Publicado en Madrid el 20/06/2019

Check Point ha desarrollado una tecnología capaz de analizar y reconocer el malware por su ADN

La compañía presenta su nuevo motor basado en inteligencia artificial, que potencia el sistema de ciberseguridad de las empresas

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder especializado en ciberseguridad a nivel mundial, lanza Malware DNA, un nuevo motor basado en inteligencia artificial que forma parte de su solución Sandblast Network, que ayuda a las empresas a optimizar su estrategia de protección de datos. Al igual que una simple gota de sangre contiene millones de muestras de ADN, las líneas de código del malware dan información básica de las ciberamenazas.

El malware es un proceso evolutivo, como lo demuestra el aumento de nuevas familias en los últimos años. La rápida evolución se entiende puesto que la mayoría de los programas maliciosos se construyen a partir de bits y fragmentos de código existentes. Los hackers, por tanto, reutilizan el código para ahorrarse tiempo y mejorar sus técnicas de ataque, así como evitar que les detecten y aumentar la eficiencia de sus ataques.

Para contrarrestar estos efectos, Check Point ha desarrollado Malware DNA, su último motor de detección basado en inteligencia artificial para identificar y prevenir ataques maliciosos de una forma revolucionaria: clasifica las nuevas formas de malware en familias de malware conocidas, creando la inteligencia necesaria para comprender los componentes básicos de las ciberamenazas, para lo que escanea buscando similitudes de código y comportamiento. Además, los procesos de aprendizaje se combinan frecuentemente con millones de muestras de malware detectadas por los cientos de millones de sensores de Check Point desplegados en todo el mundo para detectar, crear inteligencia y correlacionar las familias de malware de forma eficiente y precisa.

Asimismo, Malware DNA forma parte de la solución Sandblast Network de Check Point, que detecta y bloquea malware desconocido y día cero. Para detener estos ciberataques, Check Point ofrece Threat Emulation, una innovadora tecnología de sandboxing de día cero que tiene la mejor tasa de captura en amenazas y es inmune a prácticamente la totalidad de las técnicas de ataque evasivo. Por otra parte, para defenderse de los ataques de día cero, esta solución de ciberseguridad crea un informe de emulación de amenazas para cada archivo que pasa por su sandbox. Este análisis, además, incluye información detallada sobre cualquier intento malicioso registrado al ejecutar el archivo en el entorno de pruebas. Este informe de Threat Emulation también se enriquece con información sobre amenazas adquirida directamente desde Check Point ThreatCloud, el recurso de información sobre amenazas más grande del mundo para todas las superficies de TI: nube, red, endpoints y dispositivos móviles.

¿Por qué es tan útil para la ciberseguridad y protección frente a amenazas de día cero clasificar las nuevas formas de malware por familias genealógicas?
La posibilidad de clasificar una amenaza dentro de una familia de malware ofrece visibilidad de los riesgos a los que se enfrenta una empresa. Al rastrear el origen de la amenaza, los expertos en ciberseguridad pueden idear rápidamente estrategias Y aplicar las mejores prácticas. Además, se

puede elaborar un perfil con datos como el tipo específico de amenazas, repercusiones y daños que plantea, etc.

"Desde Check Point siempre transmitimos el mensaje de que la prevención es la mejor estrategia de ciberseguridad que las empresas puede tomar", señala Eusebio Nieva, director técnico de Check Point para España y Portugal. "Con Malware DNA, todas las empresas pueden reforzar su estrategia de seguridad y optimizar sus técnicas de prevención y detección, a la vez que al usar inteligencia artificial, reducen el tiempo de respuesta para prevenir amenazas", añade Nieva.

Datos de contacto:
Everythink PR
915519891

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Inteligencia Artificial y Robótica Programación Software Ciberseguridad Innovación Tecnológica