Publicado en Madrid el 17/05/2024

España es el séptimo país del mundo con más ransomware

Con motivo de la celebración del Día Mundial de Internet, la empresa de ciberinteligencia y ciberseguridad S2 Grupo ha presentado los resultados de su 'Informe Ransomware 2024' del que se extrae que España es el séptimo país del mundo más afectado por este tipo de ciberataques en los tres primeros meses del año, por detrás de EE.UU, Canadá, Reino Unido, Alemania, Francia e Italia

Según ha señalado la compañía en un comunicado, se ha visto que "el ransomware es uno de los tipos de malware que más ha contribuido a la acción cibercriminal en los últimos años y particularmente el RaaS", que es un modelo de negocio de la ciberdelincuencia en el que los desarrolladores de este malware lo venden a otros ciberatacantes. El objetivo principal del RaaS es el beneficio económico. S2 Grupo ha llegado a esta conclusión en un Infroem sobre el Ransomware que ha realizado a través del análisis geopolítico y del seguimiento del malware que lleva a cabo con MicroClaudia, la herramienta de "vacunación" cibernética que desarrolla junto al CCN-CERT.

"El RaaS sigue un modelo de negocio que se ha demostrado muy rentable para los grupos, que emplean parte de sus ganancias para mejorar su sistema. Esto incluye invertir en proteger cada vez más el malware que emplean durante las diferentes fases de la infección, complicando la labor de detección y respuesta", ha declarado Ana Nieto, responsable del equipo de análisis de malware de S2 Grupo.

El equipo de expertos de S2 Grupo ha indicado que el desarrollo en industrias como la manufacturera, el sector sanitario o en nuevos avances tecnológicos supone un gran interés en términos de beneficios económicos para los grupos ransomware.

Junto a esto, "en 2024 se prevé un incremento de campañas maliciosas con este malware debido a los procesos electorales previstos, como son los de EE.UU, Rusia y al Parlamento Europeo, entre otros". En estos casos se utilizaría el ransomware como herramienta para coaccionar y obtener beneficios económicos de datos filtrados, según la compañía de ciberseguridad.

El sector manufacturero, el más ciberatacado

"Cada vez más sectores se ven afectados por la actividad del RaaS". En el primer trimestre de 2024, los diez sectores más afectados por orden de impacto de este tipo de malware han sido en primer lugar el manufacturero, seguido de los servicios de atención al cliente y la salud. A estos les continúan el sector de la construcción, tecnología y educación, mientras que el financiero ocupa el décimo lugar precedido de los sectores alimentación, legal y consultoría.

Del informe también se extrae que las organizaciones pertenecientes al sector manufacturero están compuestas por cadenas de suministro muy complejas. Esto hace que sean más vulnerables contra ataques que puedan venir de terceras partes o proveedores. Las cadenas de suministro dentro de este

sector son muy importantes porque si una parte de la cadena de suministro queda inoperativa, genera un impacto en el producto final. Y hay que tener en cuenta, que cuanto mayor efecto en cadena pueda tener un ataque de ransomware en la cadena de suministro, mayores probabilidades hay de que la víctima acceda a pagar un rescate.

"El ransomware está siendo actualmente uno de los ciberproblemas que más puede perjudicar a las empresas y organizaciones porque, además de perjudicar al funcionamiento de su negocio, supone el robo de datos confidenciales, pueden afectar gravemente a su reputación y también acarrean problemas financieros", ha afirmado José Rosell, CEO de S2 Grupo.

Según se explica en el informe, en relación al sector de atención al cliente, destaca el gran impacto que puede tener sobre los clientes finales. En este ámbito hay gran dependencia de los datos almacenados en sus sistemas para poder ejercer su operativa diaria, lo que incrementa las probabilidades de ser potenciales víctimas por parte de grupos de ransomware. Además, los datos que manejan son de gran valor dentro de los mercados de la darkweb.

El sector salud, que es el tercero más impactado en el primer trimestre de 2024, es uno de los que presenta mayor criticidad debido al gran impacto que supone la posibilidad de crear una disrupción en servicios sanitarios críticos que genere daño directo a pacientes. Los servicios de emergencia de un centro sanitario son los más claves. Junto a esto, la violación de datos personales y clínicos de los pacientes podría conllevar graves consecuencias en lo que respecta a las operativas médicas de la organización sanitaria receptora del ciberataque. Y esta es una de las grandes motivaciones de los atacantes de ransomware en este sector.

Datos de contacto:
Luis Núñez Canal
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Programación Software Ciberseguridad