“Deep locker impulsado por inteligencia artificial”

Los investigadores de seguridad en redes informáticas se han apoyado en la inteligencia artificial para detectar y combatir de forma automática los ataques de malware, así como para detener cualquier tipo de ciberataque antes de que afecte a alguna organización.

Sin embargo, agentes maliciosos también pueden utilizar la misma tecnología para impulsar nuevas generaciones de malware que pueden evadir incluso las mejores medidas de seguridad e infectar una red informática o lanzar un ataque con la mínima interacción del usuario requerida.

Para ejemplificar estos escenarios catastróficos, investigadores de seguridad en redes informáticas desarrollaron *DeepLocker,* una nueva clase de herramienta de ataque informático “altamente específica y evasiva” impulsada por inteligencia artificial, que oculta sus intenciones maliciosas hasta que llega a una víctima específica.

Acorde al equipo encargado del proyecto, DeepLocker opera por debajo del radar sin ser detectado y desata sus acciones perjudiciales tan pronto como el modelo de inteligencia artificial identifica el objetivo del ataque a través de indicadores como reconocimiento facial, geolocalización y reconocimiento de voz.

Describiéndolo como una variante de ataque “*spray and pray*” tradicional, los investigadores de seguridad en redes informáticas creen que este tipo de malware sigiloso impulsado por inteligencia artificial es particularmente peligroso porque podría infectar millones de sistemas sin ser detectado.

El malware puede ocultar su carga maliciosa mientras se encuentra alojado en aplicaciones benignas (como software de videoconferencia) para evitar ser detectado por la mayoría de los antivirus y escáneres de malware hasta que llegue a víctimas específicas, identificadas gracias a la inteligencia artificial. “Lo que hace único a DeepLocker es que la inteligencia artificial hace imposible el uso de ingeniería inversa de sus condiciones de activación para desplegar el ataque”, explican los investigadores. Lo que significa que sus componentes maliciosos sólo se desbloquearán si se alcanza el objetivo deseado.

Para demostrar las capacidades de DeepLocker, los investigadores de seguridad en redes informáticas diseñaron una prueba de concepto, camuflando el famoso ransomware WannaCry en una aplicación de videoconferencia para que no fuera detectado por cualquier herramienta de seguridad.

Dadas sus condiciones de activación, DeepLocker no desbloqueó ni ejecutó el ransomware en el sistema hasta que reconoció la cara de la víctima seleccionada, objetivo que determinó a partir de fotos de la víctima disponibles en línea. De tal modo, lo único que DeepLocker requiere es una foto, cosa que puede obtener desde cualquier página de redes sociales.

Expertos en seguridad en redes informáticas del Instituto Internacional de Seguridad Cibernética aseguran que los encargados del proyecto darán a conocer más detalles y demostraciones en vivo de las pruebas de concepto de esta herramienta en futuros eventos y foros de seguridad cibernética.