



Ransomware 2.0: del cifrado de datos a la amenaza de desvelar información confidencial

Los cibercriminales generalizan una táctica de doble extorsión a las compañías víctimas de sus ataques.

Los ataques de ransomware se han sofisticado. Desde el tristemente famoso Wannacry de 2017, los cibercriminales han desarrollado nuevas tácticas de amenaza a las empresas. Este año se han generalizado los ataques en los que se realiza una doble extorsión. Las organizaciones criminales no sólo cifran los datos de las empresas víctimas, sino que amenazan con publicar información confidencial si no se avienen a pagar un rescate.

Cuando los ciberdelincuentes rompen la seguridad de una compañía, rastrean sus sistemas en busca de información confidencial. Una vez localizada, realizan el cifrado de los datos y extorsionan a las empresas amenazando con la filtración de estos datos sensibles.

Hay portales en los que se puede seguir la cuenta atrás de las compañías amenazadas

Hay portales en los que se puede ver qué compañías han sido vulneradas y se muestra la cuenta atrás para desvelar esos datos jugosos a los que han accedido los cibercriminales, explica Daniel Creus, investigador de seguridad del Global Research & Analyst Team de Kaspersky.

La publicación online de datos confidenciales supone una nueva amenaza porque, además del riesgo reputacional para las empresas víctimas, expone a las organizaciones a demandas si los datos publicados violan, por ejemplo, la regulación de protección de privacidad.

Para demostrar que su amenaza es veraz, publican una pequeña muestra de datos en la dark web, asegura la compañía de ciberseguridad Check Point, que pronostica que este tipo de ransomware seguirá siendo una de las grandes amenazas en 2021. Según sus datos, en el tercer trimestre de este año se ha incrementado la media de ataques diarios de ransomware un 50% respecto al primer semestre.

Recientemente, Endesa sufrió un ciberataque de ransomware que afectó al correcto funcionamiento de su servicio interno, aunque la firma pudo resolver la amenaza sin que llegase a afectar al servicio ni a los datos de sus empleados o clientes.

ESPECIALIZACIÓN

Creus explica que las organizaciones cibercriminales cada vez están más especializadas. Hay grupos que se dedican a escanear Internet en busca de puntos vulnerables. Luego hacen un cribado para detectar qué compañías que pueden tener datos más jugosos y venden esta información a otros cibercriminales, que son los que lanzan el ataque con códigos maliciosos que han desarrollado otros ciberdelincuentes, dice.

Fuente: Expansion