caso ha sido la invasión de Ucrania. Aunque resulta difícil para los investigadores determinarlo con total confianza, los perpetradores suelen ser simpatizantes de Rusia con objetivos militares y una clara intención de sabotaje.

Las víctimas de estos borrados suelen ser organismos gubernamentales o militares y organizaciones ucranianas. Eso sí, lo llamativo de estos ataques es que, desde que comenzó la invasión el pasado febrero, se han detectado más amenazas fuera de Ucrania que allí, aunque también relacionadas con la guerra.

Frente a las amenazas cibernéticas, que no hacen más que evolucionar y tratar de esquivar los mecanismos de defensa de los sistemas, el análisis constata la importancia de la inteligencia artificial para poder abordar los peligros de una forma más eficiente: “Las organizaciones necesitan operaciones de seguridad que puedan funcionar a la velocidad de la máquina para mantenerse al día con el volumen, la sofisticación y el ritmo de las ciberamenazas actuales”, resume el texto, que también insiste en lo necesarias que resultan la concienciación y la formación en ciberseguridad para que tanto los empleados como los equipos de seguridad estén al día de los peligros. “Los cibercriminales nunca van a dejar pasar una oportunidad. Ya sea una vulnerabilidad o una guerra, siempre va a haber alguien tratando de hacer daño para obtener un beneficio”, concluye el informe.

Fuente de información: elpais.com