Publicado en Madrid el 30/11/2020

Los cibercriminales sofistican sus ataques con la Inteligencia Artificial como consecuencia de la pandemia

Expertos de la compañía de ciberseguridad S2 Grupo han destacado que la pandemia ha incrementado la dependencia de la tecnología, por ejemplo con el teletrabajo, y a su vez los cibercriminales han sofisticado los ataques usando, entre otros métodos, la Inteligencia Artificial. Y estos hechos dificultan enormemente las tareas de ciberprotección

Hoy, lunes 30 de noviembre, se conmemora el Día Internacional de la Seguridad de la Información y desde S2 Grupo se ha enfatizado la importancia de comprender el contexto actual para frenar la acción de la ciberdelincuencia. En este sentido, expertos de la compañía de ciberseguridad han destacado que la pandemia ha incrementado la dependencia de la tecnología, por ejemplo con el teletrabajo, y a su vez los cibercriminales han sofisticado los ataques usando, entre otros métodos, la Inteligencia Artificial. Y estos hechos dificultan enormemente las tareas de ciberprotección.

Durante 2020 junto con ciberataques complejos han convivido otros más sencillos de distribución de malware. Entre las principales ciberamenazas de este año destacan los casos de ransomware, que han evolucionado haciéndose más dirigidos para obtener el mayor impacto posible; las campañas de desinformación sobre la COVID-19; o los ciberataques de ingeniería social, como el conocido “fraude al CEO” usando la Inteligencia Artificial.

“Los sistemas ofensivos son cada vez más sofisticados y las organizaciones criminales se introducen en las redes que quieren atacar, estudian los comportamientos y hasta el modo de conversaciones de las personas de la organización para hacer una suplantación de identidad y cada vez es más fácil caer en su trampa “, ha explicado José Rosell, socio-director de S2 Grupo.

“Se está utilizando el llamado “deep fake”, los vídeos que utilizan la imagen de una persona conocida y reproducen exactamente su voz diciendo cosas que nunca ha dicho, para realizar ataques de fraude al CEO. Ya no se trata de caer en la trampa de responder un correo que creemos que viene de un entorno seguro, es que podemos recibir una llamada con la voz de nuestro jefe solicitándonos, por ejemplo, realizar una transferencia de dinero a una cuenta bancaria, y que en realidad no sea él. Tenemos que saber que esto es posible para poder dudar ante estas situaciones y actuar con precaución”, ha afirmado Miguel A. Juan, socio-director de S2 Grupo.

Aumento del ciberespionaje

Junto a esto, se ha destacado el crecimiento del ciberespionaje y cómo los cibercriminales están creando nuevas tácticas, técnicas y procedimientos para intentar robar la propiedad intelectual de sus objetivos, por ejemplo. Debido a la aparición de nuevas técnicas usadas por los cibercriminales como “Living off the Land” o “fileless malware”, que dificultan la detección de las amenazas, desde S2 Grupo se ha destacado que es clave ampliar la monitorización de las organizaciones y ser capaces de

modelar su comportamiento para detectar posibles anomalías. En este sentido, S2 Grupo realiza un amplio trabajo en I+D+i para crear nuevas soluciones que ayuden a combatir estos incidentes como su software CLAUDIA que permite detectar este tipo de situaciones.

Problemas de la ciberseguridad y el teletrabajo

“Este año muchas empresas lo han pasado mal porque de repente han tenido que coger sus sistemas y trasladarse a trabajar desde casa. Eso ha provocado que lo hayan tenido que hacer muy rápido y bajando todas sus defensas. Con lo cual el proceso de migración a un entorno completamente digital ha sido muy duro. No obstante, hemos podido sobrellevarlo gracias a las infraestructuras que ya teníamos en España y a las tecnologías que estábamos utilizando”, ha declarado José Rosell.

Desde la empresa se ha explicado que esta situación puede traer problemas que ni siquiera hayamos imaginado porque hasta ahora, el reto de la ciberseguridad era la convergencia IT (Tecnologías de la Información) y OT (Tecnologías de la Operación) y esto se ha complicado para convertirse en una convergencia total IT – OT – CT (Tecnologías de Control).

“Se introduce un nuevo entorno en la ecuación que es nuestro hogar, la tecnología del usuario que antes no se tenía en cuenta y que ahora nos lo encontramos como un entorno completamente desprotegido y desde el que se realizan operaciones importantes para las compañías. Con el teletrabajo la frontera de la empresa se amplía hasta los hogares de los trabajadores”, ha asegurado Miguel A. Juan.

“La nueva situación ha creado una dependencia mayor de la tecnología. Antes ya dependíamos de la tecnología para los procesos de la organización, pero es que ahora dependemos para el trabajo diario de cada una de las personas”, ha apostillado Miguel A. Juan.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Inteligencia Artificial y Robótica Software Ciberseguridad