Publicado en Madrid el 30/11/2021

Estos son los actos cibernéticos más peligrosos a los que se expone la sociedad

Con motivo del Día Internacional de la Seguridad de la Información, la compañía especializada en ciberseguridad S2 Grupo ha elaborado el informe "Descubre el lado más oscuro de la red", en el que ha enfatizado sobre la importancia de saber que el espacio digital no siempre es seguro y que a través de ciberataques, el mercado negro o el ransomware se incrementa el número de amenazas online

Según ha indicado la compañía en un comunicado hay organizaciones de cibercriminales que funcionan de una forma muy similar a las empresas, con estructuras sólidas y grupos de personas muy cualificadas que trabajan con el fin de lucrarse a costa de los errores de otras personas. Por ello, “tenemos que ser conscientes de que ciertos aspectos, como nuestra información personal o la de la empresa en la que trabajamos, están dispuestos a ser robados y utilizados por la ciberdelincuencia para actos cibernéticos peligrosos”, ha asegurado José Rosell, socio-director de S2 Grupo.

“Los grandes peligros que encontramos en la red son de diferente rango, pero hemos de tener en cuenta que, incluso, se podría matar por Internet. No nos referimos a personas, obviamente. Sin embargo, si pensamos en la industria 4.0, en concreto en una ganadería domotizada y pensamos en la opción de que sufriera un ciberataque que manipulara la dispensación alimentación y agua del ganado, por ejemplo, veríamos que entonces ese ganado podría morir”, ha argumentado Miguel A. Juan, socio-director de S2 Grupo.

Como se recoge en el documento elaborado por el equipo de expertos de S2 Grupo, otro de los peligros más elevados son los ciberataques producidos por equipos multidisciplinares. En éstos sus integrantes disponen de conocimientos IT (tecnologías de la información) y conocimientos del funcionamiento del sistema industrial al cual pretenden atentar. Esto se ha convertido en un arma muy poderosa, ya que los atacantes no solo son capaces de acceder al sistema de control industrial, sino que pueden identificar qué parte del proceso industrial es crítica y delicada y que saboteando su sistema de control, pueden producir graves daños que afecten tanto a la producción de la planta como a la propia instalación.

En tercer lugar, desde S2 Grupo se explica que en el lado más oscuro de la red también hay que prestar atención a las organizaciones dentro del mercado negro. Éstas son muy complejas y en ellas se representan diferentes roles y actores que gestionan, administran y ejecutan sus acciones. Por un lado, se encuentran los roles técnicos, en el que se incluyen aquellas personas que se encargan de la creación y mantenimiento de los recursos utilizados para cometer las acciones delictivas. Son los responsables de crear las herramientas que se utilizarán para una campaña de fraude. Pueden, por ejemplo, realizar tareas de modificación de un malware, tomando una muestra existente de malware y adaptarla para algún otro objetivo o también desarrollar malware a medida.

También hay roles comerciales. Éstos cobran mayor sentido en los delitos bancarios donde se realizan robos de las credenciales y tarjetas bancarias. Una vez se está en posesión de dicha información, los

comerciales son los encargados de transformar los datos bancarios en beneficios. Para ello participan dos actores que son los “cashiers”, encargados de mover las ganancias económicas entre diferentes cuentas, y los “muleros”, que son aquellas personas cuya función principal es la del blanqueo de capital.

En tercer lugar, se encuentran los roles de gestión que son los encargados de coordinar, dirigir, decidir las contrataciones de las personas o grupos y supervisar las operaciones.

Por último, en el informe presentado por S2 Grupo se hace mención al ransomware, que se ha convertido en uno de lo malwares más temidos. El problema de este tipo de virus es que en algunos casos, ni pagando el rescate se ha conseguido recobrar el acceso a la información. Ha habido víctimas que después de pagar el rescate no han podido descifrar la información bloqueada o que incluso no han encontrado forma de pagarlo. La recomendación de la policía recomienda no pagar el rescate que se pide, ya que haciéndolo estamos fomentando que se continúe con la propagación del ransomware y de su chantaje asociado.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Ciberseguridad