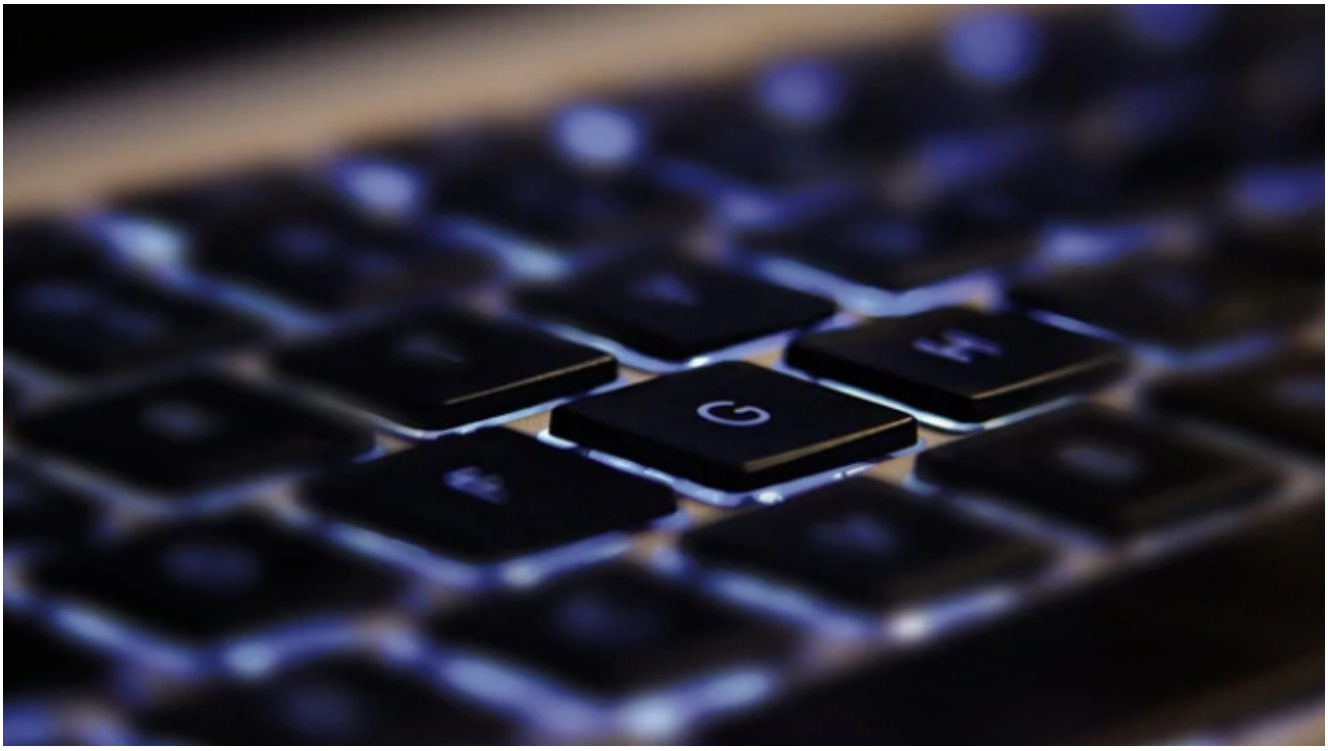

Cómo es Morpheus, el procesador “anti hackeos”

Investigadores de la Universidad de Michigan desarrollaron un procesador que se anticipa a posibles ataques cibernéticos: su arquitectura está diseñada para cifrar y reorganizar aleatoriamente los bits clave de su propio código y datos 20 veces por segundo. Esto es mucho más rápido de lo que puede actuar un hacker humano y varias veces más veloz que las técnicas automatizadas.

Este procesador “anti hackeos” se llama Morpheus y, según sus creadores, incluso cuando un cibercriminal encontrara una vulnerabilidad, le resultaría difícil explotarla porque la información desaparecería en 50 milisegundos.

“La gente está constantemente escribiendo código, y mientras

haya un nuevo código, habrá nuevos errores y vulnerabilidades de seguridad", explicó Todd Austin, uno de los desarrolladores del sistema y docente en una publicación difundida por la Universidad.

Esta investigación, desarrollada por la Universidad de Michigan, contó con el apoyo de La Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) de Estados Unidos.

"Imagina tratar de resolver un cubo de Rubik que se reorganiza cada vez que parpadeas. Eso es lo que los hackers se enfrentan con Morpheus. Hace de la computadora un rompecabezas sin solución", detalló el investigador.

Morpheus se centra en la aleatorización de bits de datos conocidos como "semántica indefinida", que son parte de la arquitectura y que incluye la ubicación, el formato y el contenido del código de un programa o app, por ejemplo.

“Imagina tratar de resolver un cubo de Rubik que se reorganiza cada vez que parpadeas. Eso es lo que los hackers se enfrentan con Morpheus. Hace de la computadora un rompecabezas sin solución”, detalló Todd Austin, uno de los investigadores detrás del proyecto (Foto: Especial)

“La semántica indefinida es parte de la maquinaria más básica de un procesador, y los programadores generalmente no interactúan con ellos. Pero los hackers pueden realizar ingeniería inversa para descubrir vulnerabilidades y hacer un ataque”, se analiza en el texto.

Morpheus es, por el momento, un prototipo basado en la arquitectura de chips de código abierto RISC-V. El chip así como la investigación fue presentada el mes pasado. Ya se realizaron pruebas exitosos y eventualmente se podría lanzar al mercado.

Esta tecnología podría usarse en diferentes clases de dispositivos. Según explican los expertos, la tasa en la que se va ajustando el código se puede ir modificando. En

principio, ellos usaron un rate de 50 milisegundos para lograr un equilibrio que permita maximizar la seguridad del procesador, minimizando el consumo de recursos y sin perjudicar el rendimiento.

¿Será realmente imposible de hackear? “Es difícil decir si Morpheus será realmente infranqueable. Nada en la vida es ‘imposible de hackear’, solo el tiempo podrá decir qué tan seguro es Morpheus y si puede o no ser vulnerado”, analizó Michal Salat, director de Inteligencia de Amenazas de Avast, al ser consultado por **Infobae** sobre este tema.

Por su parte, Santiago Pontiroli, analista de seguridad en Kaspersky, dijo que cuando en informática se refiere a tecnología “imposible de vulnerar” se hace referencia a que el costo de realizar un ataque sería tan elevado o difícil que no tendría sentido siquiera intentarlo.

“En este caso, a costa del nivel de seguridad elevado que plantea la arquitectura de este procesador se hacen sacrificios en performance y usabilidad, por lo que su utilización estará reservada a casos muy puntuales. Que una tecnología sea segura hoy no significa que lo sea el día de mañana es por eso que siempre deben existir varias barreras de defensa, en un enfoque conocido como defensa en profundidad (o defensa en capas)”, concluyó.

Por lo pronto, Morpheus plantea una solución interesante. Tuvo pruebas exitosas, se presentó “en sociedad” y ahora habrá que ver cuándo llega al mercado y si con el paso del tiempo resiste las ciberamenazas que surgen a diario.

Fuente: **Infobae**