Publicado en Madrid el 20/04/2023

El nuevo ransomware de 'triple extorsión' pone en jaque a empresas y empleados

El ransomware de triple extorsión es una de las principales ciberamenazas para las empresas y entidades de todo tipo en 2023 según los expertos de S2 Grupo. El objetivo de este nuevo tipo de ciberataques no sólo es el dinero de la empresa vulnerada, sino que también se extorsionan a terceros que puedan verse afectados por la divulgación de los datos extraídos

La empresa especializada en ciberseguridad S2 Grupo, ha explicado en un comunicado que el ransomware de triple extorsión es un novedoso tipo de ataque que, al igual que el ransomware tradicional, permite a los ciberdelincuentes infiltrarse en una red empresarial para cifrar sus datos e impedir su uso. La principal diferencia que lo hace todavía más peligroso es que el ransomware de triple extorsión se basa no sólo en buscar dinero de la empresa vulnerada, sino que también extorsionan a terceros que puedan verse afectados por la divulgación de los datos extraídos o siguen presionando a la empresa perjudicada para que acabe pagando.

Conforme las organizaciones han comenzado a implementar sistemas de respaldo para sus datos importantes, "los piratas informáticos se han vuelto cada vez más creativos y han agregado funciones nuevas y sofisticadas a sus ciberataques", ha advertido José Rosell, socio-director de S2 Grupo.

Los antecesores de este tipo de ransomware

En 2019 nació el ataque de ransomware de doble extorsión cuando ciberdelincuentes como Doppel Paymer o Maze encontraron una segunda forma de persuadir a las víctimas para que pagasen el rescate de sus datos, a pesar de tener copias de seguridad de los sistemas. Este consistió en que los ciberatacantes hacen una copia de los datos para poder usarlos en las negociaciones. De esta forma, si la víctima se niega a pagar un rescate, los datos confidenciales robados de la red se harán públicos o se venderán en el mercado negro.

"El ransomware de doble extorsión hizo que el servidor de respaldo fuera inútil porque los ciberdelincuentes tienen acceso a información confidencial e, incluso, si una organización puede restaurar su red, el problema principal ha pasado a ser que los datos se hagan públicos", ha explicado Miguel A. Juan, socio-director de S2 Grupo.

"El primer ransomware de triple extorsión tuvo lugar en octubre de 2020 cuando la clínica de psicoterapia finlandesa Vastaamo sufrió el ciberataque a sus servidores y los ciberdelincuentes extorsionaron a sus clientes amenazándolos con la divulgación de la información d sus sesiones de terapia", ha continuado Miguel A Juan.

Los piratas pueden seguir atacando a la empresa después de recuperar sus datos

El principal problema del ransomware de triple extorsión es que no sólo tiene como nueva capa persuadir a terceros para lograr su objetivo, sino que los ciberdelincuentes pueden seguir atacando a

la misma organización. Por ejemplo, si una empresa ha recuperado con éxito los datos de las copias de seguridad y no se abre a negociar, los atacantes pueden lanzar un ataque de denegación de servicio distribuido para ejercer más presión.

Expertos de S2 Grupo han concluido que el ransomware de triple extorsión es una extensión del ataque de doble extorsión añadiendo un punto de presión adicional para que su víctima pague. Además del cifrado de datos (la primera capa) y la amenaza de fuga de datos importantes (la segunda capa), el ciberdelincuente puede agregar otra táctica de su elección (la tercera capa). El tercer punto de extorsión puede ser cualquier tipo de técnica que acabe logrando que la empresa vulnerada o un tercero pague por los datos.

De esta forma, a medida que las tecnologías y estrategias de ataque se adaptan y transforman, los incidentes modernos pueden convertirse en una cadena de ransomware que no tiene por qué terminar, siendo cada vez mayor el número de víctimas extorsionadas.

Datos de contacto:
Luis Núñez Canal
667574131

Nota de prensa publicada en: Madrid

Categorías: Finanzas Ciberseguridad Recursos humanos Innovación Tecnológica