[Anuncios](#)

DeepLocker, el “francotirador” más certero y letal contra la ciberdelincuencia

Utiliza la inteligencia artificial para permanecer escondido y activarse solo cuando identifica al sospechoso

Detener el ataque de DeepLocker contra el malware criminal es prácticamente imposible, ya que sólo se puede desactivar tras haber alcanzado su blanco

Madrid - 14 dic 2018: La sofisticación de los ataques cibernéticos es cada vez mayor y es cuestión de tiempo que utilicen -si no está ocurriendo ya- herramientas de inteligencia artificial. Por eso, investigadores de IBM Research han desarrollado una nueva generación de herramientas de ciberseguridad con IA, denominada DeepLocker. Esta tecnología aúna herramientas de IA de código abierto con técnicas de malware que dan lugar a un nuevo tipo de malware evasivo -capaz de evitar de forma activa ser analizado e identificado- ultra dirigido y altamente efectivo contra el cibercrimen. La ventaja de DeepLocker es que permanece oculto en una aplicación hasta que, gracias a su entrenamiento con IA, se activa cuando identifica al sospechoso, mediante reconocimiento facial, geolocalización o reconocimiento de voz. Esta capacidad es similar al ataque de un francotirador, en contraste con el enfoque de “rociado” del malware tradicional. DeepLocker está diseñado para ser sigiloso. Vuela bajo el radar, evitando la detección hasta el momento preciso en que reconoce un objetivo específico.

Este malware es prácticamente imposible de detener ya que los ciberdelincuentes sólo podrían desbloquear su carga una vez les hubiese alcanzado. Esto es posible mediante el uso de un modelo de IA de red neuronal profunda (DNN) que evita que los ciberdelincuentes puedan desbloquearlo mediante el uso de ingeniería inversa.

Prueba de concepto

Para demostrar las capacidades de DeepLocker, los investigadores de IBM esconden ransomware en aplicaciones de videoconferencia. El ransomware no puede ser detectado por herramientas de análisis de malware tradicionales, como antivirus y entornos limitados. DeepLocker no ejecuta el ransomware en el sistema hasta que la IA reconoce al ciberdelincuente. Cuando el sospechoso se sienta frente al ordenador y usa la aplicación, Deep Locker se activa de forma secreta.

Retrospectiva

- A finales de los 80 y principios de los 90, se diseñaron las primeras variantes de virus polimórficos y metamórficos para alterar y destruir datos. Por medio de la mutación, los creadores del malware evitaban los sistemas antivirus que hacían análisis estático de los ficheros en busca de patrones.
- En la década de los 90, los autores de malware comenzaron a cifrar la carga malintencionada utilizando los denominados “empaquetadores”, de modo que el código malicioso solo podía identificarse cuando se descifrara en la memoria antes de su ejecución. La industria de la seguridad respondió creando sistemas virtualizados en

los que se ejecutaban los paquetes sospechosos.

- En la década de los 2000, surgieron las primeras formas de malware evasivo. El malware utilizaba verificaciones para identificar si se estaba ejecutando en un entorno virtualizado. Si se encontraba alguno, el malware dejaba de ejecutar su carga maliciosa para evitar el análisis. Este enfoque aún prevalece hoy: según diversos estudios, el 98% del malware analizado utiliza técnicas evasivas.
- En los últimos años, el malware se ha vuelto cada vez más sofisticado y utilizan sistemas bare metal para evitar la virtualización. Una estrategia diferente son los ataques dirigidos que inspeccionan cuidadosamente el entorno en el que se ejecutan. Solo si el punto final de destino se encuentra despejado, se busca y ejecuta el malware. Un ejemplo conocido es el gusano Stuxnet, que fue programado para apuntar y atacar sólo a sistemas de un fabricante en particular, y únicamente con ciertas configuraciones de hardware y software.

Aunque el malware evasivo sigue evolucionando, las formas más recientes de software malicioso dirigido siguen requiriendo activadores predefinidos que pueden ser identificados al verificarse el código. Es ahí dónde actúa DeepLocker.