Publicado en Madrid el 20/06/2024

S2 Grupo advierte del significativo aumento de las tasas de ciberespionaje

La empresa de ciberseguridad y ciberinteligencia S2 Grupo ha destacado que debido a que las tasas de ciberespionaje son cada vez mayores, es clave el concepto Zero Trust para combatirlo. Se trata de reducir la brecha de confianza a cero en el ámbito tecnológico, para evitar ser víctimas de cualquier ciberdelito

Según ha indicado en un comunicado la compañía, el ciberespionaje es un hecho que todo el mundo conoce en el ámbito político, entre gobiernos, en el sector industrial, incluso en el ámbito deportivo. Sin embargo, este "poco a poco se va extendiendo a cualquier sector donde pueda obtener beneficio". En este contexto hay que "hemos de desconfiar de todos los usuarios, de todos los dispositivos y debemos monitorizar todo", ha explicado José Rosell, CEO de S2 Grupo.

"Aunque no existen soluciones efectivas al 100% para evitar el ciberespionaje, sí sabemos que es esencial la acción ciberresponsable de las personas para evitar que se cuelen los ciberdelincuentes en los sistemas y, junto a esto, que muchas de las incidencias han sucedido por un exceso de confianza de algún miembro del equipo de la entidad que ha sido atacada. Si aplicamos el concepto Zero Trust, emplearemos medidas proactivas ante cualquier anomalía a la vez que se implantan técnicas defensivas activas que permitirán minimizar el impacto de los daños y conocer el origen de la causa", ha continuado José Rosell.

En este sentido, desde hace más de 20 años S2 Grupo realiza una fuerte inversión en I+D+i con el objetivo de desarrollar software propio en Europa que permita la ciberprotección y la independencia tecnológica frente a otros países, que podrían ponernos en riesgo. En esta línea, también ha colaborado con las principales instituciones del sector a nivel europeo y nacional, como el CCN-CERT, para el desarrollo de soluciones pioneras como microClaudia (que blinda frente al ransomware).

Las claves para combatir el ciberespionaje

Los expertos de la compañía han desarrollado un listado con las claves para combatir el ciberespionaje. En este sentido, "si bien Pegasus fue el medio más conocido hasta el momento, existen numerosas entidades privadas que trabajan a menor escala generando unas amenazas con capacidades de espionaje y que preparan sus propios métodos de infección y propagación, que se adecúan según los objetivos".

Es por ello que "cualquier país, puede tener alguna persona, grupo o entidad que genere estos productos y encuentre su mercado, y esto no quiere decir que estén subvencionados por los gobiernos de los países", añade el comunicado.

Actualmente, los más afectados por el ciberespionaje son los organismos gubernamentales o entidades comerciales grandes, incluso ambos pueden tener en común alguna estructura crítica o industrial, las cuales "son muy atractivas para otros países, para otras entidades privadas o para

grupos ciberterroristas".

Según indican los expertos de S2 Grupo, kas técnicas que desarrollan se aplican a "las 5 fases de un ciberataque": reconocimiento, escaneo, obtención del acceso, persistencia y limpieza de huellas. Por ejemplo, el reconocimiento requiere de técnicas para conocer la entidad objetivo y el escaneo de técnicas para encontrar vulnerabilidades en los servicios, comunicaciones y dispositivos que se están utilizando para poder seleccionar la técnica o estrategia más adecuada, que no tiene por qué ser única, ni únicos los objetivos dentro de la entidad que permitan obtener acceso a la misma. No obstante, entre los métodos más utilizados destacan el phishing, malware, ataques de inyección de código, rootkits, denegación de servicios, ataques de Man-In-The-Middle, fuerza bruta a accesos o ramsonware. Todo se reduce, a realizar un engaño, ya sea a usuarios, dispositivos o equipos informáticos e implantar herramientas que permitan quedarse para realizar las operaciones de exfiltración de información o degradación de los servicios del objetivo.

Por último, los expertos de S2 Grupos señalan que los objetivos principales del ciberespionaje son "conseguir información y datos sensibles de personas, acceso a credenciales, comunicaciones, capacidades tecnológicas que tienen implementadas, investigación y desarrollo, líneas de trabajo, en el caso de ciberespionaje empresarial puede ser cualquier información que sea útil para posicionar mejor a la competencia". Junto a estos objetivos estaban otros riesgos del ciberespionaje como el compromiso de la propia información que maneja la entidad atacada, la posible degradación de los servicios que suministra, las pérdidas económicas que podría ocasionar y el impacto a la reputación de la propia entidad.

Datos de contacto:
Luis Núñez
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Inteligencia Artificial y Robótica Ciberseguridad